Trustcenter der Deutschen Rentenversicherung

Vertrauensdiensteanbieter Deutsche Rentenversicherung Bund nach eIDAS-VO

Certificate Policy des Zertifikatsdienstes DRV QC Root CA

Dokument-OID: 1.3.6.1.4.1.22204.1.8.1.1.1

Version	06.01.00
Stand	10.05.17
Dateiname	TCDRV_CP_DRV-QC-Root-CA_060100_20170510_DE.pdf
Produktzustand	Freigegeben
Vertraulichkeit	Keine Beschränkungen

Inhaltsverzeichnis

1 Einleitung

1.1 Überblick

Die Träger der Deutschen Rentenversicherung (DRV) betreiben ein gemeinschaftliches Trustcenter der DRV zur Bereitstellung von qualifizierten Vertrauensdiensten gemäß eIDAS-VO [1]. Im Trustcenter der DRV sind die folgenden Vertrauensdiensteanbieter tätig, welche qualifizierte Vertrauensdienste bereitstellen:

(1) VDA DRV Bund stellt bereit:

- Zertifikatsdienst DRV QC Root CA:
  Qualifizierter Vertrauensdienst DRV QC Root CA für die Ausstellung von:
  - Ausstellerzertifikaten für DRV QC Root CA, DRV QC 70 MA CA, DRV QC 13 MA CA und DRV QC 11 MA CA,
  - Zertifikaten des Zeitstempeldienstes DRV QC Root TSA,
  - Zertifikaten des Validierungsdienstes DRV QC Root OCSP;
- Zeitstempeldienst DRV QC Root TSA:
  Qualifizierter Vertrauensdienst DRV QC Root TSA für die Ausstellung:
  - qualifizierter elektronischer Zeitstempel;
- Zertifikatsdienst DRV QC 70 MA CA:
  Qualifizierter Vertrauensdienst DRV QC 70 MA CA für die Ausstellung von:
  - qualifizierten EE-Zertifikaten,
  - Zertifikaten des Validierungsdienstes DRV QC 70 MA OCSP;

(2) VDA DRV Rheinland stellt bereit:

- Zertifikatsdienst DRV QC 13 MA CA:
  Qualifizierter Vertrauensdienst DRV QC 13 MA CA für die Ausstellung von:
  - qualifizierten EE-Zertifikaten,
  - Zertifikaten des Validierungsdienstes DRV QC 13 MA OCSP;

(3) VDA DRV Westfalen stellt bereit:

- Zertifikatsdienst DRV QC 11 MA CA:
  Qualifizierter Vertrauensdienst DRV QC 11 MA CA für die Ausstellung von:
  - qualifizierten EE-Zertifikaten,
  - Zertifikaten des Validierungsdienstes DRV QC 11 MA OCSP.

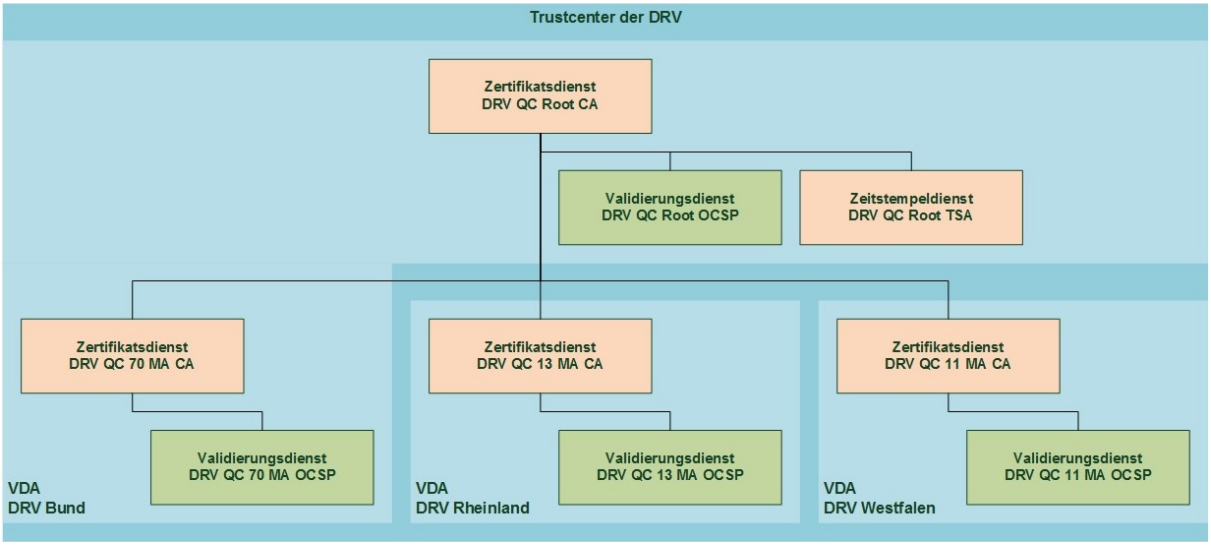

Abbildung 1 Qualifizierte Vertrauensdienste im Trustcenter der DRV

Die vom Zertifikatsdienst DRV QC Root CA ausgestellten Root-CA-Zertifikate bilden den Vertrauensanker der qualifizierten Zertifikatshierarchie des Trustcenters der DRV.

Die qualifizierten Zertifikatsdienste signieren jeweils mit ihrem Signaturschlüssel auf einer qualifizierten elektronischen Signaturerstellungseinheit (QSCD) die von ihnen erstellten qualifizierten Zertifikate.

Die Validierungsdienste (OCSP-Responder) und der qualifizierte Zeitstempeldienst signieren jeweils mit ihren Signaturschlüsseln auf qualifizierten elektronischen Signaturerstellungseinheiten die von ihnen erstellten OCSP-Auskünfte bzw. qualifizierten Zeitstempel.

Die folgende Abbildung gibt einen Überblick über die Richtlinien Dokumente des Zertifikatsdienstes DRV QC Root CA.

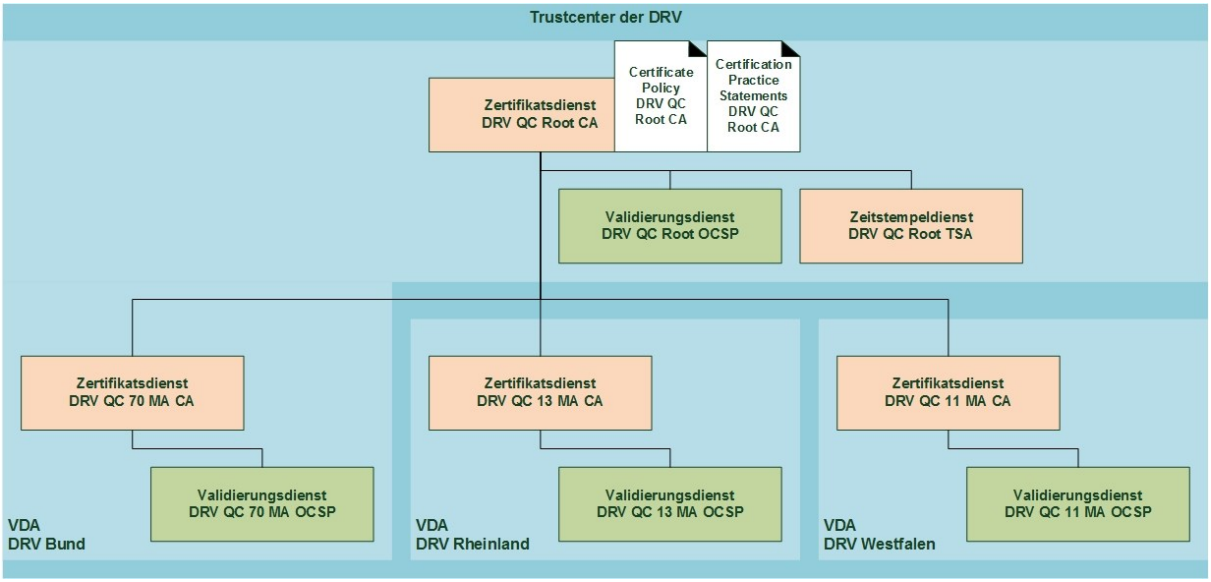

Abbildung 2 Richtlinien Dokumente des Zertifikatsdienstes DRV QC Root CA

Dieses Dokument beinhaltet die Certificate Policy zur Erstellung qualifizierter Systemzertifikate (CA-, TSA- und OCSP-Zertifikate) durch den Zertifikatsdienst DRV QC Root CA sowie qualifizierter Systemzertifikate (OCSP-Zertifikate) durch die qualifizierten Zertifikatsdienste der Mandanten.

Die qualifizierten Systemzertifikate werden für natürliche Personen auf qualifizierten elektronischen Signaturerstellungseinheiten gemäß Policy QCP-N-QSCD (siehe [7]) ausgestellt.

Diese Policy ist gemäß RFC 3647 (siehe [2]) strukturiert.

1.2 Dokumentenname sowie Identifikation

Dokumentname: Certificate Policy des Zertifikatsdienstes DRV QC Root CA

Dokument-OID: 1.3.6.1.4.1.22204.1.8.1.1.1

PEN-DRV-Bund (1.3.6.1.4.1.22204).Trustcenter (1). Policies (8). QC-CP (1). Produktivsystem (1). QC-Root-CA (1)

Diese Policy des Zertifikatsdienstes DRV QC Root CA berücksichtigt die relevanten ETSI Normen:

- ETSI EN 319 401: Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers [5];
- ETSI EN 319 411-1: Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements [6];
- ETSI EN 319 411-2: Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates [7].

Der Standard ETSI EN 319 401 definiert die generellen Anforderungen an einen Vertrauensdiensteanbieter. Für Vertrauensdiensteanbieter von Zertifikatsdiensten sind die Anforderungen im Standard ETSI EN 319 411-1 beschrieben. Erweiterte Anforderungen für qualifizierte Zertifikatsdienste werden im Standard ETSI EN 319 411-2 beschrieben.

1.3 Teilnehmer der Zertifikatsinfrastruktur (PKI)

1.3.1 Zertifikatsdienst

Die Träger der Deutschen Rentenversicherung betreiben ein gemeinsames Trustcenter der DRV. Der VDA DRV Bund betreibt den qualifizierten Zertifikatsdienst DRV QC Root CA zur Ausstellung von Ausstellerzertifikaten für sich selbst und für die qualifizierten Zertifikatsdienste der Mandanten, von Zertifikaten für den Validierungsdienst DRV QC Root OCSP sowie von Zertifikaten für den Zeitstempeldienst DRV QC Root TSA.

Die qualifizierten Zertifikatsdienste der Mandanten stellen u.a. Zertifikate für ihre Validierungsdienste aus.

Die qualifizierten Zertifikatsdienste verwenden zur Erstellung qualifizierter Zertifikate ein zentrales Zertifikatsmanagementsystem.

Das Zertifikat des Zertifikatsdienstes DRV QC Root CA ist der Vertrauensanker der qualifizierten Zertifikatshierarchie im Trustcenter der DRV. Dieses Zertifikat ist selbst-signiert.

1.3.2 Registrierungsdienst

Die Registrierung der Zertifikatsinhaber für Systemzertifikate erfolgt durch den Sicherheitsbeauftragten DRV Bund bzw. den Leiter des VDA DRV Bund.

1.3.3 Zertifikatsinhaber (Subscribers)

Die qualifizierten Zertifikatsdienste im Trustcenter der DRV erstellen Systemzertifikate für natürliche Personen als Zertifikatsinhaber:

(1) den Leiter des VDA DRV Bund für:

- Zertifikate des Zertifikatsdienstes DRV QC Root CA,
- Zertifikate der Zertifikatsdienste der Mandanten.

(2) und die Systemverwalter Server des VDA DRV Bund für:

- Zertifikate des Zeitstempeldienstes DRV QC Root TSA,
- Zertifikate des Validierungsdienstes DRV QC Root OCSP,
- Zertifikate der Validierungsdienste der Mandanten.

Zertifikatsinhaber für die Zertifikate des Zertifikatsdienstes DRV QC Root CA ist der Leiter des VDA DRV Bund. Zertifikatsinhaber für die Zertifikate der qualifizierten Zertifikatsdienste der Mandanten ist auf Grund vertraglicher Vereinbarungen mit dem jeweiligen VDA ebenfalls der Leiter des VDA DRV Bund.

Zertifikatsinhaber für die Zertifikate des Zeitstempeldienstes DRV QC Root TSA sowie der Validierungsdienste DRV QC Root OCSP, DRV QC 70 MA OCSP, DRV QC 13 MA OCSP und DRV QC 11 MA OCSP ist auf Grund vertraglicher Vereinbarungen der verantwortliche Systemverwalter Server des VDA DRV Bund.

Die Anwendungen des VDA DRV Bund für Zertifikatsinhaber sind aus technischen Gründen nicht barrierefrei. Es gibt Einschränkungen für Rolleninhaber mit Behinderungen.

1.3.4 Zertifikatsprüfer (Relying Parties)

Der Begriff Zertifikatsprüfer beinhaltet alle Anwender, welche Systemzertifikate des Trustcenters der DRV prüfen wollen. Das beinhaltet u.a.:

- die Zertifikatsinhaber,
- Mitarbeiter der Mandanten,
- Mitarbeiter anderer RV-Träger, wenn Zertifikate in Geschäftsprozessen eingesetzt werden,
- Mitarbeiter nationaler und internationaler Behörden, wenn Zertifikate in Geschäftsprozessen eingesetzt werden.

1.3.5 Weitere Teilnehmer

Beim Schlüsselwechsel des Zertifikatsdienstes DRV QC Root CA sind der Sicherbeauftragte der DRV Bund und ein VDA-unabhängiger Auditor beteiligt. Die Aufgaben dieser Personen werden in der Ablauforganisation im Dokument Certification Practice Statements beschrieben.

1.4 Anwendungsbereich

1.4.1 Geeignete Zertifikatsnutzung

Die vom Zertifikatsdienst DRV QC Root CA ausgestellten Systemzertifikate dürfen verwendet werden für:

- Ausstellerzertifikat für den Zertifikatsdienst DRV QC Root CA,
- Ausstellerzertifikate für die qualifizierten Zertifikatsdienste der Mandanten im Trustcenter der DRV,
- Zertifikate für den Validierungsdienst DRV QC Root OCSP,
- Zertifikate für den Zeitstempeldienst DRV QC Root TSA.

Die von den qualifizierten Zertifikatsdiensten der Mandanten ausgestellten Systemzertifikate dürfen verwendet werden für:

- Zertifikate für den Validierungsdienst des jeweiligen Mandanten.

1.4.2 Untersagte Zertifikatsnutzung

Die Verwendung der Zertifikate für andere als die in diesem Dokument in Kapitel 1.4.1 genannten Zwecke ist nicht erlaubt.

1.5 Verwaltung der Richtlinie

1.5.1 Änderungsmanagement

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

1.5.2 Ansprechpartner

Folgende Ansprechwege hinsichtlich dieser Policy bestehen:

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

Das Dokument "Certificate Policy des Zertifikatsdienstes DRV QC Root CA" wird gemäß Kapitel 2.2 nach seiner Freigabe veröffentlicht.

1.5.3 Verantwortliche Stelle zur Prüfung der Regelungen zum Betrieb (CPS)

Für die Prüfung der Regelungen zum Betrieb der Zertifikatsdienste im Dokument Certification Practice Statements ist die gleiche Stelle wie für diese Policy zuständig (Siehe Kapitel 1.5.2).

1.5.4 Verfahren zur Genehmigung der Regelungen zum Betrieb (CPS)

Ein Genehmigungsverfahren ist nicht festgelegt. Die Konsistenz zwischen den Dokumenten Certificate Policy und Certification Practice Statements wird dadurch erreicht, dass beide Dokumente in der Verantwortung einer organisatorischen Einheit liegen.

1.6 Definitionen und Abkürzungen

Die Begriffe und Abkürzungen sind in Kapitel 10 definiert.

2 Veröffentlichungen und Verzeichnisdienst

2.1 Verzeichnisdienste

Die vom Zertifikatsdienst DRV QC Root CA und den qualifizierten Zertifikatsdiensten der Mandanten ausgestellten Systemzertifikate (CA-, TSA- und OCSP-Zertifikate) werden im Verzeichnisdienst des Trustcenters der DRV veröffentlicht.

OCSP-Auskünfte werden für alle ausgestellten Zertifikate durch den jeweiligen Validierungsdienst (OCSP-Responder) erteilt.

Die ausgestellten Zertifikate enthalten die Dienstadressen des Verzeichnisdienstes zum öffentlichen Abruf des Aussteller CA-Zertifikates und des Validierungsdienstes zum öffentlichen Abruf von OCSP-Statusauskünften.

2.1.1 Verzeichnisdienst

Im Verzeichnisdienst werden die von den Zertifikatsdiensten ausgestellten Systemzertifikate veröffentlicht (CA-, OCSP- und TSA-Zertifikate). Diese Zertifikate sind öffentlich abrufbar.

Die veröffentlichten Informationen können vom Verzeichnisdienst über die Protokolle HTTP und LDAP aus dem Internet und dem DRV-Netz anonym abgerufen werden. Die Adressen der LDAP- und HTTP-Dienste zum Download für Aussteller CA-Zertifikate sind in den ausgestellten Zertifikaten in der Extension „IssuerAltName (IAN)“ enthalten.

Der Verzeichnisdienst wird hochverfügbar 24 Stunden am Tag, 7 Tage die Woche betrieben.

2.1.2 Validierungsdienst

Der Status der ausgestellten Zertifikate kann über den jeweiligen Validierungsdienst (OCSP-Responder) abgefragt werden. Der Validierungsdienst erteilt Vorhandenseins- und Sperrauskünfte. Die notwendigen Informationen für den Zugriff auf den Validierungsdienst sind in den ausgestellten Zertifikaten in der Extension „AuthorityInfoAccess (AIA)“ enthalten.

Der Validierungsdienst DRV QC Root OCSP gibt Auskunft über den Status von Zertifikaten, die vom Zertifikatsdienst DRV QC Root CA ausgestellt wurden. Die Auskunft wird über die Laufzeit des entsprechenden Zertifikates hinaus für 30 Jahre erteilt. Im Fall der Einstellung des Betriebes des Zertifikatsdienstes DRV QC Root CA wird der Betrieb des Validierungsdienstes DRV QC Root OCSP eingestellt und es werden Auskünfte zum Sperrstatus über eine Sperrliste (CRL) erteilt.

Der Validierungsdienst wird hochverfügbar 24 Stunden am Tag, 7 Tage die Woche betrieben.

2.1.3 Vertrauensliste der Bundesnetzagentur

Die vom qualifizierten Zertifikatsdienst DRV QC Root CA ausgestellten Systemzertifikate für qualifizierte Vertrauensdienste (CA- und TSA-Zertifikate) werden an die nationale Aufsichtsstelle gemäß Artikel 17 eIDAS-VO [1] übermittelt. Die Aufsichtsstelle veröffentlicht diese Zertifikate bei Vorliegen eines gültigen Konformitätsbewertungsberichtes (Siehe Kapitel 8) gemäß Artikel 22 eIDAS-VO in der nationalen Vertrauensliste [12].

2.2 Veröffentlichung von Informationen

Das vorliegende Dokument "Certificate Policy des Zertifikatsdienstes DRV QC Root CA" wird auf der Web-Seite des VDA DRV Bund veröffentlicht [10].

Die Nutzungsbedingungen des Zertifikatsdienstes DRV QC Root CA werden in Form eines "PKI Disclosure Statements" auf der Web-Seite des VDA DRV Bund veröffentlicht.

Dokumentname: PKI Disclosure Statements des Zertifikatsdienstes DRV QC Root CA

OID: 1.3.6.1.4.1.22204.1.8.6.1.1

Das Dokument "Certification Practice Statements des Zertifikatsdienstes DRV QC Root CA" wird nicht veröffentlicht und kann bei begründetem Bedarf beim Trustcenter der DRV über die Kontaktadresse (Siehe Kapitel 1.5.2) angefordert werden.

Die Root-CA-Zertifikate des Zertifikatsdienstes DRV QC Root CA werden zusätzlich auf der Web-Seite des VDA DRV Bund und in der Zeitschrift „RVaktuell“, dem amtlichen Veröffentlichungsblatt der DRV, veröffentlicht.

Im Fall der Einstellung des Betriebes werden die Sperrauskünfte für Zertifikate des Zertifikatsdienstes DRV QC Root CA über eine Sperrliste (CRL) erteilt. Die Veröffentlichung erfolgt auf der Web-Seite des VDA DRV Bund über einen Zeitraum von 30 Jahren.

Die Web-Seite des VDA DRV Bund wird hochverfügbar 24 Stunden am Tag, 7 Tage die Woche betrieben.

2.3 Aktualisierung der Informationen (Zeitpunkt, Frequenz)

Die Aktualisierung der Informationen hängt von ihrem Typ ab. Die folgende Tabelle fasst die relevanten Informationen zusammen:

Tabelle 1: Veröffentlichte Informationen

Information	Frequenz der Aktualisierung	Zeitpunkt der Veröffentlichung	Ziel der Veröffentlichung
Dokument CP	Aktualisierung bei Bedarf	Nach Freigabe des Dokumentes	• Web-Seite des VDA DRV Bund
Dokument PKI Disclosure Statements	Aktualisierung bei Bedarf	Nach Freigabe des Dokumentes	• Web-Seite des VDA DRV Bund
Dokument CPS	Aktualisierung nach Bedarf	Keine Veröffentlichung	• nicht relevant
Zertifikat des Zertifikatsdienstes DRV QC Root CA (Root-CA-Zertifikat)	Zertifikatserstellung vor Ablauf des aktuellen Zertifikates	Nach Erstellung des Zertifikates	• Web-Seite des VDA DRV Bund • Zeitschrift RVaktuell • Verzeichnisdienst • Validierungsdienst • Vertrauensliste
Sperrliste des Zertifikatsdienstes DRV QC Root CA	Einmalige Erstellung bei Einstellung des Zertifikatsdienstes	Nach Erstellung der Sperrliste	• Web-Seite des VDA DRV Bund
Zertifikate des Validierungsdienstes DRV QC Root OCSP	Direkt nach dem Root-CA-Zertifikat	Nach Erstellung der Zertifikate	• Verzeichnisdienst • Validierungsdienst
Zertifikate des Zeitstempeldienstes DRV QC Root TSA	Direkt nach dem Root-CA-Zertifikat	Nach Erstellung der Zertifikate	• Verzeichnisdienst • Validierungsdienst • Vertrauensliste
Zertifikate der qualifizierten Zertifikatsdienste der Mandanten	Direkt nach dem Root-CA-Zertifikat	Nach Erstellung der Zertifikate	• Verzeichnisdienst • Validierungsdienst • Vertrauensliste
Zertifikate der qualifizierten Validierungsdienste der Mandanten	Direkt nach dem Mandanten-CA-Zertifikat	Nach Erstellung der Zertifikate	• Verzeichnisdienst • Validierungsdienst

2.4 Zugangskontrolle zu Verzeichnisdiensten

Die Zugangskontrolle zu den Veröffentlichungspunkten im Trustcenter der DRV ist wie folgt vorgesehen:

Tabelle 2: Zugangskontrolle zu Veröffentlichungspunkten

Veröffentlichungspunkt	Zugriffsart	Zugriff durch	Zugriffsschutz
Web-Seite VDA DRV Bund	Erstellen, Ändern, Löschen	Web-Admin	Authentisierung erforderlich
	Lesen	Unbeschränkt	Anonym
Verzeichnisdienst	Erstellen, Ändern, Löschen	Zertifikats-managementsystem	Authentisierung erforderlich
	Lesen	Unbeschränkt für Systemzertifikate	Anonym
Validierungsdienst	Erstellen, Ändern, Löschen	Zertifikats-managementsystem	Authentisierung erforderlich
	OCSP-Auskunft	Unbeschränkt	Anonym

3 Identifizierung und Authentifizierung

In diesem Kapitel werden die Identifizierung und Authentifizierung der Inhaber der qualifizierten Systemzertifikate behandelt.

3.1 Namen

3.1.1 Namensformen

Die vom Zertifikatsdienst DRV QC Root CA sowie die von den qualifizierten Zertifikatsdiensten der Mandanten ausgestellten Systemzertifikate enthalten im Namen für Aussteller und Inhaber folgende Attribute:

- Common Name,
- Organizational Unit,
- Organization,
- Country.

Mit dem Attribut „Organizational Unit“ werden verschiedene CA's eines VDA voneinander unterschieden. Das Attribut „Common Name“ gibt dem Zertifikat einen aussagekräftigen Namen. Die verwendeten Namen für Systemzertifikate sind in der nächsten Tabelle zusammengefasst.

Tabelle 3: Namen der Systemzertifikate

Zertifikatsinhaber	Name
Zertifikatsdienst DRV QC Root CA	CN=DRV QC Root CA <JJJJ><V> OU=QC Root CA O=Deutsche Rentenversicherung C=DE
Validierungsdienst DRV QC Root OCSP	CN=DRV QC Root OCSP <JJJJ><V> OU=QC Root CA O=Deutsche Rentenversicherung C=DE
Zeitstempeldienst DRV QC Root TSA	CN=DRV QC Root TSA <JJJJ><V> OU=QC Root CA O=Deutsche Rentenversicherung C=DE
Zertifikatsdienst DRV QC 70 MA CA	CN=DRV QC 70 MA CA <JJJJ><VV> OU=QC 70 Mitarbeiter CA O=Deutsche Rentenversicherung Bund C=DE
Validierungsdienst DRV QC 70 MA OCSP	CN=DRV QC 70 MA OCSP <JJJJ><VV> OU=QC 70 Mitarbeiter CA O=Deutsche Rentenversicherung Bund C=DE
Zertifikatsdienst DRV QC 13 MA CA	CN=DRV QC 13 MA CA <JJJJ><VV> OU=QC 13 Mitarbeiter CA O=Deutsche Rentenversicherung Rheinland C=DE

Zertifikatsinhaber	Name
Validierungsdienst DRV QC 13 MA OCSP	CN=DRV QC 13 MA OCSP <JJJJ><VV> OU=QC 13 Mitarbeiter CA O=Deutsche Rentenversicherung Rheinland C=DE
Zertifikatsdienst DRV QC 11 MA CA	CN=DRV QC 11 MA CA <JJJJ><VV> OU=QC 11 Mitarbeiter CA O=Deutsche Rentenversicherung Westfalen C=DE
Validierungsdienst DRV QC 11 MA OCSP	CN=DRV QC 11 MA OCSP <JJJJ><VV> OU=QC 11 Mitarbeiter CA O=Deutsche Rentenversicherung Westfalen C=DE

Angaben in spitzen Klammern <…> sind Platzhalter.

Angaben in eckigen Klammern […] sind optionale Angaben.

Tabelle 4: Erläuterungen zu den Platzhaltern

Platzhalter	Erläuterung	Wertebereich (Beispiele)
<JJJJ>	Jahr der Erstellung	2017, 2018, …
<V>	Version für Zertifikate der ersten Ebene	a, b, …
<VV>	Version für Zertifikate der zweiten Ebene, der erste Buchstabe wird vom Ersteller der ersten Ebene übernommen	aa, ab, … ba, bb, …

Anmerkungen:

- Die Version der CA-Zertifikate der zweiten Ebene beinhaltet als ersten Buchstaben die Version des Root-CA-Zertifikates, welches diese Zertifikate ausgegeben hat.
- Die Version eines TSA-Zertifikats entspricht der Version des Root-CA-Zertifikats, welches das TSA-Zertifikat ausgegeben hat.
- Die Version eines OCSP-Zertifikats entspricht der Version des CA-Zertifikats, welches das OCSP-Zertifikat ausgegeben hat.

3.1.2 Aussagekraft von Namen

Das Attribute "Common Name" gibt jedem Zertifikat einen aussagekräftigen Namen.

3.1.3 Anonymität bzw. Pseudonyme der Zertifikatsinhaber

Die qualifizierten Systemzertifikate (CA-, OCSP- und TSA-Zertifikate) werden auf Pseudonyme ausgestellt. Auf organisatorischem Weg wird die Zuordnung der Pseudonyme zu natürlichen Personen realisiert. Das Pseudonym wird in der Extension "Subject Directory Attributes" wie folgt angegeben:

Tabelle 5: Pseudonyme in den qualifizierten Zertifikaten

Dienst	Dienstname	Pseudonym für Zertifikatsinhaber
Zertifikatsdienst	DRV QC Root CA	Zertifikatsdienst DRV QC Root CA <NN>:PN
	DRV QC 70 MA CA	Zertifikatsdienst DRV QC 70 MA CA <NN>:PN
	DRV QC 13 MA CA	Zertifikatsdienst DRV QC 13 MA CA <NN>:PN
	DRV QC 11 MA CA	Zertifikatsdienst DRV QC 11 MA CA <NN>:PN
Validierungsdienst	DRV QC Root OCSP	Validierungsdienst DRV QC Root OCSP <S><NN>:PN
	DRV QC 70 MA OCSP	Validierungsdienst DRV QC 70 MA OCSP <S><NN>:PN
	DRV QC 13 MA OCSP	Validierungsdienst DRV QC 13 MA OCSP <S><NN>:PN
	DRV QC 11 MA OCSP	Validierungsdienst DRV QC 11 MA OCSP <S><NN>:PN
Zeitstempeldienst	DRV QC Root TSA	Zeitstempeldienst DRV QC Root TSA <S><NN>:PN

Tabelle 6: Erläuterungen zu den Platzhaltern

Platzhalter	Erläuterung	Wertebereich
<S>	Abkürzung des Standortes	B für Berlin, W für Würzburg
<NN>	Laufende zweistellige Nummer	01, 02, …

3.1.4 Regeln zur Interpretation verschiedener Namensformen

Es gibt keine verschiedenen Namensformen.

3.1.5 Eindeutigkeit von Namen

Die verwendeten Namen sind von den Vorgaben her eindeutig.

3.1.6 Anerkennung, Authentifizierung und Funktion von Warenzeichen

Keine Angaben.

3.2 Identitätsüberprüfung bei Neuantrag

3.2.1 Nachweis des Besitzes des privaten Schlüssels

Die privaten Schlüssel werden in der sicheren Umgebung des Trustcenters der DRV auf qualifizierten Signaturerstellungseinheiten generiert.

Der Nachweis des Besitzes des privaten Schlüssels für qualifizierte CA-Zertifikate erfolgt implizit bei der Zertifikatserstellung durch das Zertifikatsmanagementsystem.

Der Nachweis des Besitzes des privaten Schlüssels für qualifizierte TSA- und OCSP-Zertifikate erfolgt explizit durch die Signaturprüfung des PKCS#10 Zertifikatsantrages durch das Zertifikatsmanagementsystem.

3.2.2 Identifizierung einer Organisation

Die Organisation natürlicher Personen wird über ihren Dienstausweis sicher identifiziert. Im Protokoll Schlüsselwechsel werden u.a. folgende Daten des Zertifikatsinhabers bzw. des Auditors erfasst:

- Personalnummer.

3.2.3 Identifizierung natürlicher Personen

Natürliche Personen werden über einen gültigen Personalausweis oder Reisepass sicher identifiziert. Im Protokoll Schlüsselwechsel werden u.a. folgende Daten des Zertifikatsinhabers erfasst:

- Name, Vorname(n), Titel,
- Geburtsdatum, Geburtsort, Staatsangehörigkeit,
- Art, Nummer und Gültigkeit des amtlichen Ausweisdokumentes.

3.2.4 Nicht überprüfte Teilnehmerangaben

Keine Angaben.

3.2.5 Überprüfung der Berechtigung

Zertifikatsinhaber erhalten ihre Berechtigung zum Zertifikatserhalt durch Verwaltungsvereinbarungen bzw. durch die Rollenbeschreibung für Systemverwalter Server. Die Prüfung der Berechtigung der Systemverwalter Server erfolgt durch den Leiter des VDA DRV Bund bzw. seine Stellvertreter.

3.2.6 Kriterien für Zusammenarbeit

Keine Angaben.

3.3 Identitätsüberprüfung bei Zertifikatserneuerung

3.3.1 Routinemäßige Zertifikatserneuerung

Die Identitätsprüfung bei Zertifikatserneuerung erfolgt analog zur initialen Zertifikatserstellung.

3.3.2 Zertifikatserneuerung nach einer Sperrung

Die Identitätsprüfung bei Zertifikatserneuerung nach einer Sperrung erfolgt analog zur initialen Zertifikatserstellung.

3.4 Identifizierung und Authentifizierung von Sperranträgen

Der Antrag auf Sperrung/Widerruf von Systemzertifikaten kann ausschließlich von einem Sperrberechtigten gestellt werden. Für qualifizierte Systemzertifikate sind folgende Personen sperrberechtigt:

- Mitarbeiter der Bundesnetzagentur,
- der VDA-Leiter DRV Bund oder Stellvertreter,
- der VDA-Leiter DRV Rheinland oder Stellvertreter,
- der VDA-Leiter DRV Westfalen oder Stellvertreter.

Die Sperrberechtigten wurden schriftlich über die Identifizierung des Antragstellers und die Authentifizierung des Sperrantrages informiert.

Der Ablauf der Sperrung wird im Practice Statements Dokument definiert.

4 Ablauforganisation (Certificate Lifecycle)

4.1 Zertifikatsantrag

Die Festlegungen werden im Dokument Certification Practice Statements definiert.

4.2 Bearbeitung von Zertifikatsanträgen

Die Festlegungen werden im Dokument Certification Practice Statements definiert.

4.3 Zertifikatserstellung

Die Festlegungen werden im Dokument Certification Practice Statements definiert.

4.4 Zertifikatsakzeptanz

Die Festlegungen werden im Dokument Certification Practice Statements definiert.

4.5 Verwendung des Schlüsselpaares und des Zertifikats

Die Festlegungen werden im Dokument Certification Practice Statements definiert.

4.6 Zertifikatserneuerung unter Beibehaltung des alten Schlüssels

Die Festlegungen werden im Dokument Certification Practice Statements definiert.

4.7 Schlüssel- und Zertifikatserneuerung

Die Festlegungen werden im Dokument Certification Practice Statements definiert.

4.8 Zertifikatsmodifizierung

Die Festlegungen werden im Dokument Certification Practice Statements definiert.

4.9 Widerruf / Sperrung und Suspendierung von Zertifikaten

Die Sperrung (Widerruf) von Systemzertifikaten wegen einem der nachfolgenden Sperrgründe wird im CPS geregelt.

4.9.1 Sperrgründe

Sperrgründe sind:

- der Zertifikatsinhaber verlässt die Organisation,
- bei Verlust, Defekt oder Diebstahl der System-CK,
- bei unrichtigen Angaben in einem ausgestellten Zertifikat,
- bei notwendigen Änderungen in Zertifikatsinhalten,
- Chipkarte wird als Schlüsselspeicher nicht mehr als sicher eingestuft,
- Bei Verdacht der unbefugten Nutzung des privaten Schlüssels,
- Bei Kompromittierung des Schlüssels der ausstellenden CA,
- Wenn ein Systemzertifikat nicht mehr benötigt wird (z.B. bei Betriebseinstellung),
- Unregelmäßigkeiten in den Prozessen Registrierung, Karteninitialisierung, Schlüsselgenerierung bzw. Zertifikatserstellung.

4.10 Dienst zur Statusabfrage von Zertifikaten (OCSP)

Die Festlegungen werden im Dokument Certification Practice Statements definiert.

4.11 Beendigung des Vertragsverhältnisses

Die Festlegungen werden im Dokument Certification Practice Statements definiert.

4.12 Schlüsselhinterlegung und -wiederherstellung

Die Festlegungen werden im Dokument Certification Practice Statements definiert.

5 Infrastrukturelle, organisatorische und personelle Sicherheitsmaßnahmen

5.1 Infrastrukturelle Sicherheitsmaßnahmen

Infrastrukturelle Sicherheitsmaßnahmen werden im Dokument Certification Practice Statements definiert.

5.2 Organisatorische Sicherheitsmaßnahmen

Organisatorische Sicherheitsmaßnahmen werden im Dokument Certification Practice Statements definiert.

5.3 Personelle Sicherheitsmaßnahmen

Personelle Sicherheitsmaßnahmen werden im Dokument Certification Practice Statements definiert.

5.4 Überwachung / Protokollierung

Anforderungen an die Überwachung und Protokollierung werden im Dokument Certification Practice Statements definiert.

5.5 Archivierung

Anforderungen an die Archivierung werden im Dokument Certification Practice Statements definiert.

5.6 Schlüsselwechsel des Zertifikatsdienstes

Anforderungen an den Schlüsselwechsel des Zertifikatsdienstes werden im Dokument Certification Practice Statements definiert.

5.7 Kompromittierung und Wiederherstellung

Anforderungen an die Tätigkeiten nach einer Kompromittierung von Systemen oder kryptografischen Schlüssel sowie die Maßnahmen zur Wiederherstellung der Dienste werden im Dokument Certification Practice Statements definiert.

5.8 Einstellung des Betriebs

Die Nutzer des qualifizierten Zertifikatsdienstes DRV QC Root CA sind:

- der qualifizierte Zeitstempeldienst DRV QC Root TSA,
- der qualifizierte Zertifikatsdienst DRV QC 70 MA CA,
- der qualifizierte Zertifikatsdienst DRV QC 13 MA CA und
- der qualifizierte Zertifikatsdienst DRV QC 11 MA CA.

Über die Einstellung des Betriebes des qualifizierten Zertifikatsdienstes DRV QC Root CA entscheidet der Leiter des VDA DRV Bund in Abstimmung mit der Geschäftsleitung der DRV Bund. Die Leiter der VDA DRV Rheinland und DRV Westfalen werden in diesen Prozess eingebunden.

Die Einstellung des Betriebes des qualifizierten Zertifikatsdienstes DRV QC Root CA erfolgt erst, wenn der Betrieb aller untergeordneten Vertrauensdienste eingestellt worden ist.

Bei der Einstellung des qualifizierten Zertifikatsdienstes DRV QC Root CA gelten insbesondere folgende Anforderungen:

- Übertragung der Pflichten, Aufgaben und Dokumentation:

  Die Pflichten, Aufgaben und Dokumentationen werden nicht an einen anderen VDA übergeben. Der Zertifikatsdienst wird nicht fortgesetzt.

  Alle noch gültigen vom Zertifikatsdienst DRV QC Root CA ausgestellten Zertifikate werden vor Einstellung des Betriebes gesperrt. Es wird eine komplette Sperrliste des Zertifikatsdienstes erstellt. Die Sperrliste wird auf der Web-Seite des VDA DRV Bund veröffentlicht (Siehe Kapitel 2.2).

  Die Zertifikate des Zertifikatsdienstes DRV QC Root CA sowie eine komplette Sperrliste dieses Dienstes werden auf der Web-Seite des VDA DRV Bund veröffentlicht.

  Die Konzepte und die Dokumentation des qualifizierten Zertifikatsdienstes werden durch den VDA DRV Bund archiviert und für den rechtlich notwendigen Zeitraum vorgehalten. Eine Einsicht in die Dokumentation kann in berechtigten Fällen beim VDA DRV Bund erfolgen.

- Informationspflicht:

  Die Anwender des qualifizierten Zertifikatsdienstes DRV QC Root CA und der davon abhängigen untergeordneten Vertrauensdienste werden direkt informiert, da sie in den Prozess der Einstellung des Betriebes involviert sind.

  Die nationale Aufsichtsstelle gemäß eIDAS-VO wird vorab über die beabsichtigte Einstellung des Betriebes informiert.

  Die vertrauenden Parteien werden über die Web-Seite des VDA DRV Bund über die Einstellung des Betriebes informiert.

- Geordneter Rückbau:

  Nach Einstellung des Betriebes wird der private Schlüssel des Zertifikatsdienstes zerstört. Es ist dadurch nicht möglich, weiterhin Zertifikate zu erstellen.

Die Prozeduren zur Einstellung des Betriebes des qualifizierten Zertifikatsdienstes DRV QC Root CA sind im Beendigungsplan [9] definiert.

6 Technische Sicherheitsmaßnahmen

6.1 Schlüsselerzeugung und Installation

Technische Sicherheitsmaßnahmen bzgl. Schlüsselerzeugung und Installation werden im Dokument Certification Practice Statements definiert.

6.2 Schutz privater Schlüssel und Einsatz kryptographischer Module

Technische Sicherheitsmaßnahmen bzgl. Schutz privater Schlüssel werden im Dokument Certification Practice Statements definiert.

6.3 Weitere Aspekte des Schlüsselmanagements

Technische Sicherheitsmaßnahmen bzgl. Schlüsselmanagement werden im Dokument Certification Practice Statements definiert.

6.4 Aktivierungsdaten

Technische Sicherheitsmaßnahmen bzgl. dem Management von Aktivierungsdaten werden im Dokument Certification Practice Statements definiert.

6.5 Sicherheitsmaßnahmen für Computer

Technische Sicherheitsmaßnahmen bzgl. der Sicherheit der eingesetzten Computer Systeme werden im Dokument Certification Practice Statements definiert.

6.6 Technische Maßnahmen im Lebenszyklus

Technische Sicherheitsmaßnahmen im Betrieb des Trustcenters werden im Dokument Certification Practice Statements definiert.

6.7 Sicherheitsmaßnahmen für das Netzwerk

Technische Sicherheitsmaßnahmen im Netzwerk werden im Dokument Certification Practice Statements definiert.

6.8 Zeitstempel

Technische Sicherheitsmaßnahmen bzgl. Uhrzeitmanagement werden im Dokument Certification Practice Statements definiert.

7 Profile für Zertifikate, Sperrlisten und Online-Abfragen

7.1 Zertifikatsprofil

Der VDA DRV Bund erstellt qualifizierte Zertifikate gemäß RFC 5280[3].

7.1.1 Versionsnummer

Der VDA DRV Bund erstellt X.509 Zertifikate Version 3 gemäß RFC 5280 [3].

7.1.2 Zertifikatserweiterungen

Die qualifizierten Systemzertifikate der qualifizierten Vertrauensdienste beinhalten Zertifikatserweiterungen gemäß RFC 5280 [3]. Folgende Zertifikatserweiterungen sollen verwendet werden:

Tabelle 7: Zertifikatserweiterungen für qualifizierte Zertifikate

Erweiterung	Erläuterung	Verwendung für			
		QC Root CA	QC Root OCSP QC Root TSA	QC 70 MA CA QC 13 MA CA QC 11 MA CA	QC 70 MA OCSP QC 13 MA OCSP QC 11 MA OCSP
Authority Key Identifier	Hashwert des öffentlichen Schlüssels des Herausgebers		x	x	x
Subject Key Identifier	Hashwert des öffentlichen Schlüssels im Zertifikat	x		x	
Certificate Policies	OID & URL der Policy der DRV OID & URL der Policy QCP-N-QSCD	x	x	x	x
Subject Directory - Attributes	Pseudonym des Zertifikatsinhabers	x	x	x	x
Authority Info Access	URL des OCSP-Responder für Zertifikatsstatus-prüfung		x	x	x
Issuer Alt Names	URL(s) zum Abruf des Issuer Zertifikates		x	x	x
QC Statements	Attribute QcsCompliance und QcsQcSSCD gemäß [8]	x	x	x	x
Key Usage; kritisch	Verwendungszweck des Schlüssels	keyCertSign	nonRepudiation	keyCertSign	nonRepudiation
Extended Key Usage; kritisch	Erweiterter Verwendungszweck des Schlüssels		OCSPSigning timeStamping [1]		OCSPSigning
Basic Constraints; kritisch	Einschränkungen des Zertifikates (CA- oder EE-Zertifikat)	x	x	x	x

[1] OCSP Zertifikate beinhalten das Attribut OCSPSigning, TSA Zertifikate das Attribut timeStamping.

7.1.3 Algorithmus Bezeichner (OID)

Der Zertifikatsdienst DRV QC Root CA sowie die qualifizierten Zertifikatsdienste der Mandanten erstellen qualifizierte Systemzertifikate mit dem Signaturalgorithmus sha256withRSAEncryption.

Alternativ kann der Signaturalgorithmus RSASSA-PSS genutzt werden.

Es sind die Vorgaben des nationalen Algorithmen-Katalogs [11] zu beachten.

Tabelle 8: Signaturalgorithmus für qualifizierte Zertifikate

Signaturalgorithmus	Erläuterung	OID
sha256withRSAEncryption	SHA2-256 Hashwert, PKCS#1 v1.5 Padding, RSA Verschlüsselung	1.2.840.113549.1.1.11

RSASSA-PSS	rsaPSS_Parameter Sequence {
	hashAlgorithm = { id-sha256, NULL }
	maskGenAlgorithm = { id-pkcs1-mgf,
	{ id-sha256, NULL } }
	saltLength = 32
	}
		1.2.840.113549.1.1.10

Die qualifizierten Validierungsdienste erstellen OCSP-Auskünfte mit dem Signatur-algorithmus sha256withRSAEncryption oder RSASSA-PSS.

Es sind die Vorgaben des nationalen Algorithmen-Katalogs [11] zu beachten.

Tabelle 9: Signaturalgorithmus für OCSP-Auskünfte

Signaturalgorithmus	Erläuterung	OID
sha256withRSAEncryption	SHA2-256 Hashwert, PKCS#1 v1.5 Padding, RSA Verschlüsselung	1.2.840.113549.1.1.11

RSASSA-PSS	rsaPSS_Parameter Sequence {
	hashAlgorithm = { id-sha256, NULL }
	maskGenAlgorithm = { id-pkcs1-mgf,
	{ id-sha256, NULL } }
	saltLength = 32
	}
		1.2.840.113549.1.1.10

7.1.4 Namensformen

Die zugelassenen Namen sind in Kapitel 3.1.1 definiert.

7.1.5 Namensbeschränkungen

Die zugelassenen Namen sind in Kapitel 3.1.1 definiert.

Die Extension "Name Constraints" wird nicht verwendet.

7.1.6 Bezeichner für Richtlinien (OID)

Der Zertifikatsdienst DRV QC Root CA sowie die qualifizierten Zertifikatsdienste der Mandanten erstellen qualifizierte Systemzertifikate gemäß den folgenden Policies.

Tabelle 10: Policies für qualifizierte Zertifikate

Policy	Erläuterung	OID
CP DRV	Policy der DRV des qualifizierten Zertifikatsdienstes DRV QC Root CA	1.3.6.1.4.1.22204.1.8.1.1.1
QCP-N-QSCD	Policy der EU für qualifizierte Zertifikate ausgestellt für natürliche Personen auf qualifizierten Signaturerstellungseinheiten gemäß [8]	0.4.0.194112.1.2

7.1.7 Nutzung von Erweiterungen zur Richtlinienbeschränkungen

Die Extensions "Policy Mappings", "Policy Constraints" und "Inhibit Any Policy" werden nicht verwendet.

7.1.8 Syntax und Semantik von Policy Qualifiern

Der Zertifikatsdienst DRV QC Root CA sowie die qualifizierten Zertifikatsdienste der Mandanten erstellen qualifizierte Zertifikate mit den folgenden Policy Qualifier.

Tabelle 11: Policy Qualifier für qualifizierte Zertifikate

Attribut	Erläuterung	Wert
Policy URL	URL DRV Policy	http://www.deutsche-rentenversicherung-bund.de/static/trustcenter/policy.html
	URL Norm ETSI EN 319411-2	http://www.etsi.org/deliver/etsi_en/319400_319499/31941102/

7.1.9 Verarbeitung von kritischen Erweiterungen für Richtlinien (CertificatePolicies)

Die Extension CertificatePolicies wird nicht kritisch gesetzt.

7.2 Sperrlistenprofil

7.2.1 Versionsnummer

Der VDA DRV Bund erstellt im Betrieb keine Sperrlisten für den qualifizierten Zertifikatsdienst DRV QC Root CA.

Im Fall der Betriebseinstellung erstellt der VDA DRV Bund für den Zertifikatsdienst DRV QC Root CA eine finale Sperrliste Version 3 gemäß RFC 5280 [3].

7.2.2 Sperrlisten- und Sperrlisteneintragserweiterungen

Der VDA DRV Bund erstellt im Betrieb keine Sperrlisten für den qualifizierten Zertifikatsdienst DRV QC Root CA.

Im Fall der Betriebseinstellung erstellt der VDA DRV Bund für den Zertifikatsdienst DRV QC Root CA eine Sperrliste. Die Sperrliste hat eine Laufzeit von 30 Jahren und beinhaltet Sperrinformationen zu allen gesperrten Zertifikaten des Zertifikatsdienstes DRV QC Root CA. Folgende Erweiterungen gemäß RFC 5280 sollen verwendet werden:

Tabelle 12: CRL-Erweiterungen für qualifizierte Zertifikate

Erweiterung	Erläuterung
Authority Key Identifier	Hashwert des öffentlichen Schlüssels des Herausgebers
Issuer Alt Names	URL(s) zum Abruf des Issuer Zertifikates
CRL Number	Nummer der (finalen) Sperrliste

7.3 OCSP Profil

7.3.1 Versionsnummer

Im Trustcenter der DRV werden OCSP-Responder für Auskünfte über qualifizierte Zertifikate gemäß RFC 6960 [4] Version 1 erstellt.

7.3.2 OCSP Erweiterungen

Die Validierungsdienste im Trustcenter der DRV erstellen OCSP-Auskünfte als "Authorized Responder" gemäß RFC 6960 [4]. Die OCSP-Auskünfte beinhalten das Zertifikat des OCSP-Responder und das Zertifikat des qualifizierten Zertifikatsdienstes DRV QC Root CA, welcher das OCSP-Zertifikat signiert hat.

In der OCSP-Auskunft werden die folgenden Erweiterungen verwendet.

Tabelle 13: Erweiterungen für OCSP-Auskünfte

Erweiterung	Erläuterung	Wert
OcspNonce	Zufallswert zur Verhinderung von Replay-Attacken; wird in der OCSP-Anfrage vom OCSP-Client mitgeliefert	Wiederholung des Wertes aus der OCSP-Anfrage
OcspArchiveCutoff	Das Datum wird vom OCSP-Responder berechnet.	13.09.1978 00:00:00 GMT [2]

[2] Beispielwert

8 Konformitätsprüfung (Compliance Audit, Assessments)

8.1 Häufigkeit und Umstände der Überprüfung

Die vollständige Konformitätsprüfung erfolgt regulär alle zwei Jahre gemäß Artikel 20 eIDAS-VO [1].

Nach einem Jahr ist ein Wiederholungsaudit vorgesehen. Schwerpunkte sind dabei die gefundenen Schwachstellen des letzten kompletten Audits.

Wenn größere Änderungen an den technischen Systemen oder den Prozessabläufen durchgeführt werden, ist eine Meldung an die Konformitätsbewertungsstelle erforderlich. Nach Abstimmung mit dieser kann eine außerordentliche vollständige Konformitätsbewertung erforderlich werden.

8.2 Identität und Qualifikation des Überprüfers

Die Konformitätsbewertung wird durch eine Konformitätsbewertungsstelle durchgeführt, welche durch die nationale Aufsichtsstelle gemäß Artikel 17 eIDAS-VO [1] mit der Konformitätsbewertung beauftragt ist.

8.3 Verhältnis von Prüfer zu Überprüftem

Es gibt außerhalb der Konformitätsbewertung keine geschäftlichen Bindungen zwischen dem VDA DRV Bund und der Konformitätsbewertungsstelle.

8.4 Überprüfte Bereiche

Die Konformitätsbewertung erfolgt für die produktiven Haupt- und Backup-Systeme der qualifizierten Zertifikatsdienste zur Erstellung qualifizierter Systemzertifikate.

8.5 Mängelbeseitigung

Die Mitarbeiter des VDA DRV Bund beheben die während der Konformitätsbewertung gefunden Mängel nach Vorgaben der Konformitätsbewertungsstelle.

8.6 Veröffentlichung der Ergebnisse

Das Zertifikat der Konformitätsbewertung wird durch die Konformitätsbewertungsstelle veröffentlicht [13].

9 Weitere geschäftliche und rechtliche Angelegenheiten

9.1 Gebühren

9.1.1 Gebühren für Zertifikatserstellung oder -erneuerung

Die Gebühren werden in der Verwaltungsvereinbarung mit den Mandanten des Trustcenters der DRV geregelt.

9.1.2 Gebühren für Zugriff auf Zertifikate

Die Gebühren werden in der Verwaltungsvereinbarung mit den Mandanten des Trustcenters der DRV geregelt.

9.1.3 Gebühren für Sperrung oder Statusabfragen

Die Gebühren werden in der Verwaltungsvereinbarung mit den Mandanten des Trustcenters der DRV geregelt.

9.1.4 Andere Gebühren

Keine Angaben.

9.1.5 Gebührenerstattung

Keine Angaben.

9.2 Finanzielle Verantwortung

9.2.1 Deckungsvorsorge

Die Deutsche Rentenversicherung Bund verfügt über die notwendige Deckungsvorsorge gemäß Artikel 24 eIDAS-VO [1] für den Zertifikatsdienst DRV QC Root CA für Schäden gemäß Artikel 13 eIDAS-VO.

9.2.2 Weitere Vermögenswerte

Die zentralen Systeme des Trustcenters der DRV werden durch die Deutsche Rentenversicherung Bund bereitgestellt.

9.2.3 Versicherung oder Garantie für Endteilnehmer

Keine Angaben.

9.3 Vertraulichkeit von Geschäftsinformationen

9.3.1 Vertraulich zu behandelnde Daten

Die Informationen im Sicherheitskonzept (Risikoanalyse, Sicherheitsmaßnahmen) sind als vertraulich und die Festlegungen zum Betrieb des Zertifikatsdienstes DRV QC Root CA (Certification Practice Statements, Betriebskonzept, etc.) sind als: "Nur für den Dienstgebrauch" eingestuft.

9.3.2 Nicht vertraulich zu behandelnde Daten

Keine Angaben

9.3.3 Verantwortung zum Schutz vertraulicher Informationen

Die Verantwortung zum Schutz vertraulicher Informationen tragen die Systemverwalter und die Mitarbeiter des VDA DRV Bund, welche diese Daten erstellen, nutzen und speichern.

9.4 Schutz personenbezogener Daten

9.4.1 Richtlinie zur Verarbeitung personenbezogener Daten

Der VDA DRV Bund hält die gesetzlichen Bestimmungen zum Schutz der erhobenen personenbezogenen Daten ein (BDSG).

Der Umfang der zu erhebenden Daten ergibt sich aus der eIDAS-VO. Die Inhaber der qualifizierten Systemzertifikate sind über die erhobenen Daten (Art und Umfang der Daten, Speicherort und Aufbewahrungsfrist) ausführlich informiert.

9.4.2 Vertraulich zu behandelnde Daten

Die Identifikationsdaten der Zertifikatsinhaber im Protokoll Schlüsselwechsel sind vertraulich zu behandeln.

9.4.3 Nicht vertraulich zu behandelnde Daten

Keine Angaben.

9.4.4 Verantwortung zum Schutz personenbezogener Daten

Die Verantwortung zum Schutz vertraulicher Informationen tragen die Systemverwalter und die Mitarbeiter des VDA DRV Bund, welche diese Daten erfassen, verarbeiten und speichern.

9.4.5 Einwilligung und Nutzung personenbezogener Daten

Die Zertifikatsinhaber müssen im Protokoll Schlüsselwechsel zustimmen, dass Zertifikate durch den VDA DRV Bund für sie erstellt werden.

9.4.6 Offenlegung bei gerichtlicher Anordnung oder im Rahmen gerichtlicher Beweisführung

Personenbezogene Daten können offengelegt werden, wenn dafür ein begründeter dienstlicher oder rechtlicher Grund vorliegt. Dafür ist die Kontaktadresse gemäß Kapitel 1.5.2 zuständig.

9.4.7 Andere Umstände einer Veröffentlichung

Keine Angaben.

9.5 Urheberrechte

Keine Angaben.

9.6 Pflichten

9.6.1 Pflichten des VDA bei der Zertifikatserstellung

Die Pflichten des VDA DRV Bund richten sich nach den Bestimmungen der entsprechenden ETSI-Normen [5], [6] und [7]. Insbesondere hat der VDA DRV Bund die Pflicht, Auskunft über den Sperrstatus ausgestellter qualifizierter Zertifikate zu erteilen. Die Auskunft wird über die Laufzeit des entsprechenden Zertifikates hinaus für 30 Jahre erteilt.

Für Testzertifikate kann das QS-System benutzt werden. Testzertifikate zeigen im Namen an, dass sie für Testzwecke genutzt werden.

9.6.2 Pflichten der Registrierungsstellen

Die Tätigkeiten der Registrierung werden vom Sicherheitsbeauftragen der DRV Bund bzw. vom Leiter VDA DRV Bund ausgeführt. Die Daten müssen wahrheitsgemäß aus den vorliegenden Dokumenten des Zertifikatsinhabers übernommen werden. Eine Änderung der übernommenen Daten ist nicht zulässig.

9.6.3 Pflichten des Zertifikatsinhabers

Die Pflichten der Zertifikatsinhaber richten sich nach den Bestimmungen der entsprechenden ETSI-Normen [5], [6] und [7] sowie den Verwaltungsvereinbarungen. Insbesondere ist der Zertifikatsinhaber verpflichtet, im Registrierungsprozess korrekte Angaben zu seiner Person zu machen.

Die Zertifikatsinhaber übergeben im Rahmen des Trustcenterbetriebes die Systemchipkarten an die zuständigen Systemverwalter Server. Die Systemverwalter Server sind verpflichtet, die Systemchipkarten entsprechend ihrem Verwendungszweck einzusetzen.

Im Falle der Notwendigkeit einer Sperrung von Systemchipkarten hat der Zertifikatsinhaber die Pflicht zur Mitteilung an den VDA-Leiter DRV Bund. Die Sperrgründe werden in Kapitel 4.9.1 benannt.

9.6.4 Pflichten der Zertifikatsprüfer (Relying Parties)

Zertifikatsprüfer müssen den Sperrstatus der Zertifikate der qualifizierten Zertifikatsdienste im Trustcenter der DRV mit Hilfe der Validierungsdienste (OCSP-Responder) prüfen. Im Fall der Einstellung des Betriebes des Zertifikatsdienstes DRV QC Root CA wird der Betrieb des Validierungsdienstes DRV QC Root OCSP eingestellt und es werden Auskünfte zum Sperrstatus über eine Sperrliste (CRL) erteilt. Die Veröffentlichung der CRL erfolgt auf der Web-Seite des VDA DRV Bund (siehe Kapitel 2.2). Ungültige Zertifikate dürfen nicht verwendet werden.

Zertifikatsprüfer müssen die Beschränkungen für den Einsatz der kryptografischen Schlüssel beachten. Die Beschränkungen sind im Zertifikat in den Extensions "Key Usage" und sofern vorhanden "Extended Key Usage" definiert (Siehe Kapitel 7.1).

Zertifikatsprüfer müssen Beschränkungen für den Einsatz der Zertifikate beachten. Die Beschränkungen sind in Kapitel 1.4 definiert.

Zertifikatsprüfer sollen bei Verdacht auf oder festgestelltem Missbrauch von Zertifikaten den Vertrauensdiensteanbieter darüber informieren. Dafür ist die Kontaktadresse in Kapitel 1.5.2 zu verwenden.

9.6.5 Pflichten anderer Teilnehmer

Keine Angaben

9.7 Haftung

Der VDA DRV Bund haftet nach den Bestimmungen der jeweiligen Verwaltungsvereinbarung sowie nach den gesetzlichen Vorgaben nach Artikel 13 der eIDAS-VO [1].

9.8 Haftungsbeschränkung

Haftung besteht nur im Rahmen der gesetzlichen Vorgaben.

9.9 Haftungsfreistellung

Keine Angaben.

9.10 Inkrafttreten und Aufhebung

9.10.1 Inkrafttreten

Dieses Dokument ist vom Tage seiner Veröffentlichung an gültig. Seine Gültigkeit endet mit der Einstellung des Zertifikatsdienstes DRV QC Root CA.

9.10.2 Aufhebung

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

9.10.3 Konsequenzen der Aufhebung

Wenn dieses Dokument ungültig wird, dann dürfen keine Zertifikate mehr nach dieser Richtlinie erstellt werden.

9.11 Individuelle Benachrichtigungen und Kommunikation mit Teilnehmern

Die Veröffentlichung dieser Richtlinie erfolgt auf der Web-Seite der DRV Bund (Siehe 2.2). Eine individuelle Benachrichtigung der Zertifikatsinhaber erfolgt durch den Leiter des VDA DRV Bund bzw. seine Stellvertreter.

9.12 Änderungen der Richtlinie

9.12.1 Vorgehen bei Änderungen

Der VDA DRV Bund behält sich die Änderung dieses Dokuments vor. Diese kann insbesondere durch eine Weiterentwicklung der technischen oder rechtlichen Gegebenheiten erforderlich sein.

Bei Ergänzungen oder Modifikationen entscheidet der VDA DRV Bund, ob sich daraus signifikante Änderungen der Sicherheit des Zertifikatsdienstes DRV QC Root CA sowie der qualifizierten Zertifikatsdienste der Mandanten, 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.

9.12.2 Benachrichtigungsmechanismus und Fristen

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 VDA DRV Bund 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.

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

9.12.3 Umstände, die eine Änderung des Richtlinienbezeichners (OID) erfordern

Eine Änderung der Richtlinien-OID ist dann erforderlich, wenn sich der Umfang der beinhalteten Vertrauensdienste bzw. der Umfang des Dokumentes ändert.

9.13 Konfliktbeilegung

Für die Prüfung von Beschwerden und die Beilegung von Meinungsverschiedenheiten ist die Schiedsstelle des Trustcenters der Deutschen Rentenversicherung zuständig.

Die Schiedsstelle ist erreichbar unter

E-Mail	Trustcenter-gRV@drv-bund.de
Postadresse	Deutsche Rentenversicherung Bund 1170-05 Trustcenter / Schiedsstelle D-10704 Berlin

9.14 Geltendes Recht

Es gilt grundsätzlich deutsches Recht, mit Ausnahme der eIDAS-VO, welche als Europäischer Rechtsakt unmittelbare Wirkung entfaltet und Anwendungsvorrang vor den nationalen Reglungen genießt.

9.15 Konformität mit geltendem Recht

Der Zertifikatsdienst DRV QC Root CA sowie die qualifizierten Zertifikatsdienste der Mandanten arbeiten als qualifizierte Vertrauensdienste zur Erstellung qualifizierter Zertifikate konform zur eIDAS-VO [1] und den relevanten ETSI-Normen [5], [6] und [7].

9.16 Weitere Regelungen

9.16.1 Vollständigkeit

Keine Angaben.

9.16.2 Abtretung der Rechte

Keine Angaben.

9.16.3 Salvatorische Klausel

Sollten einzelne Bestimmungen dieses Dokumentes unwirksam oder undurchführbar sein, bleibt davon die Wirksamkeit des restlichen Dokumentes unberührt.

9.16.4 Rechtliche Auseinandersetzungen / Erfüllungsort

Der Gerichtsstand ergibt sich aus dem Gesetz.

9.16.5 Force Majeure

Keine Angaben.

9.17 Andere Regelungen

Der VDA DRV Bund als Betreiber der zentralen Dienste im Trustcenter der DRV schließt mit den Mandanten im Trustcenter der DRV (RV-Träger) eine Verwaltungsvereinbarung ab, welche die Übernahme der zentralen Dienste dieses VDA regelt.

10 Abkürzungen und Begriffe

10.1 Abkürzungen

AD	Auskunftsdienst (OCSP-Statusauskünfte)
APC	Arbeitsplatz-PC
BDSG	Bundesdatenschutzgesetz
BNetzA	Bundesnetzagentur
BSI	Bundesamt für Sicherheit in der Informationstechnik
C	Country
CA	Certification Authority
CAB	Conformity Assessment Body (Konformitätsbewertungsstelle)
CAR	Conformity Assessment Report (Konformitätsbewertungsbericht)
CC	Common Criteria (ISO/IEC 15408)
CERTSN	Zertifikatsseriennummer
CK	Chipkarte
CN	Common Name
CP	Certificate Policy
CPS	Certification Practice Statements
CRL	Certificate Revocation List (Sperrliste)
DMS	Document Management System
DN	Distinguished Name
DNS	Domain Name Service
DRV	Deutsche Rentenversicherung
DRV BB	Deutsche Rentenversicherung Berlin-Brandenburg
DRV RL	Deutsche Rentenversicherung Rheinland
DRV WF	Deutsche Rentenversicherung Westfalen
DSRV	Datenstelle der Träger der Rentenversicherung
EAL	Evaluation Assurance Level
EE	End Entity
eIDAS	Electronic Identification and Trust Services for Electronic Transactions in the European Market
eIDAS-VO	eIDAS-Verordnung
EN	European Norm
ES-CK	Einzelsignaturchipkarte
ETSI	European Telecommunications Standard Institute
EU	European Union
FQDN	Fully Qualified Domain Name

HSM	Hardware Security Module
HSM-SCK	HSM-Systemchipkarte
HTTP	Hyper Text Transfer Protocol
HW	Hardware
ID	Identifikation
IETF	Internet Engineering Task Force
IT	Information Technology (Informationstechnik)
ITSEC	Information Technology Security Evaluation Criteria
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
MA	Mitarbeiter
MA-CK	Mitarbeiterchipkarte
MA-Tool	Mitarbeiter-Tool
MS-CK	Massensignaturchipkarte
NAB	National Accreditation Body (Nationale Akkreditierungsstelle)
Nonce	Number used once
NSB	National Supervisory Body (Nationale Aufsichtsstelle)
NTP	Network Time Protocol
O	Organization
OCSP	Online Certificate Status Protocol
OCSPR	OCSP-Responder (Software des AD)
OID	Object Identifier
OU	Organizational Unit
PBS	Produktiv Backup System
PC	Personal Computer
PEN	Private Enterprise Number
PHS	Produktiv Haupt System
PIN	Personal Identification Number
PKCS	Public Key Cryptography Standards
PKI	Public Key Infrastructure
PN	Pseudonym
PP	Protection Profile
PSE	Personal Security Environment
PTB	Physikalisch-technische Bundesanstalt Braunschweig
PUK	Personal Unblocking Key
QC	Qualified Certificate

QSCD	Qualifizierte elektronische Signaturerstellungseinheit (Qualified Signature Creation Device)
QTSP	Qualified Trust Service Provider (Qualifizierter Vertrauensdiensteanbieter)
RFC	Request for Comments - Internet Standards der IETF
RSA	Asymmetrischer Kryptografischer Algorithmus von Rivest, Shamir und Adleman
RV	Rentenversicherung
SHA	Secure Hash Algorithm
SigG	Signaturgesetz
SW	Software
SYS-CK	Systemchipkarte
TC	Trustcenter
TCDRV	Trustcenter der Deutschen Rentenversicherung
TSA	Time Stamp Authority (Zeitstempeldienst)
TSL	Trust Service Status List
TSP	Trust Service Provider
UHD	User Help Desk
URL	Unified Ressource Locator
UTC	Universal Time Coordinated
VD	Verzeichnisdienst (LDAP-Repository)
VDA	Vertrauensdiensteanbieter
VO	Verordnung
WAN	Wide Area Network
X.509	ITU-Standard für Zertifikate und Sperrlisten

10.2 Begriffe

Certificate Policy (CP)	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 ausführlich dargestellt. Insbesondere sollte eine Certificate Policy darlegen, • Welche Vorgaben zur Erstellung von Schlüsseln und Zertifikaten bzgl. Registrierung, Generierung und Veröffentlichung gelten, • Welche Vorgaben für die Anwendung der Zertifikate sowie der zugehörigen Schlüssel und Signaturerstellungseinheiten gelten, • Welche Bedeutung den Zertifikaten und ihrer Anwendung zukommt, das heißt welche Sicherheit, Beweiskraft, oder rechtliche Relevanz die mit ihnen erzeugten Signaturen besitzen.
Certification Practice Statements (CPS)	Nach RFC 3647 legt das „Certification Practice Statements“ (CPS) die Praktiken dar, die ein VDA bei der Erstellung und Management der Zertifikate anwendet. Das CPS Dokument macht Vorgaben bzgl. des Betriebes eines Zertifikatsdienstes. Das Dokument enthält keine Bestimmungen, die Rechte oder Pflichten von Personen begründen, ändern oder aufheben würden.
DCF77	Der Zeitzeichensender DCF77 der Bundesrepublik Deutschland wird in Mainflingen durch das PTB Braunschweig betrieben. Das PTB betreibt 4 hoch-präzise Cäsium-Uhren als Zeitnormal für die nationale Referenzzeit UTC(PTB). Die UTC(PTB) ist eine Quelle der Internationalen Atomzeit TAI des BIPM. Die bekannteste Zeitskale des BIPM ist die Weltzeit UTC.
EE-Zertifikat	Zertifikat für Endbenutzer (End Entity)
eIDAS-Verordnung	Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG
Mandant im Trustcenter der DRV	Als Mandanten werden die Träger der Deutschen Rentenversicherung bezeichnet, welche einen eigenen qualifizierten Zertifikatsdienst betreiben und damit als Vertrauensdiensteanbieter gemäß eIDAS-VO auftreten.
Qualifizierte EE-Zertifikate im Trustcenter der DRV	Qualifizierte Zertifikate für: • Mitarbeiter der DRV Rheinland bzw. DRV Westfalen auf MA-CK, • Mitarbeiter der DRV Bund auf ES-CK, • Mitarbeiter von RV-Trägern auf MS-CK.
Qualifizierte Systemzertifikate im Trustcenter der DRV	Qualifizierte Zertifikate für den Betrieb von: • Zertifikatsdienste DRV QC Root CA, DRV QC 70 MA CA, DRV QC 13 MA CA und DRV QC 11 MA CA, • Zeitstempeldienst DRV QC Root TSA, • Validierungsdienste DRV QC Root OCSP, DRV QC 70 MA OCSP, DRV QC 13 MA OCSP und DRV QC 11 MA OCSP
Qualifizierte Validierungsdienste der Mandanten im Trustcenter der DRV	Qualifizierter Vertrauensdienste: • DRV QC 70 MA OCSP • DRV QC 13 MA OCSP • DRV QC 11 MA OCSP

Qualifizierte Vertrauensdienste im Trustcenter der DRV	Qualifizierte Vertrauensdienste im Kontext des Trustcenters der DRV sind die elektronischen Dienste: • Zertifikatsdienst zur Ausstellung und Validierung qualifizierter elektronischer Zertifikate, • Zeitstempeldienst zur Erstellung qualifizierter elektronischer Zeitstempel.
Qualifizierte Zertifikatsdienste der Mandanten im Trustcenter der DRV	Qualifizierter Vertrauensdienste: • DRV QC 70 MA CA • DRV QC 13 MA CA • DRV QC 11 MA CA
Qualifizierter Vertrauensdienste-anbieter	Ein qualifizierter Vertrauensdiensteanbieter ist ein Vertrauensdiensteanbieter, der einen oder mehrere qualifizierte Vertrauensdienste erbringt und dem von der Aufsichtsstelle der Status eines qualifizierten Anbieters verliehen wurde.
Systemchipkarte	QSCD für qualifizierte Systemzertifikate
Validierungsdienst	Dienst zur Bereitstellung von Zertifikatsstatusauskünften auf Basis eines OCSP-Responder
Vertrauensdienste-anbieter	Ein Vertrauensdiensteanbieter ist eine natürliche oder juristische Person, die einen oder mehrere Vertrauensdienste als qualifizierter oder nichtqualifizierter Vertrauensdiensteanbieter erbringt.
Zeitstempeldienst DRV QC Root TSA	Qualifizierter Vertrauensdienst des VDA DRV Bund für die Ausstellung: • qualifizierter elektronischer Zeitstempel.
Zertifikatsdienst DRV QC 11 MA CA	Qualifizierter Vertrauensdienst des VDA DRV Westfalen für die Ausstellung: • qualifizierter EE-Zertifikate, • der Zertifikate des Validierungsdienstes DRV QC 11 MA OCSP.
Zertifikatsdienst DRV QC 13 MA CA	Qualifizierter Vertrauensdienst des VDA DRV Rheinland für die Ausstellung: • qualifizierter EE-Zertifikate, • der Zertifikate des Validierungsdienstes DRV QC 13 MA OCSP.
Zertifikatsdienst DRV QC 70 MA CA	Qualifizierter Vertrauensdienst des VDA DRV Bund für die Ausstellung: • qualifizierter EE-Zertifikaten, • der Zertifikate des Validierungsdienstes DRV QC 70 MA OCSP.
Zertifikatsdienst DRV QC Root CA	Qualifizierter Vertrauensdienst des VDA DRV Bund für die Ausstellung: • der Ausstellerzertifikate der Zertifikatsdienste DRV QC Root CA, DRV QC 70 MA CA, DRV QC 13 MA CA und DRV QC 11 MA CA, • der Zertifikate des Zeitstempeldienstes DRV QC Root TSA, • der Zertifikate des Validierungsdienstes DRV QC Root OCSP.

11 Informationen zum Dokument

11.1 Änderungsverzeichnis

Version	Datum	Kap.	Änderungsgrund	Bearbeiter
05.00.00	28.11.2011			DRV Bund
05.01.00	08.09.2014	Alle	Neu: NQ DRV Mitarbeiter Signatur CA	Atos
06.00.00	21.04.2017	Alle	Anpassung an eIDAS-VO / RFC 3647	Atos
06.01.00	10.05.2017	2.x, 5.8, 7.2, 9.6	Anpassung	Atos

11.2 Abbildungsverzeichnis

11.3 Tabellenverzeichnis

11.4 Referenzen

[1] eIDAS-VO: Verordnung Nr. 910/2014 der EU im Amtsblatt der Europäischen Union, L257/73; http://eur-lex.europa.eu/legal-content/DE/TXT/?uri=celex%3A32014R0910

[2] RFC 3647: Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework; Freigabe November 2003; http://www.faqs.org/rfcs/rfc3647.html

[3] RFC 5280: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, Freigabe Mai 2008; http://www.faqs.org/rfcs/rfc5280.html

[4] RFC 6960: X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP, Freigabe Juni 2013; http://www.faqs.org/rfcs/rfc6960.html

[5] ETSI EN 319 401 V2.1.1 (2016-02); Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers

[6] ETSI EN 319 411-1 V1.1.1 (2016-02); Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements

[7] ETSI EN 319 411-2 V2.1.1 (2016-02); Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates

[8] ETSI EN 319 412-5 V2.1.1 (2016-02); Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements

[9] Beendigungsplan des Trustcenters der Deutschen Rentenversicherung

[10] Web-Seite des VDA Deutsche Rentenversicherung Bund http://www.deutsche-rentenversicherung-bund.de/static/trustcenter/policy.html

[11] Web-Seite der Bundesnetzagentur zur Veröffentlichung geeigneter Algorithmen https://www.bundesnetzagentur.de/cln_1412/DE/Service-Funktionen/ElektronischeVertrauensdienste/QES/WelcheAufgabenhatdieBundesnetzagentur/GeeigneteAlgorithmenfestlegen/geeignetealgorithmenfestlegen_node.html

[12] Web-Seite der Bundesnetzagentur zur Veröffentlichung der nationalen Vertrauensliste; https://www.nrca-ds.de

[13] Web-Seite des TÜVIT zur Veröffentlichung von Konformitätsbewertungen für Vertrauensdiensteanbieter; https://www.tuvit.de/de/zertifikate-1265-4512.htm