Trustcenter der Deutschen Rentenversicherung

Vertrauensdiensteanbieter Deutsche Rentenversicherung Bund nach eIDAS-VO

Certificate Policy des Zertifikatsdienstes DRV QC 70 MA CA

Dokument-OID: 1.3.6.1.4.1.22204.1.8.1.1.2

Version	06.01.00
Stand	10.05.17
Dateiname	TCDRV_CP_DRV-QC-70-MA-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.

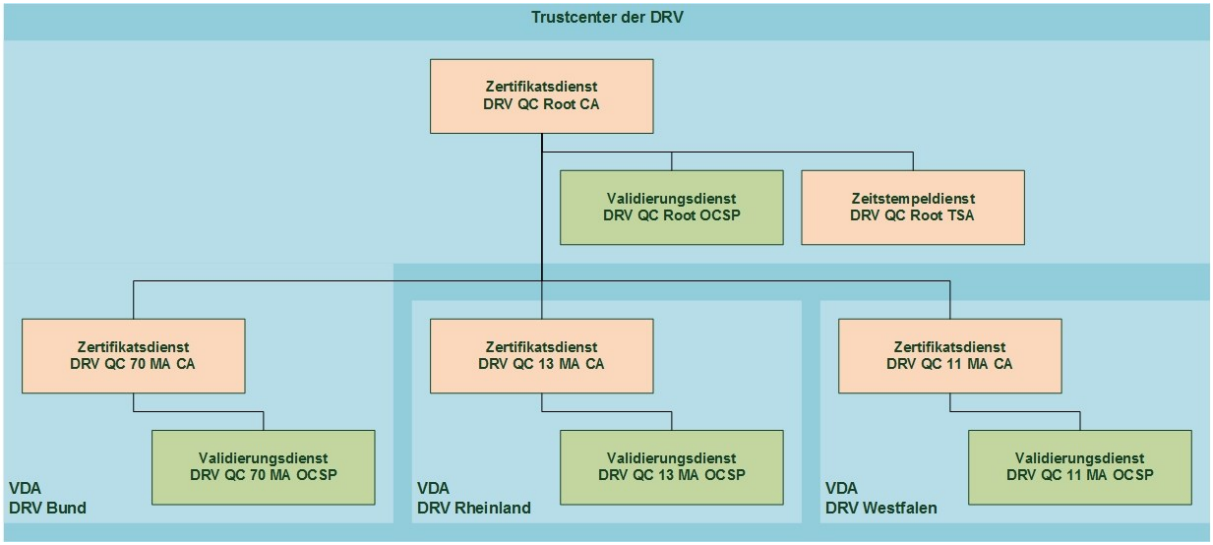

Abbildung 1 Qualifizierte Vertrauensdienste im Trustcenter der DRV

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 70 MA CA.

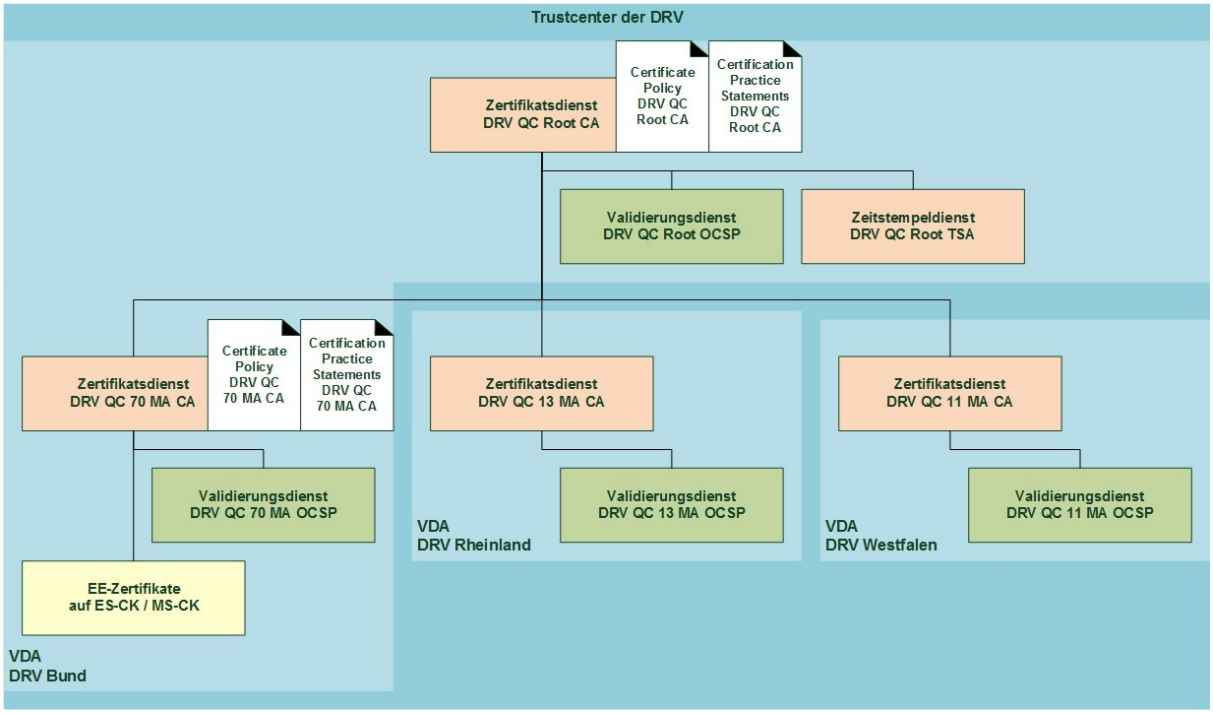

Abbildung 2 Richtlinien Dokumente des Zertifikatsdienstes DRV QC 70 MA CA

Dieses Dokument beinhaltet die Policy zur Erstellung qualifizierter EE-Zertifikate (Endbenutzerzertifikate) durch den Zertifikatsdienst DRV QC 70 MA CA des VDA DRV Bund.

Die qualifizierten EE-Zertifikate 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 70 MA CA

Dokument-OID: 1.3.6.1.4.1.22204.1.8.1.1.2

PEN-DRV-Bund (1.3.6.1.4.1.22204).Trustcenter (1). Policies (8). QC-CP (1). Produktivsystem (1). QC-Sub-CA (2)

Diese Policy des Zertifikatsdienstes DRV QC 70 MA 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 Zertifikatsdienst DRV QC 70 MA CA zur Ausstellung von qualifizierten EE-Zertifikaten für Mitarbeiter der DRV Bund auf Einzelsignaturchipkarten und für berechtigte Mitarbeiter aller RV-Träger auf Massensignaturchipkarten.

Der Zertifikatsdienst DRV QC 70 MA CA verwendet zur Erstellung qualifizierter Zertifikate ein zentrales Zertifikatsmanagementsystem.

Das Zertifikat des Zertifikatsdienstes DRV QC 70 MA CA wird vom Zertifikatsdienst DRV QC Root CA ausgestellt.

1.3.2 Registrierungsdienst

Die Registrierung erfolgt durch Rolleninhaber des VDA DRV Bund.

1.3.3 Zertifikatsinhaber (Subscriber)

Der Zertifikatsdienst DRV QC 70 MA CA erstellt Zertifikate für natürliche Personen als Zertifikatsinhaber:

(1) Mitarbeiter der DRV Bund für:
   - Qualifiziertes EE-Zertifikat auf einer Einzelsignaturchipkarte,

(2) Mitarbeiter von RV-Trägern inkl. der DRV Bund für:
   - Qualifiziertes EE-Zertifikat auf einer Massensignaturchipkarte,

(3) und die Systemverwalter Server des VDA DRV Bund für:
   - Qualifizierte OCSP-Zertifikate des Validierungsdienstes (OCSP-Responder) DRV QC 70 MA OCSP.

Zertifikatsinhaber für die OCSP-Zertifikate des Validierungsdienstes DRV QC 70 MA CA ist auf Grund vertraglicher Vereinbarungen der verantwortliche Systemverwalter Server des VDA DRV Bund. Die Erstellung und Verwaltung der OCSP-Zertifikate erfolgt gemäß Certificate Policy der DRV QC Root CA [9]. Die OCSP-Zertifikate werden in dieser Policy nicht betrachtet.

Die Anwendungen des VDA DRV Bund für Zertifikatsinhaber sind barrierefrei. Es gibt keine Einschränkungen für Anwender mit Behinderungen.

1.3.4 Vertrauende Parteien (Relying Parties)

Der Begriff vertrauende Parteien beinhaltet alle Benutzer, welche Zertifikate prüfen, die vom Zertifikatsdienst DRV QC 70 MA CA ausgestellt worden sind. Das beinhaltet u.a.:

- die Zertifikatsinhaber,
- Mitarbeiter von RV-Trägern, wenn Zertifikate in Geschäftsprozessen eingesetzt werden,
- Mitarbeiter nationaler und internationaler Behörden, wenn Zertifikate in Geschäftsprozessen eingesetzt werden.

1.3.5 Weitere Teilnehmer

Keine Angaben.

1.4 Anwendungsbereich

1.4.1 Geeignete Zertifikatsnutzung

Die vom Zertifikatsdienst DRV QC 70 MA CA ausgegebenen qualifizierten EE-Zertifikate werden von den Zertifikatsinhabern im Rahmen ihrer dienstlichen Tätigkeit verwendet.

Die Nutzung qualifizierter EE-Zertifikate für Massensignaturchipkarten wird weiter eingeschränkt. Eine entsprechende Beschränkung ist im Zertifikat in der Extension „Restriction“ enthalten.

Der private Schlüssel, der zum qualifizierten Zertifikat gehört, darf nur zur Erzeugung qualifizierter Signaturen verwendet werden.

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 dieses Dokumentes bestehen:

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

Das Dokument "Certificate Policy des Zertifikatsdienstes DRV QC 70 MA 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 des Zertifikatsdienstes im CPS Dokument 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. 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 ausgestellten qualifizierten Zertifikate auf Einzelsignaturchipkarten für Mitarbeiter der DRV Bund bzw. auf Massensignaturchipkarten für Mitarbeiter von RV-Trägern werden im Verzeichnisdienst des Trustcenters der DRV veröffentlicht und können von berechtigten Mitarbeitern DRV intern abgerufen werden. Ein öffentlicher Abruf ist nicht vorgesehen.

OCSP-Auskünfte werden für alle ausgestellten Zertifikate durch den Validierungsdienst DRV QC 70 MA OCSP erteilt.

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

2.1.1 Verzeichnisdienst

Im Verzeichnisdienst werden die vom Zertifikatsdienst DRV QC 70 MA CA ausgestellten qualifizierten Zertifikate veröffentlicht. Diese Zertifikate sind nur aus dem DRV-Netz nach vorheriger Authentisierung abrufbar.

Die öffentlich zugänglichen Informationen können vom Verzeichnisdienst über die Protokolle HTTP und LDAP anonym abgerufen werden. Die Adressen der LDAP- und HTTP-Dienste zum Download für 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 qualifizierten Zertifikate kann über den Validierungsdienst DRV QC 70 MA OCSP abgefragt werden. Der OCSP-Responder erteilt Vorhandenseins- und Sperrauskünfte. Die notwendigen Informationen für den Zugriff auf den Validierungsdienst sind in ausgestellten Zertifikaten in der Extension „AuthorityInfoAccess (AIA)“ enthalten.

Der Validierungsdienst DRV QC 70 MA OCSP gibt Auskunft über den Status von Zertifikaten, die vom Zertifikatsdienst DRV QC 70 MA 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 70 MA CA wird der Betrieb des Validierungsdienstes DRV QC 70 MA 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 (u.a. CA-Zertifikat des Zertifikatsdienstes DRV QC 70 MA CA) 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 [13].

2.2 Veröffentlichung von Informationen

Das vorliegende Dokument "Certificate Policy des Zertifikatsdienstes DRV QC 70 MA CA" wird auf der Web-Seite des VDA DRV Bund veröffentlicht [11].

Die Nutzungsbedingungen des Zertifikatsdienstes DRV QC 70 MA 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 70 MA CA

OID: 1.3.6.1.4.1.22204.1.8.6.1.2

Das Dokument "Certification Practice Statements des Zertifikatsdienstes DRV QC 70 MA CA" wird nicht veröffentlicht und kann bei begründetem Bedarf beim VDA DRV Bund über die Kontaktadresse (Siehe Kapitel 1.5.2) angefordert werden.

Im Fall der Einstellung des Betriebes werden die Sperrauskünfte für Zertifikate des Zertifikatsdienstes DRV QC 70 MA 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
Sperrliste des Zertifikatsdienstes DRV QC 70 MA CA	Einmalige Erstellung bei Einstellung des Zertifikatsdienstes	Nach Erstellung der Sperrliste	• Web-Seite des VDA DRV Bund
Qualifizierte EE-Zertifikate	Ausstellung nach Beantragung	Veröffentlichung nach Besitzüberprüfung	• Verzeichnisdienst • Validierungsdienst

2.4 Zugangskontrolle zu Verzeichnisdiensten

Die Zugangskontrolle zu den Veröffentlichungspunkten 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	Beschränkt auf berechtigte Benutzer	Authentisierung erforderlich
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 EE-Zertifikate behandelt.

3.1 Namen

3.1.1 Namensformen

Die vom Zertifikatsdienst DRV QC 70 MA CA ausgestellten qualifizierten EE-Zertifikate erhalten im Namen für die Zertifikatsinhaber (Subject-Name) u.a. folgende Attribute:

- Serial Number,
- Common Name,
- Organization,
- Country.

Die Subject-Namen für qualifizierte EE-Zertifikate, die vom Zertifikatsdienst DRV QC 70 MA CA ausgestellt werden, sind in der nächsten Tabelle zusammengefasst.

Tabelle 3: Subject-Namen der EE-Zertifikate des Zertifikatsdienstes DRV QC 70 MA CA

Zertifikatsinhaber	Name
Mitarbeiter der DRV Bund (ES-CK)	[T=<Titel>] SERIALNUMBER=<Personalnummer> SN=[<Namenszusatz>]<Name> G=<Vorname> CN=[<Namenszusatz>]<Name>, <Vorname>[, <Titel>] O=Deutsche Rentenversicherung Bund C=DE
Mitarbeiter der RV-Träger (MS-CK)	SERIALNUMBER=<Pseudo-Personalnummer> SN=Pseudonym CN=<Pseudonym> O=<Organisationsname> C=DE

Angaben in spitzen Klammern <…> sind Platzhalter.

Angaben in eckigen Klammern […] sind optionale Angaben.

Tabelle 4: Erläuterungen zu den Platzhaltern

Platzhalter	Erläuterung	Beispiel
<Titel>	Titel des Zertifikatsinhabers	Dr.
<Personalnummer>	Personalnummer des Zertifikatsinhabers	123456
<Namenszusatz>	Namenszusatz des Zertifikatsinhabers	von
<Name>	Name des Zertifikatsinhabers	Schmidt
<Vorname>	Vorname des Zertifikatsinhabers	Moritz
<Pseudo-Personalnummer>	Personalnummer für Zertifikate mit Pseudonym auf MS-CK	81234
<Pseudonym>	Pseudonym des Zertifikatsinhabers	Leiter Scanstelle 01:PN
<Organisation>	Organisation des Zertifikatsinhabers	Deutsche Rentenversicherung Bund

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 Signaturzertifikate für MS-CK werden auf Pseudonyme erstellt. Auf organisatorischem Weg wird die Zuordnung der Pseudonyme zu natürlichen Personen realisiert. Das Pseudonym wird im "Subject" wie folgt verwendet:

Tabelle 5: Pseudonyme in den qualifizierten Signaturzertifikaten für MS-CK

Zertifikatsinhaber	Name
Natürliche Person, welche innerhalb ihrer Funktion als Verfahrensverantwortlicher für den Einsatz der Massensignaturkarten vorgesehen ist	CN=<Selbst gewähltes Pseudonym>:PN

Das Pseudonym wird vom Verfahrensverantwortlichen vorgegeben. Bei der Registrierung wird geprüft, dass ein Pseudonym innerhalb einer Organisation eindeutig nur einer natürlichen Person zugeordnet wird.

3.1.4 Regeln zur Interpretation verschiedener Namensformen

Es gibt keine verschiedenen Namensformen.

3.1.5 Eindeutigkeit von Namen

Die Zertifikatsinhaber werden über ihren Namen und eine eindeutige Nummer benannt. Die Kombination aus Organisation und Personalnummer ist eindeutig. Die Personalnummer dient auch zur Unterscheidung von Zertifikatsinhabern bei Namensgleichheit. Die Personalnummer darf nur genau einer Person innerhalb einer Organisation zugeordnet sein.

- Die Personalnummer muss unverändert während des gesamten Beschäftigungsverhältnisses dem Mitarbeiter zugeordnet sein.
- Die Personalnummer darf weder während noch nach Ende dieses Beschäftigungsverhältnisses für einen anderen Zertifikatsempfänger wieder verwendet werden.
- Die Personalnummer ändert sich nicht, wenn die Person ihren Namen ändert.

Die Namen für Massensignaturchipkarten werden mit einer Pseudo-Personalnummer eindeutig gehalten (analog zu die Namen natürlicher Personen mit Personalnummer für persönliche Einzelsignaturchipkarten).

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

Private Schlüssel für Schlüsselinhaber werden in der sicheren Umgebung des Kartenlieferanten auf der qualifizierten Signaturerstellungseinheit generiert. Der Kartenlieferant bestätigt dies durch Erstellung von Prüfzertifikaten.

Der Nachweis des Besitzes des privaten Schlüssels für qualifizierte Zertifikate für ES-CK / MS-CK erfolgt durch Prüfung der Herkunft und der Signatur des Prüfzertifikates.

3.2.2 Identifizierung einer Organisation

Die Organisation natürlicher Personen wird über ihren Dienstausweis sicher identifiziert. Im Protokoll Kartenausgabe werden folgende Daten des Zertifikatsinhabers erfasst:

- Organisation, Personalnummer.

3.2.3 Identifizierung natürlicher Personen

Natürliche Personen werden über ein amtliches Ausweisdokument sicher identifiziert. Im Protokoll Kartenausgabe werden folgende Daten des Zertifikatsinhabers erfasst:

- Name, Vorname(n), Titel,
- Geburtsdatum, Geburtsort,
- 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 die unterschrieben Anträge. Die Prüfung der Berechtigung 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 Zertifikatserneuerung erfolgt analog zur initialen Zertifikatserstellung. Es wird eine neue Chipkarte erstellt.

3.3.2 Zertifikatserneuerung nach einer Sperrung

Die Zertifikatserneuerung erfolgt analog zur initialen Zertifikatserstellung. Es wird eine neue Chipkarte erstellt.

3.4 Identifizierung und Authentifizierung von Sperranträgen

Der Antrag auf Sperrung/Widerruf von EE-Zertifikaten kann ausschließlich von einem Sperrberechtigten gestellt werden. Für qualifizierte EE-Zertifikate sind folgende Personen sperrberechtigt:

- der Zertifikatsinhaber,
- Sperrbevollmächtigte der DRV Bund für Einzelsignaturchipkarten,
- Sperrbevollmächtigte der DRV für Massensignaturchipkarten,
- der Leiter des VDA DRV Bund,
- Mitarbeiter der Bundesnetzagentur.

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

Der Ablauf der Sperrung wird im Dokument Certification Practice Statements 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 EE-Zertifikaten 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 zugehörigen Chipkarte,
- Verdacht der unbefugten Nutzung des privaten Schlüssels,
- Zertifikat auf der ES-CK / MS-CK wird nicht mehr benötigt.
- bei notwendigen Änderungen in Zertifikatsinhalten,
    - ES-CK: Änderung von Angaben in einem ausgestellten qualifiziertem Zertifikat (z.B. Namensänderung durch Heirat),
    - MS-CK: Änderung von wesentlichen Angaben im Zertifikat, z.B. die Nutzungsbeschränkung,
- ein ausgestelltes Zertifikat enthält unrichtige Angaben;
- der VDA Deutsche Rentenversicherung Bund stellt seine Tätigkeit ein und der CA Dienst soll nicht durch einen anderen VDA fortgesetzt werden,
- Chipkarten und/oder Zertifikate dürfen nicht weiter für die qualifizierte elektronische Signatur verwendet werden, weil die zur Zertifikats-Signatur verwendeten Algorithmen nicht mehr als geeignet gelten oder weil die Bestätigung der Signaturerstellungseinheit mit dem zugrundeliegenden Signaturschlüssel abläuft,
- Unregelmäßigkeiten in den Prozessen Registrierung, Personalisierung, Kartenausgabe, PIN-Vergabe bzw. Besitzüberprüfung,
- Kompromittierung des Schlüssels der ausstellenden CA.

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 70 MA CA sind:

- Mitarbeiter der DRV Bund für qualifizierte Zertifikate auf Einzelsignaturchipkarten,
- Mitarbeiter von RV-Trägern für qualifiziertes Zertifikat auf Massensignaturchipkarten.

Über die Einstellung des Betriebes des qualifizierten Zertifikatsdienstes DRV QC 70 MA CA entscheidet der Leiter des VDA DRV Bund in Abstimmung mit der Geschäftsleitung der DRV Bund.

Bei der Einstellung des qualifizierten Zertifikatsdienstes DRV QC 70 MA 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 70 MA 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 70 MA 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 Mitarbeiter der DRV Bund werden über das Intranet der DRV Bund über die geplante Einstellung des Betriebes informiert.

  Mitarbeiter anderer RV-Träger, die Inhaber von MS-CK sind, werden vom VDA DRV Bund schriftlich über die Einstellung des Betriebes informiert.

  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 werden alle privaten Schlüssel des Zertifikatsdienstes zerstört. Es ist dadurch nicht möglich, weiterhin Zertifikate zu erstellen.

Die Prozeduren zur Einstellung des Betriebes des qualifizierten Zertifikatsdienstes DRV QC 70 MA CA sind im Beendigungsplan [10] 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 EE-Zertifikate gemäß RFC 5280 [3].

7.1.1 Versionsnummer

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

7.1.2 Zertifikatserweiterungen

Die qualifizierten EE-Zertifikate des VDA DRV Bund beinhalten Zertifikatserweiterungen gemäß RFC 5280 [3]. Folgende Zertifikatserweiterungen sollen verwendet werden:

Tabelle 6: Zertifikatserweiterungen für qualifizierte Zertifikate

Erweiterung	Erläuterung	Verwendung für	
		Signatur-zertifikat ES-CK	Signatur-zertifikat MS-CK
Authority Key Identifier	Hashwert des öffentlichen Schlüssels des Herausgebers	x	x
Certificate Policies	OID & URL der Policy der DRV OID & URL der Policy QCP-N-QSCD	x	x
Authority Info Access	URL des OCSP-Responder für Zertifikatsstatusprüfung	x	x
Issuer Alt Names	URL(s) zum Abruf des Issuer Zertifikates	x	x
QC Statements	Attribute QcsCompliance und QcsQcSSCD gemäß [8]	x	x
Restriction	Nutzungsbeschränkung des privaten Schlüssels	x	x
Key Usage; kritisch	Verwendungszweck des Schlüssels	nonRepudiation	nonRepudiation
Basic Constraints; kritisch	Einschränkungen des Zertifikates (EE-Zertifikat)	x	x

7.1.3 Algorithmus Bezeichner (OID)

Der Zertifikatsdienst DRV QC 70 MA CA erstellt qualifizierte EE-Zertifikate mit dem Signaturalgorithmus sha256withRSAEncryption.

Alternativ kann der Signaturalgorithmus RSASSA-PSS genutzt werden.

Es sind die Vorgaben des nationalen Algorithmen-Katalogs [12] zu beachten.

Tabelle 7: 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

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 70 MA CA erstellt qualifizierte EE-Zertifikate gemäß den folgenden Policies.

Tabelle 8: Policies für qualifizierte Zertifikate

Policy	Erläuterung	OID
CP DRV	Policy des Zertifikatsdienstes DRV QC 70 MA CA	1.3.6.1.4.1.22204.1.8.1.1.2
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 (PolicyConstraints)

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

7.1.8 Syntax und Semantik von Policy Qualifiern

Der Zertifikatsdienst DRV QC 70 MA CA erstellt qualifizierte EE-Zertifikate mit den folgenden Policy Qualifier.

Tabelle 9: 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 70 MA CA.

Im Fall der Betriebseinstellung erstellt der VDA DRV Bund für den Zertifikatsdienst DRV QC 70 MA 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 70 MA CA.

Im Fall der Betriebseinstellung erstellt der VDA DRV Bund für den Zertifikatsdienst DRV QC 70 MA CA eine Sperrliste. Die Sperrliste hat eine Laufzeit von 30 Jahren und beinhaltet Sperrinformationen zu allen gesperrten Zertifikaten des Zertifikatsdienstes DRV QC 70 MA CA. Folgende Erweiterungen gemäß RFC 5280 sollen verwendet werden:

Tabelle 10: 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 70 MA CA, welcher das OCSP-Zertifikat signiert hat.

Tabelle 11: 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 [1]

[1] 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 vollständigen 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 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 des Zertifikatsdienstes DRV QC 70 MA CA zur Erstellung qualifizierter EE-Zertifikate.

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 [14].

9 Weitere geschäftliche und rechtliche Angelegenheiten

9.1 Gebühren

9.1.1 Gebühren für Zertifikatserstellung oder -erneuerung

Keine Angaben.

9.1.2 Gebühren für Zugriff auf Zertifikate

Keine Angaben.

9.1.3 Gebühren für Sperrung oder Statusanfragen

Keine Angaben.

9.1.4 Andere Gebühren

Keine Angaben.

9.1.5 Gebührenerstattung

Keine Angaben.

9.2 Finanzielle Verantwortung

9.2.1 Deckungsvorsorge

Der VDA DRV Bund verfügt über die notwendige Deckungsvorsorge gemäß Artikel 24 eIDAS-VO [1] für den Zertifikatsdienst DRV QC 70 MA CA für Schäden gemäß Artikel 13 eIDAS-VO.

9.2.2 Weitere Vermögenswerte

Die Systeme des Zertifikatsdienstes DRV QC 70 MA CA werden durch die DRV 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 70 MA 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 EE-Zertifikate 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 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 qualifizierte Zertifikate für ES-CK explizit beantragen. Durch den Antrag stimmen sie der Nutzung der bereits erfassten personenbezogenen Daten zu.

Die Zertifikatsinhaber müssen qualifizierte Zertifikate für MS-CK explizit beantragen. Durch den Antrag stimmen sie der Erfassung und Nutzung personenbezogener Daten zu.

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 Qualitätssicherungssystem benutzt werden. Testzertifikate zeigen im Namen an, dass sie für Testzwecke genutzt werden.

Bevor der VDA qualifizierte EE-Zertifikate an Zertifikatsinhaber ausgibt, muss er den Zertifikatsinhaber über die zugelassene Nutzung der qualifizierten Zertifikate informieren. Der Informationspflicht wird entsprochen durch:

- Veröffentlichung der Nutzungsbedingungen in Form eines "PKI Disclosure Statements" auf der Web-Seite des VDA DRV Bund [11],
- Veröffentlichung dieser Richtlinie auf der Web-Seite des VDA DRV Bund [11],
- Information des Zertifikatsinhabers bzgl. zugelassener Nutzung der Signaturchipkarte und Geheimhaltung der Aktivierungsdaten in einem Merkblatt als Anlage zum Zertifikatsantrag.

Vor der Freischaltung der qualifizierten EE-Zertifikate (Veröffentlichung in den Validierungsdienst) prüft der VDA DRV Bund, dass die Angaben im ausgestellten qualifizierten Zertifikat zum Zertifikatsinhaber gehören. Dazu werden die Angaben im qualifizierten Zertifikat verglichen:

- bei ES-CK: gegen die Angaben im Personaldokument und im Dienstausweis des Zertifikatsinhabers,
- bei MS-CK: gegen die Angaben im Zertifikatsantrag.

9.6.2 Pflichten des VDA bei der Registrierung

Die Tätigkeiten der Registrierung werden von Rolleninhabern des VDA DRV Bund ausgeführt. Die Registrierungsdaten werden korrekt und vollständig aus dem Personalverwaltungssystem (ES-CK) bzw. aus dem Antrag (MS-CK) übernommen und im Registrierungsprozess zur Verfügung gestellt. Eine Änderung der Daten ist nicht zulässig.

9.6.3 Pflichten des Zertifikatsinhabers

Die Zertifikatsinhaber sind verpflichtet, die Einzel- bzw. Massensignaturchipkarten ausschließlich im Rahmen ihrer Nutzungsbeschränkungen zu verwenden. Die Pflichten der Zertifikatsinhaber richten sich nach den Bestimmungen der entsprechenden ETSI-Normen [5], [6] und [7] sowie der Geschäftsordnung der DRV Bund bzw. der jeweiligen RV-Träger.

Die Zertifikatsinhaber werden in einem Merkblatt als Anlage zum Zertifikatsantrag über ihre Rechte und Pflichten informiert.

Für Einzelsignaturkarten gilt:

- Ein besonderes Vertragsverhältnis zwischen Mitarbeiter der DRV Bund und dem VDA DRV Bund besteht nicht.

Für Massensignaturkarten gilt:

- Das Vertragsverhältnis zwischen dem jeweiligen RV-Träger und dem VDA DRV Bund ergibt sich aus der gesetzlichen Regelung §138 Absatz 1 Ziffer 1 SGB VI. Danach übernimmt die DRV Bund Grundsatz- und Querschnittsaufgaben für die gesamte deutsche Rentenversicherung. Dazu zählt u.a. die Bereitstellung von Zertifikatsdiensten. Ein besonderes Vertragsverhältnis zwischen Mitarbeiter des RV-Trägers und dem VDA DRV Bund besteht nicht.
- Bei MS-CK besteht außerdem die Pflicht zur Beachtung der Anforderungen an die Einsatzumgebung, welche sich aus der Bestätigungsurkunde der QSCD ergibt. Die Bestätigungsurkunde ist zu finden unter [15].

Der Zertifikatsinhaber muss die Sperrung seines qualifizierten Signaturzertifikates veranlassen, wenn:

- der Zertifikatsinhaber die Organisation verlässt,
- bei Verlust, Defekt oder Diebstahl der entsprechenden ES-CK / MS-CK,
- Verdacht der unbefugten Nutzung des privaten Schlüssels,
- Zertifikat auf der ES-CK / MS-CK wird nicht mehr benötigt.
- bei notwendigen Änderungen in Zertifikatsinhalten:
  - bei ES-CK: Änderung von Angaben in einem ausgestellten qualifiziertem Zertifikat (z.B. Namensänderung durch Heirat),
  - bei MS-CK: sich wesentliche Angaben im Zertifikat ändern, z.B. die Nutzungsbeschränkung.

9.6.4 Pflichten der Zertifikatsprüfer (Relying Parties)

Zertifikatsprüfer müssen den Sperrstatus der qualifizierten EE-Zertifikate des Zertifikatsdienstes DRV QC 70 MA CA mit Hilfe des Validierungsdienstes (OCSP-Responder) prüfen. Im Falle der Einstellung des Betriebes des Zertifikatsdienstes DRV QC 70 MA CA wird der Betrieb des Validierungsdienstes DRV QC 70 MA 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 im Zertifikat in der Extension "Restriction" (Siehe Kapitel 7.1) sowie 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 gesetzlichen Vorgaben gemäß 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 70 MA 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 Kommunikation mit Zertifikatsinhabern ist nicht vorgesehen.

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 70 MA CA, 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 DRV 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 70 MA CA arbeitet als qualifizierter Vertrauensdienst zur Erstellung qualifizierter EE-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 schließt mit den weiteren Mandanten im Trustcenter der DRV eine Verwaltungsvereinbarung ab, die 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
04.00.00	08.02.2011			DRV Bund
05.00.00	---	---	Aus formalen Gründen übersprungen	---
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] Certificate Policy des qualifizierten Zertifikatsdienstes DRV QC Root CA

[10] Beendigungsplan des Trustcenters der Deutschen Rentenversicherung

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

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

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

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

[15] Bestätigungsurkunde "Digitale Signatur: Sichere Signaturerstellungseinheiten CardOS V5.0 with Application for QES, V1.0", veröffentlicht durch die BNetzA; https://www.bundesnetzagentur.de/SharedDocs/QESProdukte/Signaturkarten/CardOS%20V5.0.html?nn=322598