Trustcenter der Deutschen Rentenversicherung

Vertrauensdiensteanbieter Deutsche Rentenversicherung Bund nach eIDAS-VO

PKI Disclosure Statements des Zertifikatsdienstes DRV QC Root CA

Dokument-OID: 1.3.6.1.4.1.22204.1.8.6.1.1

Version	01.04.00
Stand	08.06.18
Dokument	TCDRV_PDS_DRV-QC-Root-CA_DE
Status	Freigegeben
Vertraulichkeit	Keine Beschränkungen

1 PKI Disclosure Statements

1.1 Geltungsbereich

Dieses Dokument beinhaltet die PKI Disclosure Statements zur Erstellung qualifizierter Systemzertifikate (CA-, TSA- und OCSP-Zertifikate) durch den Zertifikatsdienst DRV QC Root CA des VDA DRV Bund sowie qualifizierter Systemzertifikate (OCSP-Zertifikate) durch die qualifizierten Zertifikatsdienste der Mandanten DRV Bund, DRV Rheinland und DRV Westfalen.

Jeder Mandant ist ein eigenständiger Vertrauensdiensteanbieter (VDA) gemäß eIDAS-VO. Der VDA DRV Bund ist Betreiber der zentralen Dienste im Trustcenter der DRV für alle drei Mandaten. Der VDA DRV Bund hat mit den Mandanten bezüglich des Betriebs der zentralen Dienste entsprechende Verwaltungsvereinbarungen für alle rechtlichen Sachverhalte geschlossen.

Die qualifizierten Systemzertifikate werden für natürliche Personen auf qualifizierten elektronischen Signaturerstellungseinheiten gemäß Policy QCP-N-QSCD (siehe [2]) ausgestellt.

1.2 Dokumentname

Dokumentname: PKI Disclosure Statements des Zertifikatsdienstes DRV QC Root CA

Dokument-OID: 1.3.6.1.4.1.22204.1.8.6.1.1

PEN-DRV-Bund (1.3.6.1.4.1.22204).Trustcenter (1). Policies (8). QC-DS (6). Produktivsystem (1). QC-Root-CA (1)

Dieses Dokument PKI Disclosure Statements ist ein Auszug aus der Certificate Policy:

- Certificate Policy des Zertifikatsdienstes DRV QC Root CA
  Dokument-OID: 1.3.6.1.4.1.22204.1.8.1.1.1

1.3 Kontaktadressen

Der folgende Ansprechweg besteht hinsichtlich dieser Richtlinie:

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

Weitere Informationen können von der angegebenen Web-Seite geladen werden:

Web-Adresse VDA DRV Bund [4]: Bereitstellung folgender Informationen zum Download:

- PKI Disclosure Statements DRV QC Root CA
- Certificate Policy DRV QC Root CA
- Zertifikate der DRV QC Root CA

1.4 Nutzer des Zertifikatsdienstes

Der Zertifikatsinhaber für qualifizierte CA-Zertifikate aller qualifizierten Zertifikatsdienste ist der Leiter des VDA DRV Bund.

Der Zertifikatsinhaber für alle in Kapitel 1.1 genannten qualifizierten TSA- und OCSP-Zertifikate ist der zuständige Systemverwalter Server des VDA DRV Bund.

1.5 Ausgestellte Zertifikate

Der qualifizierte Zertifikatsdienst DRV QC Root CA des VDA DRV Bund stellt folgende Systemzertifikate aus:

- Ausstellerzertifikat für den Zertifikatsdienst DRV QC Root CA,
- Ausstellerzertifikate für die qualifizierten Zertifikatsdienste der Mandanten (DRV QC 70 MA CA, DRV QC 13 MA CA und DRV QC 11 MA CA),
- Zertifikate für den Validierungsdienst DRV QC Root OCSP,
- Zertifikate für den Zeitstempeldienst DRV QC Root TSA.

Die qualifizierten Zertifikatsdienste der Mandanten stellen folgende Systemzertifikate aus:

- Zertifikate für ihren Validierungsdienst (DRV QC 70 MA OCSP, DRV QC 13 MA OCSP bzw. DRV QC 11 MA OCSP).

Für die qualifizierten Systemzertifikate sind folgende Anwendungsfälle vorgesehen:

- Auf Basis der CA-Zertifikate werden qualifizierte Zertifikate signiert.
- Auf Basis der OCSP-Zertifikate werden die OCSP-Auskünfte zum Status der vom jeweiligen Zertifikatsdienst ausgegebenen Zertifikate signiert.
- Auf Basis der TSA-Zertifikate werden qualifizierte Zeitstempel signiert.

Weitere Anwendungsfälle sind nicht vorgesehen.

Der Validierungsdienst DRV QC Root OCSP (OCSP-Responder) erteilt Auskunft über den Status der vom Zertifikatsdienst DRV QC Root CA ausgestellten qualifizierten Zertifikate.

Die Auskunft über den Sperrstatus wird über die Laufzeit des entsprechenden Zertifikates hinaus für 30 Jahre erteilt.

Im Fall der Einstellung des Betriebes des Zertifikatsdienstes DRV QC Root CA werden die Zertifikate des Zertifikatsdienstes, die von diesem Dienst ausgestellten Zertifikate, die komplette Sperrliste dieses Dienstes sowie mit dem OCSP-Responder des Trustcenters der DRV generierte OCSP-Responses an die BNetzA übergeben. Die BNetzA veröffentlicht die CA-Zertifikate und die Sperrliste auf ihrer Web-Seite. Die generierten OCSP-Responses können von der BNetzA für OCSP-Auskünfte benutzt werden.

1.6 Vertrauenswürdigkeit der ausgestellten Zertifikate

Die zu den qualifizierten Zertifikaten gehörenden Schlüssel werden auf Systemchipkarten generiert und genutzt. Diese Systemchipkarten sind nach Common Criteria Prüfstärke EAL4+ geprüft. Sie sind beim BSI als qualifizierte elektronische Signaturerstellungseinheiten gelistet.

Daten über ausgestellte Zertifikate werden bis 30 Jahre nach Ablauf der Zertifikate archiviert. Unter Beachtung der genutzten Zertifikatslaufzeiten ergibt sich eine Aufbewahrungsfrist von insgesamt 35 Jahren.

Bei Einstellung des Betriebes werden die archivierten Daten an die BnetzA übergeben. An der Aufbewahrungsfrist ändert sich dadurch nichts.

1.7 Pflichten der Zertifikatsinhaber

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 im CP genannt.

1.8 Pflichten der Zertifikatsprüfer

Zertifikatsprüfer müssen den Sperrstatus der qualifizierten CA- und TSA-Zertifikate im Trustcenter der DRV mit Hilfe der Validierungsdienste (OCSP-Responder) prüfen. Ungültige Zertifikate dürfen nicht verwendet werden.

Die URLs zum Download der Ausstellerzertifikate und zum Zugriff auf den Validierungsdienst (OCSP-Responder) sind in den qualifizierten Systemzertifikaten enthalten.

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 [3] Kapitel 7.1).

Zertifikatsprüfer müssen Beschränkungen für den Einsatz der Zertifikate beachten. Die Beschränkungen sind in der entsprechenden Certificate Policy definiert (siehe [3] Kapitel 1.4).

Die Certificate Policy [3] kann von der Web-Seite des VDA DRV Bund [4] geladen werden.

Zertifikatsprüfer sollen bei Verdacht auf oder festgestelltem Missbrauch von Zertifikaten den Vertrauensdiensteanbieter darüber informieren. Dafür ist die Kontaktadresse in Kapitel 1.3 zu verwenden.

Sofern Anwender nach der Einstellung des Betriebes qualifizierte elektronische Signaturen prüfen, die vor der Einstellung des Betriebes erstellt wurden, sollen sie den Status der entsprechenden Zertifikate zum Zeitpunkt der Signaturerstellung prüfen. Sie nutzen dazu die von der BnetzA veröffentlichten Sperrinformationen.

1.9 Haftung des Vertrauensdiensteanbieters

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

1.10 Richtlinien für den Zertifikatsdienst

Die Vorgaben zur Erstellung von qualifizierten Systemzertifikaten sind definiert in den Richtlinien Dokumenten:

Dokument	Klassifikation	Bezug
Certificate Policy des Zertifikats-dienstes DRV QC Root CA	Keine Einschränkungen	Web-Seite des VDA DRV Bund (Siehe Kap. 1.2)
Certification Practice Statements des Zertifikatsdienstes DRV QC Root CA	Nur für den Dienstgebrauch	Schriftlicher Antrag über die Postadresse (Siehe Kap. 1.2)

Im Fall der Einstellung des Betriebes des Zertifikatsdienstes DRV QC Root CA werden die Richtlinien an die BnetzA übergeben und können dort bei berechtigtem Interesse eingesehen werden.

1.11 Datenschutz

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.

1.12 Kosten und Rückvergütungen

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

1.13 Geltendes Recht und Konfliktbeilegung

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

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
1178-81 Trustcenter / Schiedsstelle
D-10704 Berlin

1.14 Konformitätserklärung

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 [2].

Die letzte Prüfung erfolgte in Q1 2017 durch die Konformitätsbewertungsstelle TÜV-IT GmbH. Das Zertifikat der Konformitätsbewertung wird durch die Konformitätsbewertungs-stelle veröffentlicht [5].

2 Verzeichnisse

2.1 Abkürzungen

BDSG	Bundesdatenschutzgesetz
CA	Zertifikatsdienst (Certification Authority)
CC	Common Criteria
CP	Certificate Policy
CPS	Certification Practice Statements
DRV	Deutsche Rentenversicherung
EAL	Prüfstärke (Evaluation Assurance Level)
ETSI	European Telecommunications Standard Institute
IT	Informationstechnik
MA	Mitarbeiter
OCSP	Online Certificate Status Protocol
OID	Object Identifier
PEN	Private Enterprise Number
PKI	Public Key Infrastructure
QC	Qualifiziert
TSA	Zeitstempeldienst (Time Stamp Authority)
URL	Unified Ressource Locator
VA	Validierungsdienst (Validation Authority)
VDA	Vertrauensdiensteanbieter
VDG	Vertrauensdienstegesetz
VO	Verordnung

2.2 Änderungsverzeichnis

Version	Datum	Kap.	Änderungsgrund	Bearbeiter
01.00.00	21.04.2017	Alle	Erstellung	Atos
01.01.00	10.05.2017	1.4, 1.5, 1.8	Anpassung	Atos
01.02.00	01.07.2017	1.13	Änderung Postadresse der Schiedsstelle	Atos
01.03.00	09.04.2018	1.6, 1.8, 1.10	Anpassung für Einstellung des Betriebes	Atos
01.04.00	08.06.2018	1.5	Freigabe	Atos

2.3 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] 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 http://www.etsi.org/deliver/etsi_en/319400_319499/31941102/

[3] Certificate Policy des Zertifikatsdienstes DRV QC Root CA

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

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

[6] Vertrauensdienstegesetz (VDG): Gesetz zur Durchführung der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates vom 23.07.2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG (eIDAS-Durchführungsgesetz, verabschiedet am 18.07.2017