Trustcenter der Deutschen Rentenversicherung

Vertrauensdiensteanbieter Deutsche Rentenversicherung Bund

PKI Disclosure Statements des Zertifikatsdienstes DRV RT CA

Dokument-OID: 1.3.6.1.4.1.22204.1.8.7.1.9

Version	02.00.00
Stand	24.09.24
Dokument	TCDRV_PDS_DRV-RT-CA_DE
Status	Freigegeben
Vertraulichkeit	Keine Beschränkungen

1 PKI Disclosure Statements

1.1 Geltungsbereich

Dieses Dokument beinhaltet die PKI Disclosure Statements zur Erstellung von Zertifikaten für Endbenutzer durch den Zertifikatsdienst DRV RT CA des Vertrauensdiensteanbieters Deutsche Rentenversicherung Bund.

Die Endbenutzer-Zertifikate werden für Städte, Gemeinden, Behörden und weitere Institutionen (u.a. Handwerkskammern, Sozialversicherungen, internationale Rentenversicherungsträger) zur Anmeldung an Verfahren der Deutschen Rentenversicherung ausgestellt.

1.2 Dokumentname

Dokumentname:	PKI Disclosure Statements des Zertifikatsdienstes DRV RT CA
Dokument-OID:	1.3.6.1.4.1.22204.1.8.7.1.9 PEN-DRV-Bund (1.3.6.1.4.1.22204). Trustcenter (1). Policy (8). PDS (7). Produktivsystem (1). RT-CA (9)

1.3 Kontaktadressen

Kontakt zum Trustcenter des Vertrauensdiensteanbieters Deutsche Rentenversicherung Bund:

Der folgende Ansprechweg zum Trustcenter besteht hinsichtlich dieser Richtlinie:

E-Mail:	Trustcenter-gRV@drv-bund.de
Postadresse:	Deutsche Rentenversicherung Bund Trustcenter der Deutschen Rentenversicherung 10704 Berlin

Weitere Informationen können von der Web-Seite des Trustcenters der Deutschen Rentenversicherung Bund geladen werden:

Web-Adresse VDA DRV Bund [2]:	Bereitstellung folgender Informationen zum Download: • Informationen für Zertifikatsinhaber (PKI Disclosure Statements) • Zertifikate der DRV Root CA

Kontakt zur Registrierungsstelle für Client Zertifikate zur Anmeldung an Verfahren der Deutschen Rentenversicherung:

E-Mail:	drvlogin@deutsche-rentenversicherung.de
Postadresse:	Deutsche Rentenversicherung Bund Auskunfts- und Zugangsstelle Berner Str. 1 97084 Würzburg

1.4 Nutzer des Zertifikatsdienstes

Zertifikatsinhaber für die Endbenutzer-Zertifikate des Zertifikatsdienstes DRV RT CA sind die registrierten Städte, Gemeinden, Behören und weitere Institutionen (u.a. Handwerkskammern, Sozialversicherungen, internationale Rentenversicherungsträger), welche Verfahren der Deutschen Rentenversicherung nutzen.

1.5 Ausgestellte Zertifikate

Der Zertifikatsdienst DRV RT CA stellt folgende Endbenutzer-Zertifikate aus:

- Client-Zertifikate für Städte, Gemeinden, Behören und weitere Institutionen (u.a. Handwerkskammern, Sozialversicherungen, internationale Rentenversicherungsträger) zur Anmeldung an Verfahren der Deutschen Rentenversicherung.

Die vom Zertifikatsdienst DRV RT CA ausgegebenen Client-Zertifikate werden zur Anmeldung an Verfahren der Deutschen Rentenversicherung verwendet. Weitere Anwendungsfälle sind nicht vorgesehen.

Die Auskunft über den Sperrstatus, der von der DRV RT CA ausgestellten Zertifikate, wird über die Laufzeit des ausgestellten Zertifikates erteilt.

Im Fall der Einstellung des Betriebes des Zertifikatsdienstes DRV RT CA werden das CA-Zertifikat des Zertifikatsdienstes sowie alle von diesem Dienst ausgestellten Zertifikate gesperrt. Die finale Sperrliste des Zertifikatsdienstes wird auf geeignete Weise veröffentlicht.

1.6 Vertrauenswürdigkeit der ausgestellten Zertifikate

Die Registrierung der Städte, Gemeinden, Behörden und weiterer Institutionen (u.a. Handwerkskammern, Sozialversicherungen, internationale Rentenversicherungsträger),erfolgt durch die Registrierungsstelle Abteilung GQ 0500. Die Prozeduren und Sicherheitsmaßnahmen zur Registrierung sind in [3] festgelegt.

Nach erfolgreicher Registrierung beantragt die Registrierungsstelle Abteilung GQ 0500 im Auftrag der Zertifikatsinhaber kryptografische Schlüssel und Zertifikate im Format PKCS#12 beim Trustcenter der DRV. Die PKCS#12-Token und das zugehörige Passwort wird von der Registrierungsstelle an die Zertifikatsinhaber auf sicherem Weg übergeben (Siehe [3]).

Die PKCS#12-Token sollen unter der Kontrolle der Zertifikatsinhaber genutzt werden. Ein Zugriff auf den privaten Schlüssel soll auf geeignete Weise eingeschränkt werden.

Die Daten für die Zertifikatserstellung und ggf. für die Zertifikatssperrung werden im Zertifikatsmanagementsystem des Trustcenters gespeichert und archiviert. Der Aufbewahrungszeitraum wird vom Trustcenter der Deutschen Rentenversicherung geregelt.

Bei Einstellung des Betriebes verbleiben die archivierten Daten bei der Deutschen Rentenversicherung Bund. An der Aufbewahrungsfrist ändert sich dadurch nichts.

1.7 Pflichten der Zertifikatsinhaber

Die Zertifikatsinhaber sind verpflichtet, die Client-Zertifikate ausschließlich im Rahmen der vorgesehen Nutzung zu verwenden. Zertifikatsinhaber sind verpflichtet, sich an ihre Registrierungsstelle zu wenden, wenn folgende Bedingungen vorliegen:

- bei Verlust oder Diebstahl der kryptografischen Client-Schlüssel,
- Verdacht der unbefugten Nutzung des privaten Client-Schlüssels,
- Client-Zertifikat wird nicht mehr benötigt,
- ein ausgestelltes Client-Zertifikat enthält unrichtige Angaben.

Die Registrierungsstelle soll in diesen Fällen das Client-Zertifikat sperren und ggf. ein neues Client-Zertifikat beantragen.

Kontakt zur Registrierungsstelle siehe Kap. 1.3.

1.8 Pflichten der Zertifikatsprüfer

Zertifikatsprüfer müssen vor Verwendung des Client-Zertifikates den Sperrstatus des Client-Zertifikates mit Hilfe der bereitgestellten Sperrliste prüfen. Ungültige Zertifikate dürfen nicht verwendet werden.

Die URLs zum Download der Sperrliste sind in den ausgestellten Client-Zertifikaten in der Extension „CRL Distribution Points“ enthalten.

Zertifikatsprüfer müssen die Beschränkungen für den Einsatz der kryptografischen Schlüssel beachten. Die Beschränkungen sind im Client-Zertifikat in den Extensions „Key Usage“ und „Extended Key Usage“ festgelegt.

Zertifikatsprüfer müssen Beschränkungen für den Einsatz der Zertifikate beachten. Die Beschränkungen sind im Client-Zertifikat in der Extension „Restriction“ festgelegt.

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

1.9 Haftung des Vertrauensdiensteanbieters

Der Vertrauensdiensteanbieter Deutsche Rentenversicherung Bund haftet für die Durchführung der Prozesse Zertifikatsausstellung und Zertifikatssperrung. Für die Registrierung der Zertifikatsinhaber der Städte, Gemeinden, Behören und weiterer Institutionen (u.a. Handwerkskammern, Sozialversicherungen, internationale Rentenversicherungsträger) sowie die Korrektheit der Angaben im Zertifikat ist die Registrierungsstelle Abteilung GQ 0500 zuständig (Siehe [3]).

1.10 Richtlinien für den Zertifikatsdienst

Die Vorgaben zur Erstellung von Client-Zertifikaten für Städte, Gemeinden, Behören und weiterer Institutionen (u.a. Handwerkskammern, Sozialversicherungen, internationale Rentenversicherungsträger) zur Anmeldung an Verfahren der Deutschen Rentenversicherung sind definiert in folgenden Dokumenten:

Dokument	Klassifikation	Bezug
Zertifikatsprofile der DRV RT CA	Nur für den Dienstgebrauch	Schriftlicher Antrag über die Postadresse des Trustcenters (Siehe Kap. 1.3)

1.11 Datenschutz

Der Vertrauensdiensteanbieter Deutsche Rentenversicherung Bund hält die gesetzlichen Bestimmungen zum Schutz der erhobenen personenbezogenen Daten ein (BDSG).

Der Umfang der zu erhebenden Daten soll auf notwendige Daten beschränkt bleiben. In den Antragsdaten sowie in den Client-Zertifikaten sollen keine personenbezogenen Daten enthalten sein.

Die Registrierungsstelle Abteilung GQ 0500 soll ebenfalls nur notwendige personenbezogene Daten erheben, speichern und nutzen. Die Zertifikatsinhaber sollen über die Erhebung, Speicherung und Nutzung der Daten informiert werden. Die Zertifikatsinhaber sollen vor Beantragung eines Client-Zertifikates diesen Bedingungen zustimmen.

1.12 Kosten und Rückvergütungen

Keine Angaben.

1.13 Geltendes Recht und Konfliktbeilegung

Es gilt grundsätzlich deutsches Recht.

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

Die Schiedsstelle ist erreichbar unter der folgenden Kontaktadresse:

E-Mail: Trustcenter-gRV@drv-bund.de

Postadresse: Deutsche Rentenversicherung Bund
Trustcenter der Deutschen Rentenversicherung
10704 Berlin

1.14 Konformitätserklärung

Der Zertifikatsdienst DRV RT CA arbeitet als Vertrauensdienst zur Erstellung elektronischer Zertifikate in Anlehnung an die relevanten ETSI-Normen [1]. Die Prüfung erfolgt intern durch die Leitung des Trustcenters der Deutschen Rentenversicherung sowie durch die Abt. Revision der Deutschen Rentenversicherung Bund.

Die Registrierungsstelle Abteilung GQ 0500 arbeitet gemäß [3]. Die Prüfung der Registrierungsstelle GQ 0500 erfolgt durch die Abt. Revision der Deutschen Rentenversicherung Bund.

2 Verzeichnisse

2.1 Abkürzungen

BDSG	Bundesdatenschutzgesetz
CA	Zertifikatsdienst (Certification Authority)
DRV	Deutsche Rentenversicherung
ETSI	European Telecommunications Standard Institute
OID	Object Identifier
PEN	Private Enterprise Number
PKI	Public Key Infrastructure
URL	Unified Ressource Locator
VDA	Vertrauensdiensteanbieter

2.2 Änderungsverzeichnis

Version	Datum	Kap.	Änderungsgrund	Bearbeiter
01.00.00	30.11.2022	Alle	Freigabe	DRV Bund
02.00.00	24.09.2024	Alle	Abschnitt 2.3 aktualisiert; Erneute Freigabe nach Gesamtprüfung	DRV Bund

2.3 Referenzen

[1] ETSI EN 319 411-1 (in der aktuellen Version); Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements
http://www.etsi.org/deliver/etsi_en/319400_319499/31941101/

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

[3] Prozessbeschreibung Registrierungsstelle Abteilung GQ 0500 (intern, vertraulich)