Trustcenter der Deutschen Rentenversicherung

Vertrauensdiensteanbieter Deutsche Rentenversicherung Bund

PKI Disclosure Statements des Zertifikatsdienstes DRV DRIS CA

Dokument-OID: 1.3.6.1.4.1.22204.1.8.7.1.6

Version	01.00.00
Stand	01.08.22
Dokument	TCDRV_PDS_DRV-DRIS-CA_DE
Status	Freigegeben
Vertraulichkeit	Keine Beschränkungen

1 PKI Disclosure Statements

1.1 Geltungsbereich

Dieses Dokument beinhaltet die PKI Disclosure Statements des Vertrauensdiensteanbieters Deutsche Rentenversicherung Bund für Server-Zertifikate des Zertifikatsdienstes für das Fachverfahren Digitale Rentenübersicht (DRV DRIS CA).

Die Server-Zertifikate werden für Server von Vorsorgeeinrichtungen im Rahmen des Fachverfahrens Digitale Rentenübersicht der Deutschen Rentenversicherung Bund gemäß Rentenübersichtsgesetz (RentÜG) ausgestellt.

1.2 Dokumentname

Dokumentname:	PKI Disclosure Statements des Zertifikatsdienstes DRV DRIS CA
Dokument-OID:	1.3.6.1.4.1.22204.1.8.7.1.6 PEN-DRV-Bund (1.3.6.1.4.1.22204). Trustcenter (1). Policy (8). PDS (7). Produktivsystem (1). DRIS CA (6)

1.3 Kontaktadressen

Die folgenden Ansprechwege zum Vertrauensdiensteanbieter Deutsche Rentenversicherung Bund bestehen 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 Vertrauensdiensteanbieters 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

Die Zentrale Stelle für die Digitale Rentenübersicht (ZfDR) wird durch die Deutsche Rentenversicherung Bund betrieben. Die ZfDR hat die Funktion einer Registrierungsstelle im Trustcenter der Deutschen Rentenversicherung.

Die ZfDR kann wie folgt erreicht werden:

E-Mail:	zfdr-anbindung@drv-bund.de
Postadresse:	Deutsche Rentenversicherung Bund Zentrale Stelle für die Digitale Rentenübersicht 10868 Berlin

1.4 Teilnehmer am Zertifikatsdienst

1.4.1 Registrierungsstelle

Die ZfDR prüft, ob es sich bei einem Teilnehmer um eine Vorsorgeeinrichtung nach § 2 Nummer 2 RentÜG handelt. Nur für diese Organisationen werden Zertifikate im Rahmen des Fachverfahrens Digitale Rentenübersicht ausgestellt.

1.4.2 Zertifikatsinhaber

Die registrierten Vorsorgeeinrichtungen (VE) sind berechtigt, Server-Zertifikate des Zertifikatsdienstes DRV DRIS CA im Rahmen des Datenaustausches mit der ZfDR der Deutschen Rentenversicherung Bund zu beantragen.

Zertifikatsinhaber sind die im Registrierungsprozess angegebenen Verantwortlichen dieser Vorsorgeeinrichtungen.

1.4.3 Zertifikatsprüfer

Die Server-Zertifikate der Vorsorgeeinrichtungen werden im Datenaustausch mit der ZfDR eingesetzt. Die ZfDR hat dabei die Funktion des Zertifikatsprüfers. Die ZfDR soll nur mit den Servern kommunizieren, die ein gültiges Zertifikat präsentieren.

1.5 Ausgestellte Zertifikate

Der Zertifikatsdienst DRV DRIS CA stellt folgende Server-Zertifikate aus:

- TLS-Server-Zertifikate für Vorsorgeeinrichtungen im Rahmen des Datenaustausches mit der ZfDR.

Die vom Zertifikatsdienst DRV DRIS CA ausgegebenen Server-Zertifikate werden im Rahmen des Datenaustausches mit der ZfDR verwendet. Weitere Anwendungsfälle sind nicht vorgesehen.

Die Auskunft über den Sperrstatus, der von der DRIS CA ausgestellten Zertifikate, wird über die Laufzeit der ausgestellten Zertifikate vom Trustcenter der Deutschen Rentenversicherung erteilt.

Im Fall der Einstellung des Betriebes des Zertifikatsdienstes DRV DRIS 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 zu den Server-Zertifikaten gehörenden kryptografischen Schlüssel sollen unter der Kontrolle des Antragstellers erstellt und genutzt werden. Ein Zugriff weiterer Personen auf die Server-Schlüssel soll auf geeignete Weise verhindert werden.

Die Anbindung der Vorsorgeeinrichtungen erfolgt durch die ZfDR. Im Prozess der Anbindung erfolgt die Registrierung, d.h. die Übermittlung der Daten der Vorsorgeeinrichtung. Nach erfolgreicher Validierung der übermittelten Daten können diese zur Beantragung eines Server-Zertifikates genutzt werden.

Die Prozeduren und Sicherheitsmaßnahmen zur Registrierung und Validierung sind in [3] und [4] festgelegt: Die Weiterleitung eines Zertifizierungsantrages erfolgt erst nach sorgfältiger Prüfung der von der Vorsorgeeinrichtung gemachten Angaben. Insbesondere werden die Kontaktdaten validiert – im Zweifelsfall durch eine Kontaktaufnahme mit der Vorsorgeeinrichtung.

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

Bei Einstellung des Betriebes des Zertifikatsdienstes 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 Server-Zertifikate ausschließlich im Rahmen der vorgesehen Nutzung zu verwenden. Zertifikatsinhaber sind verpflichtet, sich an die ZfDR zu wenden, wenn folgende Bedingungen vorliegen:

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

Die ZfDR behält sich vor, in diesen Fällen das Server-Zertifikat zu sperren. Ggf. muss ein neues Server-Zertifikat beantragt werden. Der Kontakt zur ZfDR erfolgt gemäß Kap. 1.3.

1.8 Pflichten der Zertifikatsprüfer

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

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

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

Zertifikatsprüfer müssen die Beschränkung für den Einsatz der Zertifikate beachten. Die Einsatzbeschränkung ist im Server-Zertifikat in der Extension „Restriction“ festgelegt.

Zertifikatsprüfer sollen bei Verdacht auf oder festgestelltem Missbrauch von Server-Zertifikaten den Vertrauensdiensteanbieter darüber informieren. Der Kontakt zum Trustcenter der Deutschen Rentenversicherung erfolgt gemäß Kapitel 1.3.

1.9 Haftung des Vertrauensdiensteanbieters

Der Vertrauensdiensteanbieter Deutsche Rentenversicherung Bund haftet für die Durchführung der Prozesse Zertifikatsausstellung und Zertifikatssperrung.

Für die Anbindung der Vorsorgeeinrichtungen, die Registrierung der Zertifikatsinhaber, die Weiterleitung eines Zertifikatsantrages, die Erstellung eines Zertifikatssperrantrages sowie die Korrektheit der Angaben im Zertifikat ist die ZfDR zuständig.

1.10 Richtlinien für den Zertifikatsdienst

Die Vorgaben zur Erstellung von Server-Zertifikaten für die Digitale Rentenübersicht sind definiert in folgenden Dokumenten:

Dokument	Klassifikation	Bezug
Zertifikatsprofile der DRV DRIS 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 personenbezogener Daten ein. Die Server-Zertifikate der Vorsorgeeinrichtungen sollen keine personenbezogenen Daten beinhalten.

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 DRIS CA arbeitet als Vertrauensdienst zur Erstellung elektronischer Zertifikate in Anlehnung an die relevanten ETSI-Normen [1].

Die Prüfung bzgl. Einhaltung der Normen erfolgt intern durch die Leitung des Trustcenters der Deutschen Rentenversicherung sowie durch die Abt. Revision der Deutschen Rentenversicherung Bund.

Die ZfDR der Deutschen Rentenversicherung Bund beachtet die Regelungen des RentÜG.

Die Prüfung der ZfDR erfolgt durch die Abt. Revision der Deutschen Rentenversicherung Bund.

2 Verzeichnisse

2.1 Abkürzungen

CA	Zertifikatsdienst (Certification Authority)
DRV	Deutsche Rentenversicherung
ETSI	European Telecommunications Standard Institute
OID	Object Identifier
PEN	Private Enterprise Number
PKI	Public Key Infrastructure
RentÜG	Rentenübersichtsgesetz
URL	Unified Ressource Locator
VDA	Vertrauensdiensteanbieter
VE	Vorsorgeeinrichtung
ZfDR	Zentrale Stelle für die Digitale Rentenübersicht

2.2 Änderungsverzeichnis

Version	Datum	Kap.	Änderungsgrund	Bearbeiter
01.00.00	01.08.2022	Alle	Freigabe	DRV Bund

2.3 Referenzen

[1] ETSI EN 319 411-1 V1.3.1 (2021-05); 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] Kommunikationshandbuch Grundlagen und Verfahren der ZfDR (öffentlich),
https://zfdr-vorsorgeeinrichtungen.drv-bund.de/vorsorgeeinrichtungen/vorsorgeeinrichtungen_node.html

[4] Zentrale Stelle für die Digitale Rentenübersicht – Handlungshilfe Anbindungsprozess (intern, vertraulich)