DIGITALE RENTEN ÜBERSICHT

Deutsche Rentenversicherung
Zentrale Stelle für die Digitale Rentenübersicht

Zentrale Stelle für die Digitale Rentenübersicht

Kommunikationshandbuch
Technische Grundlagen

Version:	15.00.00
Status:	Freigegeben
Ausgabedatum:	11.09.2026

0 Allgemeines

0.1 Änderungsübersicht zur Vorgängerversion

Vollständige Änderungshistorie siehe Kapitel 0

Änderungsübersicht

Version	Datum	Kapitel	Bemerkungen
15.00.00	11.09.2026	0.6	letzte Spalte ergänzt in Tabelle
		2.1	Änderung auf DIN-Norm 91379
		5.2	neues Feld im Anbindungsformular (Postfach)
		5.4	Kapitel ersetzt durch ‚Umwandlung von Unternehmen (insbesondere Fusion)‘
		6.1	Verlinkung zum Trustcenter eingefügt
		6.4	Anpassung bzgl. des neuen Zertifikats

Tabelle 1: Änderungsübersicht zur Vorgängerversion

0.2 Inhaltsverzeichnis

0 Allgemeines 2
0.1 Änderungsübersicht zur Vorgängerversion 2
0.2 Inhaltsverzeichnis 3
0.3 Tabellenverzeichnis 5
0.4 Abbildungsverzeichnis 5
0.5 Abkürzungsverzeichnis 6
0.6 Referenzierte Dokumente 7
1 Grundlagen 8
1.1 Wichtige Anmerkungen für die Anbindung 8
1.2 Ausgangslage 8
1.3 Zweck des Dokumentes 9
1.4 Publikationswege 9
1.5 Kosten des Verfahrens 9
1.6 Kurzbeschreibung 10
1.7 Welche Altersvorsorgeprodukte bildet die Digitale Rentenübersicht ab? 10
1.8 Freiwilligkeit und Verpflichtung zur Teilnahme 11
2 Allgemeine Grundlagen 12
2.1 Technische Grundlagen 12
3 Ablauf der Anfrage 14
3.1 Auslösen einer Anfrage 14
3.2 Antwort: Kein Vorsorgeanspruch 16
3.2.1 Antwort: Erneute Nachfrage 16
3.2.2 Antwort mit Anspruchsdaten 17
4 Fehlerrückmeldung 21
4.1 Ablauf einer Fehlerrückmeldung 21
4.2 Ablauf bei technischen Fehlern/unbekannten Statuscodes 23
5 Anbindung einer Vorsorgeeinrichtung 24
5.1 Erstmalige Anbindung einer Vorsorgeeinrichtung 24
5.2 Erläuterungen zum Anbindungsformular 27
5.3 Anbindung von Dienstleistern 35
5.4 Umwandlung von Unternehmen (insbesondere Fusion) 36
5.4.1 Meldung einer Umwandlung 36

5.4.2 Weitere Schritte 36
5.4.3 Verschiedene Fallgestaltungen 37
5.4.3.1 Fusion 37
5.4.3.2 Aufspaltung, Abspaltung, Ausgliederung 37
5.4.3.3 Rechtsformwechsel und Namensänderung 37
5.4.3.4 Verbundanbindungen 38
6 Zertifikate 39
6.1 Management von Zertifikaten 39
6.2 Anfragen an das Trustcenter 39
6.3 Beantragung eines Serverzertifikates 40
6.4 Certification Authority Zertifikat-Aussteller-Kette 42
6.5 Verlängerung eines Serverzertifikates 42
6.6 Sperren eines Serverzertifikates 44
6.7 Authentifizierung des zentralen Servers der ZfDR 44
6.8 Funktionale Elemente des Zertifikatsmanagements 44
6.9 Funktion zur Generierung und Beantragung von Zertifikaten 45
6.10 Prüfung des Schlüsselpaars 45
6.11 Generierung des CSR-Request (Certifcate Signing Request) 45
6.12 Prüfen des CSR 46
6.13 Länderliste für CSR-Datei 47
7 Beschreibung des Testvorgehens 50
7.1 Beschreibung des Testvorgehens 50
7.2 Verbindungstest im produktiven System (erforderlich) 51
7.3 Kommunikationstests in der QS-/PNT-Umgebung (optional) 51
7.3.1 Testergebnisse 53
7.3.1.1 Beipielhafte erfolgreiche Kommunikationstests 54
7.3.1.2 Beispielhafte Fehlerfälle 56
7.4 Testfälle für den Kommunikationstest 58
8 Implementation der Schnittstelle 60
8.1 Allgemeines 60
8.2 Generatoren 60
8.3 Allgemeine Generator-Konfiguration 60
8.4 Spezifische Generator-Konfiguration 61
8.5 Generator-Beispielkonfiguration 62
8.6 Potenziell erforderliche Anpassungen 64

9 Multipart-Response 65

9.1 Allgemeines 65

9.2 Erläuterung von multipart/form-data 65

9.3 Gegenüberstellung von vorherigem Format (bis Juli 2025) multipart/mixed und aktuellem Format multipart/form-data 67

9.4 Validierung 69

9.5 De-referenzierte Version des Spezifikationsdokuments 69

9.6 Linksammlung 70

10 IT-Sicherheit 71

11 Prognosen zur Kommunikationslast (Mengengerüst) 72

12 Unterstützung der Kommunikationspartner 73

13 Änderungsübersicht 74

0.3 Tabellenverzeichnis

Tabelle 1: Änderungsübersicht zur Vorgängerversion 2
Tabelle 2: Abkürzungsverzeichnis 6
Tabelle 3: Query-Parameter 15
Tabelle 4: Attribute der Fehlermeldung 21
Tabelle 5: Fehlernummern 23
Tabelle 6: Ausfüllhilfe zum Anbindungsformular 35
Tabelle 7: Attribute für Zertifikate 41
Tabelle 8: Auflistung der Testfälle 59

0.4 Abbildungsverzeichnis

Abbildung 1: Ablauf Anfrage der Altersvorsorgeansprüche bei einer Vorsorgeeinrichtung 16
Abbildung 2: Schematische Darstellung einer Antwort mit Typ multipart/form-data 18
Abbildung 3: Übersicht Anbindungsprozess 24
Abbildung 4: Zertifikate für die produktive Anbindung 26
Abbildung 5: Gegenüberstellung der unterschiedlichen Anbindungen 27
Abbildung 6: Gegenüberstellung Testvarianten 50
Abbildung 7: Schaubild Kommunikationssicherheit 71

0.5 Abkürzungsverzeichnis

Abkürzung	Beschreibung
AO	Abgabenordnung
BZSt	Bundeszentralamt für Steuern
CER	Siehe CRT, alternative Bezeichnung
CRL	Certification Revocation List, Zertifikatsperrliste
CRT	Öffentliche Zertifikatsdatei; kennzeichnet Dateien, die das fertige Zertifikat enthalten
CSR	Certificate Signing Request, Zertifikatsignierungsanforderung
IdNr	die vom Bundeszentralamt für Steuern nach § 139b der Abgabenordnung zugeteilte Identifikationsnummer
KHB	Kommunikationshandbuch
MAV	Maschinelles Anfrageverfahren zur Erlangung der IdNr
OCSP	Online Certificate Status Protocol
OpenAPI3.0	Ein Standard zur Beschreibung von REST-konformen Programmierschnittstellen
PDF	Portable Document Format
RentÜG	Rentenübersichtsgesetz
URL	Uniform Resource Locator
VE	Vorsorgeeinrichtung
*.yaml	Format für die Serialisierung verschiedener Daten
ZfDR	Zentrale Stelle für die Digitale Rentenübersicht
ZfA	Zentrale Zulagenstelle für Altersvermögen

Tabelle 2: Abkürzungsverzeichnis

0.6 Referenzierte Dokumente

Bezeichnung	Beschreibung	Ablageort
Kommunikationshandbuch Verfahren	fachliche Grundlagen zum Verfahren der ZfDR	Internetauftritt der ZfDR https://zfdr-vorsorgeeinrichtungen.drv-bund.de/vorsorgeeinrichtungen/vorsorgeeinrichtungen_node.html
vorsorgeeinrichtung.yaml	OpenAPI3.0 Spezifikation im *.yaml Format	Internetauftritt der ZfDR https://zfdr-vorsorgeeinrichtungen.drv-bund.de/vorsorgeeinrichtungen/vorsorgeeinrichtungen_node.html
ZfDR - Datenbeschreibung	Tabellarische Datenbeschreibung zu den Datensätzen	Internetauftritt der ZfDR https://zfdr-vorsorgeeinrichtungen.drv-bund.de/vorsorgeeinrichtungen/vorsorgeeinrichtungen_node.html
FAQs Digitale Renten-übersicht	Häufige Fragen zum Verfahren	Internetauftritt der ZfDR https://zfdr-vorsorgeeinrichtungen.drv-bund.de/vorsorgeeinrichtungen/vorsorgeeinrichtungen_node.html
Glossar	Glossar zu den Produktarten und weitere Glossarbegriffe	Website der Digitalen Rentenübersicht https://rentenuebersicht.de
PKI Disclosure Statements des Zertifikatsdienstes DRV DRIS CA	Detaillierte Informationen vom Trustcenter der DRV Bund zum Thema Zertifikate	Internetauftritt des Trustcenters der DRV https://www.deutsche-rentenversicherung.de/Bund/DE/Ueber-uns/Trustcenter/trustcenter_node.html

1 Grundlagen

1.1 Wichtige Anmerkungen für die Anbindung

- Laden Sie vor der Implementierung bitte die neusten Dokumentationen auf https://zfdr-vorsorgeeinrichtungen.drv-bund.de herunter (insbesondere das Technische Kommunikationshandbuch). Um kontinuierlich über Neuerungen am Verfahren unterrichtet zu sein, empfiehlt es sich auch den Newsletter für Vorsorgeeinrichtungen zu abonnieren.
- Auch wenn für das Verfahren gängige Technologien zum Einsatz kommen, planen Sie für die Implementierung bitte ausreichend Zeit ein.
- Eine Expertenkenntnis im Bereich der Fachinformatik Systemintegration wird empfohlen (siehe Kapitel 7.1).
- Zentrale Voraussetzung für die Anbindung ist, dass die IP-Adressen der ZfDR freigeschaltet (siehe Kapitel 3.1) und die Zertifikate richtig eingebunden sind.
- Aufgrund der hohen Anzahl an Vorsorgeeinrichtungen und individuellen Systemlandschaften liegt die Fehleridentifikation bei aufkommenden Komplikationen in der Verantwortung der Vorsorgeeinrichtung. Dies betrifft vorrangig die Einrichtung der individuellen Systeme der Vorsorgeeinrichtung, insbesondere die Einrichtung der Kommunikationsstrecke (Zertifikatseinbindung, Routing/IP-Adressen, Antwortausgestaltung).
- Die Anbindung beruht auf einem abgestimmten Kommunikationsverfahren (siehe Kapitel 2), das keine Sonderprozesse bzw. Abweichungen für einzelne Vorsorgeeinrichtungen vorsieht (bspw. keine Kommunikation ohne Zertifikate oder andere Schnittstellentechnologien).

1.2 Ausgangslage

Mit dem Rentenübersichtsgesetz vom 17. Februar 2021 (BGBl. I S. 154) wurde bestimmt, dass eine eigens dafür geschaffene Zentrale Stelle für die Digitale Rentenübersicht (ZfDR) bei der Deutschen Rentenversicherung Bund (DRV-Bund) eine Digitale Rentenübersicht anbietet.

Ziel des Verfahrens ist eine Verbesserung des Kenntnisstandes der Nutzenden über die eigene Altersvorsorge, um die Planungsgrundlagen zu verbessern. Den Nutzenden wird damit ein ergänzendes Angebot unterbreitet, sich nutzerfreundlich an einer Stelle einen Gesamtüberblick über die eigene Altersvorsorge zu verschaffen. Das Angebot einer Digitalen Rentenübersicht soll einen Anreiz setzen, sich intensiver mit der eigenen Altersvorsorge auseinanderzusetzen. Die Informationen sollen verlässlich, verständlich und möglichst vergleichbar sein.

Laut Rentenübersichtsanbindungsverordnung (RentÜAV) sind Vorsorgeeinrichtungen zu einer Anbindung an die Zentrale Stelle für die Digitale Rentenübersicht verpflichtet, wenn sie:

- im Sinne von § 7 Absatz 1 Satz 3 RentÜG verpflichtet sind, mindestens jährlich eine Standmitteilung zu übermitteln und

- mehr als 1.000 Altersvorsorgeansprüchen im Bestand haben, die sich noch nicht in der Auszahlungsphase befinden.
- Der Stichtag für die Anbindung wurde auf den 31.12.2024 festgelegt (§ 3 RentÜAV).

1.3 Zweck des Dokumentes

Dieses Kommunikationshandbuch (KHB) beschreibt die technischen Grundlagen zur Anfrage und Übermittlung von Informationen zu Altersvorsorgeprodukten der an dem Verfahren für die Digitale Rentenübersicht teilnehmenden Vorsorgeeinrichtungen.

Der Schwerpunkt liegt dabei in der Anbindung von Vorsorgeeinrichtungen nach § 2 Nummer 2 des Gesetzes zur Entwicklung und Einführung einer Digitalen Rentenübersicht (RentÜG) an die ZfDR als zentrale Stelle nach § 3 RentÜG sowie in der Kommunikation zwischen den Vorsorgeeinrichtungen und der ZfDR.

Der Begriff **Vorsorgeeinrichtung** erstreckt sich im Folgenden ebenfalls auf IT-Dienstleister und Daten-Intermediäre der Einrichtungen. Der Begriff **Nutzende** oder **nutzende Person** beschreibt stets Bürgerinnen und Bürger, welche die Digitale Rentenübersicht nutzen.

Dieses KHB wird von der ZfDR erstellt, gepflegt und veröffentlicht. Vorgenommene Änderungen werden unter Angabe des Abschnitts in der Änderungsübersicht dokumentiert und führen zu einer neuen Version des Dokumentes.

Da zum Zeitpunkt der Veröffentlichung dieses KHBs nicht alle Aspekte der Digitalen Rentenübersicht abschließend geklärt sind, enthält das Dokument Kapitel mit dem Hinweis „Dieses Kapitel befindet sich noch in Erstellung“. Wie das Verfahren selbst, wird auch das KHB sukzessive erweitert.

1.4 Publikationswege

Das KHB und die zugehörigen Anlagen werden in ihrer aktuellen Version auf einem Internetauftritt der ZfDR öffentlich zugänglich zum Download bereitgestellt.

zfdr-vorsorgeeinrichtungen.drv-bund.de

Die Anlagen (vgl. Kapitel 0.6 'Referenzierte Dokumente') Datenbeschreibung, OpenAPI3.0 Spezifikation im *.yaml Format und das KHB werden jeweils mit ihrer Veröffentlichung hoch versioniert. Die aktuelle Version ist jeweils maßgebend und ersetzt die Vorgängerversion. Der Zeitraum, in dem eine bereits veröffentlichte Version einer der genannten Anlagen gültig ist, ist gegebenenfalls abhängig vom kommunizierten Release Termin, dem diese Anlage zugrunde liegt. Eine parallele Gültigkeit unterschiedlicher Versionen ist ausgeschlossen. Ein Mapping zwischen Datenbeschreibung, OpenAPI3.0 Spezifikation und KHB ist demnach nicht erforderlich.

Die erforderlichen Unterlagen werden den Vorsorgeeinrichtungen rechtzeitig vor einem neuen Einsatzzeitpunkt zur Verfügung gestellt.

1.5 Kosten des Verfahrens

Nach dem Grundsatz der Kostenfreiheit des Verfahrens (§ 7 Absatz 3 RentÜG) erhalten die Vorsorgeeinrichtungen von der zentralen Stelle keinen Ersatz für Kosten, die ihnen aus dem

Verfahren gemäß § 4 RentÜG entstehen. Das bedeutet, dass die Kosten für die Datenübermittlung der jeweilige Absender trägt.

1.6 Kurzbeschreibung

Das Verfahren ‚Digitale Rentenübersicht' bei der ZfDR dient der Bereitstellung einer digitalen Übersicht über die individuellen Altersvorsorgeansprüche einer Bürgerin oder eines Bürgers (Nutzende) auf einer Onlineplattform. Das Angebot auf der Onlineplattform umfasst alle Ansprüche des Nutzenden gegenüber den am Verfahren angebundenen Vorsorgeeinrichtungen.

Der/die Nutzende erstellt ein Nutzerkonto bei der ZfDR. Die ZfDR authentifiziert die Person und verifiziert dessen persönliche Daten. Nach erfolgreicher Anlage des Nutzerprofils kann der/die Nutzende individuelle Anfrageaufträge an alle bzw. ausgewählte Vorsorgeeinrichtungen über die Onlineplattform auslösen. Maßgebliches Zuordnungskriterium ist die vom Bundeszentralamt für Steuern (BZSt) nach § 139b der Abgabenordnung (AO) zugeteilte Identifikationsnummer (IdNr) der Nutzenden. Demnach setzt das Verfahren voraus, dass die Stammdaten der angebundenen Vorsorgeeinrichtungen mit der IdNr ausgestattet sind.

Die ausgewählten Vorsorgeeinrichtungen prüfen infolge der Anfrage der ZfDR, ob und welche Informationen über die nutzende Person vorliegen und stellen die Informationen mit definiertem Inhalt und Format zur Abholung der ZfDR bereit. Die Antworten werden von der ZfDR für die Nutzenden zur Anzeige zentral aufbereitet und bei Zustimmung gespeichert. Die Speicherung und den Export einer Digitalen Rentenübersicht können Nutzende nach eigenem Ermessen steuern.

Einen hohen Stellenwert in dem Verfahren hat eine möglichst schnelle Informationsbereitstellung für die Nutzenden der Digitalen Rentenübersicht.

1.7 Welche Altersvorsorgeprodukte bildet die Digitale Rentenübersicht ab?

Nach § 2 Nummer 1 Rentenübersichtsgesetzt (RentÜG) sind Altersvorsorgeprodukte Versicherungen, Zusagen und Verträge, auf deren Grundlage Leistungen der gesetzlichen, betrieblichen oder privaten Altersvorsorge in der Zukunft erbracht werden. Diese müssen dem Zweck der Altersvorsorge dienen. Hiervon ist auszugehen, wenn der vertraglich vereinbarte Beginn des Leistungsbezugs rentennah ist. Hierfür wird frühestens die Vollendung des 60. Lebensjahres bestimmt.

Produkte oder Objekte, die sich nicht offensichtlich dem Zweck der Altersvorsorge zuordnen lassen, werden nicht von der Digitalen Rentenübersicht erfasst.

Dies sind beispielsweise:

- Riester-Bausparverträge
- der wohnungswirtschaftlich entnommene Anteil von Riester-Verträgen
- Klassische Banksparpläne, Fonds, Aktien
- Private Immobilien
- Lebensversicherungen, die keine rentennahe Auszahlung vorsehen

- Produkte zur reinen Hinterbliebenen- oder Invaliditätsabsicherung

1.8 Freiwilligkeit und Verpflichtung zur Teilnahme

Für Bürgerinnen und Bürger ist die Nutzung der Digitalen Rentenübersicht freiwillig.

Für Vorsorgeeinrichtungen ist die Freiwilligkeit oder Verpflichtung zur Teilnahme am Verfahren ab dem Stichtag nach § 7 Absatz 1 Satz 3 RentÜG i.V.m. §§ 1, 3 RentÜAV abhängig davon, wie viele Altersvorsorgeansprüche ihr gegenüber bestehen und davon, ob sie verpflichtet ist, mindestens jährlich Standmitteilungen zu übermitteln.

Der **Stichtag** für die verpflichtende Anbindung einer Vorsorgeeinrichtung an die Zentrale Stelle für die Digitale Rentenübersicht ist der **31.12.2024**. Voraussetzung für die verpflichtende Anbindung ist, dass gegen die Vorsorgeeinrichtung mehr als 1.000 Altersvorsorgeansprüche bestehen, die sich noch nicht in der Auszahlungsphase befinden und diese verpflichtet ist, mindestens jährlich Standmitteilungen zu übermitteln.

Die verpflichtende Anbindung an die Zentrale Stelle für die Digitale Rentenübersicht erfolgt in einem mehrstufigen Verfahren.

Zunächst melden sich alle verpflichteten Vorsorgeeinrichtungen bis zum **31.03.2024** bei der Zentralen Stelle für die Digitale Rentenübersicht an.

In der zweiten Stufe erfolgt die Implementierung der Schnittstellen zur ZfDR. Diese müssen spätestens bis **30.09.2024** produktiv erreichbar sein, sodass der Austausch von Daten möglich ist.

In der dritten Stufe werden die produktiven Schnittstellen getestet. Die Termine für die Tests werden von der Zentralen Stelle für die Digitale Rentenübersicht vergeben.

In der vierten Stufe sollen Vorsorgeeinrichtungen dann bis zum **31.12.2024** in der Lage sein, auf produktive Anfragen der Zentralen Stelle für die Digitale Rentenübersicht mit Daten über die Altersvorsorgeansprüche von Nutzenden an die Digitalen Rentenübersicht zu antworten.

Sofern Vorsorgeeinrichtungen nach dem **31.03.2024** die Schwelle von **1.000 Altersvorsorgeansprüchen** aus Altersvorsorgeprodukten überschreiten, melden diese sich unverzüglich bei der Zentralen Stelle für die Digitale Rentenübersicht an. Diese Vorsorgeeinrichtungen richten dann innerhalb von sechs Monaten ab dem Zeitpunkt der Anmeldung eine produktive Schnittstelle ein. Innerhalb von neun Monaten nach Anmeldung müssen die Vorsorgeeinrichtungen in der Lage sein, auf Anfrage der Zentralen Stelle für die Digitale Rentenübersicht Daten ihrer Kundinnen und Kunden zu übermitteln.

2 Allgemeine Grundlagen

Die technischen Grundlagen des Verfahrens wurden von Beginn an gemeinschaftlich mit Vertreter und Vertreterinnen der gesetzlichen (erste Säule), der betrieblichen (zweite Säule) und privaten (dritte Säue) Altersvorsorge insb. mit Organisationen und Verbänden (u.a. DRV, aba, GDV, GVI, Stiftung Warentest etc.) in mehr als 35 Fachbeiräten abgestimmt. In diesen Fachbeiräten war die Priorität ein möglichst schlankes Kommunikationsverfahren zu konzipieren, welches gängige und sichere Technologien verwendet, um so den Anbindungsaufwand für die Vorsorgeeinrichtungen möglichst gering zu halten.

2.1 Technische Grundlagen

Die Kommunikation zwischen den Vorsorgeeinrichtungen und der ZfDR erfolgt mittels HTTP RESTful Webservice-Schnittstellen. Die Vorsorgeeinrichtung stellt zwei Webservice-Endpunkte gemäß der von der ZfDR zur Verfügung gestellten Open API 3.0 Spezifikation zur Verfügung (vgl. 0.6 'Referenzierte Dokumente').

Die Open API Spezifikation umfasst zwei Ressourcen mit jeweils einer Methode.

Die Anspruchsdaten-Ressource dient zur Abfrage vorhandener Ansprüche mittels HTTP GET Aufruf. Die Fehlerrückmeldung-Ressource ermöglicht die Übermittlung von Fehlern mittels HTTP POST. Als Format für die strukturierten Daten wird JSON verwendet. Als Teil der Antwort bei vorhandenen Altersvorsorgeansprüchen müssen die jeweiligen Standmitteilungen in der Antwort übermittelt werden. Die Übermittlung der Standmitteilungsdaten erfolgt im JSON Format. Die Übermittlung der Standmitteilungs-PDF-Dateien erfolgt binär codiert. Beide Bestandteile werden innerhalb einer Multipart-Response gesendet.

Weiterhin sind die verbindlich einzuhaltenden Schemata in der Open API 3.0 Spezifikation vorhanden und ebenfalls unter https://zfdr-vorsorgeeinrichtungen.drv-bund.de zum Download bereitgestellt.

Bei der Übermittlung von Daten ist die Codepage UTF-8 (CCSID: 1208) - Zeichensatz UNICODE DIN-Norm 91379 – Datentyp C zu verwenden. Die ZfDR gibt nach § 5 Absatz 2 Satz 1 RentÜG das Dokumentenformat für die zu übermittelnden Standmitteilungen (§§ 2 Nummer 3, 5 Absatz 1 Nummer 1 RentÜG) vor. Dabei sind sowohl für die Digitale Rentenübersicht als auch für das elektronische Portal die jeweils geltenden Vorgaben zur Barrierefreiheit nach dem Behindertengleichstellungsgesetz, insbesondere die §§ 4 und 12a des Behindertengleichstellungsgesetzes, sowie die auf Grundlage des Behindertengleichstellungsgesetzes erlassenen Rechtsverordnungen zur Barrierefreiheit, insbesondere die Barrierefreie-Informationstechnik-Verordnung, zu beachten (§ 3 Absatz 3 Satz 3 RentÜG).

Den Anforderungen des § 3 Absatz 3 Satz 3 RentÜG an die Barrierefreiheit genügen Standmitteilungen in einem PDF/UA-konformen PDF-Standard. Dieser ist von den Vorsorgeeinrichtungen einzuhalten. Eine maschinelle Überprüfung durch die ZfDR ist nicht möglich.

Die ZfDR empfiehlt die bevorzugte Nutzung des Formates „PDF/A-2a“, tagged PDFs und die Vermeidung grafischer Elemente, damit Nutzende die Standmitteilung mit Hilfe eines Screen-Readers lesen können.

Für die Verfahrensteilnahme muss sich die Vorsorgeeinrichtung vorab registrieren. Im Rahmen dieser Registrierung werden neben allgemeinen Informationen auch die technischen Parameter (URLs und Zertifikate) festgelegt und überprüft.

Die Kommunikation zwischen der ZfDR und den Vorsorgeeinrichtungen erfolgt über das Internet. Die Verschlüsselung erfolgt über TLS (HTTPS) und die Authentifizierung und Autorisierung über Zertifikate. Es werden keine VPN-Verbindungen/Tunnel genutzt. Das Time-Out für den Verbindungsaufbau liegt bei 30 Sekunden und das Time-Out für die Response/Antwort liegt ebenfalls bei 30 Sekunden.

Die einzelnen Aspekte der Kommunikation und Anbindung werden in den nachfolgenden Kapiteln näher erläutert.

3 Ablauf der Anfrage

3.1 Auslösen einer Anfrage

Als Reaktion auf den Anfragewunsch einer Person initiiert die ZfDR die Kommunikation mit den Vorsorgeeinrichtungen, gemäß der als Open API 3.0 spezifizierten Schnittstelle.

Die ZfDR ruft den von der Vorsorgeeinrichtung im Anbindungsprozess hinterlegten Anfrageendpunkt auf. Der zentrale Server der ZfDR ruft die Vorsorgeeinrichtungen über einen Proxy-Server auf, der redundant ausgelegt ist.

Die IP-Adressen sind: 104.151.52.254 (Würzburg) und 217.9.49.1 (Berlin).

Die Kommunikation erfolgt verschlüsselt mittels TLS (HTTPS) und es wird zur Authentifizierung/Autorisierung eine wechselseitige, zertifikatsbasierte Prüfung (Mutual TLS) durchgeführt. Die Mutual Authentification muss gegebenenfalls am Server aktiviert werden. Die für diese Kommunikation notwendigen Zertifikate werden im Anbindungsprozess erzeugt und ausgetauscht (vgl. Kapitel 6 'Zertifikate').

Sobald der Kommunikationskanal etabliert wurde, übermittelt die ZfDR einen GET Request an den Endpunkt der Vorsorgeeinrichtung. Dieser Request enthält mehrere spezifizierte Parameter.

Parameter	Übermittelt als	Inhalt/Bedeutung
X-Identifikationsnummer	Custom Header	Die von der ZfDR geprüfte IdNr der anfragenden Person. Die IdNr dient als Identifikationskriterium für Altersvorsorgeansprüche beim jeweiligen Unternehmen.
X-Geburtsdatum	Custom Header	Das von der ZfDR ermittelte, amtliche Geburtsdatum der anfragenden Person. Dieser Parameter sollte von der Vorsorgeeinrichtung verwendet werden, um zu validieren, dass tatsächlich die richtige Person mittels der Identifikationsnummer identifiziert wurde.
X-Anfrage-Id	Custom Header	Eine eindeutige ID, die genau diese fachliche Anfrage identifiziert. Diese ID bleibt gleich, falls im Rahmen dieser Anfrage mehrere Aufrufe erfolgen (z.B. aufgrund von Fehlern oder Verschiebungswunsch). Ein späterer, erneuter Anfragewunsch einer nutzenden Person erzeugt eine neue ID.
X-Request-Id	Custom Header	Eine eindeutige ID, die genau diesen einen Webserviceaufruf identifiziert, diese

Parameter	Übermittelt als	Inhalt/Bedeutung
		ID verändert sich mit jedem weiteren Aufruf.
X-Nachfragezaehler	Custom Header	Ein fortlaufender Zähler, der angibt, der wievielte Anfrageversuch (aufgrund von Fehlern oder Verschiebungswunsch) durch die ZfDR erfolgt. Der Zähler beginnt bei 1 mit der ersten initialen Anfrage und wird mit jedem Versuch um 1 erhöht. Nach aktuellem Stand wird nach dem 5. Versuch abgebrochen und diese Anfrage als nicht erfolgreich betrachtet.
X-Max-Retry-After	Custom Header	Definiert die Zeitraumgrenze (in Sekunden) für eine Antwort mit dem „Retry-After“-Header, wenn die Vorsorgeeinrichtung eine spätere erneute Anfrage wünscht (siehe Antwort: Erneute Nachfrage)

Tabelle 3: Query-Parameter

Zusätzlich zu den aufgeführten fachlich relevanten Parametern können bei einer Anfrage weitere optionale Header übermittelt werden. Diese sind technischer Natur und haben keine Bedeutung für das Verfahren an sich. Sie dienen beispielsweise dem Monitoring von Abläufen und Verarbeitungsprozessen innerhalb unserer Anwendung und können von den Vorsorgeeinrichtungen ignoriert werden.

Der GET Request (z.B. https://server.domain.de/anspruchsdaten) wird über die zuvor aufgebaute TLS-Verbindung verschlüsselt.

Als Reaktion auf diese Anfrage können (abgesehen von technischen Fehlern) seitens der Vorsorgeeinrichtung drei Antworten gegeben werden.

1. Es besteht kein Vorsorgeanspruch: Das bedeutet, die Person konnte mit den Kriterien IdNr und Geburtsdatum nicht im Altersvorsorgebestand der Vorsorgeeinrichtung identifiziert werden.
2. Erneuter Nachfragewunsch: Das bedeutet, die Vorsorgeeinrichtung kann zum aktuellen Zeitpunkt keine abschließende Antwort geben und erbittet eine spätere erneute Anfrage.
3. Die Person konnte ermittelt werden und die Anspruchsinformationen werden übermittelt.

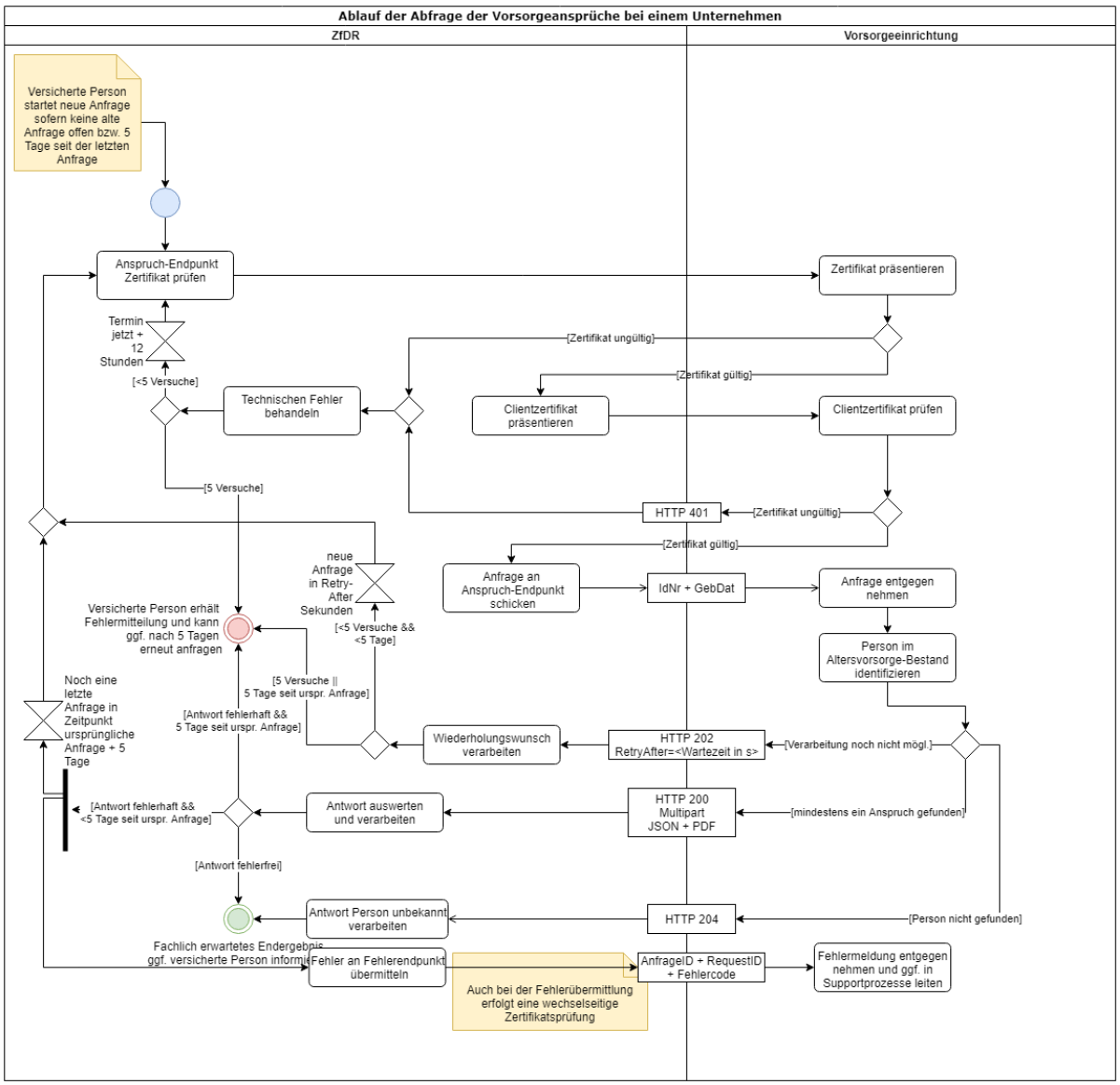

Abbildung 1: Ablauf Anfrage der Altersvorsorgeansprüche bei einer Vorsorgeeinrichtung

3.2 Antwort: Kein Vorsorgeanspruch

Falls zu den Anfragedaten IdNr und Geburtsdatum kein Altersvorsorgeanspruch bei der Vorsorgeeinrichtung ermittelt werden kann, übermittelt die Vorsorgeeinrichtung den HTTP-**Statuscode 204** als Antwort auf die Anfrage. Hier wird explizit der Statuscode 204 und nicht der Statuscode 404 verwendet. Es ist somit möglich, ohne weitere Informationen im Body eine Unterscheidung zwischen den Fällen „Person nicht gefunden“ und „Konfigurationsfehler in der Webserviceadresse“ zu treffen.

3.2.1 Antwort: Erneute Nachfrage

Eine Vorsorgeeinrichtung hat die Möglichkeit, um eine spätere erneute Nachfrage zu bitten, falls eine abschließende Antwort nicht direkt gegeben werden kann. Gründe dafür können beispielsweise Verzögerungen bei der Ermittlung in unterschiedlichen Bestandssystemen, Wartungsfenster o.ä. sein. Die Vorsorgeeinrichtung zeigt den Verschiebungswunsch mit dem

HTTP-Statuscode 202 an und übermittelt im Header Retry-After die Anzahl von Sekunden, die die ZfDR vor einer erneuten Anfrage warten soll. Für diese erneute Nachfrage gibt es allerdings einige wichtige Einschränkungen:

1. Die ZfDR kann nicht garantieren, dass die erneute Anfrage exakt nach der gewünschten Zeit erfolgt, die ZfDR wird in der Regel mindestens so lange warten. Es ist allerdings möglich, dass zum Beispiel aufgrund von Last auf Seiten der ZfDR die erneute Anfrage um einige weitere Sekunden verzögert wird.
2. Es gibt insgesamt maximal fünf Anfrageversuche für eine fachliche Anfrage, dabei zählen sowohl technische Fehler (Statuscodes ungleich 200, 204) als auch der erneute Nachfragewunsch (Statuscode 202). Nach dem fünften Versuch wird die ZfDR die Anfrageversuche abbrechen und im Portal für die anfragende Person eine entsprechende Rückmeldung anzeigen. Eine erneute, durch die Person ausgelöste, Anfrage bleibt dabei natürlich möglich.
3. Insgesamt darf der Zeitraum zwischen der ersten Anfrage und dem Abschluss der Anfrage nicht länger als fünf Tage sein. Sofern aufgrund von Verschiebungen der Zeitraum von fünf Tagen überschritten wird, wird die ZfDR den letzten Versuch auf den Zeitpunkt fünf Tage nach der ersten Anfrage terminieren (also ggf. früher als von der Vorsorgeeinrichtung gewünscht).
4. Um der Vorsorgeeirichtung die Errechnung des validen Werts für „Retry-After“ zu erleichtern, wird von der ZfDR in der Anfrage der Custom-Header „X-Max-Retry-After“ gesendet. Dieser variiert je nach bereits getätigten Anfrage-Versuche und wird mit jedem Anfrage-Versuch entsprechend kleiner, so dass alle erneuten Anfragen innerhalb der fünf Tagen erfolgen. Der Header „X-Max-Retry-After“ wird bis zum avisierten Einsatztermin1 seitens der ZfDR nicht gesendet, damit alle Vorsorgeeirichtungen sich technisch darauf vorbereiten können.
   Es wird empfohlen, die Wert-Behandlung von X-Max-Retry-After in einem IF (Bedingungsprüfung) zu prüfen und als Fallback-Default 5-Tage in Sekunden zu nehmen.

3.2.2 Antwort mit Anspruchsdaten

Sofern die Person im Altersvorsorgebestand der Vorsorgeeinrichtung identifiziert werden konnte und Ansprüche vorliegen, werden die angeforderten Informationen inklusive der Anspruchsinformationen und zugehörigen Standmitteilungen im PDF-Format von der Vorsorgeeinrichtung in einer HTTP-Multipartresponse mit dem **Statuscode 200** übermittelt.

[1] Einsatztermin ist/war der 09.07.2026 (Stand vom 17.12.2025). Terminänderungen teilt die ZfDR per Newsletter mit.

HTTP/1.1 200 OK

Content-Language: en-US

Content-Type: multipart/form-data; boundary=266cd242-31d2-4f69-bc52-657dec77650e

Date: Mon, 27 Jan 2025 11:16:30 GMT

Transfer-Encoding: chunked

--266cd242-31d2-4f69-bc52-657dec77650e

Content-Disposition: form-data; name="AnfrageDaten"

Content-Type: application/json

```
{
   "unternehmens_kontaktinformationen": {…},
   "ansprueche": [
      {
         (…),
         "standmitteilung_referenz": "Platzhalter-Standmitteilungen"
      }
   ]
}
```

--266cd242-31d2-4f69-bc52-657dec77650e

Content-Disposition: form-data; name="Platzhalter-Standmitteilungen"

Content-Type: application/pdf

%PDF-1.7

[...]

%%EOF

--266cd242-31d2-4f69-bc52-657dec77650e--

Boundary-Definition und Boundary Marks

Content-Type Header

Abbildung 2: Schematische Darstellung einer Antwort mit Typ multipart/form-data

Die Antwort der Vorsorgeeinrichtung besteht aus mehreren zusammenhängenden Teilen (daher Multipartresponse). Im ersten Teil der Antwort werden JSON Daten entsprechend dem vereinbarten und in der OpenAPI3.0 Spezifikation beschriebenen Schema erwartet. Die genauen Formate und Attribute können der OpenAPI Spezifikation bzw. der konventionellen Datenbeschreibung entnommen werden. Die folgenden vier Szenarien sind als Anspruchsklassen in der JSON-Struktur wiederzufinden.

a. Anspruch ist gegeben, aber es gibt noch keine Standmitteilung/Daten.
   Dieser Umstand kann z.B. eintreten, wenn Anwartschaften o.ä. noch nicht erfüllt sind bzw. der Vertrag gerade erst abgeschlossen wurde.
   Das ist die Anspruchsklasse **VZ0102a**.
b. Der Anspruch sieht ausschließlich Rentenzahlungen vor.
   Dies ist z.B. für die gesetzliche Rente der Fall. Es gibt ausschließlich

Rentenzahlungen und Angaben zu Rentenzahlungen oder zum zur Verrentung zur Verfügung stehenden Kapital.
Das ist die Anspruchsklasse **VZ0102b**.

c. Der Anspruch sieht ausschließlich Einmalzahlungen (auch Ratenzahlungen) vor.
Das ist die Anspruchsklasse **VZ0102c**.
d. Der Anspruch kann sowohl Rentenzahlungen als auch Einmalzahlungen umfassen, es ist dabei notwendig anzugeben, ob beides gezahlt wird bzw. eine Wahlmöglichkeit besteht und ob ggf. eine Standardauswahl schon hinterlegt ist.
Das ist die Anspruchsklasse **VZ0102d**.

In der JSON Struktur ist es möglich, auch mehr als einen Anspruch zu übermitteln. Die Ansprüche dürfen unterschiedlicher Art sein. Es ist möglich, dass zu einer Person zwei unterschiedliche Verträge (Ansprüche) auch aus unterschiedlichen Systemen vorhanden sind, wobei z.B. einer der Ansprüche nur eine Einmalzahlung (Fall a) und der andere eine Kombination (Fall d) vorsieht.

Es ist zu beachten, dass **ALLE** Ansprüche zu der Person bei der Vorsorgeeinrichtung **in einer einzigen, konsolidierten Antwort** übermittelt werden müssen, es ist nicht möglich, zu einem späteren Zeitpunkt einen weiteren Anspruch nachzuliefern.

Sobald die ZfDR eine Antwort empfängt, wird die Anfrage bezogen auf die Vorsorgeeinrichtung als abgeschlossen betrachtet und der anfragenden Person entsprechend angezeigt.

Für die Fallgestaltungen b-d müssen zusätzlich zu den strukturierten JSON Daten Standmitteilungen im PDF-Format übermittelt werden. Den Anforderungen des § 3 Absatz 3 Satz 3 RentÜG an die Barrierefreiheit genügen Standmitteilungen in einem PDF/UA-konformen PDF-Standard (vgl. Kapitel 2.1 Technische Grundlagen). Die ZfDR empfiehlt die bevorzugte Nutzung des Formates „PDF/A-2a“, tagged PDFs und die Vermeidung grafischer Elemente. Dies stellt sicher, dass die Dokumente von den anfragenden Personen - falls gewünscht - langfristig archiviert werden können und auch Personen mit Einschränkungen die Inhalte für sich bspw. mithilfe eines Screenreaders zugänglich machen können.

Diese PDF-Dokumente werden jeweils in einem eigenen weiteren Part der Multipart Response übermittelt. Jeder dieser weiteren Teile, muss einen "Content-Disposition"-Header enthalten, in dem wiederum ein zusätzlicher "name"-Parameter vorhanden sein muss. Der Wert dieses "name"-Parameters muss identisch zu einem der standmitteilung_referenz Werte in den JSON-Anspruchsdaten sein. Darüber stellt die ZfDR die Beziehung zwischen den strukturierten Daten und dem PDF-Dokument her. Es ist zulässig, dass dieselbe Standmitteilung von mehr als einem Anspruch aus den strukturierten Daten referenziert wird. Es muss allerdings darauf geachtet werden, dass für jeden Anspruch in den strukturierten Daten ein Dokument referenziert werden kann.

Die einzelnen PDF-Dokumente dürfen die Größe von 2,6 MB je Dokument nicht überschreiten. Für die Gesamtgröße der Multipart Response gibt es derzeit keine Obergrenze.

Beispiel:
Eine Antwort mit z.B. 41 Ansprüchen ist zulässig, solange jedes einzelne der 41 PDF-Dokumente kleiner als 2,6 MB ist. Die Gesamtgröße der Multipart-Response (theoretisch 41 x 2,6 MB = 106,6 MB) spielt dabei keine Rolle.

Hinweis zur Reduzierung der Dateigröße der PDF-Dokumente:

Eine Minimierung der Größe der PDF-Datei ist durch einfache Konfigurationsmöglichkeiten bei der Erstellung von PDFs zu erreichen:

- Farbraum RGB anstelle CMYK
- Einbettung von Schriftarten

Maximale Auflösung von Abbildungen auf 300 dpi bzw. ppi (Bei 300 dpi handelt es sich bereits um eine High-Resolution Auflösung; für Webformate und Bildschirmdarstellungen werden sogar nur 72 dpi empfohlen)

4 Fehlerrückmeldung

4.1 Ablauf einer Fehlerrückmeldung

Im Nachgang zu einer Anfrage kann es zu einer Reihe von Fehlern bei der Anwortverarbeitung durch die ZfDR kommen. Da es im HTTP-Protokoll nicht vorgesehen ist, dass der Client Fehlerstatuscodes an den Server übermittelt, muss die Vorsorgeeinrichtung einen Fehler Webservice Endpunkt zur Verfügung stellen, an welchen die ZfDR einen Fehler mittels HTTP POST Request übermittelt. Der Fehlerendpunkt kann auf dem gleichen Server hinterlegt sein, auf dem sich auch die Anfrageendpunkt befindet.

Im Body dieser Nachricht wird eine einfache JSON Struktur mit den folgenden Attributen übermittelt:

Attribut	**Inhalt/Bedeutung**
ursprung_anfrage_id	In diesem Attribut wird die Anfrage ID (vgl. X-Anfrage-Id Header der Anfrage) der Anfrage übermittelt, zu der der Fehler aufgetreten ist. Diese ID ermöglicht es dem Unternehmen, eine Zuordnung zu einer fachlichen Anfrage vorzunehmen.
ursprung_request_id	In diesem Attribut wird die Request ID (vgl. X-Request-Id Header der Anfrage) der Anfrage übermittelt, zu der der Fehler aufgetreten ist. Diese ID ermöglicht es dem Unternehmen, eine Zuordnung zu genau dem Webserviceaufruf vorzunehmen, für den der Fehler aufgetreten ist.
nachfragezaehler	Aktueller Nachfragezähler (vgl. den "X-Nachrfagezaehler"-Header in der Anfrage-API)
max_retry_after	Der restliche Zeitraum (in Sekunden) für eine erneute Nachfrage, den das Unternehmen im "Retry-After"-Header der 202-Antwort nicht überschreiten durfte.
fehlernummer	Gibt an, welcher Fehler aufgetreten ist.

Tabelle 4: Attribute der Fehlermeldung

Die gültigen Fehlernummern und Beschreibungen sind in der Anlage ‚ZfDR – Datenbeschreibung' (vgl. Kapitel 0.6 'Referenzierte Dokumente') aufgelistet. Die folgende Tabelle beschreibt mögliche Ursachen.

Ab/seit Einsatzzeitpunkt lt. ZfDR Newsletter (ggf. sind neuere Newsletter ab Dezember 2025 zu beachten) sendet die ZfDR den zusätzlichen Header X-Max-Retry-After. Die Attribute „nachfragezaehler" und „max_retry_after" sind ab diesem Einsatzzeitpunkt zwingender Bestandteil und müssen von den Vorsorgeeinrichtugnen angenommen werden können. Vorher werden diese von der ZfDR nicht gesendet.

Es wird empfohlen, die Wert-Behandlung von „nachfragezaehler" und „max_retry_after" in einem IF (Bedingungsprüfung) zu prüfen und als Fallback-Default jeweils 5 (Nachfragezähler) und 5-Tage in Sekunden (Max-Retry-After) zu nehmen.

Fehlernummer	Bedeutung/Ursache
_0001	**JSON Schemaverstoß:** Dieser Fehler bedeutet, dass im JSON Element der Multipart Response entweder keine Daten enthalten waren, oder diese nicht dem vereinbarten und veröffentlichten Schema entsprachen (als OpenAPI3.0).
_0002	**PDF Größenverstoß:** Mindestens eines der gesendeten PDF-Dokumente überschreitet die maximal zulässige Größe von 2,6 MB.
_0003	**Standmitteilung nicht zuordenbar/fehlt:** Zu mindestens einem der in den JSON Daten übermittelten Ansprüchen der Fallgruppen b-d konnte kein passendes PDF-Dokument gefunden werden. In den JSON Daten war möglicherweise ein "standmitteilung_referenz"Attribut angegeben, zu dem es keinen entsprechenden Multipart Teil mit einem übereinstimmenden "name"-Parameter im "Content-Disposition"-Header gab. Eine andere Ursache für diesen Fehler kann ein angehängtes PDF-Dokument ohne entsprechende Referenz aus dem JSON sein. Eine weitere mögliche Ursache ist das Vorhandensein von zwei oder mehr PDF-Dokumenten mit einem gleichen Wert im "name"-Parameter des "Content-Disposition"-Headers. D.h. jedes in der Multipart-Response vorhandene PDF-Dokument muss mindestens einmal referenziert werden und zu jeder Referenz muss genau ein passendes Dokument vorhanden sein. **Hinweis**: Mehrere Ansprüche dürfen durchaus auf die gleiche Dokumentenreferenz verweisen.
_0004	**PDF-Formatfehler**: Mindestens eines der angehängten PDF-Dokumente entsprach nicht dem geforderten Format PDF. Beispielsweise ist das angehängte Dokument kein PDF-Dokument oder in mindestens einer Multipart Response sind keine Daten enthalten.
_0005	**JSON fehlt oder nicht eindeutig:** Dieser Fehler tritt auf, wenn nicht genau ein Element (mit Content-Type application/json Daten) der Multipart Response JSON Daten enthält. In der Multipart Response sind einmal JSON Daten enthalten. Der Fehler tritt auf, wenn keine (null) oder mehr als einmal JSON Daten enthalten sind.

_0006	Unzulässigen retry-after-Zeitraum vorgegeben Die Nachricht der Vorsorgeeinrichtung mit Statuscode http202 kann nicht akzeptiert werden, da der avisierte Zeitpunkt der erneuten Anfrage außerhalb des definierten Retry-After-Zeitraums von fünf Tagen liegt.

Tabelle 5: Fehlernummern

Im Fall eines Fehlers am VZ01-Datensatz (laut Fehlerkatalog) wird von der ZfDR noch eine letzte Nachfrage auf fünf Tage nach der ersten Anfrage terminiert, um ggf. eine kurzfristige Fehlerkorrektur durch die Vorsorgeeinrichtung wirksam ermöglichen zu können. Im Fall eines technischen Fehlers oder unbekannten Statuscodes wird eine erneute Anfrage nach 12 Stunden ausgelöst, sofern die maximale Anzahl an Anfrageversuchen noch nicht ausgeschöpft ist.

4.2 Ablauf bei technischen Fehlern/unbekannten Statuscodes

Neben den in den vorhergehenden Kapiteln erläuterten erwarteten Abläufen gibt es grundsätzlich noch eine Reihe nicht erwarteter Ergebnisse/Verhaltensweisen, beispielsweise dann, wenn technische Komponenten nicht korrekt funktionieren oder es aufgrund anderer Umstände zu tiefer liegenden technischen Problemen kommt.

Dies sind grundsätzlich alle Antworten mit einem Statuscode, der nicht 200, 202 oder 204 entspricht.

Zu diesen Ereignissen zählen z.B.:

- Timeouts beim Verbindungsaufbau oder unerwartete Verbindungsabbrüche
- Fehler bei der Verifikation des Serverzertifikates (ungültig, abgelaufen, nicht vorhanden…)

In allen o.g. Fällen wird die ZfDR automatisch einen erneuten Versuch auf 12 Stunden nach dem Ereignis terminieren und eine erneute Anfrage nach 12 Stunden auslösen, sofern die maximale Anzahl an Anfrageversuchen noch nicht ausgeschöpft ist.

5 Anbindung einer Vorsorgeeinrichtung

5.1 Erstmalige Anbindung einer Vorsorgeeinrichtung

Grundsätzlich ist eine Anmeldung einer Vorsorgeeinrichtung an die ZfDR dann ratsam, wenn die Vorsorgeeinrichtung anschließend auch produktive Daten bei entsprechenden Anfragen durch Nutzerinnen und Nutzer übermitteln kann.

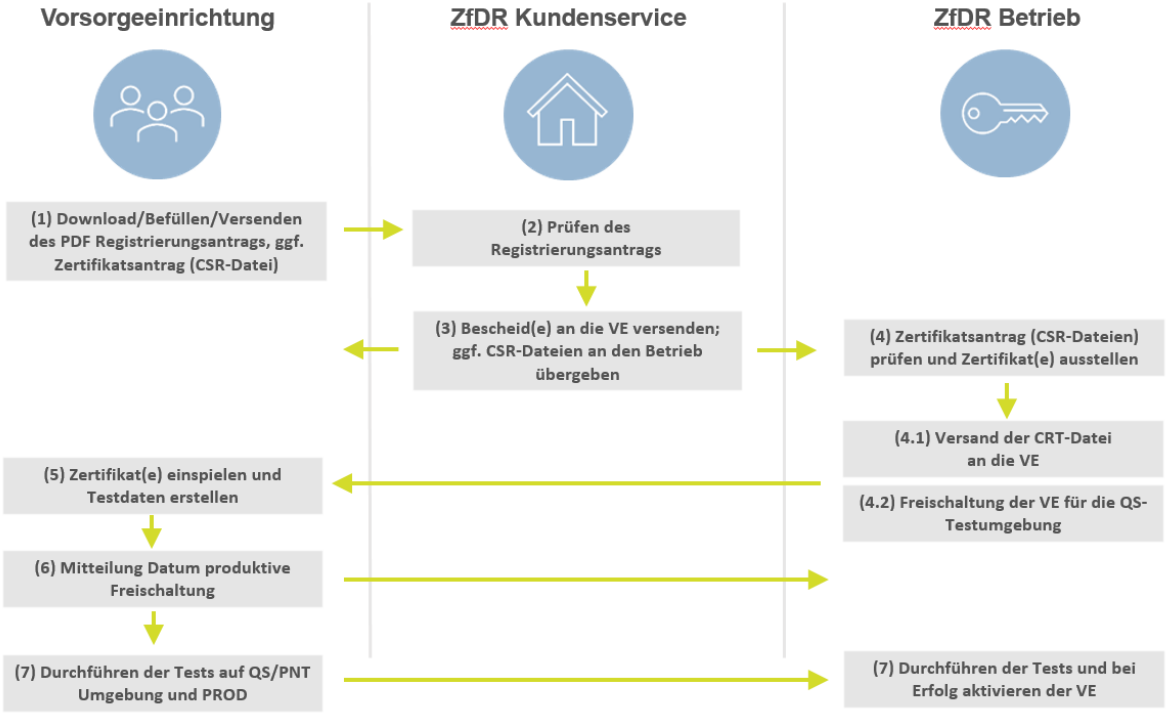

Abbildung 3: Übersicht Anbindungsprozess

Die Anbindung der Vorsorgeeinrichtung an die Digitalen Rentenübersicht erfolgt nach dem oben dargestellten Ablauf in sechs Schritten, die nachfolgend erläutert werden:

1. Initiiert wird die Anbindung durch Befüllung und Versand des PDF-Anmeldungsformulars seitens der Vorsorgeeinrichtung an die ZfDR. Hiermit bestätigt die Vorsorgeeinrichtung ihren Anbindungswillen und übermittelt die zur Anbindung notwendigen Informationen an die ZfDR. Das PDF-Anbindungsformular steht zum Download auf dem Internetauftritt der ZfDR bereit (https://zfdr-vorsorgeeinrichtungen.drv-bund.de). Das Formular wird mit allen erforderlichen Anlagen per E-Mail an den Postkorb zfdr-anbindung@drv-bund.de gesendet.

   Weitere Informationen zum Anmeldeformular sind dem Kapitel 5.2 'Erläuterungen zum Anbindungsformular' zu entnehmen.

   Im Rahmen dieser Anmeldung übermittelt die Vorsorgeeinrichtung folgende Daten und Unterlagen an die ZfDR:

- Formular „Anbindungsformular“
- Ggf. „Anlage zur Verbundsanbindung“
- Ggf. Nachweis für Vertretungsmacht
- Ggf. Nachweis(e) zur Produktart
- Ggf. CSR-Datei(en) als ZIP verpackt

2. Der Kundenservice der ZfDR prüft daraufhin die Plausibilität und Vollständigkeit der Daten. Hierbei vergibt die ZfDR für die Vorsorgeeinrichtung eine individuelle Kundennummer (numerisch, in der Form XX-XXXXXXX-X), die für die zukünftige Korrespondenz zwischen der Vorsorgeeinrichtung und ZfDR als Aktenzeichen dient.

   Die Sachbearbeitung bei der ZfDR muss sich eine eigene Überzeugung über das Vorliegen der gesetzlichen Voraussetzungen für eine Anbindung des Antragstellers als Vorsorgeeinrichtung bilden, sodass keine vernünftigen Zweifel mehr verbleiben. Sollte der Kundenservice Fragen zum ausgefüllten Anbindungsformular haben, wird Kontakt zum fachlichen bzw. technischen Ansprechpartner aufgenommen.

   Kann eine anbindungswillige Person/Stelle glaubhaft machen, dass sie zu einer Anbindung an das Verfahren der ZfDR berechtigt ist, wird sie zugelassen.
   Kann eine anbindungswillige Person/Stelle nicht zweifelsfrei glaubhaft machen, dass sie zu einer Anbindung an das Verfahren der ZfDR berechtigt ist, muss sie abgelehnt werden. In diesem Fall wird die Begründung im Ablehnungsbescheid (s.u.) beschrieben.

3. Das Ergebnis des Antrags auf Anbindung wird der beantragenden Person per Bescheid zugestellt. Auch bei einer Verbundsanbindung werden die Bescheide für die einzelnen Vorsorgeeinrichtungen an die beantragende Person gesendet.

Im Rahmen des Anbindungsprozesses werden zwischen der Vorsorgeeinrichtung und der ZfDR Zertifikate ausgetauscht. Wurde im Anbindungsprozess ein Zertifikatsantrag (CSR-Datei) eingereicht, erstellt der Betrieb der ZfDR ein entsprechendes Serverzertifikat. Die ZfDR verwendet ein Clientzertifikat, um ihre Identität und damit die Berechtigung auf die Endpunkte zuzugreifen, zu beweisen. Die Server der ZfDR werden mit öffentlich prüfbaren Zertifikaten versehen, sodass die Vorsorgeeinrichtungen prüfen können, ob eine Anfrage wirklich von einem Server der DRV-Bund ausgeht und umgekehrt. Die ZfDR stellt der Vorsorgeeinrichtung den öffentlichen Teil des Zertifikats zur Verfügung, damit die Vorsorgeeinrichtung eine Prüfung der Signatur vornehmen kann (zum Download verfügbar unter https://zfdr-vorsorgeeinrichtungen.drv-bund.de). Jede Vorsorgeeinrichtung benötigt außerdem ihrerseits für jeden Server, der als Endpunkt dient, ein Serverzertifikat, mit dem durch die ZfDR beim Aufruf der Webservices geprüft werden kann, ob tatsächlich der erwartete Service aufgerufen wird. Dieses Zertifikat wird durch das ZfDR Betriebsteam im Verbund mit dem DRV Trust Center vergeben. Außerdem wird auf Basis dieses Zertifikates die TLS-Verschlüsselung initiiert. Die ZfDR übersendet das Serverzertifikat an die Vorsorgeeinrichtung und stellt anschließend Ihre Systeme für die fachlichen und technischen Tests bereit. Die Freischaltung für Tests in der PNT oder Produktionsumgebung erfolgt nach

Aufforderung durch die Vorsorgeeinrichtung. Im Regelfall ist diese innerhalb einer Arbeitswoche abgeschlossen.

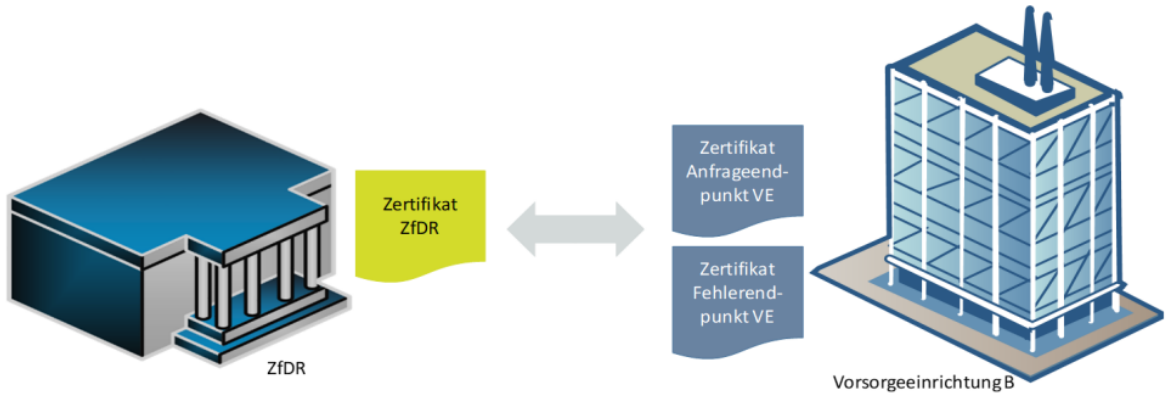

Abbildung 4: Zertifikate für die produktive Anbindung

Die Zertifikatsausstellung erfolgt für die produktive Umgebung und die Testumgebung (PNT/QS-Umgebung) jeweils separat.

> **HINWEIS:**
>
> IT-Dienstleister, die ein Zertifikat für mehrere Vorsorgeeinrichtungen nutzen, erhalten ihr Zertifikat für den Server über die erste anzubindende Vorsorgeeinrichtung. Ein IT-Dienstleister hat im Anbindungsprozess bei der ZfDR keine eigene Rolle und tritt nur implizit über die Vorsorgeeinrichtung auf.
>
> In der produktiven Anbindung können Anfrageendpunkt und Fehlerendpunkt auf unterschiedlichen Servern liegen. Dadurch können zwei Zertifikate der Vorsorgeeinrichtung erforderlich sein. In der Testanbindung müssen Anfrageendpunkt und Fehlerendpunkt auf einem Server liegen und es gibt nur ein Zertifikat.

Weitere Informationen hierzu sind Kapitel 6 'Zertifikate' zu entnehmen.

4. Die Vorsorgeeinrichtung spielt die Zertifikate in die jeweiligen Umgebungen (QS bzw. Produktionsnahe Testumgebung (PNT) und Produktionsumgebung) ein und erstellt die für die Tests notwendigen Daten. Details zum Testvorgehen werden in Schritt 6 und im Kapitel 7 ‚Beschreibung des Testvorgehens' näher beschrieben.
5. Die Vorsorgeeinrichtung muss dem Betrieb der ZfDR das Datum der gewünschten Produktivschaltung mitteilen.
6. Zum abgestimmten Termin erfolgen die Schnittstellentests im bilateralen Austausch mit technischen Ansprechpartnern der Vorsorgeeinrichtung via Telefon bzw. Videokonferenz. Dabei erfolgt ein

   ⇨ **Kommunikationstest** in der QS-/PNT-Umgebung zur Überprüfung der Akzeptanz und Verarbeitung der Antwortdatensätze (optional) und ein

   ⇨ **Verbindungstest** in der produktiven Umgebung zum Test der Verbindungsstrecke (erforderlich für die Produktivsetzung).

Der Verbindungstest wird auch vorgenommen, wenn keine Einbindung neuer Zertifikate erforderlich ist (insb. relevant für Dienstleister).

Erhält die ZfDR nicht die erwarteten Antworten in den Schnittstellentests, dann wird der Fehler gemeinsam geklärt und der entsprechende Test wird wiederholt.

HINWEIS:

Nach erfolgreichen Schnittstellentests muss sich die Vorsorgeeinrichtung beim Kundenservice der ZfDR melden und ein gewünschtes Datum der Aktivierung angeben. Diese Aktivierungen finden grundsätzlich am Montag statt und können bis 12 Uhr des vorausgehenden Freitags angemeldet werden.

Ab diesem Zeitpunkt (Montag) muss die Vorsorgeeinrichtung mit Anfragen von Nutzerinnen und Nutzern der Digitalen Rentenversicherung rechnen.

Die Vorsorgeeinrichtung wird auf dem Internetauftritt der ZfDR öffentlich einsehbar gelistet.

Weitere Informationen zum Testvorgehen sind Kapitel 7 'Beschreibung des Testvorgehens' zu entnehmen.

Einzelanbindung:	Anbind. über gemeinsamen Server:	Verbundsanbindung:
• Eine VE bindet sich an, ohne Verbund oder gemeinsame Server	• Eine VE bindet sich an und nutzt den Server eines Dienstleisters	• Ein Verbund bzw. Konzern bindet sich an und hat nachgeordnete VE
• Name der VE im Anbindungsformular	• Name der VE im Anbindungsformular	• Name des Verbunds bzw. Konzerns im Anbindungsformular
• Keine Anlage Verbundsanbindung	• Keine Anlage zur Verbundsanbindung	• Anlage zur Verbundsanbindung erforderlich
• Immer individueller Server und individuelle URL	• Eine eigene URL wird genutzt – auf einem Server, den auch andere VE nutzen können	• Ein Server und eine URL für alle VE in diesem Verbund ggf. je Anfrage- und Fehlerendpunkt
• Zertifikat immer erforderlich (CSR/CRT)	• Zertifikat (CSR/CRT) nur für die erste VE erforderlich, die diesen Server nutzt, für alle Weiteren kein Zertifikat erforderlich	• Zertifikat nur für Verbund erforderlich (CSR/CRT), sofern nicht zusätzlich auch über IT-Dienstleister angebunden
• Ein Bescheid	• Ein Bescheid	• Mehrere Bescheide

Abbildung 5: Gegenüberstellung der unterschiedlichen Anbindungen

5.2 Erläuterungen zum Anbindungsformular

Bitte beachten Sie:

- ⇨ Der PDF-Antrag wird bevorzugt elektronisch ausgefüllt und versendet. Es bedarf dann keiner Unterschrift.
- ⇨ Alle Änderungen in den der Anbindung als Vorsorgeeinrichtung an die Zentrale Stelle für die Digitale Rentenübersicht (ZfDR) zugrundeliegenden Verhältnissen sind unverzüglich der ZfDR mitzuteilen.

Bezeichnung	Hinweise
Grunddaten der Vorsorgeeinrichtung	
Name der Vorsorgeeinrichtung (inkl. Rechtsform) bzw. des Konzerns bzw. Konzernverbundes	In diesem Feld gibt die Vorsorgeeinrichtung ihren Namen oder im Fall eines Konzerns bzw. Verbundes, der direkt mehrere Vorsorgeeinrichtungen anbinden möchte, den Namen des Konzerns/Verbundes ein. Maßgeblich ist die juristisch korrekte Bezeichnung. Der hier eingegebene Name wird auf dem Portal der ZfDR angezeigt. **Art**: Pflicht
Alternative Unternehmensbezeichnungen für die Nutzersuche	Eine Eingabe in diesem Feld soll die Auffindbarkeit der Vorsorgeeinrichtung bei abweichenden Sucheingaben unterstützen. Das Feld ist nicht zwangsläufig für die Anzeige in der Digitalen Rentenübersicht vorgesehen. Es muss sich nicht um eine juristisch korrekte Bezeichnung handeln, könnte aber geläufige Abkürzungen oder umgangssprachliche Bezeichnungen beinhalten. Es können auch mehrere Bezeichnungen eingegeben werden. Die Information wird getrennt durch Komma und ein Leerzeichen eingegeben. **Art**: optional
Rechtsform	**Art**: Pflicht sofern vorhanden
Handelsregisternummer	Die Angabe ist in Verbindung mit der Angabe ‚Registergericht' gemeinsam zu betrachten. Beides ist ggf. auszufüllen **Art**: optional
Registergericht	Das zuständige Amtsgericht ist einzutragen. **Art**: optional
Zahl der Altersvorsorgeansprüche	Die geschätzte Anzahl der Altersvorsorgeansprüche ist einzutragen, die gegenüber der sich anmeldenden Vorsorgeeinrichtung bestehen. **Art:** Pflicht

Checkbox	„Ich möchte eine Verbundsanbindung vornehmen. Die Anlage zur Verbundsanbindung sowie geeignete Nachweise sind beigefügt.“ In diesem Fall ist die ‚Anlage zur Verbundsanbindung‘ beizufügen.
Ladungsfähige Anschrift der Vorsorgeeinrichtung	
Straße, Hausnummer, PLZ und Ort	In diesen Feldern soll die ladungsfähige Anschrift der anbindungswilligen Stelle eingetragen werden. Die Adresse sollte mit der Adresse in anderen Quellen (bspw. Impressum der Website der Vorsorgeeinrichtung, Zertifizierungsliste des BZSt, Handelsregister) übereinstimmen. **Art**: Pflicht, falls vorhanden
Postfach	Sollte es sich bei der ladungsfähigen Adresse um ein Postfach handeln, ist das Postfach in diesem Feld einzutragen. **Art:** Pflicht, falls vorhanden
Angabe zur handelnden Person	
Unternehmensname	Das Feld ist anzugeben, wenn die handelnde Person, die die Willenserklärung zur Anbindung bei der ZfDR nicht MitarbeiterIn der Vorsorgeeinrichtung ist. Dies kann beispielsweise dann der Fall sein, wenn die (ggf. mit der Vertretungsmacht ausgestattete) handelnde Person einem externen Dienstleister angehört. **Art**: optional
Name	**Art**: Pflicht
Vorname	**Art**: Pflicht
E-Mailadresse	Mit dieser E-Mailadresse wird der Kundenservice der ZfDR ggf. aktiv kommunizieren und ggf. den Bescheid über die Anbindung zuleiten. **Art**: Pflicht
Telefonnummer	**Art**: Pflicht
Dienstlicher Aufgabenbereich	Der dienstliche Aufgabenbereich eines Beauftragten ergibt sich in aller Regel aus Geschäftsordnung und Geschäftsverteilungsplan. **Art**: Pflicht

Nachweis zur Vertretungsmacht	
Angabe zur Vertretung	**Art**: Pflicht Im Regelfall wird auf Ebene der Vorsorgeeinrichtung eine juristische Person (bspw. AG oder GmbH) durch eine natürliche Person (bspw. organschaftlicher Vertreter, besonders Beauftragter oder Bevollmächtigter) vertreten. Letztlich geht es um die ununterbrochene Legitimationskette von der handelnden Person zu den anzubindenden Stellen. Aus dem Nachweis soll erkennbar sein, dass die s.o. eingetragene handelnde Person (ggf. Bevollmächtigte) berechtigt ist, im Namen der Vorsorgeeinrichtung Willenserklärungen abzugeben. Bei Bedarf nimmt die Sachbearbeitung der ZfDR für weitere Unterlagen Kontakt mit der Vorsorgeeinrichtung auf. **Die Vorsorgeeirichtung fügt dem Antrag ggf. einen Nachweis als Anlage bei.** Im Verwaltungsverfahren kann sich ein Beteiligter durch einen Bevollmächtigten vertreten lassen. Die Vollmacht ermächtigt zu allen das Verwaltungsverfahren betreffenden Verfahrenshandlungen, sofern sich aus ihrem Inhalt nicht etwas anderes ergibt. Der Bevollmächtigte hat auf Verlangen seine Vollmacht schriftlich nachzuweisen (§ 14 Absatz 1 Satz 1 bis 3 VwVfG). Ein Muster für die Bevollmächtigung eines Dritten im Sinne des § 7 Absatz 2 Satz 2 RentÜG kann seitens der ZfDR nicht zur Verfügung gestellt werden. Die Ausgestaltung der (vertrags-)rechtlichen Beziehungen zu Dritten obliegt der anbindungswilligen Stelle.
Produktarten und weitere Checkboxen	
Von der Vorsorgeeinrichtung angebotene Produktarten	Mindestens eine Checkbox muss die anbindungswillige Stelle bei Absenden der Informationen auswählen. **Art**: Pflicht (mindestens eine)

Produktnachweise	Diese Checkbox soll daran erinnern, bei Bedarf geeignete Nachweise für eine der ausgewählten Produktarten als Anlage beizufügen. Im Zweifelsfall reicht es aus, wenn eine Produktart nachgewiesen wurde. Nicht jede angekreuzte Produktart muss nachgewiesen werden. Bei Bedarf nimmt die Sachbearbeitung der ZfDR für weitere Unterlagen Kontakt mit der Vorsorgeeinrichtung auf.
Erklärung	
Willenserklärung zur Anbindung	Die Willenserklärung der handelnden Person für die anbindungswillige Stelle wird durch eine Checkbox abgegeben. Diese muss die handelnde Person bei Absenden der Informationen auswählen, anderenfalls ist keine positive Entscheidung über den Antrag möglich. **Art**: Pflicht
Einwilligung zur Übermittlung elektronischer Schriftstücke	Das Feld beschreibt, ob Bescheide usw. wirksam per E-Mail an die Vorsorgeeinrichtung übermittelt werden dürfen (Zugangseröffnung für elektronische Schriftstücke). Dadurch wird der Bescheid später nicht als Brief versandt, sondern per E-Mail. Die ZfDR ist bestrebt, Papier zu vermeiden und bittet daher darum, diese Einwilligung grundsätzlich mit einem Kreuz zu bestätigen. **Art**: optional
Sonstiges	
Ansprechpartner*in Unternehmenskommunikation	Dieses Feld ist anzugeben, wenn die Vorsorgeeinrichtung entsprechendes Informations- und Kommunikationsmaterial von der ZfDR erhalten möchte. **Art:** optional
Angaben zum technischen Ansprechpartner	
Unternehmensname	Das Feld ist anzugeben, wenn der technische Ansprechpartner nicht Mitarbeiter der Vorsorgeeinrichtung ist. Dies kann beispielsweise dann der Fall sein, wenn der technische Ansprechpartner von einem beauftragten Dritten nach § 7 Absatz 2 Satz 2 RentÜG (IT-Dienstleister) bereitgestellt wird. **Art**: optional

Name	**Art**: Pflicht
Vorname	**Art**: Pflicht
E-Mailadresse	**Art**: Pflicht
Telefonnummer	**Art**: Pflicht
Bevorzugtes Testdatum	Unabhängig von dem eingetragenen Datum können abweichende oder weitere Termine zum Test vereinbart werden. Dieses Datum dient zur Priorisierung der Tests. **Art:** Pflicht
Hauptkategorie: Angaben zum technischen Endpunkt	
‚Anfrage-Endpunkt-URL' Funktionsfähige URL[2] für Anspruchsdaten	Hier gibt die Vorsorgeeinrichtung eine funktionsfähige URL für den Anfrage-Endpunkt an, welche die Vorsorgeeinrichtung als Schnittstelle mit der ZfDR verbindet. Diese soll folgendermaßen beginnen: https:// Underscores in den URL's sind unzulässig -> Underscore "_" = unzulässiges Zeichen **Achtung: Es handelt sich hierbei nur um die BASIS URL, die von der ZfDR im Fall einer Anfrage oder Fehlerrückmeldung um die jeweiligen Pfade ergänzt wird ‚/anspruchsdaten' bzw. /fehlerrueckmeldung'.** → **siehe auch die Open-API-Schnittstellenbeschreibung** **Art**: Pflicht

[2] Uniform Resource Locator (Abk. URL; englisch für einheitlicher Ressourcenzeiger); Das ist der Pfad bzw. die Zieladresse, unter welcher ein Server bzw. eine bestimmte abgelegte Information (bspw. eine bestimmte Website) zu erreichen ist.

‚Fehler-Endpunkt-URL' Funktionsfähige URL für Fehlerrückmeldungen	Hier gibt die Vorsorgeeinrichtung eine funktionsfähige URL für den Fehler-Endpunkt an, welche die Vorsorgeeinrichtung als Schnittstelle mit der ZfDR verbindet. Underscores in den URL's sind unzulässig -> Underscore "_" = unzulässiges Zeichen Es ist auch möglich, dass die Vorsorgeeinrichtung für Anspruchsdaten und Fehlerrückmeldungen nur einen Server nutzt und keine abweichende Fehler-Endpunkt-URL erforderlich ist. In diesem Fall wird lediglich eine URL und ein Zertifikat vorgegeben und dieses zweite URL Feld bleibt leer. Achtung: Es handelt sich hierbei nur um die BASIS URL, die von der ZfDR im Fall einer Anfrage oder Fehlerrückmeldung um die jeweiligen Pfade ergänzt wird ‚/anspruchsdaten' bzw. ‚/fehlerrueckmeldung'. → siehe auch die Open-API-Schnittstellenbeschreibung **Art**: optional
Checkbox Zertifikatsantrag für Anspruchsdaten	Ist diese Checkbox ausgefüllt, benötigt die ZfDR als Anlage einen Zertifikatsantrag in Form einer CSR [3]-Datei. Diesen fügt die Vorsorgeeinrichtung als ZIP-verpackte Anlage den Antragsunterlagen bei. Die CSR-Datei ist nur dann nicht zu befüllen, wenn die Vorsorgeeinrichtung über einen Dritten angebunden wird, dessen Serveradresse (s.o. URL) **mit genau dem angegebenen Hostname** bei der ZfDR bereits verwendet wird. Nutzt eine Vorsorgeeinrichtung den gleichen Server aber eine abweichende Subdomain als eine andere Vorsorgeeinrichtung, ist ein separater Zertifikatsantrag erforderlich. **Art**: optional **Form**: CSR-Datei vom Typ PKCS10

[3] englisch: Certificate Signing Request; Abk.: CSR

Checkbox Zertifikatsantrag für Fehlerrückmeldungen	**Ist diese Checkbox ausgefüllt, benötigt die ZfDR als Anlage einen weiteren Zertifikatsantrag in Form einer CSR-Datei. Diesen fügt die Vorsorgeeinrichtung als ZIP-verpackte Anlage den Antragsunterlagen bei.** Es ist auch möglich, dass die Vorsorgeeinrichtung für Anspruchsdaten und Fehlerrückmeldungen nur einen Server nutzt. In diesem Fall wird lediglich eine URL und ggf. ein Zertifikat vorgegeben. **Art**: optional **Form**: → CSR-Datei vom Typ PKCS10
Checkbox "Für meine Vorsorgeeinrichtung ist bereits ein Server angebunden und ich benötigen keinen weiteren."	Dieses Feld ist immer zu aktivieren, wenn die in der URL genannte Serverbezeichnung mit der gleichen Domain bereits bei einer anderen Anbindung einer Vorsorgeeinrichtung bei der ZfDR verwendet wird. **Art**: optional
Anfrage- Endpunkt-URL (QS- bzw. PNT-Umgebung, optional)‘ Funktionsfähige URL für Anfragen	Vergleichbar mit den URL für die Produktionsumgebung, nur das diese separate URL ausschließlich für den Test genutzt werden soll. Diese Möglichkeit ist freiwillig. Underscores in den URL's sind unzulässig -> Underscore "_" = unzulässiges Zeichen **Art:** optional **Form:** s.o.
Fehler-Endpunkt-URL (QS- bzw. PNT-Umgebung, optional)‘ Funktionsfähige URL für Fehlerrückmeldungen	Vergleichbar mit den URL für die Produktionsumgebung, nur das diese separate URL ausschließlich für den Test genutzt werden soll. Diese Möglichkeit ist freiwillig. Underscores in den URL's sind unzulässig -> Underscore "_" = unzulässiges Zeichen **Art:** optional **Form:** s.o.

Checkbox Zertifikatsantrag für Anspruchsdaten QS/PNT-URL	Ist diese Checkbox ausgefüllt, benötigt die ZfDR als Anlage einen weiteren Zertifikatsantrag in Form einer CSR-Datei. Diesmal allerdings für den Test (freiwillig). Diesen fügt die Vorsorgeeinrichtung als ZIP-verpackte Anlage den Antragsunterlagen bei. **Art:** optional **Form:** CSR-Datei vom Typ PKCS10; ZIP-verpackt
Checkbox Zertifikatsantrag für Fehlerrückmeldungen QS/PNT-URL	Ist diese Checkbox ausgefüllt, benötigt die ZfDR als Anlage einen weiteren Zertifikatsantrag in Form einer CSR-Datei. Diesmal allerdings für den Test (freiwillig). Diesen fügt die Vorsorgeeinrichtung als ZIP-verpackte Anlage den Antragsunterlagen bei. **Art:** optional **Form:** CSR-Datei vom Typ PKCS10; ZIP-verpackt
Checkbox "Für meine Vorsorgeeinrichtung ist bereits ein QS- bzw. PNT-Server angebunden und ich benötige keine weiteren Zertifikate."	Dieses Feld ist immer zu aktivieren, wenn die in der URL genannte Serverbezeichnung mit der gleichen Domain bereits bei einer anderen Anbindung einer Vorsorgeeinrichtung bei der ZfDR verwendet wird. Siehe oben, nur für die QS-/PNT-Umgebung. **Art:** optional
Angaben zum Durchführungsverantwortlichen **E-Mail**	Diese E-Mailadresse wird benötigt, um die automatisierten Tests durchzuführen. Ohne diese Angabe würde die automatisierte Testanforderung auf Fehler laufen und der Tester erhält keine Rückmeldung. **Art:** optional

Tabelle 6: Ausfüllhilfe zum Anbindungsformular

5.3 Anbindung von Dienstleistern

Eine Kennzeichnung von Anbindungen über Dienstleister wird bei der ZfDR nicht vorgenommen. Für die ZfDR ist unerheblich, ob die Webserviceendpunkte von einem Dienstleister oder dem Unternehmen selbst zur Verfügung gestellt werden. Unternehmen/Dienstleister sind frei in ihrer Entscheidung, wie sie den Endpunkt benennen und ggf. Einzelunternehmen über unterschiedliche Pfade oder ähnliches abbilden.

5.4 Umwandlung von Unternehmen (insbesondere Fusion)

Vorsorgeeinrichtungen können als Unternehmen Gegenstand von Umstrukturierungsmaßnahmen sein, die Auswirkungen auf Altersvorsorgeansprüche und ihre Anbindung bei der ZfDR haben können. Zu den möglichen Umstrukturierungsmaßnahmen zählen die Umwandlung durch Verschmelzung (Fusion), Spaltung und Vermögensübertragung. Akteure dieser Umwandlungsarten sind jeweils Vermögen übertragende Vorsorgeeinrichtungen auf der einen und übernehmende Vorsorgeeinrichtungen auf der anderen Seite.

Die Umwandlung kann in rechtlicher Hinsicht die Erteilung von Anbindungs- und Rücknahmebescheiden („Abbindungsbescheiden“) erforderlich machen und sich in technischer Hinsicht auf die Nutzung von Schnittstellen auswirken.

Durch die Vornahme einer Fusion bzw. die umwandlungsbedingte Beendigung einer Vorsorgeeinrichtung bei der ZfDR können Kommunikationsschnittstellen geklärt und Informationen an Nutzende der Digitalen Rentenübersicht gesteuert werden. Zudem bietet sie die Möglichkeit, die alternativen Unternehmensbezeichnungen zu klären und den Rechtsnachfolger bei der ZfDR abzulegen.

5.4.1 Meldung einer Umwandlung

Um einen reibungslosen Bearbeitungsprozess sicherzustellen, ist eine rechtzeitige Meldung an die ZfDR notwendig. Es wird empfohlen, bei einer geplanten Umwandlung mindestens 8 Wochen im Voraus alle zur Bearbeitung notwendigen Unterlagen auf dem üblichen Weg einzureichen (Kontakt: zfdr-anbindung@drv-bund.de). Wenn keine rechtzeitige Meldung erfolgt oder unvollständige Unterlagen eingereicht werden, wird keine fristgerechte Bearbeitung gewährleistet.

Insbesondere ist darzulegen, ob die bei der Digitalen Rentenübersicht angebundene Vorsorgeeinrichtung ihre Rechtspersönlichkeit ändert oder ein bloßer Rechtsformwechsel vorliegt. Die vorliegenden Dokumente werden auf Plausibilität geprüft, wobei der Handelsregisterauszug oder eine Meldung der BaFin geeignete Nachweise sind. Bleibt die Handelsregisternummer des Unternehmens unverändert, bleibt auch dessen Rechtsidentität erhalten. Andersherum lässt allein der Wechsel der Handelsregisternummer noch nicht mit Sicherheit auf eine Änderung der rechtlichen Identität schließen, da ein solcher auch bei einem Sitzwechsel in einen anderen Gerichtsbezirk und einem Formwechsel von einer Personen- in eine Kapitalgesellschaft begründet sein kann. Bei Unklarheiten versendet die ZfDR ein formloses Anhörungsschreiben, um den Sachverhalt aufzuklären.

Den maßgeblichen Zeitpunkt der Umsetzung vereinbart die Vorsorgeeinrichtung individuell mit der ZfDR. Es ist zu beachten, dass die technische Durchführung einer Unternehmensfusion und weiterer Umwandlungsarten bei der ZfDR nur möglich ist, wenn bereits beide Vorsorgeeinrichtungen bei der ZfDR angebunden sind.

Aufgrund komplexer Fallgestaltungen wird jede Umwandlung einer Vorsorgeeinrichtung individuell betrachtet und in enger Abstimmung mit dem Kundenservice behandelt.

5.4.2 Weitere Schritte

Unternehmensbezeichnungen: Wenn sich der Name der Vorsorgeeinrichtung durch eine Umwandlung ändert, sollten alternative Unternehmensbezeichnungen entsprechend an die

ZfDR übermittelt werden. Auch der „alte“ Name des übertragenden Rechtsträgers wird möglichst als alternative Unternehmensbezeichnung für den neuen (übernehmenden) Rechtsträger genutzt. Auf diese Weise können Nutzende der Digitalen Rentenübersicht die Vorsorgeeinrichtung auch nach durchgeführter Fusion auf der Ergebnisliste der Webseite finden.

Schnittstelle: Ist die übernehmende VE bereits angebunden, kann sie ihre bisherige ZfDR-Kundennummer beibehalten und ihre bestehende Schnittstelle weiternutzen. Je nach individuellem Fall ist es auch möglich, dass die bestehende Schnittstelle einer der übertragenden Vorsorgeeinrichtungen für den übernehmenden Rechtsträger genutzt wird.

5.4.3 Verschiedene Fallgestaltungen

5.4.3.1 Fusion

Die Fusion von Vorsorgeeinrichtungen beschreibt die Verschmelzung von mindestens zwei voneinander unabhängigen Vorsorgeeinrichtungen. Dabei übertragen ein oder mehrere Rechtsträger – VE (A) und ggf. VE (B) – ihr gesamtes Vermögen auf einen anderen Rechtsträger – VE (C). Die übertragenden Rechtsträger VE (A) und VE (B) erlöschen infolgedessen. Die Verschmelzung kann durch Übertragung des gesamten Vermögens auf einen bereits bestehenden Rechtsträger (Verschmelzung durch Aufnahme) oder auf einen neuen, hierdurch gegründeten Rechtsträger (Verschmelzung durch Neugründung) erfolgen.

Ist der übernehmende Rechtsträger VE (C) noch nicht an die Digitale Rentenübersicht angebunden, ist dieser nach dem üblichen Anbindungsprozess an die Digitale Rentenübersicht anzubinden.

Eine Fusion wird in der Digitalen Rentenübersicht angezeigt, wenn der Anspruch vor der Fusion abgelegt wurde.

5.4.3.2 Aufspaltung, Abspaltung, Ausgliederung

Eine weitere Form der Unternehmensumwandlung stellt die Spaltung (Aufspaltung/Abspaltung/Ausgliederung) von VE (A) zu VE(B) und VE(C) dar. VE(A) wird beendet oder bleibt bestehen. Diese Umwandlungen können von der ZfDR nicht durch eine Fusion abgebildet werden, sondern müssen gegebenenfalls mit einer Beendigung umgesetzt werden. Die Beendigung wird in der Digitalen Rentenübersicht angezeigt, wenn der Anspruch vor der Fusion abgelegt wurde.

Sind die übernehmenden Rechtsträger VE (B) und VE (C) schon angebunden, können sie ihre bestehenden Anbindungen weiter nutzen. Entsteht erst mit der Übernahme des Vertragsbestands von VE (A) eine Verpflichtung zur Anbindung, ist der übliche Anbindungsprozess durchzuführen.

5.4.3.3 Rechtsformwechsel und Namensänderung

Ein reiner Rechtsformwechsel, bei dem der Rechtsträger seine Identität wahrt und lediglich sein „rechtliches Gewand“ wechselt, stellt ebenfalls einen Fall der Umwandlung dar, hat aber keine Auswirkungen auf die rechtliche Anbindung bei der ZfDR. Hier reicht eine Mitteilung der Bezeichnung mit der neuen Rechtsform inklusive Nachweis sowie der alternativen Unternehmensbezeichnungen. Infolge der Änderung der Stammdaten, erhält die

Vorsorgeeinrichtung eine Änderungsmitteilung. Der neue Name der VE wird in der Digitalen Rentenübersicht angezeigt.

5.4.3.4 Verbundanbindungen

Bei einer Umstrukturierung von Vorsorgeeinrichtungen, die technisch innerhalb eines Verbunds angebunden sind, gelten die gleichen rechtlichen Mechanismen wie bei unabhängigen Vorsorgeeinrichtungen.

Auch bei einem Verbund sind die relevanten Veränderungen mitzuteilen.

Aufgrund von unterschiedlichen Fallkonstellationen ist auch hier jede Veränderung individuell zu betrachten und mit dem Kundenservice der ZfDR abzustimmen.

6 Zertifikate

6.1 Management von Zertifikaten

Zur Absicherung der Kommunikation der ZfDR mit den Vorsorgeeinrichtungen werden Zertifikate eingesetzt, mit denen sich die Server beim Aufbau einer TLS-Verbindung identifizieren.

Die Server der ZfDR werden mit öffentlich prüfbaren Zertifikaten versehen, so dass die Vorsorgeeinrichtungen prüfen können, ob eine Anfrage von einem Server der Deutschen Rentenversicherung ausgeht.

Für die Server der Vorsorgeeinrichtungen werden durch das Trustcenter der Deutschen Rentenversicherung (https://www.deutsche-rentenversicherung.de/Bund/DE/Ueber-uns/Trustcenter/trustcenter_node.html) individuelle Zertifikate ausgestellt.

Die zentrale Erstellung und Verwaltung der Zertifikate durch das Trustcenter der Deutschen Rentenversicherung ermöglicht:

- ein einheitliches Vertrauensniveau
- eine einfache Verwaltung der gültigen Zertifikate
- eine Unterstützung durch den Kundenservice zur Verlängerung und zur Sperrung von Zertifikaten
- eine einheitliche und passende Nutzungspolicy, auf die auch im Zertifikat referenziert wird.

Die Gültigkeitsprüfung dieser Zertifikate erfolgt nur durch die Deutsche Rentenversicherung, eine weitere Verwendung dieser Zertifikate außerhalb dieser Anwendung ist weder erforderlich noch zulässig und wird auch nicht unterstützt.

Client-Zertifikate, die der ZfDR Client zum Aufbau der Verbindung zur Vorsorgeeinrichtung nutzt, werden ausschließlich für die Kommunikation für die Digitale Rentenübersicht genutzt.

Die Root CA (Certificate Authority) wird von der Deutschen Rentenversicherung noch für andere Verfahren genutzt, der Intermediate CA kann von der Vorsorgeeinrichtung für dieses Verfahren grundsätzlich getraut werden.

Nach Möglichkeit soll auf eine Certificate Pinning verzichtet und grundsätzlich allen Zertifikaten der entsprechenden CAs für die Etablierung der Verbindung vertraut werden.

Dazu sollte die intermediate CA als Vertrauensanker verwendet werden. Aufgrund dessen veröffentlicht die ZfDR die CA-Zertifikate und nicht das individuelle Clientzertifikat.

6.2 Anfragen an das Trustcenter

Die Kommunikation zwischen dem Mitarbeitenden der Vorsorgeeinrichtung, der ein Zertifikat erstellen, verlängern oder sperren will und der ZfDR, erfolgt immer über eine Anwendung, die die Berechtigung des Antragstellers zur Auslösung einer entsprechenden Anfrage (derzeit daher eingebettet in den Registrierungsvorgang) und zu bestimmende Eigenschaften der Anfrage bzgl. Form und Inhalt überprüft. Die Anwendung nutzt das REST API der Registration Authority des Trustcenters für die Kommunikation mit dem Trustcenter.

Das Ergebnis der Anfrage wird von der Anwendung verarbeitet und ggf. an den Anfragenden zurück übertragen.

6.3 Beantragung eines Serverzertifikates

Zunächst generiert die Vorsorgeeinrichtung ein Schlüsselpaar **(4096 bit)** für den Verbindungsserver. Dieses Schlüsselpaar verbleibt bei der Vorsorgeeinrichtung. Bei jeder Generierung einer neuen CSR-Datei ist es erforderlich, vorher ein neues Schlüsselpaar zu generieren.

Dann generiert die Vorsorgeeinrichtung eine Zertifikatsanfrage (Certificate Signing Request (CSR)), z.B. mit Hilfe des Programms OpenSSL.

Folgende Attribute werden dabei belegt, die optionalen Attribute müssen nicht belegt werden:

Attribut	Max. Länge	Kodierung	Bedeutung	Festlegung durch	Beispiel
common-Name	64	printableString oder utf8String	vollqualifizierter Servername der VE bzw. des Dienstleisters	VE	server01.drv-dris.pfefferminzia.de
alternative-Name	64	printableString oder utf8String	alternativer Servername der VE	VE	server01.drv-dris.pfefferminzia.de
Organization-Name	64	printableString oder utf8String	Dachorganisation der VE bzw. des Dienstleisters	VE	Pfefferminzia SE
Organization-UnitName	64	printableString oder utf8String	Bereich der VE bzw. des Dienstleisters **(optional)**	VE	Pfefferminzia Pensionskasse
localityName	64	printableString oder utf8String	Ort der VE bzw. des Dienstleisters **(optional)**	VE	Duesseldorf
stateName	64	printableString oder utf8String	Bundesland der VE bzw. des Dienstleisters **(optional)**	VE	Nordrhein-Westfalen
countryName	2	printableString	zulässige Länderkennzei-	VE	DE, CH, IT

Attribut	Max. Länge	Kodierung	Bedeutung	Festlegung durch	Beispiel
			chen gem. Kapitel 6.13		

Tabelle 7: Attribute für Zertifikate

Common-name und alternative-Name müssen identisch sein.

Der CSR darf keine Schlüsselverwendungen (RFC 5280[4] Kapitel 4.2.1.3.) und keine erweiterten Schlüsselverwendungen (RFC 5280 Kapitel 4.2.1.12.) enthalten. Ohne diese Einträge kann der CSR fehlerfrei verarbeitet werden. Die Werte werden vom Trustcenter der DRV automatisch wie folgt richtig gesetzt:

- Key Usage: critical, digitaleSignature und keyEncipherment und
- Extended Key Usage: critical, TLS Web Server Authentication bzw. ServerAuth

Falls für Key Usage im CSR Werte angegeben werden, muss sichergestellt werden, dass

- diese nicht im Widerspruch zur geplanten Verwendung des Zertifikates stehen (s.o.) und
- dass Key Usage und Extended Key Usage nicht im Widerspruch stehen,

(siehe RFC 5280 Kapitel 4.2.1.12).

Die Kombination von Data Encipherment und ServerAuth ist beispielsweise nicht zulässig.

Eine Überprüfung der Attribute des CSR kann mit folgender Kommandozeile erfolgen:

```
openssl req -in test.csr -noout -text | grep -e "X509v3 Key Usage:" -e "X509v3 Extended Key Usage:" - A 1
```

Das Ergebnis

```
X509v3 Key Usage: Key Encipherment, Data Encipherment
X509v3 Extended Key Usage:
TLS Web Server Authentication
```

wäre beispielsweise nicht zulässig, da Data Encipherment kein zulässiges Attribut ist (s.o.).

Der private Schlüssel verbleibt lokal, der CSR wird als Textdatei im Eingabeformular als Teil der Registrierungsinformation der Vorsorgeeinrichtung an die ZfDR übergeben.

Der/die Sachbearbeiter*in plausibilisiert den CSR:

- Es wird automatisch geprüft, ob für den Server bereits ein Zertifikat ausgestellt wurde. Dies wird dem/der Antragsteller*in mitgeteilt, eine neue Erstellung eines Zertifikates erfolgt dann nicht. (Dies kann z.B. vorkommen, wenn ein Dienstleister mehrere Vorsorgeeinrichtungen über einen Server bedient. Dann könnten mehrere Endpunkte - ggf. mit unterschiedlichen Pfaden, auf dem gleichen Server liegen. Dies sollte allerdings auch dem Dienstleister bei der Generierung des CSR auffallen).

[4] Beschreibung eines Standards für Zertifikate, kein Dokument der ZfDR

- Der/die Sachbearbeiter*in prüft, ob der Servername, OrganizationName und OrganizationUnitname zum Antragsteller passen, und dass die CSR-Datei keine weiteren Felder als die o.a. enthält.

Wenn die Plausibilisierung Fehler erkennt, wird der/die Antragsteller*in mit der Aufforderung benachrichtigt, den Antrag noch einmal in berichtigter Form zu stellen.

Das Zertifikat in Form einer CRT-Datei wird generiert und an die im Antrag auf Zulassung angegebene E-Mail-Adresse versendet. Sollte das Trustcenter einen Fehler in der CSR feststellen, wird ein Fehlerprotokoll versandt, der Antrag muss dann noch einmal berichtigt gestellt werden.

Die CRT-Datei wird mit der Endung .CRT verschickt. Vorsorgeeinrichtungen müssen sicherstellen, dass sie E-Mails mit dieser Anlage verarbeiten können und die E-Mails weder blockieren noch die Anhänge löschen.

HINWEIS:

Bei den Anfragen an die Vorsorgeeinrichtungen wird SNI (Server Name Indication) unterstützt. Im Feld ‚server_name' wird der Hostname der URL des aufgerufenen Webservice-Endpunkts übertragen.

6.4 Certification Authority Zertifikat-Aussteller-Kette

Das produktive CA-Zertifikat (Certification Authority) wird vom Server der Vorsorgeeinrichtung anhand der Zertifikatskette validiert. Auf diese Weise kann der Client der ZfDR ausgetauscht oder um weitere Instanzen ergänzt werden, ohne dass die Vorsorgeeinrichtungen Änderungen an ihrer Serverkonfiguration vornehmen müssen (zum Download verfügbar unter https://zfdr-vorsorgeeinrichtungen.drv-bund.de).

Die "DRV TM CA" des Produktiv-Systems stellt das eigentliche CA-Zertifikat der ZfDR aus.

Das CA-Zertifikat der "DRV TM CA" wurde von der "DRV Root CA" des Produktiv-Systems ausgestellt.

Die Serverzertifikate der VEs werden durch das "DRV DRIS CA" ausgestellt.

Die jeweils aktuelle Zertifikatskette ist zu finden in der .zip-Datei "CA-Zertifikate" unter dem oben genannten Link.

6.5 Verlängerung eines Serverzertifikates

Bei jeder Generierung einer neuen CSR-Datei ist es erforderlich, vorher ein neues Schlüsselpaar (4096 bit) zur Erzeugung der neuen CSR auf Seiten der Vorsorgeeinrichtung zu generieren. Neuere Zertifikate haben eine Gültigkeit von maximal drei Jahren. Die Verlängerung entspricht weitestgehend der Beantragung. Die CSR-Datei wird per E-Mail an die Anwendung geschickt. Die Verlängerung muss vor dem Ablauf des Zertifikates erfolgen, damit immer ein gültiges Zertifikat genutzt werden kann.

Die Anwendung prüft zusätzlich, ob die E-Mail-Adresse der dem Zertifikat zugeordneten Adresse entspricht und ob das bestehende Zertifikat gesperrt ist. Dabei nutzt die Anwendung das Trustcenter der Deutschen Rentenversicherung in gleicher Form wie bei der

Erstbeantragung eines Zertifikates. Die Antwort des Dienstes und der weitere Verlauf sind die gleichen wie bei der Beantragung.

Im Detail läuft die Zertifikatserneuerung wie folgt ab: Etwa vier Monate vor Ablauf des Zertifikates der Vorsorgeeinrichtung schreibt die ZfA dem bei ihr hinterlegten technischen Ansprechpartner der Vorsorgeeinrichtung eine automatisierte E-Mail mit der Aufforderung, eine neue CSR-Datei an die ZfDR zu übermitteln. Die Vorsorgeeinrichtungen sind daher angehalten, ihre Stammdaten bei der ZfDR aktuell zu halten. Die betroffene Endpunkt-URL und die Art der betroffenen Zertifikate werden darin mitgeteilt (z.B: Anfrage-Endpunkt (Produktionsumgebung): https://av-zfdr.pfefferminzia.de/ve01234).

Nun muss die Vorsorgeeinrichtung aktiv werden und eine CSR-Datei im Sinne des Kapitels 6.3 ‚Beantragung eines Serverzertifikates' per E-Mail an den Postkorb zfdr-anbindung@drv-bund.de übermitteln. Demnach sind auch die entsprechenden Anforderungen an die CSR-Datei aus dem genannten Kapitel einzuhalten. Die neue CSR-Datei sollte bis 60 Tage vor Ablauf des alten Zertifikates an die ZfDR übermittelt werden, damit das Trustcenter der DRV ein neues Zertifikat ausstellen und die Vorsorgeeinrichtung das neue Zertifikat noch vor Ablauf des Alten einbinden kann.

Vorsorgeeinrichtungen müssen bei einem Zertifikatswechsel auch die aktuellen ZfDR-Zertifikate im Downloadbereich der ZfDR beachten, um sich auf die korrekten Zertifikate zu beziehen. Das neue Zertifikat auf Basis der neuen CRT-Datei und des aktuell gültigen Root-Zertifikates wird der Vorsorgeeinrichtung wie im Kapitel 6.3 ‚Beantragung eines Serverzertifikates' beschrieben als CRT-Datei per E-Mail übermittelt.

Das neue Zertifikat ist auf Seiten der ZfDR sofort aktiv. Die Digitale Rentenübersicht kann nun beide Zertifikate bedienen. Die Vorsorgeeinrichtung kann nun innerhalb von vier Wochen jederzeit nach eigenem Ermessen auf das neue Zertifikat wechseln, sofern das alte Zertifikat nicht vorher abläuft. Das bedeutet, **vier Wochen nach Ausstellung des neuen Zertifikates bzw. mit Ablauf des alten Zertifikates (was zuerst eintritt) ist eine Kommunikation mit dem alten Zertifikat nicht mehr möglich.** Damit eine lückenlose Kommunikation zwischen ZfDR und Vorsorgeeinrichtung sichergestellt ist, muss die Vorsorgeeinrichtung das neue Zertifikat dementsprechend rechtzeitig einbinden.

Teilen sich mehrere Vorsorgeeinrichtungen ein Zertifikat, bspw. aufgrund der Zusammenarbeit mit einem IT-Dienstleister bzw. Datenintermediär, reicht es aus, wenn der Zertifikatswechsel über eine der betroffenen Vorsorgeeinrichtungen vorgenommen wird. Die ZfDR wird bevorzugt mit der Vorsorgeeinrichtung Kontakt aufnehmen, die auch das ursprüngliche Zertifikat beantragt hat. Aufgrund von beispielsweise Unternehmensfusionen kann es aber auch vorkommen, dass die ZfDR über den technischen Ansprechpartner einer anderen Vorsorgeeinrichtung Kontakt aufnimmt.

Ohne ein neues Zertifikat könnten VE und ZfDR nicht mehr kommunizieren und ihre gesetzliche Aufgabe nicht mehr erfüllen. Anfragen zu betroffenen Vorsorgeeinrichtungen würden nach Ablauf des Zertifikates als "abgeschlossen - nicht erfolgreich" angezeigt. Die ZfDR müsste die Vorsorgeeinrichtung dann aus der Digitalen Rentenübersicht entfernen, bis die Kommunikation wieder funktioniert.

HINWEIS:

Sicherheitsbetrachtung

Das Versenden einer CRT-Datei ist unkritisch, da der private Teil des Zertifikates das Haus der Vorsorgeeinrichtung nicht verlässt. Der öffentliche Teil des Schlüssels allein ermöglicht keine Verwendung.

Bei der Zertifikatserneuerung übermittelt die ZfDR die neue CRT-Datei. Im Anschluss hat die Vorsorgeeinrichtung maximal vier Wochen Zeit, das neue Zertifikat zu verwenden. **Nach vier Wochen** wird das alte Zertifikat spätestens deaktiviert (revoked) sofern es nicht bereits vorher regulär abläuft.

6.6 Sperren eines Serverzertifikates

Die Sperrung eines Zertifikates kann von der Sachbearbeitung im Kundenservice der ZfDR veranlasst werden.

Für Zertifikate in der Produktions- und in der QS-Umgebung werden Sperrlisten bereitgestellt. Diese können über HTTP und LDAP entsprechend den Eintragungen im jeweiligen Zertifikat von folgenden Servern abgerufen werden:

- für die Produktionsumgebung: dir.tc.deutsche-rentenversicherung.de
  (im Internet erreichbar)
- für die QS-Umgebung: dir.qstc.deutsche-rentenversicherung.de
  (nur im Intranet der DRV erreichbar)

6.7 Authentifizierung des zentralen Servers der ZfDR

Zur Authentifizierung des zentralen Servers (als anfragender Client) gegenüber den Servern der Vorsorgeeinrichtungen werden den Vorsorgeeinrichtungen folgende Informationen zur Verfügung gestellt:

- Zertifikat für den zentralen Server der DRV, generiert durch die CA für zentrale Dienste der DRV, TM-CA
- Zugehöriges Zertifikat
- Adresse der Server zum Abruf von Sperrlisten (Certificate Revocation List = CRL) und OCSP-Responder (OCSP = Online Certificate Status Protocol)

6.8 Funktionale Elemente des Zertifikatsmanagements

Zur Unterstützung der Mitarbeitenden der Vorsorgeeinrichtungen werden im Folgenden die einzelnen Funktionen zum Zertifikatsmanagement detaillierter beschrieben.

(Als Passwort wurde immer **powerdris** gewählt. Der variable Teil des Namens der Dateien ist dris. Die Beispiele sind der vorangegangenen Seite entnommen. Die Parameter sind so gesetzt, wie gefordert.)

6.9 Funktion zur Generierung und Beantragung von Zertifikaten

Erstellen eines Schlüsselpaars auf dem Server mit OpenSSL

Der folgende Aufruf von OpenSSL von der Konsole aus kann verwendet werden:

```
$ openssl genpkey -out dris.key -algorithm RSA -pkeyopt rsa_keygen_bits:4096 -aes-128-cbc
.....+++++
Enter PEM pass phrase: powerdris
Verifying - Enter PEM pass phrase: powerdris
```

Es wird eine Datei dris.key erzeugt, welche das Schlüsselpaar enthält. Diese Datei muss sicher verwahrt werden.

6.10 Prüfung des Schlüsselpaars

Mit diesem Aufruf kann die Integrität und die Schlüssellänge des Schlüsselpaars geprüft werden. Der folgende Aufruf von OpenSSL von der Konsole aus kann verwendet werden:

```
$ openssl pkey -in dris.key -text -noout
Enter pass phrase for dris.key: powerdris
RSA Private-Key: (4096 bit)
modulus:
```

[...] / der Rest ist nicht informativ

6.11 Generierung des CSR-Request (Certifcate Signing Request)

Die Eingabe der Parameter kann entweder von der Commandline oder aus einer Konfigurationsdatei heraus erfolgen. Um die Parametrierung nachvollziehbarer zu machen, wird hier der Weg über die Konfigurationsdatei gewählt:

Die Konfigurationsdatei dris.cnf hat folgende Inhalte:

```
[req]
prompt = no
distinguished_name = req_dn
req_extensions = req_v3
input_password = powerdris
[req_dn]
CN = server01.drv-dris.pfefferminzia.de
O = Pfefferminzia SE
OU = Pfefferminzia Pensionskasse
C = DE
```

[req_v3]

subjectAltName = @alt_names

[alt_names]

DNS.1 = server01.drv-dris.pfefferminzia.de

Hierfür können sie folgenden OpenSSL-Befehl verwenden:

$ openssl req -new -config dris.cnf -key dris.key -out dris.csr

Es wird eine Datei dris.csr erzeugt.

6.12 Prüfen des CSR

Der folgende Aufruf von OpenSSL von der Konsole aus kann verwendet werden:

$ openssl req -text -in dris.csr -noout

Certificate Request:

Data:

Version: 1 (0x0)

Subject: CN=server01.drv-dris.pfefferminzia.de, O=Pfefferminzia SE, OU=Pfefferminzia Pensionskasse, C=DE

Subject Public Key Info:

Public Key Algorithm: rsaEncryption

Public-Key: (4096 bit)

Modulus: [...]

Attributes:

Requested Extensions:

X509v3 Subject Alternative Name:DNS:server01.drv-dris.pfefferminzia.de

Signature Algorithm: sha256WithRSAEncryption

[...] / der Rest ist nicht informativ

Die CSR-Datei kann natürlich auch mit einem ASN.1 Editor geöffnet und geprüft werden.

Die CSR-Datei wird von der Vorsorgeeinrichtung generiert und an die ZfDR im Zuge des Erstantrages oder einer Zertifikatserneuerung übertragen.

6.13 Länderliste für CSR-Datei

Diese Liste enthält die Länder mit einem angemessenen Datenschutzniveau, insbesondere EU/EWR Länder. Nur diese Länder dürfen in der CSR-Datei als 'countryName' vorgegeben werden. Andere Länder führen zur Abweisung des Datensatzes.

Name	Begründung	Kennzeichen nach ISO-Liste 3166-1
Belgien	EU-Mitglied	BE
Bulgarien	EU-Mitglied	BG
Dänemark	EU-Mitglied	DK
Deutschland	EU-Mitglied	DE
Estland	EU-Mitglied	EE
Finnland	EU-Mitglied	FI
Frankreich	EU-Mitglied	FR
Griechenland	EU-Mitglied	GR
Irland	EU-Mitglied	IE
Italien	EU-Mitglied	IT
Kroatien	EU-Mitglied	HR
Lettland	EU-Mitglied	LV
Litauen	EU-Mitglied	LT
Luxemburg	EU-Mitglied	LU
Malta	EU-Mitglied	MT
Niederlande	EU-Mitglied	NL
Österreich	EU-Mitglied	AT

Polen	EU-Mitglied	PL
Portugal	EU-Mitglied	PT
Rumänien	EU-Mitglied	RO
Schweden	EU-Mitglied	SE
Slowakei	EU-Mitglied	SK
Slowenien	EU-Mitglied	SI
Spanien	EU-Mitglied	ES
Tschechien	EU-Mitglied	CZ
Ungarn	EU-Mitglied	HU
Zypern	EU-Mitglied	CY
Island	EWR-Mitglied	IS
Lichtenstein	EWR-Mitglied	LI
Norwegen	EWR-Mitglied	NO
Guernsey	von der Europäischen Kommission anerkannt als angemessenes Datenschutzniveau im Sinne der EU	GG
Jersey	von der Europäischen Kommission anerkannt als angemessenes Datenschutzniveau im Sinne der EU	JE
Färöer-Inseln	von der Europäischen Kommission anerkannt als angemessenes Datenschutzniveau im Sinne der EU	FO
Vereinigtes Königreich	von der Europäischen Kommission anerkannt als	GB

	angemessenes Datenschutzniveau im Sinne der EU	
Andorra	von der Europäischen Kommission anerkannt als angemessenes Datenschutzniveau im Sinne der EU	AD
Isle of Man	von der Europäischen Kommission anerkannt als angemessenes Datenschutzniveau im Sinne der EU	IM
Schweiz	von der Europäischen Kommission anerkannt als angemessenes Datenschutzniveau im Sinne der EU	CH

7 Beschreibung des Testvorgehens

7.1 Beschreibung des Testvorgehens

Zum abgestimmten Termin erfolgen die Schnittstellentests. Zur verlässlichen Durchführung der Verbindungstest in der produktiven Testumgebung benötigen technische Ansprechpartner Kenntnisse über die etablierten Standard-Kommunikationstechnologien im Sinne der Fachinformatik Systemintegration REST-API, HTTPS, mTLS und JSON.

Diese Kenntnisse sind insbesondere für die mit dem Test verbundenen Aufgabenbereiche der Serverkonfiguration, Erstellung von Zertifikatsanträgen, Testdurchführung und Debugging relevant.

Es erfolgen ein

- **verpflichtender** Verbindungstest in der produktiven Umgebung zum Test der Verbindungsstrecke (erforderlich für die Produktivsetzung) als auch
- **optionaler** Kommunikationstests in der QS-/PNT-Umgebung zur Überprüfung der Akzeptanz und Verarbeitung der Antwortdatensätze.

Der Betrieb der ZfDR stimmt das Testvorgehen mit der Vorsorgeeinrichtung jeweils individuell ab.

> **HINWEIS:**
>
> Die Vorsorgeeinrichtung sollte das Testverfahren erst in Anspruch nehmen, wenn sichergestellt werden kann, dass mit anschließender Produktivsetzung auch **Anfragen durch Nutzerinnen und Nutzer entsprechend beantwortet werden können**.

Abbildung 6: Gegenüberstellung Testvarianten

7.2 Verbindungstest im produktiven System (erforderlich)

Nach erfolgreicher Anmeldung und Einbindung der Zertifikate auf den Servern der Vorsorgeeinrichtung wird zum Test der Verbindungsstrecke in der Produktion ein Testaufruf mit einer von der ZfDR definierten IdNr, die nicht im produktiven Bestand der Vorsorgeeinrichtung hinterlegt sein kann, gestartet. Dieser Testaufruf erfolgt in Abstimmung mit der angemeldeten Vorsorgeeinrichtung, sobald diese die Zertifikate implementiert hat, die sie im Rahmen der Anbindung von der ZfDR erhalten hat.

Nach der erfolgreichen Einrichtung erfolgt zudem ein Test durch den Betrieb der ZfDR. Erhält die ZfDR als Antwort den Statuscode 204, ist der Test der Kommunikationsstrecke erfolgreich. Erst dann wird die Vorsorgeeinrichtung produktiv gesetzt und kann mit den ersten produktiven Anfragen rechnen.

Produktivsetzungen finden immer montags statt.

Erhält die ZfDR nicht die erwartete Antwort, dann erfolgt die gemeinsame Klärung des Fehlers und der Test der Verbindungsstrecke wird wiederholt.

7.3 Kommunikationstests in der QS-/PNT-Umgebung (optional)

Zusätzlich zum Test der Verbindungsstrecke in der produktiven Umgebung gibt es von Seiten der ZfDR optional die Möglichkeit, auf einer produktionsnahen Testumgebung Anfragen mit dreizehn zuvor festgelegten Tupeln aus IDNR und Geburtsdatum an ein QS- oder PNT-System der Vorsorgeeinrichtung zu senden. Hierdurch wird die Annahme des Antwortdatensatzes bei der ZfDR geprüft.

Die Testdaten sind, um hierbei möglichst nah an der Produktion zu sein, durch die Vorsorgeeinrichtung zu erstellen und in den QS- bzw. PNT-Systemen zu hinterlegen, die die ZfDR anfragt. Nicht alle der in der Tabelle 7 gelisteten Testfälle müssen durch die Vorsorgeeinrichtung zur Verfügung gestellt werden. Die Liste ist eine Empfehlung seitens der ZfDR zu einer möglichst hohen Abdeckung der verschiedenen Kommunikationsmöglichkeiten.

Es sei darauf verwiesen, dass in der Testumgebung keine Produktivdaten zu hinterlegen sind. Von der ZfDR wird empfohlen, Testdaten von Produktarten zu erstellen, die am häufigsten bei der Vorsorgeeinrichtung vertreten sind. Auch ist es empfohlen, möglichst produktionsnahe PDFs für die Standmitteilungen zu verwenden.

Für diese Tests bedarf es ebenfalls eines Zertifikatsaustausches für die Kommunikation der QS- bzw. PNT-Systeme. Der Prozess ist hierbei äquivalent zum Austausch der Zertifikate für die produktive Kommunikationsstrecke.

Voraussetzungen

Die Kommunikation erfolgt ohne Authentifizierung per E-Mail. Daher ist es notwendig, dass der automatisierte Kommunikationstest nur von Vorsorgeeinrichtungen genutzt werden kann, die der ZfDR bereits bekannt **und** dort freigeschaltet sind. Dafür müssen folgende Informationen im Vorfeld von der Vorsorgeeinrichtung bekannt gegeben werden:

- Die E-Mail-Adresse des Durchführungsverantwortlichen
- URL(s) des Endpunkts für den Kommunikationstest

- Das Server-Zertifikat für die QS-Umgebung muss aktiviert sein. Siehe auch Kapitel **"Zertifikate"**

Bitte beachten Sie, dass es sich bei dem Anbindungstest um eine Testumgebung handelt, welche unter Umständen nicht rund um die Uhr zur Verfügung steht. Sollte der Anbindungstest nicht funktionieren, bitten wir Sie darum, den Test nach 48 Stunden nochmals durchzuführen, bevor Kontakt mit der ZfDR aufgenommen wird.

Ablauf

Um den Test auszulösen, ist eine E-Mail (von der zuvor mitgeteilten **und** freigeschalteten E-Mailadresse) mit den entsprechenden Testdaten an folgenden Postkorb zu senden: zfdr-anbindungstest@drv-bund.de

Die Testdaten müssen in Form einer JSON-Datei definiert werden. Die Datei ist als Anhang an die E-Mail anzuhängen. Betreff sowie Inhalt der E-Mail spielen keine Rolle.

Der Postkorb wird regelmäßig automatisiert auf E-Mails geprüft. Von bekannten Absendern werden die Testdaten in den E-Mails automatisiert ausgewertet. Können die Testdaten erfolgreich geparst werden, wird der Kommunikationstest gegen den angegebenen Endpunkt durchgeführt. Das Ergebnis wird anschließend zurück an den bekannten Empfänger gesandt.

> **HINWEIS:**
>
> Ist der Absender der E-Mail im Testsystem der ZfDR nicht freigeschaltet, wird der Kommunikationstest nicht durchgeführt.
>
> In diesem Fall erfolgt auch keine Rückmeldung per E-Mail.

Definition der Testdaten

Um die Anbindung zu testen, müssen durch die Vorsorgeeinrichtung Testdaten vorgegeben werden. Die Testdaten müssen folgende Informationen enthalten:

URL der Endpunkte

IdNr des Testnutzers

Geburtsdatum des Testnutzers

Es ist möglich, mehrere Testnutzer in einer Liste anzugeben. Gegen den Endpunkt werden Standmitteilungen von allen Testnutzern ermittelt.

Beispiel:

Testdaten.json


```
{
  "anfrageEndpunkt": "http://dris-vorsorgeeinrichtung-mock-universal.flex.entw.bund.drv/vorsorgeeinrichtungen/drv",
  "fehlerEndpunkt": "http://dris-vorsorgeeinrichtung-mock-universal.flex.entw.bund.drv/vorsorgeeinrichtungen/drv",
  "nutzer": [
    {
      "testfall": "1",
      "geburtsdatum": "1972-08-01",
      "idNr": "02365489751"
    }
  ]
}
```


Das Schema für die Testdaten ist in der Komponente AnbindungstestRequest in OpenAPI-Schema definiert.

7.3.1 Testergebnisse

Die eingelesenen Testdaten werden geparst. Entsprechen die Testdaten den Vorgaben, wird der Anbindungstest durchgeführt. Das Ergebnis des Kommunikationstest wird in JSON-Form per E-Mail an den bekannten Empfänger zurückgegeben. Ist der Kommunikationstest erfolgreich, sind die ermittelten Standmitteilungen im Ergebnis enthalten. Bei einem erfolglosen Test erhält das Ergebnis entsprechende Fehlermeldungen.

7.3.1.1 Beipielhafte erfolgreiche Kommunikationstests

Statuscode 200:


```
{
  "requestorEmail": "mustermann@drv-bund.de",
  "endpoint": "https://dris-vorsorgeeinrichtung-mock-examples-dev.flex.entw.bund.drv/
vorsorgeeinrichtungen/valid-b",
  "nutzerTestergebnisse": [
    {
      "anprueche": [
        {
          "ordnungsbegriff": "15070649C103",
          "produktBezeichnung": "Teststring",
          "nochKeinAnspruch": true,
          "keineBeitragszahlung": true,
          "datumLeistungsbeginnRente": "2060-05-01",
          "garantiertErreichterKapitalwert": 123456789.12,
          "kontaktPostfach": "8 15",
          "steuerpflicht": true,
          "ansprechpartnerEmail": "john.smith@example.com",
          "rentenanpassung": true,
          "kontaktStrasse": "Heidestrasse",
          "standKapital": 0.01,
          "datumLeistungsendeRente": "2080-05-01",
          "produktArt": "_1_1_0",
          "kontaktStaat": "Deutschland",
          "sozialabgabenpflicht": true,
          "gesellschaftOderMarkeBezeichnung": "Testversicherung",
          "hinterbliebenenAbsicherung": true,
          "stichtagWertangaben": "2020-12-31",
          "prognostiziertErreichteRente": 999999999.99,
          "kontaktOrt": "Koeln",
          "kontaktHausNr": "17",
          "garantiertErreichbareRente": 123456789.12,
          "garantiertErreichbarerKapitalwert": 123456789.12,
          "prognostiziertErreichbareRente": 123456789.12,
          "kontaktPlz": "51147",
          "url": "https://www.example.com/index.html",
          "anrechnung": false,
          "intervallRentenangabe": "Monatsrente",
          "invalidenAbsicherung": true,
          "garantiertErreichteRente": 123456789.12,
          "unterbaustein": "_02b",
          "prognostiziertErreichterKapitalwert": 123456789.12,
          "standmitteilungReferenz": "TestPDF",
          "prognostiziertErreichbarerKapitalwert": 123456789.12,
          "ansprechpartnerTelefon": "30123456",
          "kontaktUrl": "https://www.example.com/index.html"
        }
      ],
      "nutzer": {
        "geburtsdatum": "1972-08-01",
        "idNr": "02365489778"
      }
    }
  ]
}
```

Erfolgreicher Kommunikationstest mit Statuscode 204:


```
{
   "anfrageEndpunkt": "https://dris-vorsorgeeinrichtung-mock-universal-
dev.flex.entw.bund.drv/vorsorgeeinrichtungen/drv",
   "nutzerTestergebnisse": [
      {
         "nutzer": {
            "geburtsdatum": "1972-08-01",
            "idNr": "02365489751"
         },
         "fehler": {
            "name": "EndpunktException",
            "message": "Anfrage-Endpunkt lieferte den HTTP-Status-Code \"204\". Dieser ist fachlich korrekt und in
der API für eine \"Nutzer unbekannt\"-Antwort definiert, wird jedoch im Test-Workflow als inkorrekt evaluiert.",
            "restResponseDaten": {
               "headers": {
                  "Content-Language": [
                     "en-US"
                  ],
                  "Date": [
                     "Fri, 10 May 2024 11:20:12 GMT"
                  ],
                  "X-Powered-By": [
                     "Servlet/4.0"
                  ]
               },
               "code": 204
            },
            "anfragedaten": {
               "Anfrage-Endpunkt": "https://dris-vorsorgeeinrichtung-mock-universal-
dev.flex.entw.bund.drv/vorsorgeeinrichtungen/drv",
               "Fehler-Endpunkt": "https://dris-vorsorgeeinrichtung-mock-universal-
dev.flex.entw.bund.drv/vorsorgeeinrichtungen/drv",
               "X-Anfrage-Id": "0b1c912f-0669-40d0-99a6-d48ca1e40e2e",
               "X-Geburtsdatum": "1972-07-05",
               "X-Identifikationsnummer": "02365489760",
               "X-Request-Id": "3d0475cf-4f8d-4e70-b18f-af2670bacb5b"
            }
         }
      }
   ],
   "requestorEmail": "test1@test.com"
}
```

7.3.1.2 Beispielhafte Fehlerfälle

Fehler in den Testdaten

Endpunkt nicht bekannt:


```
{
   "fehler": "Endpunkt http://dris-vorsorgeeinrichtung-mock-universal-test.flex.entw.bund.drv/vorsorgeeinrichtungen/drv vom Absender test1@test.com ist unbekannt.",
   "requestorEmail": "test1@test.com"
}
```


Fehler in der Zertifikat-Kette

Zertifikat fehlt im Truststore:


```
{
  "anfrageEndpunkt": "https://dris-vorsorgeeinrichtung-mock-examples-test.flex.entw.bund.drv/vorsorgeeinrichtungen/valid-a",
  "nutzerTestergebnisse": [
    {
      "fehler": "Exception beim REST-Aufruf. Message: javax.net.ssl.SSLException: SSLException invoking https://dris-vorsorgeeinrichtung-mock-examples-test.flex.entw.bund.drv/vorsorgeeinrichtungen/valid-a/anspruchsdaten: Unexpected error: java.security.InvalidAlgorithmParameterException: the trustAnchors parameter must be non-empty",
      "nutzer": {
        "geburtsdatum": "1972-08-01",
        "idNr": "02365489751"
      }
    }
  ],
  "requestorEmail": "test1@test.com"
}
```


Falscher CN im Zertifikat:


```
{
  "anfrageEndpunkt": "https://vorsorgeeinrichtung-mock-examples-test-nodeport-service.digitalerentenuebersicht-test-nutzer-infra.svc.cluster.local/vorsorgeeinrichtungen/valid-a",
  "nutzerTestergebnisse": [
    {
      "fehler": "Exception beim REST-Aufruf. Message: java.io.IOException: IOException invoking https://vorsorgeeinrichtung-mock-examples-test-nodeport-service.digitalerentenuebersicht-test-nutzer-infra.svc.cluster.local/vorsorgeeinrichtungen/valid-a/anspruchsdaten: HTTPS hostname wrong:  should be <vorsorgeeinrichtung-mock-examples-test-nodeport-service.digitalerentenuebersicht-test-nutzer-infra.svc.cluster.local>",
      "nutzer": {
        "geburtsdatum": "1972-08-01",
        "idNr": "02365489751"
      }
    }
  ],
  "requestorEmail": "test1@test.com"
}
```

HTTP Timeout

SocketTimeout:


```
{
  "anfrageEndpunkt": "http://dris-vorsorgeeinrichtung-mock-universal-
test.flex.entw.bund.drv/vorsorgeeinrichtungen/timeout",
  "nutzerTestergebnisse": [
    {
      "fehler": "Exception beim REST-Aufruf. Message: java.net.SocketTimeoutException: SocketTimeoutException
invoking http://dris-vorsorgeeinrichtung-mock-universal-
test.flex.entw.bund.drv/vorsorgeeinrichtungen/timeout/anspruchsdaten: Read timed out",
      "nutzer": {
        "geburtsdatum": "19721-08-01",
        "idNr": "02365489751"
      }
    }
  ],
  "requestorEmail": "test1@test.com"
}
```


Das Schema für die Testdaten ist in der Komponente AnbindungstestResponse im OpenAPI-Schema definiert.

7.4 Testfälle für den Kommunikationstest

Für die Kommunikationstests sind folgende Fälle für den Test vorgesehen:

Nr	Umge-bung	IdNR[5]	Geburts-datum[6]	Testfall	Testziel	Ergebnis ZfDR	Ergebnis VE
1	QS/ PNT, PROD	02365489751	01.08.1972	Gutfall	Szenario 1 – Person nicht gefunden	Prüfung des grundsätzlichen Kommunikations-weges	HTTP204 vom VE Webservice
2	QS/ PNT	02365489760	01.08.1972	Gutfall	Szenario 2a - Einfacher Gutfall ohne Standmitteilung	Grundlegende Validierung des Schemas für Szenario 2a	HTTP200 vom VE Webservice, Schemaprüfung, kein PDF
3	QS/ PNT	02365489778	01.08.1972	Gutfall	Szenario 2b - Gutfall für ausschließliche Rentenzahlungen	Grund-legende Validierung des Schemas für Szenario 2b	HTTP200 vom VE Webservice, Schemaprüfung, PDF Prüfung
4	QS/ PNT	02365489786	01.08.1972	Gutfall	Szenario 2c - Gutfall für ausschließliche Einmalzahlungen	Grundlegende Validierung des Schemas für Szenario 2c	HTTP200 vom VE Webservice, Schemaprüfung, PDF Prüfung
5	QS/ PNT	02365489794	01.08.1972	Gutfall	Szenario 2d - Gutfall für Kombinationen von Renten- und Einmalzahlungen	Grundlegende Validierung des Schemas für Szenario 2d	HTTP200 vom VE Webservice, Schemaprüfung, PDF Prüfung
6	QS/ PNT	02365489817	01.08.1972	Gutfall	Mehrere Ansprüche	HTTP Multipart mit mehreren PDFs	HTTP200 vom VE Webservice, Schemaprüfung, PDF Prüfung, alle PDF zuordenbar
7	QS/ PNT	02365489876	01.08.1972	Gutfall	Erneuter Anfrage-wunsch	Prüfung der erneuten Anfrage/ Verschiebung einer Anfrage	HTTP202 vom VE Webservice
8	QS/ PNT	02365489884	01.08.1972	Gutfall	Offener Testfall für HTTP200	Offener Testfall für die Vorsorge-einrichtungen	HTTP200 vom VE Webservice
9	QS/ PNT	02365489190	01.08.1972	Fehler-fall	Schemaverstoß	Grundlegende Kommunika-tionsprüfung Fehlerendpunkt, Prüfung des Fehlercodes für Schemafehler	HTTP201 vom Fehlerendpunkt
10	QS/ PNT	02365489913	01.08.1972	Fehler-fall	PDF Größenverstoß	Grundlegende Kommunika-tionsprüfung Fehlerendpunkt,	HTTP201 vom Fehlerendpunkt

[5] Bei den "IdNr" handelt es sich um rein fiktive Testdaten, welche nicht zwingend plausibel sein müssen

[6] Bei dem "Geburtsdatum" handelt es sich um ein rein fiktives Testdatum.

Nr	Umge-bung	IdNR[5]	Geburts-datum[6]	Testfall	Testziel	Ergebnis ZfDR	Ergebnis VE
						Prüfung des Fehlercodes für PDF Größe	
11	QS/ PNT	02365489972	01.08.1972	Fehler-fall	PDF fehlt/nicht zuordenbar	Grundlegende Kommunika-tionsprüfung Fehlerendpunkt, Prüfung des Fehlercodes für PDF fehlt	HTTP201 vom Fehlerendpunkt
12	QS /PNT	02365490075	01.08.1972	Fehler-fall	PDF-Format fehlerhaft	Grundlegende Kommunika-tionsprüfung Fehlerendpunkt, Prüfung des Fehlercodes für PDF-Formatfehler	HTTP201 vom Fehlerendpunkt
13	QS/ PNT	02365490083	01.08.1972	Fehler-fall	Strukturierte JSON Daten fehlen	Grundlegende Kommunika-tionsprüfung Fehlerendpunkt, Prüfung des Fehlercodes für JSON Daten fehlen	HTTP201 vom Fehlerendpunkt

Tabelle 8: Auflistung der Testfälle

Die Testfälle sollen eine höchstmögliche Testabdeckung liefern, es müssen aber nicht alle Testfälle durch die Vorsorgeeinrichtungen durchgespielt werden.

8 Implementation der Schnittstelle

8.1 Allgemeines

Dieses Kapitel bietet Hinweise zur Implementation der von der ZfDR definierten Schnittstelle (vorsorgeeinrichtung.yaml) zur Anlieferung von Anspruchsdaten und Standmitteilungen an die ZfDR.

In den nachfolgenden Beispielen erfolgt die Implementation in Java mit Maven als Build Management System. Aus der OpenAPI Spezifikation (vorsorgeeinrichtung.yaml) kann ein Java Code generiert werden. Die Generierungsmöglichkeiten sind umfangreich konfigurierbar, weisen in Details ggf. aber auch Defizite auf, die eine manuelle Implementation spezifischer Code Artefakte erforderlich machen. In dieser Hilfestellung wird grundlegend davon ausgegangen, dass durch einen Code Generator eine Java Schnittstelle sowie Datentransferobjekte (DTO) erzeugt werden, die eigentliche Implementation der Java Schnittstelle jedoch manuell erfolgt. Die Verwendung eines Generators kann hilfreich sein, ist jedoch nicht verpflichtend.

8.2 Generatoren

Die Einbindung eines Code Generators erfolgt mit dem openapi-generator-maven-plugin. Dieses wird in der root pom.xml des jeweiligen Backend Service Projektes in der build → plugins Sektion als Plugin eingebunden (Maven-Phase: generate-sources, Goal: generate). Kernintention ist es, eine Java Schnittstelle mit Methoden und Ein-/Ausgabeparametern und zugehörigen POJO Klassen erzeugt zu bekommen, die den Operationen und Schemata der Schnittstellenspezifikation entsprechen.

Es existiert eine Vielzahl an verwendbaren Server-Stub Generatoren, wie dieser Liste der Server-Generatoren zu entnehmen ist. In nachfolgenden Erläuterungen dient der jaxrs-spec Generator als Beispiel, wobei sich die Parametrisierungsmöglichkeiten der Generatoren relativ ähnlich sind.

Generator Konfiguration: Die Konfiguration der Generatoren ist separiert in allgemeine Parameter des openapi-generator-maven-plugin

- die für alle Validatoren gültig sind und
- in generatorspezifische Parameter.

8.3 Allgemeine Generator-Konfiguration

In der <configuration> Sektion des openapi-generator-maven-plugin erfolgt die allgemeine Konfiguration des Plugins. Sämtliche potenziell möglichen Parameter sind in der Allgemeinen Generatorkonfiguration des openapi-generator-maven-plugin angegeben. Im Folgenden erfolgt eine Erläuterung einiger weniger Parameter, die relevant sein könnten:

<inputSpec>

Damit wird der Pfad zum Spezifikationsdokument definiert (vorsorgeeinrichtung.yaml). Dies kann ein Pfad zu einer lokalen Datei sein oder auch eine URL zu einem Repository, in dem sich das Spezifikationsdokument zentralisiert befindet.

<generatorName>

Es gibt eine Vielzahl an möglichen Generatoren für Webservice-Clients und Server-Stubs. Verwendet wird hier im Beispiel der jaxrs-spec Generator zur Erzeugung des Server-Stubs.

<modelNameSuffix>

Für die Namen der generierten Java Klassen kann eine Endung definiert werden (z.B. TO oder DTO). Aus einem im vorsorgeeinrichtung.yaml definiertem Schema "Anfrage" wird somit eine AnfrageTO.java Klasse generiert.

<typeMappings>

Hiermit lassen sich, entweder in CSV-Schreibweise oder mit separaten Unterknoten <typeMapping></typeMapping>, die zu tätigenden Mappings von Schema Datentypen auf Java Datentypen konfigurieren (Muster: SchemaDatatype=JavaDatatype). Standardmäßig wird bspw. ein Schema boolean auf ein Java Boolean Objekt abgebildet. Um in der generierten Java Klasse stattdessen den primitiven boolean Typen zu realisieren, wird dies mittels boolean=boolean definiert.

<importMappings>

Damit in einer generierten Java Klasse der Import einer in Sektion <typeMappings> angegebenen Datenstruktur korrekt funktioniert, kann ein Import-Mapping nach dem Muster NameDerDatenstruktur=package.der.Datenstruktur definiert werden. Analog zu den Type-Mappings ist die Angabe in CSV-Schreibweise (NameDerDatenstruktur1=package.der.Datenstruktur1,NameDerDatenstruktur2=package.der.Datenstruktur2) oder mittels separaten Unterknoten <importMapping></importMapping> möglich.

<templateDirectory>

Der OpenAPI-Generator nutzt für die Generierung Template-Dateien im *.mustache Format. Für jedes Generierungsartefakt gibt es ein entsprechendes Template in dem der zu generierende Inhalt definiert ist. Wird ein templateDirectory definiert, so wird jedes gültige Template in diesem Verzeichnis an Stelle des Standard-Template verwendet (Standard-Templates des jaxrs-spec Generators). Dies kann ggf. für spezifische Modifikationen nützlich sein, die sich nicht über typeMappings und importMappings lösen lassen. Beispielsweise erzeugt der Generator (je nach verwendeter Version) in generierten POJO-Klassen die Annotation com.fasterxml.jackson.annotation.JsonProperty und erzwingt damit Abhängigkeiten, die mitunter nicht gewollt sind, wenn bspw. stattdessen die Annotation javax.json.bind.annotation.JsonbProperty der JSON Binding API (JSR 367) zum Mapping verwendet werden soll. Um dafür zu sorgen, dass in einem solchen Fall eine speziell intendierte Annotation im Generierungsartefakt verwendet wird, genügt es im templateDirectory das pojo.mustache Template zu platzieren und in dieser Datei die Imports von Jackson Klassen durch Imports der gewünschten API sowie den Namen der Annotation an den relevanten Stellen zu ersetzen. Es spricht nichts gegen die Verwendung von jackson Abhängigkeiten - das genannte Beispiel dient lediglich der Veranschaulichung.

8.4 Spezifische Generator-Konfiguration

Je nach verwendetem Generator können in der untergeordneten Sektion generatorspezifische Konfigurationen vorgenommen werden. Im Folgenden erfolgt eine Erläuterung einiger weniger jaxrs-spec spezifischer Einstellungen, die relevant sein könnten:

<apiPackage>

Java Package, in dem die generierten Java Schnittstellen abgelegt werden (target/generatedsources/openapi/src/gen/java/<apiPackage>, wobei der vorausgehende Teilpfad mittels <output> in den allgemeinen Konfigurationsoptionen des Plugins und mittels <sourceFolder> generatorspezifisch auch angepasst werden kann).

<modelPackage>

Java Package, in dem die generierten Java POJOs abgelegt werden (target/generatedsources/openapi/src/gen/java/<modelPackage>, wobei der vorausgehende Teilpfad mittels <output> in den allgemeinen Konfigurationsoptionen des Plugins und mittels <sourceFolder> generatorspezifisch auch angepasst werden kann).

<dateLibrary>

Es stehen einige DateTime APIs zur konfigurativen Verfügung. Abhängig von den zur Verfügung stehenden Bibliotheken und der verwendeten Java-Version kann ggf. auch eine andere Bibliothek verwendet werden.

<interfaceOnly>

Es besteht die Möglichkeit Schnittstellenimplementationen zu generieren. Diese müssen jedoch durch weitere Konfigurationsmaßnahmen oder Subklassen weiter ausimplementiert bzw. angereichert werden. Zur Vereinfachung kann die Generierung ausschließlich darauf beschränkt werden, die Java Schnittstellen und Java POJOs zu generieren.

<prependFormOrBodyParameters>

Definiert die Reihenfolge von POJOs und Pfadparametern in Methodensignaturen. Der Wert ist auf true zu setzen, um zuerst die POJOs und anschließend Pfadparameter in der Methodensignatur generieren zu lassen.

<returnResponse>

Bestimmt, ob eine Operation bzw. Methode ein javax.ws.rs.core.Response oder ein generiertes POJO zurückgibt.

8.5 Generator-Beispielkonfiguration

Im Folgenden sei ein Beispiel für die Konfiguration eines Generators in der pom.xml gegeben:

```
<plugin>
  <groupID>org.openapitools
  </groupId>
  <artifactID>openapi-generator-maven-plugin
  </artifactId>
  <version>5.1.1</version>
  <executions>
    <execution>
      <id>java_server_stub</id>
```

```
      <goals>
        <goal>generate</goal>
      </goals>
      <configuration>
        <inputSpec>${project.basedir}/openapi/vorsorgeeinrichtung.yaml</inputSpec>
        <generatorName>jaxrs-spec</generatorName>
        <languageSpecificPrimitives>boolean</languageSpecificPrimitives>
        <modelNameSuffix>TO</modelNameSuffix>
        <importMappings>
          <importMapping>java.time.OffsetDateTime=java.time.Instant</importMapping>
        </importMappings>
        <typeMappings>
          <typeMapping>boolean=boolean</typeMapping>
          <typeMapping>OffsetDateTime=Instant</typeMapping>
          <typeMapping>Double=java.math.BigDecimal</typeMapping>
        </typeMappings>
        <templateDirectory>${project.basedir}/openapi/generator-templates</templateDirectory>
        <configOptions>
          <apiPackage>de.firmenname.anspruchsdaten.rest.api</apiPackage>
          <modelPackage>de.firmenname.anspruchsdaten.rest.model</modelPackage>
          <sourceFolder>src/gen/java</sourceFolder>
          <booleanGetterPrefix>is</booleanGetterPrefix>
          <dateLibrary>java8</dateLibrary>
          <generatePom>false</generatePom>
          <interfaceOnly>true</interfaceOnly>
          <library>openlibery</library>
          <prependFormOrBodyParameters>true</prependFormOrBodyParameters>
          <returnResponse>true</returnResponse>
          <useBeanValidation>false</useBeanValidation>
          <useSwaggerAnnotations>false</useSwaggerAnnotations>
        </configOptions>
      </configuration>
    </execution>
  </executions>
</plugin>
```

8.6 Potenziell erforderliche Anpassungen

Die OpenAPI-Generatoren können nicht mit jeder Ausprägung der Spezifikation umgehen.

Im Speziellen sei hier die Definition der Menge der Anspruchsdaten als oneOf Zusammenstellung genannt. Dabei ist definiert, dass die Anspruchsdaten (Schema VZ01) aus Unternehmenskontaktinformationen (Schema VZ01-01) und einem Array bzw. einer Liste aus Ansprüchen bestehen (Schema VZ01- 02), wobei jeder Anspruch genau einem von vier definierten Schemata entspricht (VZ01-02a, VZ01- 02b, VZ01-02c, VZ01-02d). Je nach verwendetem Generator und konfigurierten typeMappings wird eine VZ01 Datenstruktur generiert, die als Member eine VZ0101 Datenstruktur für die Unternehmenkontaktinformationen beinhaltet, sowie eine Liste von OneOfVZ0102aVZ0102bVZ0102cVZ0102d Instanzen. Diese OneOfVZ0102aVZ0102bVZ0102cVZ0102d Klasse kann ggf. von aktuellen Generatorversionen nicht erzeugt werden (Stand November 2021) und muss manuell angelegt werden. Name und Packagepfad lassen sich bei Bedarf mit typeMapping und importMapping in der Generator-Konfiguration in der pom.xml modifizieren. Die Implementationsweise der Klasse ist grundlegend freigestellt. Eine Schnittstelle oder eine abstrakte Klasse erfordern ggf. auch Erweiterungen bzw. Custom-Implementationen der generierten VZ0102a, VZ0102b, VZ0102c und VZ0102d Klassen, um die implements- bzw. extends-Definitionen zu integrieren (Generatorkonfiguration um auf die selbst erstellten bzw. erweiterten Klassen zu verweisen, ist dann auch mittels typeMapping und importMapping in der pom.xml zu realisieren). Alternativ bietet sich eine Holder-Klasse an, die jeweils eine Non-Null Referenz auf die konkrete Anspruchsklasse (VZ0102a, VZ0102b, VZ0102c, VZ0102d) beinhaltet.

Im Zusammenhang mit der zuvor genannten Datenstruktur zur Abbildung der oneOf Zusammenstellung (OneOfVZ0102aVZ0102bVZ0102cVZ0102d) kann es erforderlich sein, einen spezifischen Serialisierer zu implementieren, der aus der Abstraktion die jeweils konkrete Implementation zur Serialisierung heranzieht. Dafür bietet sich im JavaEE Umfeld bspw. eine Implementation eines JsonbSerializer an. Dieser kann anhand der konkreten Instanz der Anspruchsklasse oder des Wertes des Attributes unterbaustein entscheiden, welche konkrete Klasse die Basis für die Serialisierung bildet. Zumeist werden in den generierten Klassen auch Converter für Enumerationen erzeugt. Sollte dies für spezifische Enumerationen wie bspw. Produktart nicht der Fall sein, so kann hierbei auch ein Custom Serialisierer dienlich sein, der aus der Enum-Instanz den jeweiligen Wert extrahiert.

9 Multipart-Response

9.1 Allgemeines

Multipart ist ein Content-Typ, der die Kombination von mehreren Parts mit unterschiedlichen Content-Typen in einer Response ermöglicht. Obwohl unter Multipart nach Bedarf noch weitere Subtypen z.B. multipart/mixed, multipart/alternative, etc. definiert sind, haben alle Subtypen eine gemeinsame Syntax über den Aufbau des Responses. Vor allem ist die Trennung (Boundary) der Parts im RFC-2046 definiert.

Die ZfDR akzeptiert nur den Subtype multipart/form-data.

9.2 Erläuterung von multipart/form-data

Die folgende Dokumentation und darin aufgezeigte Lösungsideen auf Basis von Java dienen der Veranschaulichung und als Beispiel. Sie sind keine Produktempfehlung. Es können auch andere Programmiersprachen verwendet werden.

Mit der Einführung von Jakarta Restful Webservice 3.1 wurde die Unterstützung von Multipart durch die neu eingeführte Schnittstelle "EntityPart" standardisiert. Wie im Javadoc beschrieben ist, bietet diese Schnittstelle eine Java-Lösung für den Standard RFC 7578. In diesem RFC ist die Multipart-Response mit dem Subtyp "multipart/form-data" definiert. Weitere Information für die Nutzung von "EntityPart" können der Javadoc entnommen werden.

Die ZfDR hat diesen Standard übernommen. Die Response mit dem Subtyp "multipart/form-data" ist für die ZfDR in der Schnittstellen-Beschreibung (OpenAPI-Spezifikation) Version 3.0.1 definiert.

Für die Erstellung der Multipart-Response gibt es unterschiedliche Möglichkeiten. In der aktuellen Jakarta-EE-Version etwa sind das Interface "jakarta.ws.rs.core.EntitiyPart" und dazugehörige Instanz-Konstruktionsmechanismen vorhanden. Kompatible Server-Runtimes müssen eine Implementierung dieses Interfaces und der zugehörigen JAX-RS Komponenten enthalten.

Das Jakarta-Interface "EntityPart" bietet Methoden an, die für die Part-Konstruktion vom Typ "multipart/form-data" nach RFC 7578 restriktiv ausgelegt sind.

Pflichtdaten in den Parts, die aus den Anwendungsdaten stammen, werden durch die Interface-API immer gefordert.

Für den Header "Content-Disposition" etwa wird der Teil "name:..." durch die Interface-API gefordert, so dass "Content-Disposition: form-data;name=<,,,>" im jeweiligen Part nicht ausgelassen werden kann.Im Folgenden wird ein auf dem Openliberty-Microprofile-Server funktionierender Java-Code am Beispiel eines Anspruchsdaten-JSONs mit drei Ansprüchen und zwei Standmitteilungs-Dokumenten (PDFs) illustriert. Zwei Ansprüche im JSON referenzieren dabei dasselbe PDF-Dokument und der dritte Anspruch referenziert das andere PDF-Dokument.

```
@GET
@Path("/anspruchsdaten")
```

```
@Produces("multipart/form-data")
public Response getAnspruchsdaten(
  @HeaderParam("X-Anfrage-Id") UUID xAnfrageId,
  @HeaderParam("X-Request-Id") UUID xRequestId,
  @HeaderParam("X-Nachfragezaehler") Integer xNachfragezaehler,
  @HeaderParam("X-Identifikationsnummer")  String xIdentifikationsnummer,
  @HeaderParam("X-Geburtsdatum")  String xGeburtsdatum) throws IOException {

  List<EntityPart> entityParts = List.of(
    EntityPart.withName("Anspruchsdaten")
      .mediaType("application/json")
      .content(new ByteArrayInputStream(
        """
          {
            "unternehmens_kontaktinformationen": "...",
            "ansprueche: [
              { ...
                "standmitteilung_referenz": "Referenz-1",
                ...
              },
              { ...
                "standmitteilung_referenz": "Referenz-1",
                ...
              },
              { ...
                "standmitteilung_referenz": "Referenz-2",
                ...
              }
            ]
          """.getBytes()))
      .build(),
    EntityPart.withName("Referenz-1")
      .mediaType("application/pdf")
      .content(new ByteArrayInputStream("%PDF-1% < Irgendein inhalt 1 >
%EOF".getBytes()))
      .build(),
    EntityPart.withName("Referenz-2")
      .mediaType("application/pdf")
      .content(new ByteArrayInputStream("%PDF-1% < Irgendein inhalt 2 >
%EOF".getBytes()))
      .build()
  );

  return Response.ok(new GenericEntity<List<EntityPart>>(entityParts){}).build();
}
```

9.3 Gegenüberstellung von vorherigem Format (bis Juli 2025) multipart/mixed und aktuellem Format multipart/form-data

Der von der ZfDR vormals verwendete Media-Typ multipart/mixed kommt aufgrund der neu eingeführten Multipart-Unterstützung von JakartaEE nicht mehr zum Einsatz.

Die wesentliche Änderung von multipart/mixed zu multipart/form-data ist die Referezierung der PDF-Parts in Multipart-Response. Der Content-Typ multipart/form-data bietet über einen Content-Disposition Header die Möglichkeit an, für Multipart's Namen zu vergeben. Die ZfDR nutzt diesen Header, um die Referenz zwischen dem Baustein im JSON-Part und der dazugehörigen PDF herzustellen.

Der Content-Disposition Header hat dabei folgenden Aufbau:

Content-Disposition: form-data; name="standmitteilung_referenz_01"

Die Namensgebung des Parts folgt über das Feld "name", das für die Herstellung der Referenz zu dem dazugehörigen Unterbaustein über das JSON-Feld "standmitteilung_referenz" benutzt wird.

Der Aufbau der Nachricht kann auch Kapitel 3.2.2, Abbildung 2, entnommen werden.

Für die Erkennung seitens DRIS von Anfragedaten-JSON und PDFs in HTTP-Multiparts sind in beiden Varianten folgende Header zu verwenden.

multipart/form-data

- Anfragedaten-JSON:
  Content-Type: application/json
  Content-Disposition: form-data; name="[beliebig]"

- PDF:
  Content-Type: application/pdf
  Content-Disposition: form-data; name="[Referenz-ID aus Anfragedaten-JSON]"

multipart/mixed

- Anfragedaten-JSON:
  Content-Type: application/json
- PDF:
  Content-Type: application/pdf
  X-Standmitteilung-Referenz:"[Referenz-ID aus Anfragedaten-JSON]"

Um die Unterschiede am realen Beispiel zu sehen, sind hierbei zwei Multipart-Response jeweils mit " form-data" und " mixed" exemplarisch dargestellt.

```
HTTP/1.1 200 OK
Content-Language: en-US
Content-Type: multipart/form-data; boundary=266cd242-31d2-4f69-bc52-657dec77650e
Date: Mon, 27 Jan 2025 11:16:30 GMT
Transfer-Encoding: chunked

--266cd242-31d2-4f69-bc52-657dec77650e
Content-Disposition: form-data; name="AnfrageDaten"
Content-Type: application/json

{
   "unternehmens_kontaktinformationen": {…},
   "ansprueche": [
      {
         (…),
         "standmitteilung_referenz": "Platzhalter-Standmitteilungen"
      }
   ]
}
--266cd242-31d2-4f69-bc52-657dec77650e
Content-Disposition: form-data; name="Platzhalter-Standmitteilungen"
Content-Type: application/pdf

%PDF-1.7
[...]
%%EOF
--266cd242-31d2-4f69-bc52-657dec77650e--
```

Beispiel-Payload für eine multipart/form-data Nachricht

```
HTTP/1.1 200 OK
Content-Language: en-US
Content-Type: multipart/mixed; boundary=266cd242-31d2-4f69-bc52-657dec77650e
Date: Mon, 27 Jan 2025 11:16:30 GMT
Transfer-Encoding: chunked

--266cd242-31d2-4f69-bc52-657dec77650e

Content-Type: application/json

{
   "unternehmens_kontaktinformationen": {…},
   "ansprueche": [
      {
         (…),
         "standmitteilung_referenz": "Platzhalter-Standmitteilungen"
      }
   ]
}

--266cd242-31d2-4f69-bc52-657dec77650e

Content-Type: application/pdf

X-Standmitteilung-Referenz: Platzhalter-Standmitteilungen

%PDF-1.7

[...]

%%EOF
--266cd242-31d2-4f69-bc52-657dec77650e—
```

Beispiel-Payload für eine multipart/mixed Nachricht

9.4 Validierung

Die ZfDR validiert jeden Antwortdatensatz auf Konformität zum definierten Schema. Dies beinhaltet alle Facetten der darin definierten Schemata, wie Pattern-, Type-, Format- und Längenrestriktionen, Existenz und Befüllung von required-Attributen, sowie die Zuordenbarkeit der Anspruchsdaten zu den PDF-Dokumenten. Bei einer erkannten Verletzung des Schemas wird von der ZfDR der definierte Endpunkt zur Übermittlung von Fehlern mit entsprechendem Fehlercode aufgerufen. Der fehlerhafte Datensatz wird von der ZfDR nicht weiterverarbeitet und auch dem/der Nutzenden nicht dargestellt. Exemplarische Hinweise zur Validierung einzelner Datensatzattribute sind im 'KHB Allgemeine und fachliche Grundlagen' aufgeführt.

9.5 De-referenzierte Version des Spezifikationsdokuments

Im Spezifikationsdokument werden Referenzen $ref: auf einzelne Teil-Schemata verwendet, um Redundanzen zu reduzieren und das Dokument möglichst kompakt zu halten. Sollte es erforderlich sein, eine Variante der Spezifikation mit vollständig aufgelösten Referenzen zu

verwenden, so kann aus einer Variante mit Referenzen eine dereferenzierte Variante erzeugt werden.

Hierfür bietet die swagger-cli einen entsprechenden Befehl (im Beispiel trägt das Quell-Dokument den Namen vorsorgeeinrichtung.yaml und das Zieldokument den Namen vorsorgeeinrichtung-deref.yaml)

```
swagger-cli bundle vorsorgeeinrichtung.yaml --outfile vorsorgeeinrichtung-deref.yaml --type yaml --dereference
```

9.6 Linksammlung

Begleitend zum Kapitel 8 'Implementation der Schnittstelle' wird auf folgende frei verfügbare Informationsquellen aus dem Internet verwiesen.

- openapi-generator-maven-plugin
- Liste der Server-Generatoren
- Allgemeine Generator-Konfiguration des openapi-generator-maven-plugin
- jaxrs-spec-Generator
- Standard-Templates des jaxrs-spec Generators
- JsonbSerializer
- Multipart-Handling mit org.apache.cxf
- Multipart-Handling mit resteasy-multipart-provider
- Multipart-Handling mit websphere-appserver-api-jaxrs20
- Swagger-cli

10 IT-Sicherheit

Die Deutsche Rentenversicherung richtet ihre Maßnahmen zur Sicherstellung der Informationssicherheit am IT-Grundschutz des Bundesamtes für Sicherheit in der Informationstechnik (BSI) aus.

Ziele und (Mindest-)Standards zur Sicherheit der Informationstechnik für die Rentenversicherung sind in einem mehrstufigen Regelwerk zur Sicherheit bei der Informationsverarbeitung (Informationssicherheits-Policy) festgehalten. Die Leitlinie zur Informationssicherheit und Grundzüge der Informationssicherheit stehen unter dem folgenden Link zur Verfügung:

Leitlinie zur Informationssicherheit und Grundzüge der Informationssicherheit

Um Gefährdungen entgegenzuwirken, hat die DRV Bund geeignete und angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse, die für die Funktionsfähigkeit der betriebenen kritischen Infrastrukturen maßgeblich sind, getroffen. Diese werden in vertraulichen Basis- und Verfahrens IT-Sicherheitskonzepten dokumentiert. Dabei wird der aktuelle Stand der Technik eingehalten.

Abbildung 7: Schaubild Kommunikationssicherheit

HINWEIS:

Erkennt die ZfDR bei der Verarbeitung einer Antwort von einer Vorsorgeeinrichtung einen Virus, dann wird die Verarbeitung im angepasst synchronen Verfahren direkt abgebrochen.

Es erfolgt kein erneuter Anfrageversuch und die individuelle Anfrage wird als nicht beantwortet abgeschlossen. Für diesen Fall gibt es keine gesonderte Fehlerrückmeldung. Ggf. nehmen Mitarbeiter der ZfDR Kontakt mit der Vorsorgeeinrichtung auf.

11 Prognosen zur Kommunikationslast (Mengengerüst)

Zur Einschätzung der Kommunikationslast werden Lastszenarien dargestellt, welche mit Maximalwerten sehr vorsichtige Annahmen treffen:

Personenkreis: 55 Mio[7] . Personen im Alter 18-67 in Deutschland

Nutzungszeitraum: primär in der Freizeit Mo-Fr 17-22 Uhr, Sa-So 8-24; ca. 55 Std/Woche | ca. 230 Std/Monat | 2760 Std/Jahr

Häufigkeit: Alle betroffenen Personen prüfen jährlich ihren Stand

Die Szenarien gehen davon aus, dass alle 55 Mio. Personen die Abfrage durchführen. Die Zahlen sind als Maximalwerte zu betrachten. Die Szenarien gehen von den oben dargestellten Nutzungszeiträumen aus. Bei Öffnung dieser Zeiten würde sich die Last verteilen. Die Szenarien gehen davon aus, dass stets alle Vorsorgeeinrichtungen angefragt werden – für die einzelnen Vorsorgeeinrichtungen ergeben sich damit voraussichtlich nochmals niedrigere Zahlen, wenn nicht immer alle Vorsorgeeinrichtungen angefragt werden. Ausgenommen aus der Betrachtung sind eventuelle Stoßzeiten durch mediale Berichterstattungen.

Szenario 1 (Worst Case): Alle betroffenen Personen prüfen monatlich ihren Stand

~70 Anfragen/Sekunde/Vorsorgeeinrichtung

Szenario 2 (Use Case): Alle betroffenen Personen prüfen jährlich ihren Stand

~6 Anfragen/Sekunde/Vorsorgeeinrichtung

Realistischer Case: Die meisten Personen prüfen nur alle paar Jahre

~1 Anfragen/Sekunde/Vorsorgeeinrichtung

[7] Quelle:
Statista, circa 51 Millionen Menschen im Alter von 18-65 Jahren; aufgerundet, um die Altersgruppe 66-67 zu erfassen

12 Unterstützung der Kommunikationspartner

Sie erreichen die ZfDR wie folgt:

Website:	https://zfdr-vorsorgeeinrichtungen.drv-bund.de
	https://rentenuebersicht.de (für Bürgerinnen und Bürger)
E-Mail:	zfdr-anbindung@drv-bund.de
Anschrift:	Deutsche Rentenversicherung Bund
	Zentrale Stelle für die Digitale Rentenübersicht
	10868 Berlin
Servicetelefon:	030 865 78787

(nur für Vorsorgeeinrichtungen, nicht zur Weitergabe an Nutzende der Digitalen Rentenübersicht)

Vorsorgeeinrichtungen wird empfohlen den Newsletter der ZfDR zu abonnieren (siehe Website).

13 Änderungsübersicht

Version	Datum	Kapitel	Bemerkungen
15.00.00	11.09.2026	0.6	letzte Spalte ergänzt in Tabelle
		2.1	Änderung auf DIN-Norm 91379
		5.2	neues Feld im Anbindungsformular (Postfach)
		5.4	Kapitel ersetzt durch ‚Umwandlung von Unternehmen (insbesondere Fusion)‘
		6.1	Verlinkung zum Trustcenter eingefügt
		6.4	Anpassung bzgl. des neuen Zertifikats
14.00.00	03.02.2026	6.3/6.5	Neue CSR erfordert auch neuen privaten Schlüssel
		6.11	OrganizationName (O) und OrganizationUnitName (OU) im Beispiel-Code mit Zeilenumbruch voneinander getrennt
13.00.00	10.12.2025	3.1	Beispielhafter zusätzlicher nicht verarbeitungsrelevanter Parameter eingefügt
		4.1	Neue Fehlernummer_0006 eingefügt ‚unzulässigen retry-after-Zeitraum‘
		6.5	Beschreibung der Zertifikatserneuerung ergänzt
		6.13	Länderliste um Frankreich (FR) ergänzt
12.00.00	24.06.2025	0.6	Links ausgetauscht
		3.2.2	insbesondere Kapitel 3.2.2; Übernahme der Bilder aus dem Tech-Café, Text zu der Fehlernummer _0003, Beispiel XML in Kapitel 7.3.1.1, 9.5
		4.1	Text zu der Fehlernummer _0003
		9.2 und ehemals 9.5	Zusammenfassung der Kapitel 9.5 Multipart/form-data

		9.3 (alt)	Multipart/mixed Kapitel gelöscht (veraltet)
		9.3 (neu)	Ehem. Kapitel 5 - redaktionelle Überarbeitung, Übernahme der Bilder aus dem Tech-Café
11.00.00	27.02.2025	6.3	Aufnahme countryName
		6.13	zulässige Länderkennzeichen gem. ISO-Liste 3166
10.00.00	26.11.2024	3.1	Link unter Tabelle 3 ausgetauscht
09.00.00	19.11.2024	9	Komplette Überarbeitung
08.00.00	23.10.2024	2.1	Kleine Textanpassung
		3.1	Kleine Textanpassung
		3.2.2	Textanpassung für multipart/form-data
		5.2	Anpassung in den Erläuterungen zur Anfrage-/Fehler-Endpunkt-URL (QS/PROD)
		9	Einführung multipart/form-data
07.00.00	28.08.2024	0.6	Anpassung der Links (Ablageort)
		5.1	Schaubild und Text angepasst
		6.3.	Attribut alternative-Name aufgenommen
		6.11	kleinere Textanpassung
		7.2	Text komplett überarbeitet
		9.1	Text überarbeitet
06.00.00	14.05.2024	7.3	Beschreibung des automatisierten Testverfahrens aktualisiert
05.00.00	30.04.2024	6.3	Hinweis zur CRT-Datei aufgenommen
		7.3	Beschreibung des automatisierten Testverfahrens
04.00.00	15.03.2024	1.1	Aufnahme neues Kapitel mit wichtigen Anmerkungen zur Anbindung
		1.2	Hinweis zur verpflichten Anbindung aufgenommen
		1.7	Aufnahme Kapitel 1.6 analog zum "KHB Verfahren"

		1.8	Hinweis zur verpflichten Anbindung aufgenommen
		5.2	Anpassungen in Tabelle 6: Aufnahme neuer Felder aus dem neuen Anbindungsformular
		7.2	Aufnahme Produktivsetzung
03.00.00	15.12.2023	3.1	Kapitel bezüglich Entfalls der Übermittlung des Geburtsdatums und der Steuer-Identifikationsnummer aus den Query-Parametern angepasst
		9.1	Multipart-Response bezüglich der Query- und Header-Parameter angepasst
02.00.00	02.10.2023	3.2.2	Reduzierung der Dateigröße der PDF-Standmitteilung
		6.3	Feldbelegungen der CSR-Datei
		6.9	Schreibfehler korrigiert
		6.11	Schreibfehler korrigiert
		7.1	Anforderungen an die Fachinformatik Systemintegration
01.00.00	30.06.2023	3.1	Hinweis zur Aktivierung der Mutual Identification Bevorstehende Änderungen im Anfragedatensatz ZV01
		4.1	Ablauf bei technischen Fehlern spezifiziert
		4.2	Fehlerereignisse aktualisiert
		5.1	Zeitraum der optimalen Anbindung ergänzt Zusammenhang Schnittstellentest und Aktivierung hinzugefügt
		7.1	Hinweis zum Zeitpunkt der Inanspruchnahme des Testverfahren
		13	URL der Website für Bürger*innen hinzugefügt