DVDV

Architekturkonzept und technische Dokumentation

Version: 2.0

Status: freigegeben

Stand: 21.12.2023

Änderungshistorie

Version	Datum	Änderung	Bearbeiter
2.0	21.12.2023	Komplette Überarbeitung des Dokumentes „DVDV 2.0 – Feinkonzept Architektur“	Birger Streckel, Ulrich Horst, Oliver Matz

Inhaltsverzeichnis

1 Einführung und Ziele

Dieses Dokument beschreibt die (Software-) Architektur, den Aufbau und die verwendeten Technologien des Deutschen Verwaltungsdiensteverzeichnisses (DVDV). Aufbau und Inhalt des Dokumentes orientieren sich am arc42-Standard für Architekturdokumentation[1].

1.1 Aufgabenstellung

1.1.1 DVDV

Das DVDV ist eine Infrastrukturkomponente für die sichere und verlässliche Adressierung von Behördendiensten. In diesem Verzeichnisdienst können technische Verbindungsdaten von Online-Diensten der öffentlichen Verwaltung hinterlegt werden, die zu ihrer Adressierung und Nutzung benötigt werden. Auskunftssuchende und Nutzer des DVDV sind in erster Linie Fachverfahren und Online-Dienste, keine menschlichen Nutzer.

Das DVDV bildet eine Basis für den Datenaustausch verschiedener Fachverfahren im deutschen Verwaltungsraum und hat damit die Funktion einer zentralen Registrierungsstelle für Online-Dienste der öffentlichen Verwaltung in Deutschland. Es trägt zum Aufbau von rechtsverbindlicher, elektronischer Kommunikation von und mit Behörden über die vorhandenen Fachverfahren auf höchstem Sicherheitsniveau bei.

Der Kern des DVDV ist der zentrale DVDV-Bundesmaster, der durch das ITZBund bereitgestellt wird. Er ist die einzige Stelle, bei der ein schreibender Zugriff auf die Datenbestände erfolgen kann. Der DVDV-Bundesmaster spiegelt seinen Datenbestand kontinuierlich auf dezentral aufgestellte DVDV-Server. Der Zugriff abfragender Stellen erfolgt ausschließlich auf DVDV-Servern.

Das ursprüngliche Konzept für das DVDV stammt aus dem Jahr 2004 und wurde nach Beauftragung durch den KoopA ADV implementiert. Das DVDV nahm nach einer Erprobungsphase am 1. Januar 2007 den operativen Betrieb auf, den es seither ohne Unterbrechung erbringt.

1.1.2 Aufgabenstellung bei der Neuentwicklung

In den Jahren 2018 und 2019 wurde die Codebasis des DVDV komplett modernisiert und funktional wesentlich erweitert. Dies sollte die Zukunftssicherheit des Systems gewährleisten. Zentrales Motiv war dabei, neben der Verbesserung der IT-Sicherheit, Stabilität, Performanz und Benutzerfreundlichkeit, insbesondere die Vorbereitung auf zukünftige Anforderungen, die sich aus den nationalen und europäischen Kontexten zur Digitalisierung von Verwaltungsdienstleistungen schon zu diesem Zeitpunkt abzeichneten. Die Migration von dem vorhergehenden auf das neue System erfolgte im Oktober 2019 ohne Einschränkung oder Unterbrechung der Nutzerverfügbarkeit.

Die Neuentwicklung des DVDV („DVDV 2.0“) wurde ausgeschrieben und enthielt bereits in den Ausschreibungsunterlagen detaillierte Vorgaben zu Anforderungen, Softwarearchitektur, einzusetzenden Technologien, Datenmodell und Schnittstellen, die umzusetzen waren.

[1] https://arc42.org/

1.2 Qualitätsziele

Aus den grundlegenden Anforderungen an die Neuentwicklung in 2018/19 des DVDV ließen sich insbesondere die folgenden Qualitätsziele ableiten.

Q-1	Die Integrität der Daten im DVDV muss jederzeit gewährleistet sein.
Q-2	Ein hohes Niveau der Softwarequalität nach ISO 9126 wird angestrebt.
Q-3	Es wird eine einfach zu bedienende Oberfläche erwartet.
Q-4	Stabile Performanz bei steigenden Nutzerzahlen.
Q-5	Sicherstellung der Funktionalität des abzulösenden Systems DVDV 1 bei gleichzeitiger Erweiterbarkeit des Datenmodells.

Tabelle 1: Qualitätsziele bei der Neuentwicklung des DVDV

1.3 Stakeholder

Die wesentlichen Stakeholder, die mit dem DVDV interagieren, sind in diesem Abschnitt aufgelistet.

Rolle	Beschreibung	Erwartungshaltung
Expertengruppe DVDV	Vertreter von Bund, Ländern und Kommunen entscheiden über die Ausrichtung von DVDV.	• Vorbereitung von Entscheidungen durch Fachgruppe und Produktmanagement
Koordinierende Stelle DVDV (KS)	Diese ist beim ITZBund am Standort Köln eingerichtet und übernimmt operative Aufgaben zur Sicherstellung des Betriebs sowie der fachlichen und technischen Weiterentwicklung des Produktes DVDV. Sie ist zentraler Ansprechpartner für alle weiteren Stakeholder.	• Einfache Administration • Gute Erweiterbarkeit • Kontinuierliche Wartung und Pflege
Produktmanagement DVDV	Das Produktmanagement bei der Föderalen IT-Kooperation AöR (FITKO) übernimmt die Beauftragung aller Maßnahmen zur Pflege, Anpassung und Weiterentwicklung, das Herbeiführen strategischer Entscheidungen, die Planung und Bewirtschaftung der Haushaltsmittel, die Leitung der Fach- und der Expertengruppe DVDV sowie die Vorbereitung von Entscheidungen des IT-Planungsrats.	• Kostengünstige und bedarfsorientierte Weiterentwicklung und Pflege • Unterstützung der technischen Stakeholder
Fachgruppe DVDV	Die Fachgruppe repräsentiert die Bedarfsträger, also die Behörden und anderen Organisationen der öffentlichen Verwaltung; sie übernimmt die Rolle des Lenkungsausschusses.	

Rolle	Beschreibung	Erwartungshaltung
Dienstanbietende Organisationen oder Service Provider	Die Daten ihrer Dienste bilden den Kern des DVDV. Hinterlegt sind die technischen Verbindungsparameter für die Dienstnutzung.	• Hohe Verfügbarkeit der Daten • Schutz gegen Manipulation
Pflegende Stellen (PS)	Diese pflegen die Daten im DVDV im Auftrag der Dienstanbieter. Pro Bundesland gibt es eine PS, nur diese darf die Daten pflegen.	• Einfache Datenpflege
Provider	Dies sind IT-Dienstleister für die öffentliche Verwaltung, die Infrastruktur und Zertifikate im DVDV-Kontext betreiben und bereitstellen.	• Überprüfung der korrekten Pflege durch Bereitstellung geeigneter Sichten im Auskunfts-Client.
DVDV-Bundesmaster-Betreiber	Das ITZBund ist der Betreiber des zentralen DVDV-Bundesmasters.	• Einfache Betreibbarkeit des DVDV-Bundesmasters, Systemumsetzung entsprechend der Betriebsvorgaben
DVDV-Server-Betreiber	In 14 über das Bundesgebiet verteilten Rechenzentren werden DVDV-Server betrieben.	• Einfache Betreibbarkeit des DVDV-Servers • Betrieb auf Basis von Open-Source-Software
Fachverfahrenhersteller	Fachverfahren und Clearingstellen nutzen das DVDV zum Abrufen von Dienstinformationen.	• Möglichst einfache Integration in die eigene Software • Performanz und hohe Verfügbarkeit bei Datenabrufen • Anforderungsgetriebene Umsetzung der Schnittstellen

Tabelle 2: Liste der Stakeholder

2 Randbedingungen

2.1 Technische Randbedingungen

2.1.1 Grobkonzept DVDV

Im Vorfeld der Ausschreibung zu DVDV 2.0 im Jahr 2018 wurde vom Auftraggeber ein detailliertes Grobkonzept für die zu entwickelnde Software erstellt. In diesem wurde das System bereits modelliert und wichtige Architekturentscheidungen wurden getroffen und vorgegeben. Das Grobkonzept ging als Grundlage in dieses Architekturkonzept ein und lieferte den konzeptionellen Rahmen. In weiten Teilen waren die dort getroffenen Entscheidungen verbindliche Vorgaben für die anschließende Phase der Softwareerstellung (vgl. Abschnitt 4.1).

2.1.2 Mengengerüst

Für das Mengengerüst werden unterschiedliche Quellen herangezogen. Einerseits werden die Vorgaben aus der Ausschreibung aufgeführt und den aktuellen Zahlen gegenübergestellt. Die aktuelle Prognose stellt eine stark steigende Zahl an Daten und Datenabrufen in Aussicht, da im Rahmen der OZG-Umsetzung eine Vielzahl von neuen Verfahren, Schnittstellen und Kommunikationsszenarien berücksichtigt werden muss.

2.1.2.1 Daten

Für das Mengengerüst werden die Anforderungen aus der Ausschreibung den aktuellen Zahlen zum Zeitpunkt der Erstellung des Dokumentes gegenübergestellt.

	Anforderung aus der Ausschreibung	**Stand 08/2023**
Zahl von Behörden und Einrichtungen der öffentlichen Verwaltung	50.000	35.472
Zahl von eingetragenen Diensten	Keine Vorgabe	78.715
Zahl von eingetragenen Dienstbeschreibungen	Keine Vorgabe	634

Tabelle 3: Mengengerüst Daten

2.1.2.2 Datenabrufe

Die Datenabrufe durch Fachverfahren werden in der absehbaren Zukunft durch die OZG-Umsetzung und viele neue Stakeholder weiter stark steigen. Für das Mengengerüst werden die Anforderungen aus der Ausschreibung den aktuellen Zahlen zum Zeitpunkt der Erstellung des Dokumentes und den Messungen aus einem Last- und Performancetest vom Oktober 2022 gegenübergestellt.

	Anforderung aus der Ausschreibung	**im Betrieb gemessen Stand 08/2023**	**Maximum lt. Lasttest**
Maximale Anzahl lesender Zugriffe pro Sekunde auf jedem DVDV-Server	1,5 Zugriffe / s	In Stoßzeiten 7 Zugriffe / s auf dem Dataport-Server aus 5 Bundesländern	150 Zugriffe / s über einen längeren Zeitraum

Tabelle 4: Mengengerüst Datenabrufe

2.1.2.3 Infrastruktur

Die Anzahl der Betreiber von DVDV-Servern ändert sich absehbar nur wenig.

	Stand 08/2023
Anzahl Bundesmaster	1
Anzahl DVDV-Server	14

Tabelle 5: Mengengerüst Infrastruktur

2.2 Betriebliche Randbedingungen

Das DVDV wird in einer föderal verteilten Struktur betrieben. Dabei übernimmt das ITZBund den DVDV-Bundesmaster. In der Verantwortlichkeit der Bundesländer wird eine Reihe von DVDV-Servern betrieben, die mit dem DVDV-Bundesmaster kommunizieren und Anfragen der Anwender beantworten. Diese Server vertreten sich gegenseitig bei Ausfällen. Diese Struktur wurde mit den Anfängen von DVDV in 2004 so entworfen und organisatorisch und vertraglich umgesetzt und sollte bei der Neuentwicklung 2018 beibehalten werden.[2]

Aus diesem Betriebsmodell ergeben sich Anforderungen für die einzusetzende Infrastruktur, außerdem sind die betrieblichen Vorgaben des ITZBund einzuhalten.

	Betriebliche Randbedingungen
BR1	Die betriebliche Struktur von DVDV 1 mit DVDV-Bundesmaster und DVDV-Servern muss in DVDV 2.0 beibehalten werden.
BR2	Für den DVDV-Bundesmaster wird die einzusetzende Server-Software wie folgt vorgegeben: • Application Server auf JBoss EAP in der aktuellen Version • Datenbank auf MySQL unter Linux
BR3	Für den Datenaustausch mit den DVDV-Servern wird die binäre Replikation der MySQL-Datenbank vorgeschrieben. Diese stellt betriebliche Anforderungen an die DVDV-Server-Betreiber hinsichtlich der einzusetzenden Datenbank.
BR4	Die Datenbanken der DVDV-Server werden nicht individuell gepflegt, sondern entsprechen immer zu 100% dem Datenbestand des DVDV-Bundesmasters.
BR5	Die DVDV-Server werden in unterschiedlichen Umgebungen betrieben, hier müssen die Systemanforderungen einen Mindeststandard vorschreiben.

Tabelle 6: Betriebliche Randbedingungen für DVDV

[2] vgl. Abschnitt 4.1

3 Kontextabgrenzung

Das folgende Diagramm stellt die beteiligten Systeme im vollständigen Kontext dar. Das Gesamtsystem DVDV umfasst dabei alle im Rahmen dieses Konzeptes aufzubauenden Systeme, also den DVDV-Bundesmaster und alle DVDV-Server.

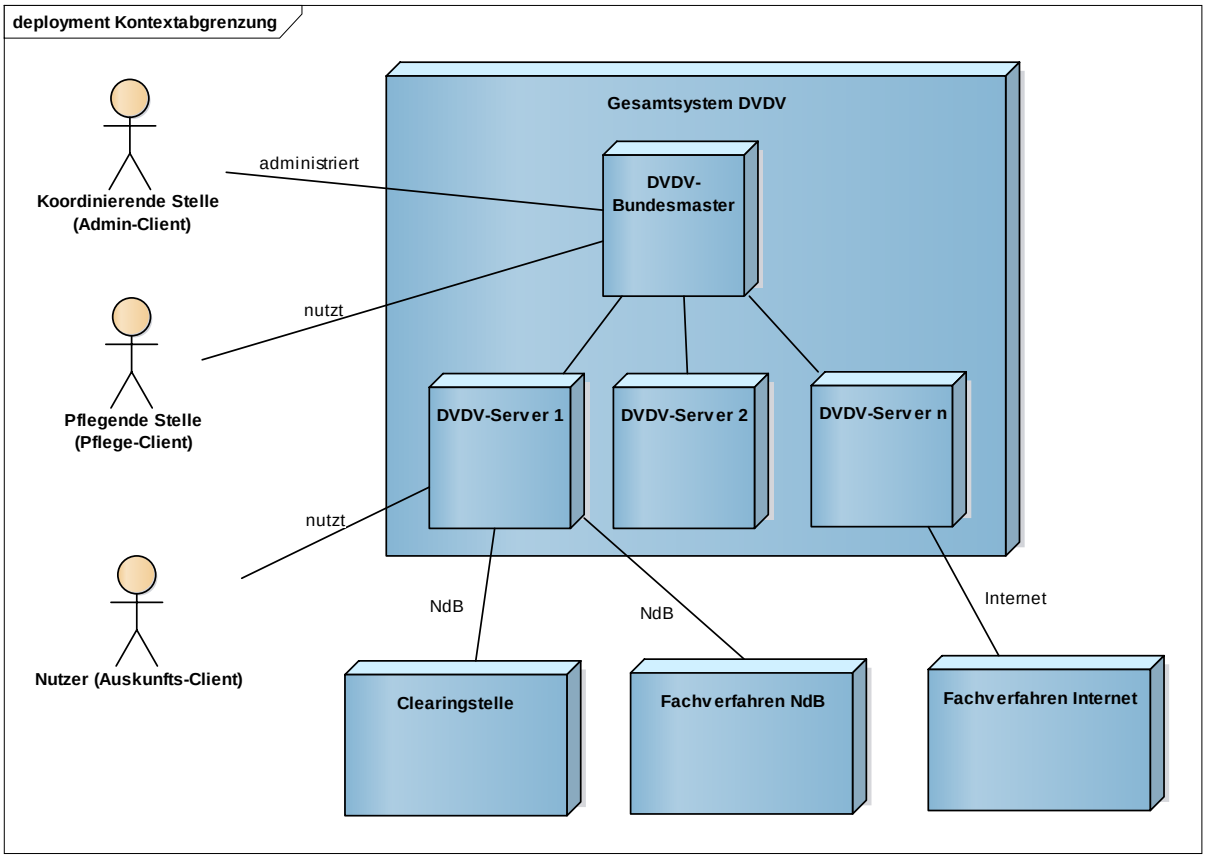


Abbildung 1: Kontextabgrenzung

Der Systemkontext teilt sich auf in zwei primäre Systemgruppen: Webapplikationen für Zugriffe über den Browser und angebundene Systeme für Datenabfragen.

Diese können jeweils über das Internet oder über das Netz des Bundes (NdB) auf das System zugreifen. Alle Zugriffe auf das System werden durch Authentifizierung und Autorisierung abgesichert.

3.1 Browserzugriffe auf Webapplikationen

Anwender können über einen Browser auf Webapplikationen des Systems zugreifen, um Auskünfte zu erhalten und zur Datenpflege. Die Webapplikationen teilen sich auf in drei separate Systeme:

1. Admin-Client am DVDV-Bundesmaster (lesender und schreibender Zugriff)
2. Pflege-Client am DVDV-Bundesmaster (lesender und schreibender Zugriff)
3. Auskunfts-Client an jedem DVDV-Server (nur lesender Zugriff)

3.2 Angebundene Systeme

Fachverfahren und Clearingstellen kommunizieren über Dienste miteinander. Diese Dienste werden im Allgemeinen von den Fachverfahren angeboten. Die Informationen zu diesen Diensten sind im DVDV hinterlegt und werden dort zum Zwecke des Kommunikationsaufbaus und zur Überprüfung der Kommunikationspartner abgerufen.

Schnittstellen

Alle Schnittstellen für angebundene Systeme des DVDV sind als http-Schnittstellen umgesetzt, die nach den REST-Designprinzipien entwickelt werden. Sie sind als klassische Webservices ausgeprägt.

Der DVDV-Bundesmaster bietet die folgenden Schnittstellen für externe Systeme an:

- Die Komponente DVDV-IAM (Identity und Access Management) innerhalb des DVDV-Bundesmasters bietet Schnittstellen für Authentifizierung und Autorisierung entsprechend der Keycloak-Dokumentation. Insbesondere wird auch eine Schnittstelle zur Herausgabe von Authentifizierungs-Token angeboten. Diese Token können an den DVDV-Servern für den Datenzugriff über die Directory-Schnittstelle genutzt werden.
- Zusätzlich setzt die Komponente DVDV-IAM zur Provisionierung von Identitäten den SCIM-Standard[3] um. Diese wurde als separates Modul implementiert und an den Keycloak angebunden.

Der DVDV-Server bietet die folgenden Schnittstellen für externe Systeme an:

- Directory-Schnittstelle: Die Directory-Schnittstelle wird für Datenabfragen durch Fachverfahren und Clearingstellen genutzt. Sie bietet die im DVDV-hinterlegten Daten sehr performant und für hohe Anfragelasten optimiert an. Sie wird in drei Varianten bereitgestellt:
    1. Ohne Authentifizierung für anfragende Systeme aus dem gleichen Rechenzentrum
    2. Mit Authentifizierung mittels JWT-Token, herausgegeben an der Token-Schnittstelle des DVDV-Servers
    3. Mit Authentifizierung mittels JWT-Token, herausgegeben an der Token-Schnittstelle des DVDV-Bundesmasters (Komponente DVDV-IAM)
- Token-Schnittstelle: Herausgabe von Authentifizierungs-Token für den Datenzugriff über die Directory-Schnittstelle
- Legacy-Schnittstelle: Für zu DVDV1 kompatible OSCI-Anfragen durch Fachverfahren und Clearingstellen; diese soll mittelfristig abgebaut und durch die Directory-Schnittstelle ersetzt werden.

[3] RFC 7644, System for Cross-domain Identity Management (SCIM): Protocol, September 2015 (https://tools.ietf.org/html/rfc7644)

4 Lösungsstrategie

Die Lösungsstrategie wurde durch die Vorgängeranwendung und die Ausschreibungsunterlagen weitgehend vorgegeben. Architekturentscheidungen waren daher nur in Einzelfällen zu treffen.

4.1 Vorgaben aus der Ausschreibung

Die folgenden Vorgaben wurden bei der Entwicklung von DVDV umgesetzt.

	Vorgaben Lösungsstrategie
VL1	Nutzung von JBoss oder WildFly als Application-Server
VL2	Nutzung von Keycloak als IAM-Komponente
VL3	Nutzung von MySQL als Datenbank
VL4	Verteilte Architektur mit einem Bundesmaster und verteilten, redundanten DVDV-Servern auf Länderebene
VL5	Datenabgleich zwischen DVDV-Bundesmaster und DVDV-Servern mittels binärer Replikation auf Datenbankebene
VL6	Umsetzung in der Programmiersprache Java
VL7	Umsetzung der Clients als Web-Clients in der JSF-Technologie
VL8	Umsetzung der Directory-Schnittstelle nach dem REST-Paradigma
VL9	Einhaltung des Styleguides der Bundesregierung für Webanwendungen im Stand von 2018
VL10	Umsetzung der Benutzerprovisionierung am DVDV-IAM über eine Schnittstelle nach dem SCIM-Standard[4]
VL11	Umsetzung der Autorisierung nach dem OAuth 2.0 und OpenID Connect Standard
VL12	Umsetzung des Logging mit Log4j und einem Mapped Diagnostic Context
VL13	Absicherung durch Https in Verbindung mit Client-Zertifikaten

Tabelle 7: Betriebliche Randbedingungen für DVDV

4.2 Architekturentscheidungen bei der Systemkonzeption

Über diese Vorgaben hinaus wurden einige ergänzende Architekturentscheidungen getroffen, die in den Ausschreibungsunterlagen offengeblieben waren. Wesentliche Entscheidungen betrafen die Aufteilung des Gesamtsystems in separat zu entwickelnde Komponenten sowie die

[4] RFC 7644, System for Cross-domain Identity Management (SCIM): Protocol, September 2015 (https://tools.ietf.org/html/rfc7644)

Schnittstellenarchitektur und Schnittstellentechnologien zwischen diesen Komponenten. Weitere Entscheidungen betrafen den Daten- und Kompetenz-Schnitt zwischen IAM-Komponente und Kernsystem, die Authentifizierung sowie für das Framework zur Oberflächentechnologie.

Die getroffenen Architekturentscheidungen werden im Folgenden erläutert. Die Komponentenzerlegung wird in der Bausteinsicht in Abschnitt 5 erläutert.

4.2.1 Schnittstellentechnologie Client-Server-Kommunikation

ID	**AE_1**
Thema	Schnittstellentechnologie zwischen Client-Anwendungen und Server-Komponenten
Motivation	Unabhängigkeit der Client-Anwendungen von den Server-Komponenten
Annahmen	
Alternativen	1. Zugriff über eine http-Schnittstelle nach dem REST-Paradigma 2. Zugriff über JavaBean-Technologie (RMI/IIOP)
Entscheidung	Zugriff über eine http-Schnittstelle nach dem REST-Paradigma (Alternative 1).
Erläuterung	Der Zugriff über eine http-Schnittstelle nach dem REST-Paradigma bietet die folgenden Vorteile, die in der Summe überwiegen: Maximale Entkopplung von Client und Serverkomponenten. Dies ist wichtig für die zukünftige Pflege und Weiterentwicklung. Damit wird der Austausch einzelner Clientkomponenten oder die Hinzunahme weiterer Clients für Spezialabfragen ermöglicht. Ein späterer Wechsel des Application-Servers wird erleichtert, da nicht alle Application-Server die RMI-Technologie unterstützen. Demgegenüber steht ein etwas höherer Entwicklungsaufwand für die REST-Fassade der Serversysteme, da diese alle Funktionalitäten der Clientanwendungen komplett unterstützen muss. Zudem ist bei der Client-Server-Kommunikation ein minimaler Performance-Verlust der Client-Anwendung zu erwarten, der sich jedoch in der Nutzererfahrung nicht bemerkbar machen wird.

4.2.2 Komponentenframework zur Erweiterung von JSF

ID	**AE_2**
Thema	Komponentenframework zur Erweiterung von JSF
Motivation	Einfachere Umsetzung von einheitlichen und attraktiven Benutzeroberflächen durch Nutzung einer Komponentenbibliothek
Annahmen	
Alternativen	1. Nutzung von PrimeFaces 2. Nutzung von ICEfaces 3. Nutzung von Apache MyFaces 4. Nutzung von RichFaces

	5. Nutzung von nativem JSF
Entscheidung	Nutzung von PrimeFaces (Alternative 1).
Erläuterung	Die Nutzung einer Komponentenbibliothek ist für die Umsetzung einer attraktiven Benutzeroberfläche in JSF beinahe eine Notwendigkeit, da eine Umsetzung auf Basis von reinem JSF einen sehr hohen Aufwand darstellt. Von den untersuchten Komponentenbibliotheken hatte zum Zeitpunkt des Entwicklungsstarts allein PrimeFaces eine nennenswerte Verbreitung, die anderen Frameworks wurden kaum noch eingesetzt oder die Weiterentwicklung war im Falle von RichFaces bereits eingestellt.

4.2.3 Verortung der Autorisierung

ID	**AE_3**
Thema	Verortung der Autorisierung im Gesamtsystem
Motivation	Die Autorisierung von Identitäten für den Datenzugriff ist an einer zentralen Stelle unterhalb der Serviceschicht des Kernsystems durchzuführen. Die Autorisierung muss auf Basis von gemeinsamen Daten zwischen den Systemen Kernsystem und IAM getroffen werden. Für die Übermittlung der Autorisierungsinformationen bzw. der Autorisierungsentscheidung ist eine Schnittstelle zwischen den Teilsystemen Kernsystem und IAM notwendig.
Annahmen	
Alternativen	1. Die Autorisierung wird im DVDV-IAM durchgeführt. Die Software Keycloak, mit der das DVDV-IAM umgesetzt wird, bietet eine entsprechende Schnittstelle an, die eine Delegation der Entscheidung vom Kernsystem an das IAM unterhalb der Service-Schicht ermöglicht. 2. Die Autorisierung wird im Kernsystem durchgeführt, dazu werden die Rechte an ResourceGroups gebunden. Diese umfassen jeweils eine Menge von Ressourcen im Kernsystem, für die die Autorisierung gilt. Es wird dem Kernsystem vom IAM mitgeteilt, für welche ResourceGroups die anfragende Identität welche Berechtigungen besitzt.
Entscheidung	Die Autorisierung wird im Kernsystem durchgeführt (Alternative 2).
Erläuterung	Die Schnittstelle von Keycloak ermöglicht lediglich Autorisierungen für alle Daten eines Typs, so kann z.B. der Zugriff auf alle Ressourcen im System autorisiert werden, aber nicht der Zugriff auf Ressourcen mit einer bestimmten Eigenschaft, z.B. alle Ressourcen aus einem bestimmten Bundesland. Dies reicht für die gegebenen Anforderungen an die Autorisierung nicht aus. Alternative 2 ist damit die einzige Umsetzungsmöglichkeit, die die Anforderungen abbilden kann.

4.2.4 Datenschnitt zwischen Kernsystem und IAM

ID	AE_4
Thema	Datenschnitt zwischen Kernsystem und IAM und Erweiterung von Keycloak
Motivation	Die Anforderungen beschreiben ein Rollen- und Rechtekonzept, das mit dem Datenmodell von Keycloak nicht ohne Anpassung abbildbar ist. Es bleibt freigestellt, ob eine Erweiterung des Datenmodells im DVDV-IAM oder im Kernsystem erfolgen soll.
Annahmen	
Alternativen	Die Erweiterung des Datenmodells erfolgt: 1. Im DVDV-IAM 2. Im Kernsystem mit einem Vertrauensanker im DVDV-IAM
Entscheidung	Die Erweiterung des Datenmodells erfolgt im DVDV-IAM als Erweiterung der Keycloak-Software (Alternative 1).
Erläuterung	Für eine Implementierung im Kernsystem spricht: • Geringerer Pflegeaufwand, da die Erweiterung beim Wechsel auf eine neuere Keycloak-Version nicht migriert werden muss. Gegen eine Implementierung im Kernsystem spricht: • Eine verteilte Datenhaltung im IAM und Kernsystem erfordert eine transaktionale Schnittstelle zwischen beiden Systemen, um inkonsistente Datenstände auszuschließen. Eine transaktionale Schnittstelle ist komplex in der Realisierung. • Die Rollen und Rechte werden für jeden authentisierten Benutzer ermittelt und im Access-Token weitergegeben. Jede Authentifizierung würde deshalb eine Abfrage der Rollen und Rechte vom IAM am Kernsystem erfordern. Das ist teuer und soll vermieden werden. Für eine Implementierung im DVDV-IAM spricht: • Die Erweiterungen sind überschaubar. Lediglich das Konzept der Stellvertreterregelungen ist in Keycloak nicht nativ implementiert. • Die Erweiterungen lassen sich mittels dafür vorgesehener öffentlicher API mit den Service Provider Interfaces in Keycloak einbinden. Gegen eine Implementierung im DVDV-IAM spricht: • Erweiterungen in Keycloak erhöhen den Pflegeaufwand, da die Erweiterung beim Wechsel auf eine neuere Keycloak-Version mit Schnittstellenänderung migriert werden muss. Die Vorteile einer Implementierung im DVDV-IAM überwiegen, weshalb diese Alternative gewählt wird.

4.2.5 Authentifizierungsverfahren

ID	AE_5

Thema	Authentifizierungsverfahren bei der Anmeldung der Pflegenden Stellen am DVDV-System
Motivation	Die IAM-Komponente Keycloak bietet für das Protokoll OAuth 2 verschiedene Verfahren zur Authentifizierung an. Hier ist eine eindeutige Entscheidung zu treffen.
Annahmen	
Alternativen	1. Benutzername und Passwort 2. Software-Zertifikat
Entscheidung	Software-Zertifikat (Alternative 2).
Erläuterung	Die Schutzbedarfsfeststellung hat den Schutzbedarf „hoch“ für das Schutzziel „Integrität“ ermittelt, was ein Vertrauensniveau „substanziell“ bei der Identifizierung nahelegt. Das Vertrauensniveau „substanziell“ setzt die Authentisierung mit zwei Faktoren voraus. Daher wird die Alternative der Authentisierung mittels Benutzername und Password (ein Faktor) verworfen zugunsten der Authentisierung mittels Software-Zertifikat. Ob die Verwendung von Software-Zertifikaten tatsächlich zu einer Einordung in das Vertrauensniveau „substanziell“ führt, hängt von weiteren Faktoren ab, vergleiche hierzu auch die BSI-TR-03107-1, Version 1.1, Abschnitt 4.2. Eine ausreichende Vorbereitung entsprechend der Anforderung ist durch die Verwendung dieses Authentisierungsverfahrens jedoch gegeben.

5 Bausteinsicht und Verteilungssicht

Da bei DVDV das Deployment des Gesamtsystems über mehrere Betreiber verteilt ist, können die Bausteinsicht und die Verteilungssicht nicht getrennt voneinander betrachtet werden und werden daher an dieser Stelle gemeinsam dargestellt.

5.1 Gesamtsystem

Das Gesamtsystem setzt sich aus mehreren Teilsystemen zusammen, die bei unterschiedlichen Betreibern und verteilt über mehrere Rechenzentren betrieben werden.

Darüber hinaus ist jedes der Teilsysteme in separat deploybare Systemkomponenten aufgeteilt, die sich jedes für sich aufsetzen und betreiben lassen. Diese Systemkomponenten sind bei den jeweiligen Teilsystemen beschrieben.

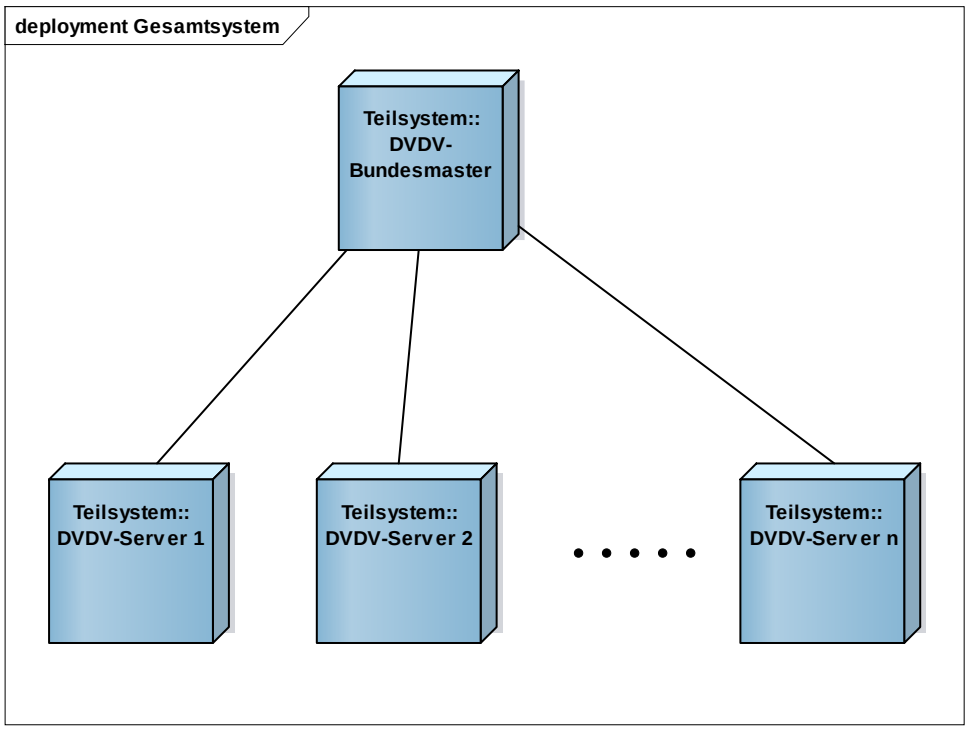


Abbildung 2: Deployment Gesamtsystem

Teilsystem	Zweck
DVDV-Bundesmaster	Administration des Gesamtsystems und Datenerfassung
DVDV-Server	Datenabruf und Dateneinsicht durch Externe

Tabelle 8: Teilsysteme des DVDV

5.1.1 DVDV-Bundesmaster

Der DVDV-Bundesmaster ist das führende System für alle Fach- und Authentifizierungsdaten, er wird zentral beim ITZBund betrieben. Am DVDV-Bundesmaster werden alle Datenänderungen durchgeführt, die im DVDV-Bundesmaster vorgehaltenen Daten sind maßgeblich. Der DVDV-Bundesmaster ist ausschließlich aus dem Netz des Bundes erreichbar.

Der Bundesmaster stellt das DVDV-Referenzsystem dar, sämtliche schreibende Zugriffe auf das DVDV erfolgen ausschließlich an diesem zentralen System durch dazu berechtigte „Pflegende Stellen“.

Regelungen für den Betrieb des Bundesmasters sind in einer Policy zusammengefasst, die von der Koordinierenden Stelle DVDV erarbeitet und herausgegeben wird.

5.1.2 DVDV-Server

Neben dem DVDV-Bundesmaster gibt es eine Reihe von DVDV-Servern. Entsprechend der Architektur des DVDV als Verbundverfahren mit föderalen Strukturen, werden die DVDV-Server vor allem von Rechenzentren in Länderhoheit betrieben. Es gibt einige Bundesländer mit genau einem DVDV-Server, andere Länder haben zwei DVDV-Server, während auch DVDV-Server betrieben werden, die für mehrere Bundesländer zuständig sind.

Lesende Zugriffe auf die DVDV-Daten werden ausschließlich an den in der ganzen Republik verteilten DVDV-Servern durchgeführt. Anfragen von Fachverfahren richten sich somit immer an einen der DVDV-Server, niemals an den zentralen Bundesmaster.

Dem Anspruch möglichst hoher Verfügbarkeit dient das Prinzip, dass jeder DVDV-Server einen anderen DVDV-Server vertraglich als Vertreter verpflichten muss. Der Vertreter übernimmt bei Ausfall des eigentlich zuständigen DVDV-Servers die während dieser Zeit eingehenden Anfragen. Der anfragende Client muss dazu die Vertretungsbeziehungen kennen und den Vertretungsserver in diesem Fall anfragen.

Durch die geschilderten Prinzipien zur Verteilung des Datenbestands über viele Standorte und die Vertreterregelung wird den wichtigen Forderungen nach Georedundanz und hoher Verfügbarkeit des Gesamtsystems DVDV Rechnung getragen.

Regelungen für den Betrieb und die Zusammenarbeit der DVDV-Server-Betreiber sind in einer Policy zusammengefasst, die von der Koordinierenden Stelle DVDV erarbeitet und herausgegeben wird.

5.1.3 Kommunikation zwischen den Teilsystemen

Die Teilsysteme DVDV-Bundesmaster- und DVDV-Server haben Kommunikationsbeziehungen und Schnittstellen sowohl auf Ebene der Application-Server, als auch auf Datenbankebene.

5.1.3.1 Schnittstellen auf Ebene der Application-Server

Alle Teilsysteme nutzen das zentrale DVDV-IAM des DVDV-Bundesmasters. Das DVDV-IAM wird sowohl vom Bundesmaster selbst, als auch von den DVDV-Servern zur Authentifizierung verwendet.

5.1.3.2 Schnittstellen auf Datenbankebene

Alle DVDV-Server erhalten exakt die gleichen Daten wie der DVDV-Bundesmaster. Datenänderungen finden ausschließlich am DVDV-Bundesmaster statt, dessen Bestand zu den DVDV-Servern synchronisiert wird. Entsprechend der Vorgabe VL5 muss die Synchronisation der Daten mittels binärer Replikation auf Datenbankebene erfolgen, sie findet daher laufend durch Source-Replica-Replikation der Bundesmaster-Datenbank als Quelle in die DVDV-Server-Datenbanken als Replika statt. Alle Daten sowie auch alle Benutzer und deren Zugriffsrechte sind damit an den DVDV-Servern exakt so wie am DVDV-Bundesmaster verfügbar.

5.2 Teilsysteme

Da beim DVDV das Deployment über mehrere Betreiber verteilt ist, sind die Deployment-Diagramme unterhalb des Gesamtsystems angesiedelt und werden in der Bausteinsicht betrachtet.

Die Teilsysteme DVDV-Bundesmaster und DVDV-Server werden als 3-Tier-Architekturen aufgesetzt.

- Im 1. Tier wird die Absicherung des 2. Tiers durch einen Reverse-Proxy vorgenommen, der Anfragen an das System filtert und weiterleitet.
- Im 2. Tier sind die Application-Server des DVDV angesiedelt. Auf diesen werden einerseits die Web-Clients (Pflege-Client, Admin-Client und Auskunfts-Client) gehostet und andererseits die Backend-Systeme Kernsystem und Identity and Access Management (IAM). Die Client-Systeme sind als JSF-Anwendungen umgesetzt. Alle Systeme werden auf JBoss EAP oder WildFly betrieben. Der Zugriff auf die Application-Server erfolgt aus dem Internet bzw. aus dem Netz des Bundes. Der Zugriff auf die Backend-Systeme (DVDV-Kernsystem) erfolgt ausschließlich über eine http-Schnittstelle.
- Im 3. Tier ist die MySQL Datenbank angesiedelt, in der die Application-Server die Daten persistieren.

In der folgenden Tabelle sind die Systemkomponenten des DVDV den Teilsystemen zugeordnet.

Systemkomponente	**Teilsystem**	**Zweck**
DVDV-Bundesmaster		
Admin-Client	DVDV-Bundesmaster	Administration des Gesamtsystems
Pflege-Client	DVDV-Bundesmaster	Datenerfassung für das Gesamtsystem
DVDV-IAM	DVDV-Bundesmaster	Keycloak-Server zur Benutzerverwaltung und Authentisierung/Autorisierung
Kernsystem	DVDV-Bundesmaster	Backend-System für die Fachdaten
Datenbank	DVDV-Bundesmaster	Datenhaltung für Kernsystem und IAM; hier werden Änderungen an den Daten durchgeführt
DVDV-Server		
Auskunfts-Client	DVDV-Server	Dateneinsicht durch Externe
Legacy-Facade	DVDV-Server	DVDV1-kompatibler Datenabruf
Kernsystem	DVDV-Server	Backend-System für die Fachdaten, hier für den Datenabruf verwendet
Datenbank	DVDV-Server	Datenhaltung für Kernsystem, hier ausschließlich Datenabruf
Unterstützung für angebundene Systeme		

DVDV-DevKit Java		Bibliothek und Beispiele für Java-Entwickler zur Unterstützung bei der DVDV-Anbindung über die Directory-Schnittstelle
DVDV-DevKit .NET		Bibliothek und Beispiele für .NET-Entwickler zur Unterstützung bei der DVDV-Anbindung über die Directory-Schnittstelle
DVDV1-SDK Java		Bibliothek und Beispiele für Java-Entwickler zur Unterstützung bei der DVDV1-kompatiblen Anbindung über die Legacy-Facade
DVDV1-SDK .NET		Bibliothek und Beispiele für .NET-Entwickler zur Unterstützung bei der DVDV1-kompatiblen Anbindung über die Legacy-Facade

Tabelle 9: Systemkomponenten des DVDV

5.2.1 DVDV-Bundesmaster

Der DVDV-Bundesmaster besteht aus den Clientkomponenten Pflege-Client und Admin-Client und den Serverkomponenten Kernsystem und IAM. Die Komponenten DVDV-Kernsystem und DVDV-IAM haben jeweils einen MySQL-Datenbank-Server zur Datenspeicherung.

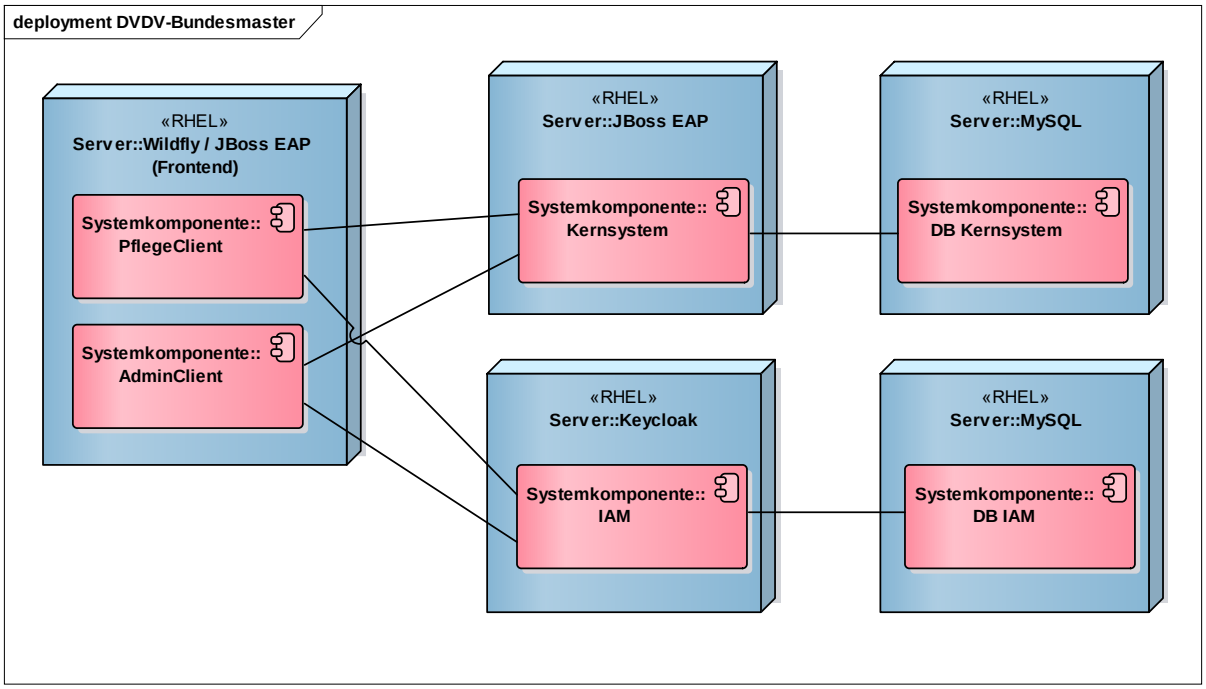


Abbildung 3: Deployment DVDV-Bundesmaster

Alternativ wäre es ebenso möglich, die einzelnen Clients und das Kernsystem auf einem gemeinsamen Application-Server zu betreiben.

5.2.1.1 Pflege-Client

Der Pflege-Client wird zur Datenpflege im Gesamtsystem DVDV von den Pflegenden Stellen genutzt. Er wird als Webanwendung ausschließlich über die Netze des Bundes (NdB-VN) bereitgestellt und über ihn können Datenänderungen im Kernsystem durchgeführt werden.

Er erlaubt die Pflege von allen im DVDV gehaltenen Daten wie Organisationen, Providern, Diensten, Dienstbeschreibungen, Zertifikaten und Favoriten. Auch die Suche und Filterung sowie die Anzeige dieser Ressourcen sind im Pflege-Client möglich. Es können darüber hinaus Statistiken und Änderungshistorie eingesehen werden. Der Pflege-Client wird ausschließlich am DVDV-Bundesmaster eingesetzt und greift über die http-Schnittstelle auf das IAM und das Kernsystem zu.

Der Pflege-Client hat keine eigene Persistenz und ist weitgehend statuslos umgesetzt, kurzzeitiges Caching von Stammdaten zur Optimierung der Performance ist möglich. Das UI gliedert sich nach Use-Cases und kommuniziert mit dem Kernsystem zur Prozessierung und Abwicklung der Nutzerinteraktion. Das User-Interface (UI) wird mittels JSF mit PrimeFaces umgesetzt. Der Pflege-Client ist lauffähig auf einem Application-Server JBoss EAP oder WildFly.

Für die Datenpflege müssen sich die Nutzer am DVDV-IAM authentifizieren. Der Pflege-Client greift über die http-Schnittstellen auf das Kernsystem zu, an denen er sich ebenfalls mittels des DVDV-IAM authentifiziert.

5.2.1.2 Admin-Client

Der Admin-Client dient der Administration des DVDV. Er wird ausschließlich am DVDV-Bundesmaster eingesetzt und greift über die http-Schnittstelle auf das Kernsystem und das DVDV-IAM zu. Er erlaubt die Pflege von Benutzern und Benutzergruppen, Stellvertreterregelungen, Rollen und Rechten sowie Ressourcengruppen für die Steuerung der Authentisierung und Autorisierung. Des Weiteren sind administrative Tätigkeiten rund um die Ressourcenpflege möglich. Dazu gehören die Anlage neuer Dienst-Typen, die Erstellung neuer Ressourcen-Typen und die Erweiterung von Ressourcen um benutzerdefinierte Attribute.

Alle Clientanwendungen (Pflege-Client, Auskunfts-Client, Admin-Client) sind nach identischen Architekturprinzipien erstellt. Daher gelten die Ausführungen für den Pflege-Client an dieser Stelle entsprechend.

Für die den Zugriff auf den Admin-Client müssen sich die Administratoren am DVDV-IAM authentifizieren. Für die Administration nutzt der Admin-Client die http-Schnittstellen des Kernsystems und des Benutzermanagements des DVDV-IAM, an denen er sich mittels der Zugriffskontrolle des DVDV-IAM authentifiziert.

5.2.1.3 DVDV-Kernsystem

Das Kernsystem realisiert die Persistierung und Bereitstellung aller fachlichen Daten des Systems. Hierbei handelt es sich insbesondere um

- Informationen zu Organisationen und Behörden, die ggf. Dienste anbieten
- Informationen zu den von Organisationen und Behörden angebotenen Diensten und deren Dienstelementen, wie z.B. Zertifikaten und URIs
- Dienstbeschreibungen, die die angebotenen Dienste spezifizieren
- vorläufig erfasste Daten zur Qualitätssicherung und Übernahme in das System
- Zugriffsprotokollierung und Historie der Änderungen an diesen Daten
- Daten zu Favoriten und Vorbelegungen (Defaults) von Masken

Diese Komponente ist als reine Serverkomponente ausgeprägt, lauffähig auf einem JBoss EAP oder WildFly Application-Server. Der Zugriff erfolgt ausschließlich über die angebotenen Schnittstellen.

5.2.1.4 DVDV-IAM

Das DVDV-IAM realisiert das Benutzermanagement und das Management der Zugriffskontrolle auf das Gesamtsystem DVDV. Das Benutzermanagement umfasst die

- Pflege von Benutzern (Identitäten), Benutzergruppen und deren Anmeldeinformationen, sowie die
- Pflege von Rollen, Rechten und Vertreterregelungen.

Das Management der Zugriffskontrolle umfasst die

- Pflege von Vertrauensbeziehungen von abfragenden Anwendungen, die
- Authentifizierung von Benutzern und Client-Systemen sowie das
- Ausstellen und Validieren von Berechtigungs-Token.

Das DVDV-IAM wird laut Vorgabe VL2 durch Keycloak umgesetzt. Keycloak ist ein Open Source Projekt unter der Verwaltung der Firma Red Hat. Sofern Keycloak benötigte Funktionalitäten nicht besitzt, werden diese erweitert.

Keycloak steht als Standalone-Anwendung zur Verfügung und wird daher nicht in einem JBoss-Application-Server betrieben.

Das DVDV-IAM ist das führende System für die Authentisierung von Nutzer-Zugriffen auf das Gesamtsystem DVDV. Zu diesem Zweck sind im DVDV-IAM die Anmeldeinformationen aller Benutzer hinterlegt, welche einen authentisierten Zugriff auf das DVDV benötigen. In der Datenbank des DVDV-IAM werden daher Informationen zu allen Benutzern und ihren Anmeldeinformationen und Authentisierungskonfigurationen gespeichert.

Das DVDV-IAM ist als zentrale Authentisierungskomponente für alle Systemkomponenten verantwortlich. Da eine Authentisierung sowohl für Systemkomponenten im Netz des Bundes (bspw. der Pflege-Client auf dem DVDV-Bundesmaster) als auch für Systemkomponenten im Internet (bspw. der Auskunfts-Client auf einem DVDV-Server) notwendig ist, muss auch das DVDV-IAM sowohl im Netz des Bundes als auch im Internet verfügbar sein.

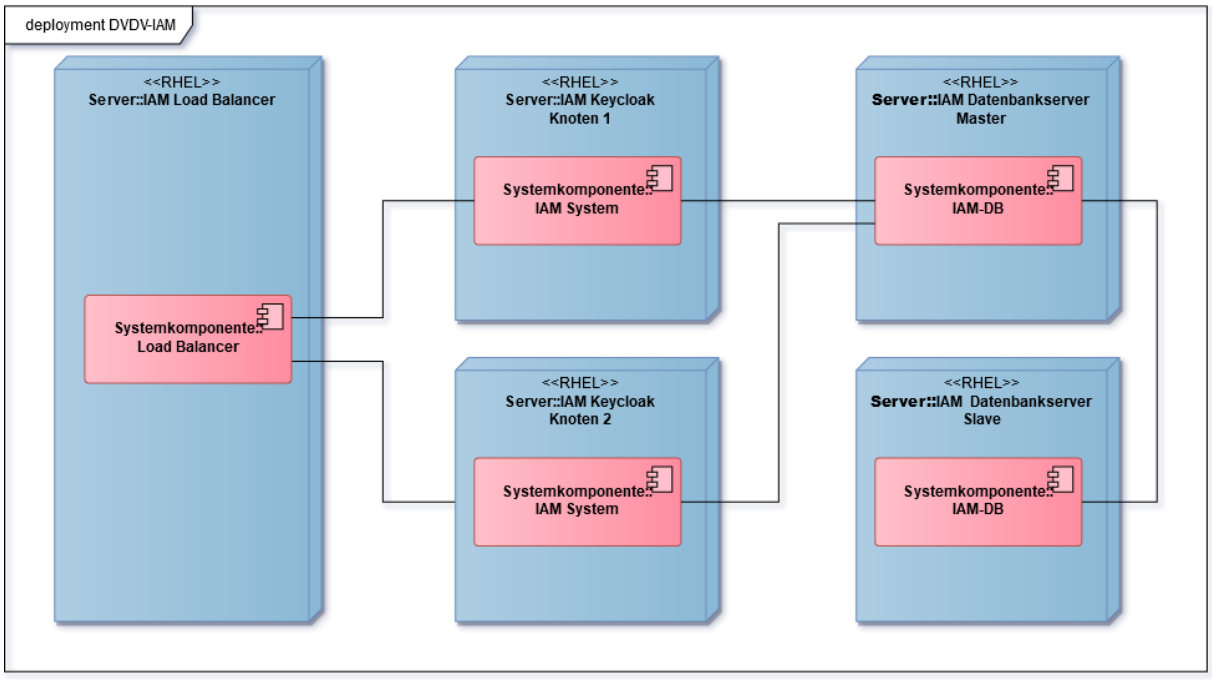


Abbildung 4: Deployment DVDV-IAM

Aufgrund der Architektur des Keycloak ist ein verteilter Betrieb wie bei den DVDV-Servern zur Erreichung einer hohen Verfügbarkeit nicht möglich. Das DVDV-IAM wird daher ausschließlich beim Bundesmaster betrieben.

Der Admin-Client ist an das DVDV-IAM angebunden, um damit Benutzer und Clients zu pflegen. Der Pflege-Client des DVDV-Bundesmasters und die Auskunfts-Clients der DVDV-Server sind an das DVDV-IAM angebunden, um Kontoinformationen abzurufen und per User-Self-Service zu pflegen. Alle Teilsysteme nutzen das IAM zur Authentisierung.

5.2.2 DVDV-Server

5.2.2.1 Bausteinsicht

Ähnlich dem DVDV-Bundesmaster, besteht ein DVDV-Server aus einem Application-Server und einem nachgelagerten MySQL-Datenbankserver. Auf dem Application-Server werden zusammen mit dem Kernsystem auch der Auskunfts-Client und die Legacy-Facade betrieben.

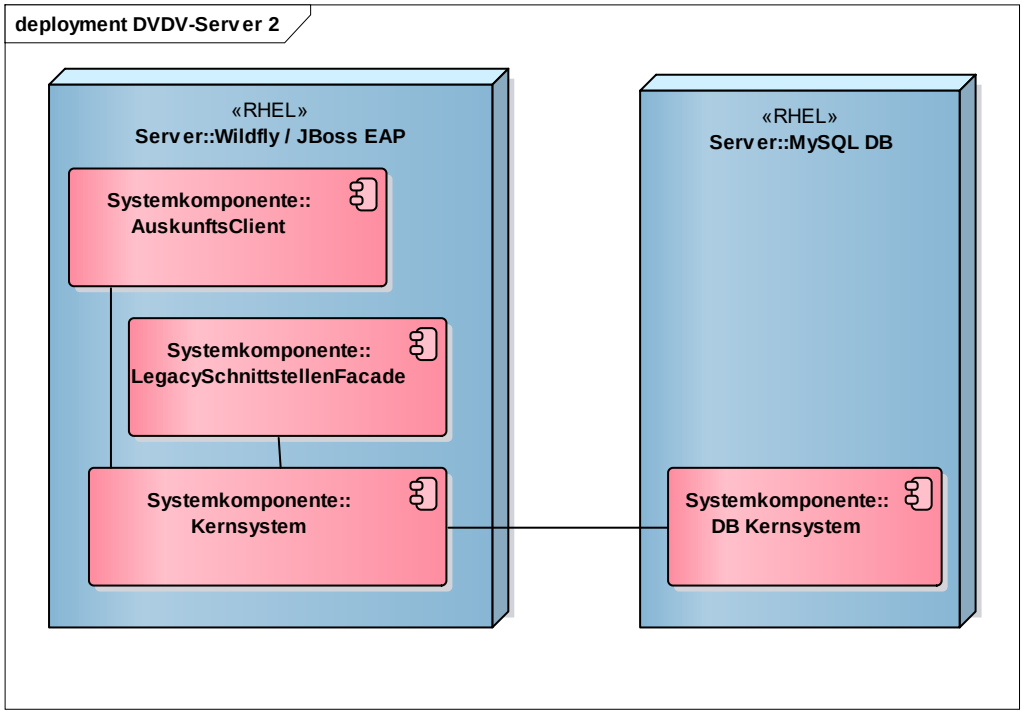


Abbildung 5: Deployment DVDV-Server

Alternativ wäre es ebenso möglich, die einzelnen Clients und das Kernsystem auf getrennten Servern zu betreiben.

5.2.2.2 DVDV-Kernsystem

Die Komponente DVDV-Kernsystem entspricht der Komponente DVDV-Kernsystem des DVDV-Bundesmasters mit dem einzigen Unterschied, dass diese Komponente im DVDV-Server auf lesende Zugriffe beschränkt ist. Ebenso sind auf der Datenbank des DVDV-Servers nur Leserechte vergeben, ein Ändern der Daten ist nur durch Replikation vom Bundesmaster möglich.

5.2.2.3 Auskunfts-Client

Mit dem Auskunfts-Client können die im DVDV gespeicherten Daten auch auf DVDV-Servern eingesehen werden. Er dient damit insbesondere den Dienstanbietern und Dienstnutzern zur Verifikation der gespeicherten Dienstinformationen. Ebenso können Nutzungsstatistiken des DVDV erstellt werden.

Für den Datenzugriff nutzt der Auskunfts-Client die http-Schnittstellen des Kernsystems, an denen er sich mittels des DVDV-IAM authentifiziert. Weitere Schnittstellen sind nicht vorgesehen.

5.2.3 Legacy-Facade

Die Legacy-Facade setzt die Legacy-Schnittstellen des DVDV 1 um. Sie wird als eigene Komponente / Deployable umgesetzt. Es ist möglich, diese Komponente nur für eine Übergangszeit einzusetzen und nach einer Umstellung der angebundenen Systeme abzuschalten.

Da diese Komponente auf Legacy-Code aus dem DVDV 1 System basiert, werden die querschnittlichen Konzepte und Kodierrichtlinien hier nicht durchgängig eingehalten. Eine langjährige Pflege dieser Komponente ist nicht vorgesehen. Für den Datenzugriff nutzt die Legacy-Facade die http-Schnittstellen des Kernsystems, eine Authentifizierung ist nicht notwendig.

Für die Nutzer der Legacy-Facade bleibt damit die Benutzung über einen OSCI-Intermediär ohne eigene Authentifizierung möglich.

5.2.4 DVDV-DevKits Java und .NET

Mit dem System DVDV werden zwei Development-Kits erstellt, die den Herstellern von angebundenen Systemen eine leichte Implementierung der DVDV-Anbindung ermöglichen. Die Hersteller sollten diese für die Kommunikation mit den DVDV-Servern verwenden.

Die DevKits enthalten Implementierungsbeispiele und Bibliotheken. Die Implementierungsbeispiele zeigen, wie eine DVDV-Anbindung in der jeweiligen Programmiersprache umsetzbar ist. Die Bibliotheken vereinfachen die Anbindung stark. Entwickler können die Bibliotheken in ihre Software integrieren und konfigurieren und damit eine Anbindung des DVDV mit Authentifizierung und Failover erzielen.

5.2.4.1 DVDV-Bibliotheken

Die DVDV-Bibliotheken werden regelmäßig weiterentwickelt und der Funktionsumfang wird ständig ausgebaut. Insbesondere unterstützen sie aber auch die drei Szenarien für Anfragedienste des DVDV 1

1. find.servicedescription
2. find.authoritydescription
3. verify.category

Über den Funktionsumfang von DVDV 1 hinaus bietet das DVDV jetzt eine Menge weiterer Funktionen, die über die Directory-Schnittstelle des Kernsystems genutzt werden können. Die Liste wird ständig bedarfsgerecht erweitert.

Die Bibliotheken nutzen für Datenabfragen die Directory-Schnittstelle des DVDV-Kernsystems an den DVDV-Servern. Die vom Kernsystem übermittelten Daten werden von den Bibliotheken geparst und aufbereitet und den Entwicklern in geeigneter Form zur Verfügung gestellt.

In der Bibliothek wird die URL des zu nutzenden DVDV-Servers per Konfiguration hinterlegt. Zur Erhöhung der Verfügbarkeit können mehrere URLs zu alternativen DVDV-Servern hinterlegt werden. Falls ein DVDV-Server nicht erreichbar ist oder mit einem technischen http-Fehler antwortet, führt die Bibliothek automatisch einen Failover durch und die Bibliothek versucht, mit dem nächsten Server der Liste zu kommunizieren.

Gegebenenfalls kann die Nichtverfügbarkeit von DVDV-Servern erst nach einer konfigurierbaren Wartezeit (z.B. Timeout) wahrgenommen werden. Aus diesem Grund werden, sofern der primäre DVDV-Server nicht verfügbar ist, weitere Anfragen nicht unmittelbar wieder gegen

diesen versucht. Stattdessen werden für einen konfigurierbaren Zeitraum alle weiteren Anfragen gegen den letzten erfolgreichen Server gestellt.

Kernfunktionalität der Bibliotheken ist auch die Authentifizierung. Die Authentifizierung der anfragenden Organisation wird von der Bibliothek eigenständig durchgeführt und ist für die Entwickler transparent.

5.2.4.2 Implementierungsbeispiele

In .NET und in Java werden einige Implementierungsbeispiele bereitgestellt, die den Entwicklern in der jeweiligen Programmiersprache als Vorlage für die Integration der Bibliotheken und für die Anbindung des DVDV dienen können.

6 Laufzeitsicht

In der Laufzeitsicht werden fachliche und administrative Use-Cases dargestellt. Da eine komplette Ausformulierung und Modellierung aller Use-Cases den Rahmen dieses Architekturkonzepts sprengen würde, werden die umzusetzenden fachlichen Use-Cases für die drei Client-Applikationen Pflege-Client, Admin-Client und Auskunfts-Client, sowie die technischen Use-Cases von Kernsystem und IAM benannt und kurz beschrieben.

6.1 Fachliche Use-Cases Pflege-Client

Im Pflege-Client werden die in den folgenden Tabellen beschriebenen Use-Cases umgesetzt. Sie werden aber ständig im Dialog mit unterschiedlichen Stakeholdern angepasst und erweitert.

Pflege von Organisationen

ID	Name	Beschreibung
PC_O_01	Organisation anlegen	Anlegen einer neuen Organisation mit allen Attributen (z.B. Anschrift, Beschreibung, Zertifikate)
PC_O_02	Organisation anzeigen	Anzeige einer Organisation mit allen Attributen
PC_O_03	Organisation bearbeiten	Bearbeiten einer bestehenden Organisation mit Änderung von allen Attributen
PC_O_04	Organisation löschen	Löschen einer bestehenden Organisation
PC_O_05	Organisation suchen	Suche von Organisationen nach Filterkriterien, insbes. z.B. • Organisationen, die einen Dienst für eine angegebene Dienstbeschreibung anbieten • Organisationen nach Dienstelementen (transitiv über die dem Provider zugeordneten Dienstelemente) • Organisationen nach Stellvertretern Es werden zwei Masken für einfache und erweiterte Suche angeboten.
PC_O_06	Gruppe von Organisationen pflegen	Bearbeitung einer Gruppe von bestehenden Organisationen zur gleichen Zeit (alle Attribute, die die gewählten Organisationen gemeinsam haben)
PC_O_07	Gruppe von Organisationen löschen	Löschen einer Gruppe von bestehenden Organisationen
PC_O_08	Organisation kopieren	Anlegen einer Organisation als Kopie einer bereits bestehenden Organisation mit Möglichkeiten zum anschließenden Ändern
PC_O_09	Organisationen exportieren	Export von Organisationen mit allen Attributen im XML-Format

ID	Name	Beschreibung
PC_O_10	Organisationen importieren	Import von Organisationen mit allen Attributen aus einer geeigneten XML-Datei
PC_O_11	Änderungshistorie für Organisationen anzeigen	Anzeige der Historie für alle Organisationen

Tabelle 10: Liste der Anwendungsfälle zur Pflege von Organisationen

Pflege von Organisation-Stellvertretern

ID	Name	Beschreibung
PC_S_01	Organisation-Stellvertreter anlegen	Anlegen eines neuen Organisation-Stellvertreters mit allen Attributen (z.B. Anschrift, Beschreibung, Zertifikat(e))
PC_S_02	Organisation-Stellvertreter anzeigen	Anzeige eines Organisation-Stellvertreters mit allen Attributen
PC_S_03	Organisation-Stellvertreter bearbeiten	Bearbeiten eines bestehenden Organisation-Stellvertreters mit Änderung von allen Attributen.
PC_S_04	Organisation-Stellvertreter löschen	Löschen eines bestehenden Organisation-Stellvertreters
PC_S_05	Organisation-Stellvertreter suchen	Suche von Organisation-Stellvertretern nach Filterkriterien. Es werden zwei Masken für einfache und erweiterte Suche angeboten.
PC_S_06	Organisation-Stellvertreter kopieren	Anlegen eines Organisation-Stellvertreters als Kopie eines bereits bestehenden Stellvertreters mit Möglichkeiten zum anschließenden Ändern
PC_S_07	Organisation-Stellvertreter exportieren	Export von Organisation-Stellvertretern mit allen Attributen im XML-Format
PC_S_08	Organisation-Stellvertreter importieren	Import von Organisation-Stellvertretern mit allen Attributen aus einer geeigneten XML-Datei
PC_S_09	Änderungshistorie für Organisation-Stellvertreter anzeigen	Anzeige der Historie für alle Organisation-Stellvertreter

Tabelle 11: Liste der Anwendungsfälle zur Pflege von Organisation-Stellvertretern

Pflege von Providern

ID	Name	Beschreibung
PC_P_01	Provider anlegen	Anlegen eines neuen Providers mit allen Attributen
PC_P_02	Provider anzeigen	Anzeige eines Providers mit allen Attributen

ID	Name	Beschreibung
PC_P_03	Provider bearbeiten	Bearbeiten eines bestehenden Providers mit Änderung von allen Attributen
PC_P_04	Provider löschen	Löschen eines bestehenden Providers
PC_P_05	Provider suchen	Suche von Providern nach Filterkriterien. Es werden zwei Masken für einfache und erweiterte Suche angeboten.
PC_P_06	Provider kopieren	Anlegen eines Providers als Kopie eines bereits bestehenden Providers mit Möglichkeiten zum anschließenden Ändern
PC_P_07	Provider exportieren	Export von Providern mit allen Attributen im XML-Format
PC_P_08	Provider importieren	Import von Providern mit allen Attributen aus einer geeigneten XML-Datei
PC_P_09	Änderungshistorie für Provider anzeigen	Anzeige der Historie für alle Provider

Tabelle 12: Liste der Anwendungsfälle zur Pflege von Providern

Pflege von Diensten

ID	Name	Beschreibung
PC_D_01	Dienst anlegen	Anlegen eines neuen Dienstes mit allen Attributen (z.B. Dienstelemente, Gültigkeit). Der Dienst wird immer mit einer bestehenden Organisation verknüpft.
PC_D_02	Dienst anzeigen	Anzeige eines Dienstes mit allen Attributen inkl. Gültigkeitszeitraum und zugeordneten Dienstelementen
PC_D_03	Dienst bearbeiten	Bearbeiten eines bestehenden Dienstes mit Änderung von allen Attributen, insbes. des fachlichen Behördenschlüssels
PC_D_04	Dienst löschen	Löschen eines bestehenden Dienstes
PC_D_05	Dienste suchen	Suche von Diensten nach Filterkriterien, insbes. z.B. • Gültigkeitszeitraum • Name und Kategorie Es werden zwei Masken für einfache und erweiterte Suche angeboten.
PC_D_06	Gruppe von Diensten pflegen	Bearbeitung einer Gruppe von bestehenden Diensten zur gleichen Zeit (alle Attribute, die die gewählten Dienste gemeinsam haben)
PC_D_07	Gruppe von Diensten löschen	Löschen einer Gruppe von bestehenden Diensten
PC_D_08	Dienst kopieren	Anlegen eines Dienstes als Kopie eines bereits bestehenden Dienstes mit Möglichkeiten zum anschließenden Ändern

ID	Name	Beschreibung
PC_D_09	Änderungshistorie für Dienste anzeigen	Anzeige der Historie für alle Dienste

Tabelle 13: Liste der Anwendungsfälle zur Pflege von Diensten

Pflege von benutzerspezifischen Ressourcen

ID	Name	Beschreibung
PC_BR_01	Benutzerdefinierte Ressource anlegen	Anlegen einer neuen benutzerdefinierten Ressource mit allen benutzerdefinierten Attributen, die für Ressourcen der ResourceCategory konfiguriert sind
PC_BR_02	Benutzerdefinierte Ressourcen anzeigen	Anzeige einer benutzerdefinierten Ressource mit allen benutzerdefinierten Attributen
PC_BR_03	Benutzerdefinierte Ressource bearbeiten	Bearbeiten einer bestehenden benutzerdefinierten Ressource mit allen benutzerdefinierten Attributen
PC_BR_04	Benutzerdefinierte Ressource löschen	Löschen einer benutzerdefinierten Ressource
PC_BR_05	Benutzerdefinierte Ressourcen suchen	Suche von benutzerdefinierten Ressourcen nach Filterkriterien mit allen benutzerdefinierten Attributen

Tabelle 14: Liste der Anwendungsfälle zur Pflege von benutzerdefinierten Ressourcen

Pflege von Zertifikaten

ID	Name	Beschreibung
PC_Z_01	Zertifikate suchen	Suche von Zertifikaten nach Filterkriterien, insbes. z.B. • Gültigkeitszeitraum • Organisationskategorie (transitiv über die Dienste der Organisationen) Es werden zwei Masken für einfache und erweiterte Suche angeboten.
PC_Z_02	Zertifikat anzeigen	Anzeige eines Zertifikats mit allen Attributen
PC_Z_03	Zertifikat herunterladen	Download eines Zertifikats
PC_Z_04	Organisation für ein Zertifikat bearbeiten	Aus der Zertifikatssuche kann direkt in den Use-Case „PC_O_03 Organisation bearbeiten“ navigiert werden, um die mit dem gefundenen Zertifikat verknüpfte Organisation zu ändern.
PC_Z_05	Provider für ein Zertifikat editieren	Aus der Zertifikatsuche kann direkt in den Use-Case „PC_P_03 Provider bearbeiten“ navigiert werden, um den mit dem gefundenen Zertifikat verknüpften Provider zu ändern.

Tabelle 15: Liste der Anwendungsfälle zur Pflege von Zertifikaten

Ressourcenübergreifende Funktionen

ID	Name	Beschreibung
PC_RU_01	Ressourcenübergreifend suchen	Übergreifende Suche nach Ressourcen der Typen Dienst, Organisation, Provider und Organisation-Stellvertreter in einer Suche, mindestens nach Ortsangaben. Für Dienste ist dabei der Ort der Organisation maßgeblich, zu der dieser Dienst gehört.

Tabelle 16: Liste der Anwendungsfälle zu ressourcenübergreifenden Funktionen

Pflege von Ressourcengruppen

ID	Name	Beschreibung
PC_RG_01	Ressourcen gruppieren	Auf Basis einer gefilterten Liste können Ressourcen ausgewählt und einer Ressourcengruppe zugeordnet werden. Mögliche Attribute für die Filterregeln sind: • ResourceCategory (Organisation, Provider, Behördenstellvertreter) • Organisationskategorien (nur für Organisationen) • Lokation (Bundesland, Regierungsbezirk, Kreis)

Tabelle 17: Liste der Anwendungsfälle zur Pflege von Ressourcengruppen

Anzeige von Statistiken

ID	Name	Beschreibung
PC_S_01	Ablaufende Zertifikate	Anzahl der im angegebenen Zeitraum ablaufenden Zertifikate
PC_S_02	Bearbeitungshistorie Ressourcengruppe	Auswertung aller Änderungen an Daten einer Ressourcengruppe (einer pflegenden Stelle) in einem angegebenen Zeitraum
PC_S_03	Clientnutzung	Auswertung der Anzahl der Aufrufe des Pflege-Clients
PC_S_04	Datenänderungen	Auswertung der Anzahl der Änderungen an Ressourcen (Organisationen, Stellvertreter, Provider, Dienste inkl. Dienstelemente)
PC_S_05	Dienstanzahl	Auswertung der Anzahl der Dienste im DVDV
PC_S_06	Organisationen nach Diensten	Auswertung der Anzahl von Organisationen, die einen bestimmten Dienst nutzen
PC_S_07	Organisationen nach Kategorien	Auswertung der Anzahl von Organisationen, die einer gewählten Organisationskategorie angehören
PC_S_08	Organisationen nach Präfix	Auswertung der Anzahl von Organisationen mit einem bestimmten Präfix des Organisationsschlüssels
PC_S_09	Intermediärsliste	Liste aller Intermediäre im DVDV; Optionen zum Download als csv- und xlsx-Datei und Möglichkeit zum Sprung zur betreibenden Organisation bzw. Provider

Tabelle 18: Liste der Anwendungsfälle zur Anzeige von Statistiken

Pflege und Nutzung von Favoriten und Vorlagen

ID	Name	Beschreibung
PC_F_01	Favorit für Suchergebnisse anlegen	Anlegen eines neuen Favoriten für Suchergebnisse von Organisationen, Organisation-Stellvertretern, Providern und Diensten. Diese Favoriten können dann insbesondere bei wiederkehrenden Massenpflegeoperationen verwendet werden. Zuordnung des Favoriten zu der aktuell angemeldeten Identität oder zu einer Gruppe von Identitäten, zu der diese Identität gehört.
PC_F_02	Favorit anzeigen	Anzeige eines Favoriten mit allen zugeordneten Ressourcen
PC_F_03	Favorit bearbeiten	Bearbeiten eines bestehenden Favoriten
PC_F_04	Favorit löschen	Löschen eines bestehenden Favoriten
PC_F_05	Vorlage für Dienstelemente anlegen	Anlegen einer Vorlage für Dienstelement-Vorbelegung; diese kann beim Anlegen von Diensten als Vorbelegung verwendet werden
PC_F_06	Vorlage umbenennen	Ändern des Namens einer bestehenden Vorlage
PC_F_07	Vorlage löschen	Löschen einer bestehenden Vorlage

Tabelle 19: Liste der Anwendungsfälle zur Pflege und Nutzung von Favoriten und Vorlagen

Durchführung der Qualitätssicherung

ID	Name	Beschreibung
PC_QS_01	Erstellen von unbestätigten Änderungen	Abhängig von der Rolle des angemeldeten Benutzers werden Änderungen als „vorläufig“ gekennzeichnet. Diese werden erst nach einer Bestätigung in die reguläre Datenbasis des DVDV überführt.
PC_QS_02	Bestätigung von unbestätigten Änderungen	Bestätigung von „vorläufigen“ Änderungen, die von einem Pfleger mit eingeschränkten Rechten erfasst wurden. Diese sind nach der Bestätigung wirksam.

Tabelle 20: Liste der Anwendungsfälle zur Durchführung der Qualitätssicherung

User-Self-Service im Pflege-Client

ID	Name	Beschreibung
PC_US_01	Nutzer ändert seine Daten	Ein Benutzer des Pflege-Client möchte seine eigenen Benutzerdaten ändern.
PC_US_02	Nutzer ändert sein Passwort/Zertifikat	Ein Benutzer des Pflege-Client möchte bzw. muss seine Credentials (Passwort oder Zertifikat) ändern, mit denen er sich am DVDV authentifiziert.

Tabelle 21: Liste der Anwendungsfälle für User-Self-Service im Pflege-Client

6.2 Fachliche Use-Cases Admin-Client

Im Admin-Client werden die in den folgenden Tabellen beschriebenen Use-Cases umgesetzt.

Pflege von Organisationskategorien

ID	Name	Beschreibung
AdC_OK_01	Organisationskategorien der Ebene 1, 2, 3 und 4 pflegen	Pflege der Struktur der Organisationskategorien. Es können neue Organisationskategorien geschaffen und existierende umbenannt oder gelöscht werden. Der baumartige Aufbau der vierstufigen Kategorisierung wird dabei berücksichtigt und auf der Pflegemaske geeignet abgebildet. Ein Löschversuch von verwendeten Organisationskategorien führt zu einer entsprechenden Fehlermeldung.

Tabelle 22: Liste der Anwendungsfälle zur Pflege von Organisationskategorien

Pflege von Dienstbeschreibungen

Dienstbeschreibungen werden als XML-Dokument in DVDV hinterlegt, für die XÖV-Dienste wird die Beschreibung mittels WSDL beibehalten, für andere Dienst-Typen müssen neue XML-Schemata hinterlegt werden.

Die Software ermöglicht damit eine spätere Definition und Einbindung anderer Dienstbeschreibungen. Somit wäre dann auch eine spätere Erweiterung auf andere Dienst-Technologien möglich.

ID	Name	Beschreibung
AdC_DB_01	Dienstbeschreibung anlegen	Anlegen einer Dienstbeschreibung für einen neuen Diensttypen durch Upload eines WSDL-Templates und Zuweisung einer Organisationskategorie
AdC_DB_02	Dienstbeschreibung anzeigen	Anzeige einer Dienstbeschreibung
AdC_DB_03	Dienstbeschreibung bearbeiten	Bearbeiten einer bestehenden Dienstbeschreibung, Änderung der zugeordneten Organisationskategorien
AdC_DB_04	Dienstbeschreibung löschen	Löschen einer bestehenden Dienstbeschreibung
AdC_DB_05	Dienstbeschreibung suchen	Suche von Dienstbeschreibungen nach Filterkriterien

Tabelle 23: Liste der Anwendungsfälle zur Pflege von Dienstbeschreibungen

Pflege von Ressourcengruppen

ID	Name	Beschreibung
AdC_RG_01	Neue Ressourcengruppe anlegen	Anlegen einer Ressourcengruppe
AdC_RG_02	Ressourcengruppe bearbeiten	Bearbeiten einer bestehenden Ressourcengruppe

AdC_RG_03	Ressourcengruppe löschen	Löschen einer bestehenden Ressourcengruppe; hierbei wird geprüft, dass keine Ressource ohne Ressourcengruppe bleibt.
AdC_RG_04	Ressourcengruppe suchen	Suche von Ressourcengruppen nach Filterkriterien

Tabelle 24: Liste der Anwendungsfälle zur Pflege von Ressourcengruppen

Pflege von Benutzern

ID	Name	Beschreibung
AdC_B_01	Benutzer anlegen	Anlegen eines Benutzers
AdC_B_02	Benutzer bearbeiten	Ändern von Attributen eines bestehenden Benutzers, bspw. die zugehörigen Zertifikate
AdC_B_03	Benutzer löschen	Löschen eines bestehenden Benutzers
AdC_B_04	Benutzer suchen	Suche von Benutzern nach Filterkriterien

Tabelle 25: Liste der Anwendungsfälle zur Pflege von Benutzern

Pflege von Benutzergruppen

ID	Name	Beschreibung
AdC_BG_01	Benutzergruppe anlegen	Anlegen einer Benutzergruppe
AdC_BG_02	Benutzergruppe bearbeiten	Ändern von Attributen einer Benutzergruppe, bspw. zugehörige Benutzer und Rollen
AdC_BG_03	Benutzergruppe löschen	Löschen einer Benutzergruppe
AdC_BG_04	Benutzergruppe suchen	Suche von Benutzergruppen nach Filterkriterien

Tabelle 26: Liste der Anwendungsfälle zur Pflege von Benutzergruppen

Pflege von Stellvertreterregeln

ID	Name	Beschreibung
AdC_S_01	Stellvertreterregelung anlegen	Ein Administrator, der Rechte zum Editieren von Benutzern hat, kann für diese eine Stellvertretung anlegen. Als Spezialfall kann er diese auch für sich selbst anlegen.
AdC_S_02	Stellvertreterregelung bearbeiten	Bearbeiten von Stellvertreterregelungen. Als Spezialfall kann der Administrator seine eigenen Stellvertretungen bearbeiten.
AdC_S_03	Stellvertreterregelungen löschen	Löschen von Stellvertreterregelungen. Als Spezialfall kann der Administrator seine eigenen Stellvertretungen löschen.

AdC_S_04	Stellvertreterrege-lungen suchen	Suche von Stellvertreterregelungen nach Filterkriterien

Tabelle 27: Liste der Anwendungsfälle zur Pflege von Stellvertreterregeln

Pflege von Föderationsbeziehungen

Über die Keycloak-Admin-Konsole können beliebige Föderationsbeziehungen zu anderen Identitäts-Repositories initiiert und gepflegt werden. Es ist dort auch möglich, Mapper festzulegen, die Attribute der föderierten Identität (bspw. SAFE-Rollen einer SAFE-Identität) auf Attribute der DVDV-Domäne (bspw. Rollen) abbilden können. Konkrete Use-Cases im Admin-Client zum vereinfachten Workflow zum Aufbau von Föderationsbeziehungen sind derzeit nicht umgesetzt.

Anlegen von neuen Ressourcen und benutzerdefinierten Attributen

ID	Name	Beschreibung
AdC_BR_01	Neuen Ressourcen-typen anlegen und bearbeiten	Anlage eines neuen Ressourcentyps und einer Definition für Ressourcen dieses Typs als komplexe Geschäftsobjekte. Der Ressourcentyp umfasst die Basis-Klasse „Resource“ mit zusätzlichen benutzerdefinierten Attributen, die hier festgelegt werden können.
AdC_BR_02	Pflege der Datenty-pen zur Laufzeit des Systems	Anlage von neuen benutzerdefinierten Datentypen für Attribute von benutzerdefinierten Geschäftsobjekten als Liste von Einzelattributen mit jeweils Name, Typ (nur primitive Datentypen), Beschreibung und Wertebereich.

Tabelle 28: Liste der Anwendungsfälle zum Anlegen von neuen Ressourcen und benutzerdefinierten Attributen

User-Self-Service

ID	Name	Beschreibung
AdC_US_01	Nutzer ändert seine Daten	Ein Benutzer des Admin-Client möchte seine eigenen Benutzerdaten ändern.
AdC_US_02	Nutzer ändert sein Passwort/Zertifikat	Ein Benutzer des Admin-Client möchte bzw. muss seine Credentials (Passwort oder Zertifikat) ändern, mit denen er sich am DVDV authentifiziert.

Tabelle 29: Liste der Anwendungsfälle für User-Self-Service im Admin-Client

Auskunfts-Client

Auskunfts-Clients können derzeitig nicht im Admin-Client angelegt werden. Dies muss durch einen manuellen Prozess direkt im Keycloak erfolgen. Der Admin-Client bietet allerdings die Möglichkeit, Benutzer einem Auskunfts-Client zuzuweisen und eine Übersicht der bestehenden Auskunfts-Clients anzuzeigen.

ID	Name	Beschreibung
AdC_AC_01	Übersicht der Aus-kunfts-Clients an-zeigen	Anzeige aller im Keycloak angelegten Auskunfts-Clients in einer Liste

AdC_AC_02	Auskunfts-Client anzeigen	Anzeigen eines im Keycloak angelegten Auskunfts-Client
AdC_AC_03	Benutzer einem Auskunfts-Client zuordnen	Zuordnung eines Benutzers zu seinem primären Auskunfts-Client. Jeder Benutzer kann generell jeden Auskunfts-Client nutzen, der Betreiber eines Auskunfts-Client kann aber protokollieren, welchem Auskunfts-Client die Benutzer zugeordnet sind, die sich bei ihm anmelden.

Tabelle 30: Liste der Anwendungsfälle für Auskunfts-Clients im Admin-Client

OpenID-Clients

Ein OpenID-Client ist eine externe Anwendung, die Zugang zum Kernsystem erhalten soll. Über den Admin-Client können OpenID-Clients angelegt werden, damit externe Anwendungen sich über zertifikatsbasierte Authentifizierung am Keycloak anmelden können, womit diese Zugriff auf das Kernsystem erhalten sollten (s. Anwendungsfall IAM_A_02 in Abschnitt 6.6).

Dies ist eine Alternative zur Authentifizierung am Kernsystem, wenn die zugreifenden Nutzer nicht als Organisationen im DVDV hinterlegt sind und nicht die Authentifizierung am Kernsystem nutzen können (s. Anwendungsfall KS_A_01 in Abschnitt 6.5).

ID	Name	Beschreibung
AdC_OC_01	Übersicht der OpenID-Clients anzeigen	Anzeigen aller angelegten OpenID-Clients in einer Liste
AdC_OC_02	OpenID-Client löschen	Löschen eines OpenID-Clients
AdC_OC_03	OpenID-Client ändern	Anzeigen und Ändern eines OpenID-Clients

Tabelle 31: Liste der Anwendungsfälle für OpenID-Clients im Admin-Client

6.3 Fachliche Use-Cases Auskunfts-Client

Im Auskunfts-Client werden die in den folgenden Tabellen beschriebenen Use-Cases umgesetzt.

Anzeige von Organisationen

ID	Name	Beschreibung
AuC_O_01	Organisation anzeigen	Anzeige einer Organisation mit allen Attributen
AuC_O_02	Organisationen suchen (einfach)	Suche von Organisationen nach einfachen Filterkriterien wie Name, Lokation und Organisationskategorie
AuC_O_03	Organisationen suchen (erweitert)	Suche von Organisationen nach erweiterten Filterkriterien, insbes. Organisationen, die einen Dienst für eine angegebene Dienstbeschreibung anbieten; die erweiterte Suche ist in der Standard-Konfiguration deaktiviert

Tabelle 32: Liste der Anwendungsfälle zur Auskunft über Organisationen im Auskunfts-Client

Anzeige von Organisation-Stellvertretern

ID	Name	Beschreibung
AuC_O_01	Organisation-Stell-vertreter anzeigen	Anzeige eines Organisation-Stellvertreters mit allen Attributen
AuC_O_02	Organisation-Stell-vertreter suchen (einfach)	Suche von Organisation-Stellvertretern nach einfachen Filterkriterien wie Name, Lokation und Organisationskategorie
AuC_O_03	Organisation-Stell-vertreter suchen (er-weitert)	Suche von Organisation-Stellvertretern nach erweiterten Filterkriterien; die erweiterte Suche ist in der Standard-Konfiguration deaktiviert

Tabelle 33: Liste der Anwendungsfälle zur Auskunft über Organisation-Stellvertreter ím Auskunfts-Client

Anzeige von Providern

ID	Name	Beschreibung
AuC_P_01	Provider anzeigen	Anzeige eines Providers mit allen Attributen
AuC_P_02	Provider suchen (einfach)	Suche von Providern nach einfachen Filterkriterien wie Name oder Lo-kation
AuC_P_03	Provider suchen (er-weitert)	Suche von Providern nach erweiterten Filterkriterien; die erweiterte Suche ist in der Standard-Konfiguration deaktiviert

Tabelle 34: Liste der Anwendungsfälle zur Auskunft über Provider im Auskunfts-Client

Anzeige von Diensten

ID	Name	Beschreibung
AuC_D_01	Dienst anzeigen	Anzeige eines Dienstes mit allen Attributen inkl. Gültigkeitszeitraum und zugeordneten Dienstelementen
AuC_D_02	Dienste suchen (ein-fach)	Suche von Diensten nach einfachen Filterkriterien wie Name
AuC_D_03	Dienste suchen (er-weitert)	Suche von Diensten nach erweiterten Filterkriterien inkl. Gültigkeits-zeitraum, sowie Name und Kategorie; die erweiterte Suche ist in der Standard-Konfiguration deaktiviert

Tabelle 35: Liste der Anwendungsfälle zur Auskunft über Dienste im Auskunfts-Client

Anzeige von Zertifikaten

ID	Name	Beschreibung
AuC_Z_01	Zertifikat anzeigen	Anzeige eines Zertifikates mit allen Attributen inkl. Gültigkeitszeitraum

AuC_Z_02	Zertifikate suchen (einfach)	Suche von Zertifikaten nach einfachen Filterkriterien wie Inhaber oder Seriennummer
AuC_Z_03	Zertifikate suchen (erweitert)	Suche von Zertifikaten nach erweiterten Filterkriterien inkl. Gültigkeitszeitraum; die erweiterte Suche ist in der Standard-Konfiguration deaktiviert

Tabelle 36: Liste der Anwendungsfälle zur Auskunft über Zertifikate im Auskunfts-Client

Anzeige von Statistiken

ID	Name	Beschreibung
AuC_S_01	Intermediärsliste	Liste aller Intermediäre im DVDV; Optionen zum Download als csv- und xlsx-Datei und Möglichkeit zum Sprung zur betreibenden Organisation bzw. Provider

Tabelle 37: Liste der Anwendungsfälle zur Anzeige von Statistiken im Auskunfts-Client

User-Self-Service

ID	Name	Beschreibung
AuC_US_01	Nutzer ändert seine Daten	Ein Benutzer des Auskunfts-Client möchte seine eigenen Benutzerdaten ändern.
AuC_US_02	Nutzer ändert sein Passwort	Ein Benutzer des Auskunfts-Client möchte bzw. muss sein Passwort ändern, mit dem er sich am DVDV authentifiziert.

Tabelle 38: Liste der Anwendungsfälle für User-Self-Service im Auskunfts-Client

6.4 Technische Use-Cases DVDV-Bibliotheken

Die DVDV-Bibliotheken setzen die Use-Cases der Directory-Schnittstelle clientseitig um, vereinfachen die Authentifizierung der Organisationen am DVDV und implementieren eine Failover-Funktionalität.

Es wird je eine Bibliothek in .NET und eine in Java bereitgestellt, diese sind funktionsgleich und setzen die gleichen Anwendungsfälle um.

ID	Name	Beschreibung
Bib_01	Dienstbeschreibung finden	Fachverfahrenshersteller möchten eine Dienstbeschreibung abrufen, dazu geben sie eine Dienstbeschreibungs-URI und einen Organisationsschlüssel an.
Bib_02	Organisationsbeschreibung finden	Fachverfahrenshersteller möchten eine Organisationsbeschreibung abrufen, dazu geben sie eine Organisationskategorie und einen Organisationsschlüssel an.
Bib_03	Dienstnutzer verifizieren	Fachverfahrenshersteller möchten die Zugehörigkeit einer Organisation zu einer Organisationskategorie prüfen, dazu geben sie den Fingerabdruck eines Client-Zertifikates und eine Organisationskategorie an.

ID	Name	Beschreibung
Bib_04	Organisationen anhand eines Dienstelementes finden	Fachverfahrenshersteller möchten alle Organisationen finden, die ein bestimmtes Dienstelement (z.B. einen gemeinsamen Intermediär) nutzen.
Bib_05	Organisationskategorien finden	Fachverfahrenshersteller möchten alle Organisationskategorien finden, zu denen es eine Organisation mit dem angegebenen Client-Zertifikat und Organisationsschlüssel gibt.
Bib_06	Zertifikat finden	Fachverfahrenshersteller möchten ein im DVDV hinterlegtes Zertifikat finden, dazu geben sie einen Zertifikats-Fingerprint an.
Bib_07	Intermediäre finden	Fachverfahrenshersteller möchten eine Liste aller im DVDV hinterlegten Intermediäre abrufen.
Bib_08	Stapelverarbeitung	Senden einer großen Zahl von Anfragen der Anwendungsfälle Bib_01, Bib_02 und Bib_03 an das Kernsystem in einer gemeinsamen Anfrage.
Bib_09	Authentifizierung mit Client-Zertifikat	Ein Fachverfahren muss sich mit einem JWT-Token an der DVDV-Directory-Schnittstelle authentifizieren. Die Token-Generierung und Authentifizierung wird von den DVDV-Bibliotheken implizit für jede Anfrage mit durchgeführt.
Bib_10	Caching von Authentifizierungstoken	DVDV-Server-Betreiber möchten die Last auf ihren Servern möglichst gering halten. Dazu cachen die DVDV-Bibliotheken die JWT-Token für die Authentifizierung an der Directory-Schnittstelle für einen konfigurierbaren Zeitraum.
Bib_11	Failover	DVDV-Server-Betreiber möchten eine Vertreter-Beziehung mit einem anderen DVDV-Server-Betreiber eingehen. Die Bibliotheken setzen dazu eine Failover-Logik um, die in Fällen eines Serverausfalls automatisch auf den Vertretungsserver umschwenkt und bei einer Wiederverfügbarkeit des Ursprungsservers auf diesen zurück wechselt. Das ist für die Bibliotheksnutzer transparent.

Tabelle 39: Liste der Anwendungsfälle der DVDV-Bibliotheken

6.5 Technische Use-Cases Kernsystem

ID	Name	Beschreibung
KS_A_01[5]	Authentifizierter Zugriff eines dezentralen Fachverfahrens mit Authentifizierung am Kernsystem	Ein dezentrales Fachverfahren meldet sich am Kernsystem mit seinem dort hinterlegten Client-Zertifikat an und erhält authentifizierten Zugriff auf die Directory-Schnittstelle des Kernsystems. Der Vorteil dieser Authentifizierungsvariante ist, dass die im DVDV-Kernsystem bereits hinterlegten Zertifikate ohne eine erneute Anlage von Nutzerkonten im IAM für die Authentifizierung verwendet werden können und das DVDV auch bei Nichterreichbarkeit des DVDV-IAM für diese Nutzergruppe erreichbar ist.

Tabelle 40: Liste der Anwendungsfälle zur Authentifizierung am Kernsystem

Die Use-Cases zur Authentifizierung werden in Abschnitt 8.2 genauer beschrieben.

6.6 Technische Use-Cases IAM-System

Das IAM-System stellt im Rahmen von DVDV u.a. Funktionalitäten aus den Bereichen Zugriffskontrolle und Benutzermanagement zur Verfügung. In diesem Abschnitt werden Use-Cases dargestellt, die die Funktionalität Zugriffskontrolle und Plausibilisierung von Daten betreffen.

Automatische Prozesse

Im IAM-System wird ein automatisch ablaufender Prozess angestoßen, der ohne Benutzerinteraktion fachliche Funktionen ausführt.

ID	Name	Beschreibung
IAM_IA_01	Rollen automatisch löschen	Es wird eine periodische Bereinigung (z.B. monatlich) von Rollen vorgesehen, die auf Ressourcengruppen oder Benutzergruppen verweisen, die nicht mehr existieren.

Tabelle 41: Liste der Anwendungsfälle der automatischen Prozesse im IAM-System

[5] Die detaillierte Beschreibung dieses Anwendungsfalls finden Sie in Abschnitt 8.2.2.2.

Authentifizierung

ID	Name	Beschreibung
IAM_A_01[6]	Authentifizierter Benutzerzugriff	Ein Benutzer meldet sich mit seinen DVDV-Zugangsdaten am System an und erhält authentifizierten Zugriff auf eine Webapplikation (Pflege-Client, Admin-Client oder Auskunfts-Client) und Daten im DVDV-Bundesmaster oder DVDV-IAM.
IAM_A_02[7]	Authentifizierter Zugriff eines dezentralen Fachverfahrens	Ein dezentrales Fachverfahren meldet sich am System an und erhält authentifizierten Zugriff auf die Directory-Schnittstelle des Kernsystems.

Tabelle 42: Liste der Anwendungsfälle zur Authentifizierung im IAM-System

[6] Die detaillierte Beschreibung dieses Anwendungsfalls finden Sie in Abschnitt 8.2.1

[7] Die detaillierte Beschreibung dieses Anwendungsfalls finden Sie in Abschnitt 8.2.2.1

7 Software-Verteilung

Die Verteilung der Applikation auf Komponenten wurde bereits in Abschnitt 5 beschrieben. In diesem Abschnitt werden die Hardware-Anforderungen für die einzelnen Systemkomponenten, die auszuliefernden Artefakte, sowie Überlegungen zur Ausfallsicherheit betrachtet.

7.1 Hardware-Anforderungen

Frontend-Server

Der Frontend-Server stellt die Weboberfläche dar und koordiniert die Benutzerinteraktion. Er leitet Anfragen weiter an Kernsystem und DVDV-IAM. Eigene Fachlogik und komplexe Berechnungen finden nicht statt. Ausgehend von maximal 20 gleichzeitigen Benutzern genügt eine schlanke Ausstattung.

Am DVDV-Server wird das Frontend üblicherweise mit dem Kernsystem auf einem gemeinsamen Server betrieben und der explizite Frontend-Server entfällt.

Backend-Server

Auf dem Backend-Server wird das DVDV-Kernsystem betrieben. Er beantwortet die Anfragen der Dienstnutzer und des Frontend-Servers.

Am DVDV-Bundesmaster wird das Kernsystem nur über den Frontend-Server durch die Pflegenden Stellen verwendet, hier ist von einer geringen Last auszugehen.

Am DVDV-Server beantwortet das Kernsystem die Anfragen von Fachverfahren und Clearingstellen entweder über die Directory-Schnittstelle oder über die Legacy-Facade. Hier ist von einer hohen Last auszugehen. Der Backend-Server ist auf mindestens 120 Anfragen pro Sekunde im Dauerbetrieb ausgelegt. Genaue Lastzahlen wurden in einem aufwändigen Last- und Performancetest in 2022 ermittelt und nachgewiesen.

IAM-Server

Der IAM-Server authentifiziert die Client-Nutzer des Pflege-Clients und des Auskunfts-Clients. Eine Authentifizierung von Organisationen zum Zweck der Datenabrufe ist möglich, dieses Einsatzszenario ist aber absehbar nicht oder nur in Einzelfällen im Einsatz. Es ist daher von einer geringen Last auszugehen.

Datenbank-Server

Ausgehend vom Mengengerüst für DVDV und mit einer entsprechenden Reserve wird für die Datenbanken mit den folgenden maximalen Datenvolumina gerechnet:

- Datenbank Kernsystem: 12 GB
- Datenbank IAM: 8 GB

Die Hardwareanforderungen für den Datenbankserver leiten sich aus dieser Kalkulation und den erwarteten Zugriffen ab.

Grundlagen für die Kalkulation waren:

Datenbank Kernsystem:

- Max. 200.000 Ressourcen (Organisationen, Dienste, Provider) mit durchschnittlich 3-4 Zertifikaten und weiteren Metadaten
- Protokollierung von monatlich 1.000 Datenänderungen
- Puffer für DB-interne Daten

Datenbank IAM:

- Max. 100.000 Objekte (User, Clients) mit Authentisierungszertifikat und weiteren Metadaten.
- Protokollierung von monatlich 1.000 Datenänderungen
- Puffer für DB-interne Daten

7.1.1 DVDV-Bundesmaster

Beim DVDV-Bundesmaster werden Frontend und Kernsystem auf getrennten Servern betrieben.

Server	CPUs	RAM[8]	HD
Application-Server Frontend	4	Mind. 2 GB	10 GB frei
Application-Server Kernsystem	4	Mind. 2 GB	10 GB frei
Datenbank	8	Mind. 4 GB	20 GB für die DB
IAM Keycloak Knoten 1, IAM Keycloak Knoten 2	2	Mind. 2 GB	10 GB frei
IAM Datenbankserver Source, IAM Datenbankserver Replica	4	Mind. 4 GB	20 GB für die DB

Tabelle 43: Hardeware-Anforderungen an den DVDV-Bundesmaster (getrennter Betrieb von Frontend und Kernsystem)

7.1.2 DVDV-Server

Beim DVDV-Server werden Frontend und Kernsystem auf einem gemeinsamen Server betrieben.

Server	CPUs	RAM[9]	DB
Application-Server Frontend + Kernsystem	4	Mind. 4 GB	15 GB frei
Datenbank	8	Mind. 4 GB	20 GB für die DB

Tabelle 44: Hardware-Anforderungen an die DVDV-Server (gemeinsamer Betrieb von Frontend und Kernsystem)

7.2 Auslieferung der Software

Die DVDV-Software umfasst vier unterschiedliche Auslieferungs-Artefakte:

- Den DVDV-Bundesmaster zur Installation beim ITZ-Bund,

[8] Angaben zu RAM-Speicher beziehen sich auf den für den DVDV-Application-Server / die DVDV-Datenbank exklusiv zur Verfügung stehenden Speicherplatz.

[9] Angaben zu RAM-Speicher beziehen sich auf den für den DVDV-Application-Server / die DVDV-Datenbank exklusiv zur Verfügung stehenden Speicherplatz.

- den DVDV-Server zur Installation bei allen DVDV-Server-Betreibern und
- die DVDV-Bibliotheken in Java und .NET für die Hersteller von Clearingstellen und Fachverfahren zur einfachen Anbindung des DVDV.

Der DVDV-Bundesmaster wird als Zip-Paket ausgeliefert. Das Auslieferungspaket enthält diese Artefakte:

- Betriebshandbuch DVDV Bundesmaster
- Änderungshistorie
- Update-Anleitung zur Vorversion
- Project-Report mit verwendeten Drittbibliotheken und Lizenzen für die Komponenten Pflege-Client, Kernsystem und Legacy-Facade
- Verwundbarkeitsanalyse
- Adminclient-Handbuch
- Pflegeclient-Handbuch
- Auskunftsclient-Handbuch
- Auskunfts-Client Extended-Search-Handbuch
- Backend-Handbuch (Dokumentation der Kernsystem-API, intern wie öffentlich)
- Backend als rpm
- IAM als rpm
- Legacy-Facade als rpm
- Admin-Client als rpm
- Pflege-Client als rpm
- Auskunfts-Client als rpm
- Auskunfts-Client Extended-Search als rpm
- Komponente Betreibertest zum Test der Directory-Schnittstelle
- SQL-Skripte für Datenbankupdates

Der DVDV-Server wird als Zip-Paket ausgeliefert. Das Auslieferungspaket enthält diese Artefakte:

- Betriebshandbuch DVDV Server
- Änderungshistorie
- Update-Anleitung zur Vorversion
- Project-Report mit verwendeten Drittbibliotheken und Lizenzen für die Komponenten Auskunfts-Client, Kernsystem und Legacy-Facade
- Auskunftsclient-Handbuch
- Auskunfts-Client Extended-Search-Handbuch
- Backend-Handbuch (Dokumentation der Kernsystem-API, intern wie öffentlich)
- Backend als rpm
- Legacy-Facade als rpm
- Auskunfts-Client als rpm
- Auskunfts-Client Extended-Search als rpm
- Komponente Betreibertest zum Test der Directory-Schnittstelle

Das DVDV-DevKit Java wird auf dem Entwicklungsportal der FITKO[10] bereitgestellt, dort können die folgenden Artefakte bezogen und eingesehen werden:

- Dokumentation auf den Webseiten der FITKO
- DVDV-Bibliothek als jar
- API-Dokumentation der DVDV-Bibliothek als javadoc

[10] https://docs.fitko.de/dvdv/

- Beispiele für die Bibliotheksnutzung: simple-sample und controlfile-sample

Das DVDV-DevKit .NET wird auf dem Entwicklungsportal der FITKO[11] bereitgestellt, dort können die folgenden Artefakte bezogen und eingesehen werden:

- Dokumentation auf den Webseiten der FITKO
- DVDV-Bibliothek als Nuget-Package inkl. Dokumentation und Sourcecode
- API-Dokumentation der DVDV-Bibliothek in HTML
- Beispiel für die Bibliotheksnutzung: controlfile-sample

7.3 Lastverteilung und Ausfallsicherheit

Wie in den Abschnitten 2.2, 4.1 und 5.1 bereits beschrieben, ist das DVDV als verteilte Anwendung umgesetzt und wird in unterschiedlichen Rechenzentren, die über die ganze Bundesrepublik Deutschland verteilt sind, redundant betrieben. Über Vertreterregelungen wird eine wechselseitige Redundanz erreicht.

Den Kern des verteilten Systems bildet dabei der DVDV-Bundesmaster, der eine zentrale Rolle übernimmt. Auf diesem Teilsystem werden zentral alle Änderungen der Pflegenden Stellen über den Pflege-Client eingetragen und mittels Datenreplikation an die DVDV-Server weitergegeben.

Der DVDV-Bundesmaster spiegelt seinen Datenbestand damit kontinuierlich auf die dezentralen DVDV-Server, die sich die Anfragelast der einzelnen Datenabrufe teilen. Da die gesamten Fachdaten des Kernsystems gespiegelt werden, erhalten alle DVDV-Server den gleichen und vollständigen Datenbestand. Das bedeutet, dass jeder DVDV-Server jeden anderen DVDV-Server bei einem Ausfall oder bei Überlastung vertreten kann und damit eine hohe Ausfallsicherheit besteht. Auf den DVDV-Servern sind ausschließliche lesende Zugriffe zugelassen. Das DVDV-IAM wird, auf Basis der Software Keycloak, als Teil des Bundesmasters ebenfalls zentral betrieben und für die Anmeldung von Benutzern des Pflege-Clients und der Auskunfts-Clients verwendet.

Der Bundesmaster ist nicht ausfallsicher und redundant aufgesetzt. Das gilt für alle Komponenten des DVDV-Bundemasters und damit auch für das DVDV-IAM. Bei einem Ausfall dieses Systems würde zwar die Datenerfassung und Dateneinsicht gestört, nicht jedoch die abfragenden Datenzugriffe durch Fachverfahren und Clearingstellen. Aus diesem Grund sind die Verfügbarkeitsanforderungen an den Bundesmaster nicht so hoch, dass sie ein redundantes System rechtfertigen würden.

Die Anforderungen an die Verfügbarkeit der DVDV-Server für Datenabfragen ist ungleich höher. Hier führt ein längerer Ausfall zu erheblichen Konsequenzen in unterschiedlichsten Kommunikationsszenarien der öffentlichen Hand. Auch die Zahl der Anfragen und Nutzungen ist ungleich höher als auf dem Bundesmaster. Daher sind die DVDV-Server, die für die Beantwortung dieser Anfragen zuständig sind, bundesweit verteilt und mit einer georedundanten Vertreterregelung umgesetzt. Sollte ein DVDV-Server ausfallen oder überlastet sein, wird er durch einen anderen DVDV-Server vertreten.

Für die Dienstnutzer, die über die DVDV-Bibliotheken auf die DVDV-Server zugreifen, wird die Vertretung so gelöst, dass in den DVDV-Bibliotheken für Java und .NET eine Liste von DVDV-Server-Adressen hinterlegt werden kann. Sollte der erste DVDV-Server in der Liste nicht erreichbar sein und innerhalb einer konfigurierbaren Zeit keine Antwort liefern, so wird automa-

[11] https://docs.fitko.de/dvdv/

tisch der in der Liste folgende DVDV-Server genutzt. In regelmäßigen Abständen wird die Verfügbarkeit des primären DVDV-Servers geprüft, bei Wiederverfügbarkeit wird auf diesen zurück geschwenkt.

Der Auskunfts-Client und das Kernsystem eines DVDV-Servers sind üblicherweise auf einem gemeinsamen System aufgesetzt. Bei Nichtverfügbarkeit dieses Systems kann ebenfalls ein alternativer DVDV-Server genutzt werden. Dazu ist es lediglich nötig, die URL des alternativen Auskunfts-Clients im Browser zu verwenden. Der Zugriff auf diesen alternativen Server muss netzwerkseitig ermöglicht werden.

8 Querschnittliche Konzepte

8.1 Styleguide

Entsprechend der Vorgabe VL9 wurde das DVDV unter Einhaltung des Styleguides der Bundesregierung für Webanwendungen im Stand von 2018 umgesetzt. Dieser Styleguide macht insbesondere die folgenden Vorgaben:

- Einheitlich festgelegte Breite für den Contentbereich
- Gestaltung des Headers, des Footers und der Menüführung
- Begrenzung der Höhe des Contentbereichs, so dass auf einem marktüblichen 21 Zoll-Monitor kein Scrolling notwendig ist. Für größere Seiteninhalte wird daher primär auf Wizards, Tab-Reiter und Paging von Listen gesetzt.

Für aktuelle Änderungen an der Software wird der Styleguide weiterhin soweit eingehalten, wie es für eine durchgängige, gleichartige Bedienbarkeit der Anwendung notwendig ist, in Einzelfällen wird aber zugunsten einer besseren Bedienbarkeit davon abgewichen.

8.2 Authentifizierung

Sowohl Benutzer der Webapplikationen als auch Dienstnutzer der REST-Schnittstellen des DVDV-Bundesmasters und DVDV-IAM müssen sich am IAM-System authentifizieren. In der Architekturentscheidung AE_5 wurde die Verwendung von Software-Zertifikaten für die Authentisierung festgelegt.

Mit der Umsetzungsvorgabe VL11 wurde für das Gesamtsystem DVDV das Authentifizierungsprotokoll OAuth 2 festgelegt. OAuth 2 sieht verschiedene Authentifizierungs-Workflows vor. Der Authentifizierungs-Workflow unterscheidet sich je nach Szenario.

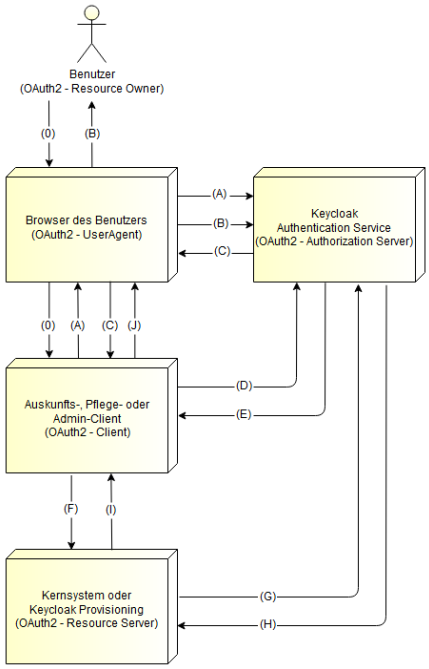
8.2.1 Authentifizierung eines Nutzers an einer Webapplikation

Die Authentisierung eines Nutzers beim Zugriff auf eine Webapplikation erfolgt mit Hilfe des Browsers des Benutzers. Beim Zugriff auf die Webapplikationen handelt es sich um Mensch-Maschine-Kommunikation, denn den Zugriff erhalten Benutzer des Systems. Das IAM-System leitet den Browser auf eine URL, die per TLS mit Client-Authentisierung abgesichert ist. Daher authentisiert sich der Benutzer mittels eines im Zertifikatsspeicher des Browsers hinterlegten Benutzer-Zertifikats. Dieses X.509-Zertifikat wird dann beim Aufbau der TLS-Verbindung in der TLS-Message „Client Certificate“ übermittelt und zur Authentifizierung des Nutzers im IAM-System verwendet.

Der „Authorization Code Grant“ bildet den webbasierten Zugriff eines menschlichen Nutzers auf Ressourcen ab. In der Ausdruckweise von OAuth 2 fragt hier ein Resource-Owner (der Benutzer) mittels Client-Software (den Webapplikationen) Daten eines Resource-Servers (den Services des Kernsystems und des IAM-Systems) nach Authentisierung mit Hilfe eines User-Agents (dem Browser) am Authorization-Server (dem IAM-System) ab. Dieser Workflow wird am DVDV-System für die Authentifizierung an den Webapplikationen verwendet. Das auf diesem Wege erhaltene Access Token nutzen die Webapplikationen, um autorisierten Zugriff auf die Web-Services zu bekommen. Dabei wird beim Aufruf der Webservices das Access Token im HTTP-Header „Authorization“ übermittelt. Das Access Token enthält u.a. die folgenden Daten:

- den Benutzernamen
- die Benutzergruppen des Benutzers
- die Rollen des Benutzers

- das Vertrauensniveau der Registrierung
- das Vertrauensniveau der Authentisierung
- eine Signatur über das gesamte Access Token

Use-Case:	**Authentifizierter Benutzerzugriff**
Dieser Use-Case beschreibt, wie sich ein Nutzer am DVDV anmeldet und dann authentifizierten Zugriff auf eine Webapplikation und auf Daten des DVDV-Bundesmasters und des DVDV-IAM erhält.	
Referenziert: Anwendungsfall IDM_A_01	
Vorbedingung	
1. Der Nutzer ist als Identität im IAM-System angelegt und besitzt Rollen, die ihm Rechte auf Benutzergruppen oder Ressourcengruppen einräumen. 2. Der Nutzer ist an keiner Webapplikation angemeldet. 3. Der Nutzer ist in der Lage, mit dem Browser den DVDV-Bundesmaster über das NdB zu erreichen.	
Szenarien	
Standardablauf	
Der Authentifizierungsablauf entspricht dem „Authorization Code Flow“ von OAuth 2.[12]  	

[12] Siehe https://tools.ietf.org/html/rfc6749#section-1.3.1 und https://tools.ietf.org/html/rfc6749#section-4.1

Schritt (0): Aufruf einer Webapplikation im Browser

Der Benutzer ruft in seinem Browser eine Webapplikation des DVDV auf. Für den Ablauf der Authentifizierung ist es unerheblich, ob der Auskunfts-Client, der Pflege-Client oder der Admin-Client aufgerufen wird. Unterschiedlich sind nur die durch die Webapplikation angezeigten Daten und somit auch die zum Datenabruf angesprochenen Backend-Systeme.

In der Sprechweise von OAuth 2 ist der Browser der User-Agent des Benutzers, die Webapplikation ist der Client, welcher Daten abrufen möchte.

Schritt (A): Weiterleitung an das IAM-System

Die Webapplikation stellt fest, dass der Benutzer nicht angemeldet ist und führt eine Weiterleitung auf den OAuth 2 Authorization Endpoint des DVDV-IAM durch. D.h. der Browser des Nutzers wird per Redirect (bspw. durch den http-Statuscode 303 „See Other“ mit der URL des DVDV-IAM im HTTP-Header „Location“) auf das IAM-System geleitet. Dabei wird eine Authentisierungsanfrage des Clients (der Webapplikation) an das IAM-System transportiert.

Der Authorization Endpoint des IAM-Systems nimmt die Authentisierungsanfrage entgegen und prüft, ob es sich um einen am IAM-System registrierten Client handelt.

Schritt (B): Authentisierung und Authentifizierung des Nutzers

Das IAM-System führt die Authentifizierung des Benutzers durch. Bspw. authentisiert sich der Benutzer durch Angabe von Benutzername und Kennwort oder durch TLS-Client-Authentisierung.

Schritt (C): Übermittlung des Authorization Code

Nach erfolgreicher Authentifizierung des Benutzers übermittelt das IAM-System per Redirect-Mechanismus einen Authorization Code (eine Art Authentifizierungs-Session-Identifier) an die Webapplikation.

Schritt (D): Anfordern des Access Token

Unter Vorlage des Authorization Code und der Client Credentials fordert die Webapplikation das Access Token am Token Endpoint des DVDV-IAM an. Das IAM-System ermittelt den konfigurierten Client und prüft die Client Credentials.

Schritt (E): Übermittlung des Access Token

Das IAM-System erstellt ein signiertes Access Token mit allen dem authentifizierten Benutzer zugeordneten Rollen und übermittelt dies an die Webapplikation.

Schritt (F): Aufruf der REST-Schnittstelle

Die Webapplikation ruft die REST-Schnittstelle des Kernsystems oder die SCIM-Schnittstelle des DVDV-IAM auf und übergibt im HTTP-Header „Authorization“ das Access Token.

Schritte (G) und (H): Prüfung des Access Token Das Kernsystem oder die Provisionierungsschnittstelle des IAM-Systems ruft die JWKS-URI des DVDV-IAM auf. Dort wird der Signaturschlüssel des IAM abgerufen, mit dem die Access Token signiert sind. Durch Signaturprüfung wird die Gültigkeit des Access Token verifiziert. **Schritte (I) und (J): Rückgabe und Anzeige der Daten** Entsprechend den Rollen im Access Token werden Daten an die Webapplikation zurückgegeben, welche diese dem Benutzer im Browser anzeigt.
Ergebnis:
Der Benutzer ist erfolgreich an der Webapplikation angemeldet und bekommt Daten entsprechend seinen Rollen angezeigt.

8.2.2 Authentifizierung eines Fachverfahrens an der Directory-Schnittstelle

Die Authentifizierung eines dezentralen Fachverfahrens für den Zugriff auf die Directory-Schnittstelle des DVDV erfolgt beim Aufruf des Token Endpoints am DVDV-IAM oder des Token Endpoints am DVDV-Kernsystem durch das Fachverfahren. Beim Zugriff auf die Schnittstellen handelt es sich um Maschine-Maschine-Kommunikation, denn Zugriff auf die Schnittstellen erhalten sowohl Organisationen, die als Dienst oder Dienstnutzer agieren, als auch dezentrale Fachverfahren.

Für eine Authentifizierung des Fachverfahrens am IAM muss dort ein entsprechender Client hinterlegt sein. Organisationen (als Nutzer von Fachverfahren), die im DVDV bereits verzeichnet sind, können alternativ mit ihrem Organisationszertifikat ein Access-Token vom DVDV-Kernsystem an dessen Token-Schnittstelle beziehen und müssen nicht zusätzlich im DVDV-IAM hinterlegt werden.

Beim Token-Abruf überträgt das dezentrale Fachverfahren im HTTP-Header „client_assertion“ ein mit seinem Software-Zertifikat signiertes JSON Web Token. Durch die mathematische Signaturprüfung wird das Fachverfahren vom IAM-System oder DVDV-Kernsystem gegen das im jeweiligen System hinterlegte öffentliche Zertifikat authentifiziert.

Der „Client Credentials Flow“ bildet den maschinellen Zugriff auf Ressourcen ab. In der Ausdruckweise von OAuth 2 greift hier ein Client (das dienstnutzende Software-System) auf den Resource-Server (den Services des Kernsystems und des IAM-Systems) nach Authentisierung des Clients am Authorization-Server (hier IAM-System oder DVDV-Kernsystem) zu. Dieser Workflow wird am DVDV-System für die Authentifizierung an der Directory-Schnittstelle verwendet. Das vom IAM-System oder alternativ vom DVDV-Kernsystem erhaltene Access Token wird dann an der Directory-Schnittstelle zur Autorisierung verwendet. Dabei wird beim Aufruf der Webservices das Access Token im HTTP-Header „Authorization“ übermittelt. Das Access Token enthält u.a. die folgenden Daten:

- die Client-ID
- die Rollen des Clients
- das Vertrauensniveau der Authentisierung
- eine Signatur über das gesamte Access Token

8.2.2.1 Authentifizierung am DVDV-IAM

Use Case:	**Authentifizierter Zugriff eines Fachverfahrens mittels Authentifizierung am DVDV-IAM**

Dieser Use-Case beschreibt, wie sich ein dezentrales Fachverfahren am DVDV-IAM anmeldet und dann authentifizierten Zugriff auf Daten des Kernsystems erhält (bspw. zur Überprüfung von Zugriffsberechtigungen einer dienstnutzenden Behörde).

Referenziert: Anwendungsfall IDM_A_02

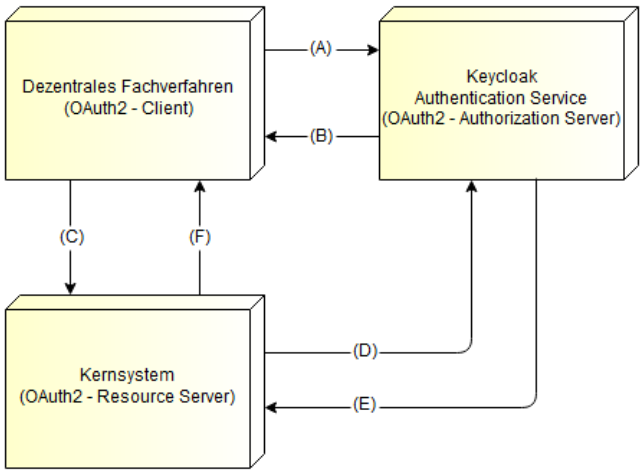
Vorbedingung

1. Das dezentrale Fachverfahren ist im IAM-System als OAuth 2 Client angelegt und besitzt Rollen, die ihm Rechte auf Ressourcengruppen einräumen.
2. Das dezentrale Fachverfahren besitzt kein gültiges Access Token.

Szenarien

Standardablauf – Authentifizierung am DVDV-IAM

Der Authentifizierungsablauf entspricht dem „Client Credentials Flow“ von OAuth 2.[13]



<u>Schritt (A): Anfordern des Access Token</u>

Das dezentrale Fachverfahren ruft den Token Endpoint des DVDV-IAM auf. In seiner Anfrage übermittelt es im HTTP-Header seine Client Credentials. Das IAM-System nimmt die Anfrage entgegen, ermittelt den konfigurierten Client zum dezentralen Fachverfahren und validiert die Client Credentials.

[13] Siehe https://tools.ietf.org/html/rfc6749#section-1.3.4 und https://tools.ietf.org/html/rfc6749#section-4.4

Schritt (B): Übermittlung des Access Token

Das IAM-System erstellt ein signiertes Access Token mit allen dem dezentralen Fachverfahren zugeordneten Rollen und übermittelt dieses zurück zum Fachverfahren.

Schritt (C): Aufruf der Directory -Schnittstelle

Das dezentrale Fachverfahren ruft die Directory-Schnittstelle des Kernsystems auf und übergibt im HTTP-Header „Authorization“ das Access Token.

Schritte (D) und (E): Prüfung des Access Token

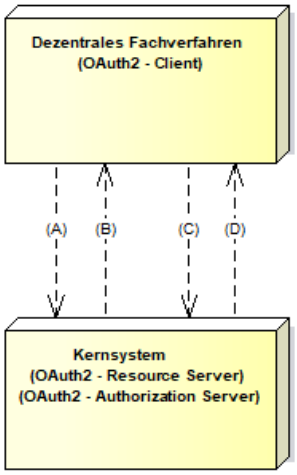
Das Kernsystem ruft die JWKS-URI des DVDV-IAM auf. Dort wird der Signaturschlüssel des IAM abgerufen, mit dem die Access Token signiert sind. Durch Signaturprüfung wird die Gültigkeit des Access Token verifiziert.

Schritt (F): Rückgabe der Daten

Die angeforderten Daten werden an das dezentrale Fachverfahren zurückgegeben.

8.2.2.2 Authentifizierung am Token-Endpunkt des DVDV-Kernsystems

Use Case: Authentifizierung am Token-Endpunkt des DVDV-Kernsystems
Dieser Use-Case beschreibt, wie sich ein dezentrales Fachverfahren am DVDV-Kernsystem anmeldet und dann authentifizierten Zugriff auf Daten des Kernsystems erhält.
Referenziert: Anwendungsfall KS_A_01
Vorbedingung
1. Das dezentrale Fachverfahren wird von einer Organisation betrieben, die im DVDV hinterlegt ist. Für diese Organisation ist im DVDV ein gültiges Client-Zertifikat hinterlegt. 2. Die Organisation besitzt den privaten Schlüssel für dieses Client-Zertifikat und das Fachverfahren hat darauf Zugriff. 3. Das dezentrale Fachverfahren besitzt kein gültiges Access Token.



Schritt (A): Anfordern des Access Token

Das dezentrale Fachverfahren ruft den Token Endpoint des DVDV-Kernsystems auf. In seiner Anfrage übermittelt es im HTTP-Header ein JWT-Token, signiert mit einem Client-Zertifikat der betreibenden Organisation als Client Credentials. Das Kernsystem nimmt die Anfrage entgegen, ermittelt die Organisation zum dezentralen Fachverfahren und validiert die Client Credentials.

Schritt (B): Übermittlung des Access Token

Das Kernsystem erstellt ein signiertes Access Token mit Angaben zur Organisation des dezentralen Fachverfahrens und übermittelt dies zurück zum Fachverfahren.

Schritt (C): Aufruf der REST-Schnittstelle

Das dezentrale Fachverfahren ruft die REST-Schnittstelle des Kernsystems auf und übergibt im HTTP-Header „Authorization“ das Access Token.

Prüfung des Access Token

Da das Kernsystem alle Daten zur Prüfung des Access-Token selbst hält, ist eine Kommunikation hierfür nicht notwendig. Das Kernsystem prüft selbst die Claims des Access-Token gegen das hinterlegte Client-Zertifikat der Organisation.

Schritt (D): Rückgabe der Daten

Entsprechend den Rollen im Access Token werden Daten an das dezentrale Fachverfahren zurückgegeben.

Ergebnis:

Das dezentrale Fachverfahren ist erfolgreich authentifiziert, besitzt ein gültiges Access Token und hat damit Daten entsprechend seinen Rollen abgerufen.

8.3 Rollenkonzept und Autorisierung

Autorisierungsentscheidungen werden im DVDV Gesamtsystem auf der Ebene der Systemkomponenten (Teilsysteme der Anwendung DVDV) und auf Ressourcenebene (im DVDV gespeicherte Datenobjekte = Ressourcen, z.B. Organisationen oder Dienste) getroffen. Das Konzept sieht vor, dass Benutzer Rollen besitzen können. Rollen gewähren Rechte auf Systemkomponenten oder einzelne Objekte.

Die Autorisierung wird im DVDV auf Basis von Rollen durchgeführt. Eine Rolle ist immer die Zuordnung eines Entitlements zu einer Ressourcengruppe/Benutzergruppe.

- Eine Ressourcengruppe oder ResourceGroup gruppiert eine Menge von Ressourcen und wird im Kernsystem gepflegt. Es können neue ResourceGroups angelegt und Ressourcen diesen ResourceGroups zugeordnet werden. Über die ResourceGroups soll die Autorisierung im Kernsystem durchgeführt werden, indem das IAM-System immer Berechtigungen für komplette ResourceGroups vergibt und diese dem Kernsystem mitteilt.
- Eine Benutzergruppe oder IdentityGroup gruppiert eine Menge von Benutzern und wird im IAM gepflegt. Es können neue IdentityGroups angelegt und Benutzer diesen IdentityGroups zugeordnet werden. Über die IdentityGroup soll die Autorisierung in der SCIM-Schnittstelle des IAM-Systems durchgeführt werden, indem das IAM-System immer Berechtigungen für komplette IdentityGroups vergibt und diese der SCIM-Schnittstelle mitteilt.
- Mittels Entitlements (s. 8.3.2) werden die Rechte von IdentityGroups auf ResourceGroups definiert.

Zum Beispiel bedeutet eine Rolle mit Entitlement = „Create“ und ResourceGroup = „Meldebehörden Schleswig-Holstein“, dass eine Gruppe von Benutzern berechtigt ist, Schleswig-Holsteinische Meldebehörden anzulegen.

Im IAM-System ist die Rolle einer IdentityGroup zugeordnet, z.B. IdentityGroup = „Pflegende Stelle Dataport“, alle Identitäten in dieser IdentityGroup sind Datenpfleger:innen in der pflegenden Stelle Dataport und dürften bei entsprechender Zuordnung durch ein Entitlement die Datenpflege für alle Ressourcen in der ResourceGroup=“Organisationen - Dataport“ vornehmen.

Die Erstellung der Rollen und die Pflege dieser Rollenzuordnungen zu Benutzergruppen sind im Admin-Client möglich.

Das Kernsystem bekommt mit dem Authentifizierungstoken alle Rollen mitgeteilt, die für den angemeldeten Benutzer gelten und trifft auf Basis dieser Rollen und der enthaltenen Ressourcengruppen die Autorisierungsentscheidung unterhalb der REST-Service-Schicht. In analoger Weise führt die SCIM-Schnittstelle des IAM-Systems Autorisierungsentscheidungen durch.

8.3.1 Rollen für Systemkomponenten

Um den Zugriff auf die Systemkomponenten des Gesamtsystems DVDV für Benutzer steuern zu können, werden für Systemkomponenten explizite Zugriffsrollen eingeführt.

Systemkomponente	**Erforderliche Rolle**
Kernsystem	CoreAccess
SCIM-Schnittstelle des IAM	Keine explizite Rolle notwendig, Steuerung mittels Rollen- und Rechtekonzept für Objekte

Admin-Client	AdminClient
Pflege-Client	PflegeClient
Auskunfts-Client	AuskunftsClient

Tabelle 45: Rollenkonzept Systemkomponenten

8.3.2 Rollen und Entitlements für Datenobjekte

Autorisierungsentscheidungen für Datenobjekte, die Ressourcen oder Benutzer sind, werden anhand des Rollen- und Rechtekonzepts unterhalb des Servicelayers getroffen. Rollen gewähren hier Rechte (Entitlements) auf Ressourcengruppen oder Benutzergruppen, in denen die entsprechenden Datenobjekte gruppiert sind. Als Entitlements werden hier Rechte für die vier CRUD-Operationen benötigt. Zusätzlich wird ein zusammengesetztes Recht für alle CRUD-Operationen sowie ein Recht zur Bestätigung von Änderungen modelliert.

Name	Beschreibung
Create	Wird benötigt, um Ressourcen oder Benutzer anzulegen
Read	Wird benötigt, um Benutzer zu lesen. Hierbei werden die Informationen, wer wann einen Datensatz geändert hat, nicht mitgeliefert. Leserechte auf Ressourcen werden ohne dieses Entitlement vergeben, da diese Daten quasi öffentlich einsehbar sind und es für einen lesenden Zugriff keiner expliziten Berechtigung bedarf.
Update	Wird benötigt, um Ressourcen oder Benutzer zu ändern
Delete	Wird benötigt, um Ressourcen oder Benutzer zu löschen
CRUD	Ein zusammengesetztes Recht, das die vier Rechte Create, Read, Update und Delete beinhaltet
Approve	Wird für die vorläufigen Änderungen benötigt. Besitzt ein Benutzer nur das Recht „Approve“, so ist keine direkte Bearbeitung der Ressourcen möglich. Der Benutzer ist nur berechtigt, Änderungsvorschläge an den jeweiligen Ressourcen zu erstellen. Diese müssen durch einen Pfleger mit Schreibrechten (Create, Update, Delete, CRUD) bestätigt werden.

Tabelle 46: Rechte auf Ressourcengruppen oder Identitätsgruppen

Daneben gibt es Datenobjekte, die keine Ressourcen oder Benutzer sind und damit auch keiner Ressourcengruppe oder einer Benutzergruppe zugeordnet sind. Das sind u.a.:

- IdentityGroup
- Role
- Representation
- ResourceGroup
- ServiceDescription
- ServiceElement
- Bookmarks
- Statistics

Da für diese Objekte Schnittstellen am IAM-System oder Kernsystem des DVDV-Bundesmasters existieren, muss der Zugriff darauf durch das Rollen- und Rechtekonzept autorisiert erfolgen. Dazu wird das folgende Entitlement eingeführt:

Name	Beschreibung
SuperAdmin	Berechtigt zum Pflegen von Dienstbeschreibungen, Organisationskategorien, komplexen Attributen und benutzerdefinierten Ressourcen
GroupAdmin	Berechtigt zum Pflegen (Anlegen, Ändern, Löschen) von allen Gruppen und Rollen
SubstituteAdmin	Berechtigt zum Pflegen (Anlegen, Ändern, Löschen) von allen Vertretungsregelungen

Tabelle 47: Allgemeine Rechte für Datenobjekte, die keine Ressourcen oder Benutzer sind

8.3.3 Darstellungsform von Rollen

Rollen besitzen im Datenmodell von Keycloak keine beliebigen Attribute und sind deshalb nicht generisch erweiterbar. Um keine Anpassung an Keycloak vornehmen zu müssen, werden bei DVDV daher alle Informationen im Rollennamen kodiert, der damit eine semantische Bedeutung bekommt. Nach den obigen Ausführungen werden drei Typen von Rollen unterschieden:

1. Rollen, die Rechte (Entitlement) auf Benutzergruppen (IdentityGroup) verleihen. Rollen dieses Typs haben einen Rollennamen nach dem Schema
   <Entitlement>_IG_<IdentityGroup>,
   also z.B.
   Create_IG_PflegerBremen oder
   Delete_IG_Pfleger.

2. Rollen, die Rechte (Entitlement) auf Ressourcengruppen (ResourceGroup) verleihen. Rollen dieses Typs haben einen Rollennamen nach dem Schema
   <Entitlement>_RG_<ResourceGroup>,
   also z.B.
   Create_RG_BehoerdenBremen oder
   Delete_RG_RessourcenDataport.

3. Rollen, die allgemeine Rechte (Entitlement) verleihen und ohne die Angabe einer Benutzergruppe oder Ressourcengruppe verwendet werden. Rollen dieses Typs sind:
   SuperAdmin,
   GroupAdmin,
   SubsituteAdmin,
   AdminClient,
   PflegeClient oder
   AuskunftsClient.
4. Rollen, die Rechte auf allen Benutzern oder Ressourcen verleihen. Rollen dieses Typs sind:

   Create_Users, Read_Users, Update_Users, Delete_Users und CRUD_Users

   sowie

   Create_Resources, Read_Resources, Update_Resources, Delete_Resources und CRUD_Resources.

8.3.4 Zuordnung von Rollen

Rollen werden Benutzergruppen zugeordnet. Damit erhalten alle Benutzer, die Mitglieder einer Benutzergruppe sind, die mit der Rolle verbundenen Rechte. Ist ein Benutzer Mitglied in mehreren Benutzergruppen, so besitzt er die Vereinigungsmenge der Berechtigungen dieser Benutzergruppen.

8.4 Datenbank

8.4.1 Replikation

Gemäß der Vorgabe VL5 werden alle Daten des Kernsystems für den Anwender transparent vom DVDV-Bundesmaster zu den DVDV-Servern repliziert. Die Daten werden vom DVDV-Bundesmaster als Source zu den DVDV-Servern als Replicas mittels binärer Datenbankreplikation direkt übertragen. Das heißt, der DVDV-Bundesmaster und alle DVDV-Server enthalten jederzeit einen identischen Datenbestand.

Da im ITZBund ein Zugriff von außen immer im Application-Layer der Anwendung enden muss, wurde für die praktische Umsetzung eine Intermediate-DB hinter einem MySQL-Router in diesem Layer platziert. Dies unterbricht die direkte Replikation zu den DVDV-Servern aus dem DB-Layer des Bundesmaster. Die Intermediate-DB agiert gegenüber der Bundesmaster-DB als Replica und gegenüber der DVDV-Server-DB als Source. Zur weiteren Absicherung wird der Replikationsdatenstrom durch einen TLS-Tunnel geroutet.

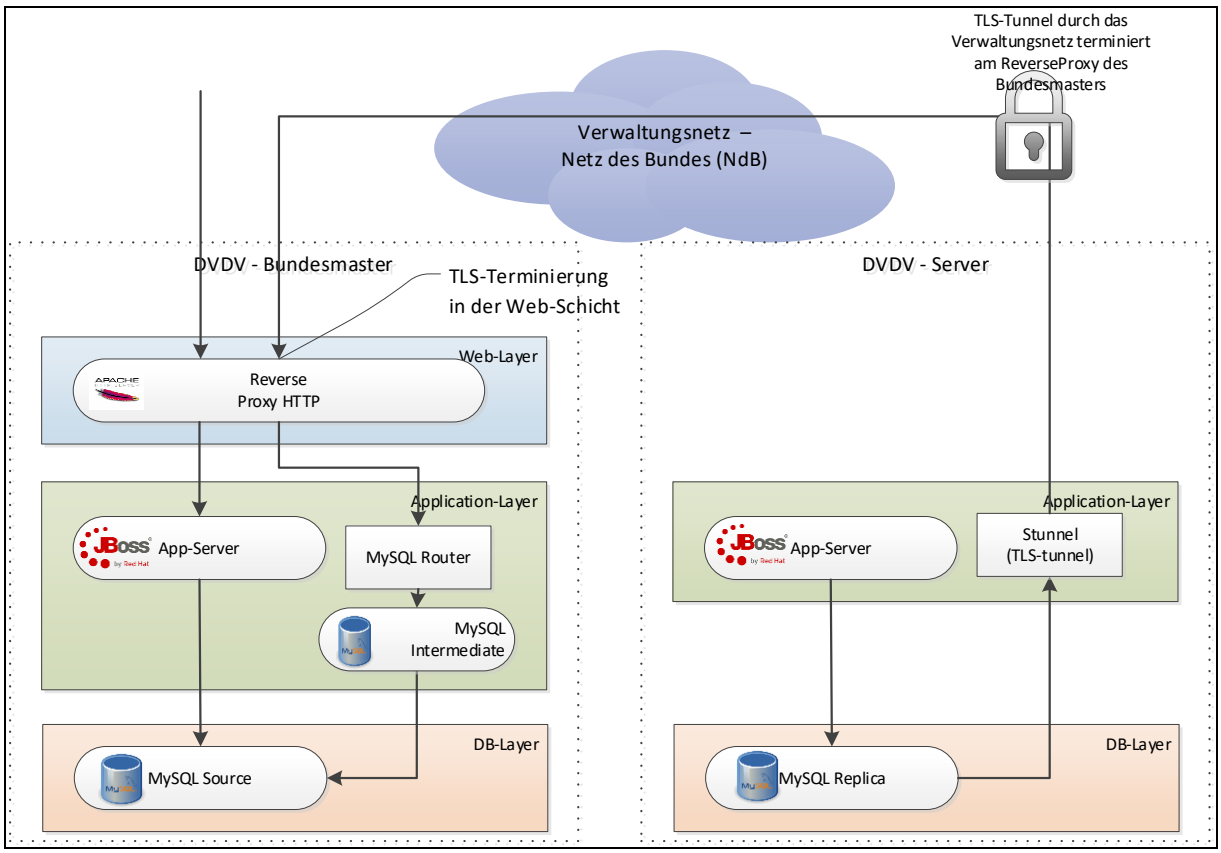


Abbildung 6: Umsetzung der Replikation in der Praxis

Die Informationsverteilung wird direkt auf der Datenbankebene mit Hilfe der integrierten Replikationsmechanismen des MySQL realisiert:

Binäre Replikation über GTIDs (Global Transaction Identifiers)

- Jede Transaktion des Source-Servers erhält eine eindeutige ID. Diese enthält die UUID des Servers und eine fortlaufende Nummer der Transaktion.
- Der Source-Server führt eine Transaktion durch und ermittelt die GTID. Für die Replikation werden beide Komponenten in das Binary Log geschrieben.
- Die Replica-Server übernehmen die Logs vom Source-Server in ihre Relay Logs und übertragen die GTID in die interne Datenbankvariable „GTID_NEXT“.
- Bevor die Transaktion des Source-Servers ausgeführt wird, überprüft der Replica-Server, ob die GTID bereits ausgeführt wurde. Ist dies nicht der Fall, wird die Transaktion ausgeführt.
- Die Verbindungen zwischen dem Source-Server und den Replica-Servern sind über TLS (Transport Layer Security) gesichert.

Die Umsetzung der Replikation mit Mitteln der Betriebsinfrastruktur stellt hohe Anforderungen an den Betrieb. Diese sind insbesondere:

- Eine strenge Vorgabe von Versionsständen der eingesetzten Datenbanken bei DVDV-Bundesmaster und DVDV-Servern ist zwingend notwendig.
- Updates zwischen DVDV-Servern und DVDV-Bundesmaster müssen zeitlich koordiniert erfolgen, um mögliche Inkompatibilitäten zwischen den eingesetzten Versionen zu vermeiden.
- Es sind Szenarien möglich (z.B. ein Rollback des DVDV-Bundesmasters), die nicht automatisch und transparent von den Replizierungsmechanismen der Datenbanken behandelt werden können. Hier ist ein manueller Eingriff der Datenbankadministratoren des DVDV-Bundesmasters und auch der jeweiligen DVDV-Server notwendig.
- Es ist nicht möglich, Replikationsfehler fachlich zu identifizieren. Um die Integrität der Daten der DVDV-Server sicherzustellen, ist eine Überwachung der Replikationsparameter (GTID) durch den Betrieb (DVDV-Bundesmaster und DVDV-Server) erforderlich.

8.4.2 Anbindung der Datenbank

Die Datenbank wird an die Anwendung über die Java Persistence API (JPA) angebunden. Als Implementierung der API wird Hibernate verwendet. Zum Herstellen der Datenbankverbindung über den Application-Server ist ein JDBC-Connector erforderlich, der als Modul im Server installiert wird; dieser wird von MySQL mitgeliefert.

Je nach Anwendungsfall werden innerhalb des Kernsystems zur Abfrage der Datenbank folgende Hilfsmittel verwendet:

- Hibernate Named Query
- Hibernate Query Language (HQL)
- Hibernate Criteria API

8.4.3 Versionierung der Datenbank

Für die regelmäßigen Deployments von Datenbankänderungen (DDL) ist es notwendig, den Versionsstand des Datenbankschemas eindeutig zu identifizieren. Es muss gewährleistet sein, für jedes Release die Änderungen an den Datenbankstrukturen reibungslos migrieren zu können.

Um das zu gewährleisten, werden DDL-Skripte fortlaufend nummeriert und die fortlaufende Nummer jedes DDL-Skripts wird durch das Skript selbst in die Datenbank-Tabelle

SCHEMA_VERSION geschrieben. An dem Inhalt dieser Tabelle kann man auf allen beteiligten Servern jederzeit die Version des aktuellen Datenbankschemas ablesen.

8.5 Datenmodell

Das Datenmodell von DVDV ist folgendermaßen aufgeteilt:

- Im DVDV-IAM werden alle Daten gehalten, die im Kontext stehen mit Benutzeranmeldungen, Pflegegruppen, Vertretungsregelungen, Rollen und Rechten.
- Im DVDV-Kernsystem werden alle Daten gehalten, die im Kontext stehen mit Organisationen, Behörden, Diensten, Dienstbeschreibungen, Komplexen Geschäftsobjekten, Favoriten und Bookmarks.

Als Schnittmenge zwischen diesen Systemen sind die Ressourcengruppen vorgesehen. Diese gruppieren Ressourcen (Organisation (=Behörde), Dienst, Provider, benutzerdefinierte Ressourcen) und dienen der Autorisierung. Das DVDV-IAM kann einer Identität ein Entitlement (=Berechtigung) auf einer Ressourcengruppe und damit auf alle enthaltenen Ressourcen zuweisen, siehe auch in Abschnitt 8.3.2

8.5.1 Fachdatenmodell des Kernsystems

Das Fachdatenmodell enthält die fachlichen Daten von DVDV. Die Darstellung gliedert sich in die Bereiche

- Ressource als Oberbegriff und Basisobjekt für Fachdaten, wie Dienste, Organisationen, Behörden, Behördenstellvertreter und Provider
- Daten zu Favoriten und Vorbelegungen (Bookmarks, Defaults) von Masken
- Daten, die benutzerdefinierte Ressourcen und Attribute beschreiben
- Daten zur fachlichen Protokollierung von Änderungen

Diese Teilmodelle sind größtenteils unabhängig und werden daher getrennt dargestellt. Zur besseren Lesbarkeit ist der Bereich Ressourcen in einzelne Diagramme aufgeteilt. Die Daten liegen in einer gemeinsamen Datenbank.

Datenobjekt	**Beschreibung**
Organization	Organisation oder Behörde (als spezielle Organisation): • Metadaten wie Name und Beschreibung (zweisprachig), Adresse • Lokation der Organisation (Bundesland, Regierungsbezirk, Kreis); für Bundesbehörden oder kreisübergreifende Organisationen ist dies der Sitz der Organisation • 4-stufige Kategorisierung der Organisation • Zugeordnete Organisationsschlüssel (OrganizationKey) (mehrere) • ClientCertificates als Authentifizierungszertifikate der Organisation. Diese Zertifikate dienen der Organisation zur Authentifizierung in unterschiedlichen Fachszenarien und zur Nutzung der Directory-Schnittstelle des DVDV. Dienstnutzer, die in einem solchen Fachszenario kommunizieren, können die erhaltenen Zertifikate gegen das DVDV prüfen.

Datenobjekt	Beschreibung
	• Zugeordnete Dienste • Zugeordnete Dienstelemente • Gültigkeitszeitraum, aktuell ohne Verwendung • Pending für Organisationen, die noch in der QS geprüft werden müssen • Zuordnung zu ResourceGroups für die Autorisierung
OrganizationRepresentative	Stellvertreter von Organisationen und Behörden • Ein Stellvertreter von Organisationen; entspricht im Aufbau und Metadaten einer Organisation • Zusätzlich enthält er eine Liste von Referenzen auf die vertretenen Organisationen
Provider	Provider (Anbieter von Infrastruktur, wie Intermediären und Webservern) • Metadaten, wie Name und Beschreibung (zweisprachig), Adresse • Lokation des Providers (Bundesland, Regierungsbezirk, Kreis), im Zweifelsfall der Sitz des Providers • Zugeordnete Dienstelemente • Gültigkeitszeitraum • Pending für Provider, die noch in der QS geprüft werden müssen • Zuordnung zu ResourceGroups für die Autorisierung
Service	Dienst (wird von einer Organisation angeboten) • Metadaten, wie Name und Beschreibung (zweisprachig) • Verweis auf die zugehörige Dienstbeschreibung • Referenzierte Dienstelemente • Eindeutiger Dienstbezeichner • Gültigkeitszeitraum • Pending für Dienste, die noch in der QS geprüft werden müssen • Der Ort des Dienstes wird nicht gespeichert, sondern entspricht dem Ort der Organisation, die den Dienst anbietet
ServiceElement	Dienstelement Dienstelemente sind die Daten, die die Ausprägung eines Dienstes eindeutig beschreiben und dem Dienstnutzer Informationen zur Erreichbarkeit des Dienstes liefern. Insbesondere sind dies Intermediäre, URIs, Zertifikate und ähnliches.

Datenobjekt	Beschreibung
	Dienstelemente sind eindeutig genau einer Ressource vom Typ Organisation, Stellvertreter oder Provider zugeordnet. Diese stellt das Dienstelement technisch zur Verfügung (z.B. Provider als Betreiber eines Intermediärs oder Organisation als Besitzerin eines Signaturzertifikates). Dienste referenzieren diese Dienstelemente, dabei kann ein Dienst mehrere Dienstelemente referenzieren und ein Dienstelement von mehreren Diensten referenziert werden. Es gibt Dienstelemente in sechs vorgegebenen Ausprägungen: 1. Verschlüsselungszertifikat 2. Signaturzertifikat 3. OSCI-Intermediär 4. OSCI-Empfänger 5. Text 6. Webserver Neben diesen vorgegebenen Ausprägungen können Dienstelemente auch frei vom Nutzer definiert werden. Hier kann der Nutzer einen eigenen Namen vergeben und beliebige Datenfelder vorgeben.
CustomServiceElementType, CustomServiceElementType-Attribute	Eindeutige Beschreibung von benutzerdefinierten Dienstelement-Typen und ihren Attributen. Aus diesen Informationen wird u.a. der Aufbau der Dateneingabe-Maske abgeleitet.
CustomResource	Fachklasse für benutzerdefinierte Ressourcen Benutzerdefinierte Ressourcen sind Ressourcen, deren Ressourcentypen erst zur Laufzeit des Systems neu erstellt werden und deren Metadatenstruktur bei der Erstellung von DVDV noch nicht feststeht und mit benutzerdefinierten Attributen abgebildet und konfiguriert wird.
FederalState	Bundesländer, initiale Liste wurde vom Statistischen Bundesamt (Destatis) übernommen; die Pflege dieser Daten wird bei Bedarf durch ChangeRequests angefordert und per Datenbankskript umgesetzt
GovernmentDistrict	Regierungsbezirke, initiale Liste wurde vom Statistischen Bundesamt (Destatis) übernommen; die Pflege dieser Daten wird bei Bedarf durch ChangeRequests angefordert und per Datenbankskript umgesetzt
District	Kreise und kreisfreie Städte, initiale Liste wird wurde vom Statistischen Bundesamt (Destatis) übernommen; die Pflege dieser Daten wird bei Bedarf durch ChangeRequests angefordert und per Datenbankskript umgesetzt
ServiceDescription und ServiceElementDescription	Eindeutige Beschreibung eines Dienst-Typs mit den zugehörigen Dienstelementbeschreibungen. Letztere legen die Dienstelemente fest, die für den Dienst angelegt werden können oder müssen.
Certificate und CertificateType	Zertifikat mit expliziter Darstellung der Zertifikatattribute für die Zertifikatsuche

Datenobjekt	Beschreibung
OrganizationCategoryEbene1 OrganizationCategoryEbene2 OrganizationCategoryEbene3 OrganizationCategoryEbene4 OrganizationSubCategory	4-stufige Kategorisierung der Organisation. Die Kategorisierung ist Wald-artig strukturiert • Es kann mehrere Wurzelknoten der Ebene 1 geben, jeder spannt einen Baum auf. • Eine Kategorie der Ebene2 ist immer ein Kindelement einer Kategorie der Ebene1. • Eine Kategorie der Ebene3 ist immer ein Kindelement einer Kategorie der Ebene2 • Eine Kategorie der Ebene4 ist immer ein Kindelement einer Kategorie der Ebene3 Für eine Organisation ist die Kategorisierung eindeutig. Jeder Organisation ist eine Kategorie der Ebene 1 zugeordnet (z.B. Behörde) und ein Kategorien-Tupel für Ebene 2, 3 und 4 (z.B. Justiz/Registergericht). Ebene 1und 2 sind verpflichtend, Ebene 3 und 4 sind optional. Ebene 4 wird derzeit nicht genutzt und ist in der Benutzeroberfläche nicht abgebildet.
ResourceGroup	Gruppe von Ressourcen für Autorisierungsentscheidungen Ressourcen werden beim Anlegen einer ResourceGroup zugeordnet. Neue Resourcegroups können erstellt werden, indem die entsprechenden Ressourcen mittels einer filterbaren Liste ausgewählt werden.

Tabelle 48: Liste der Fachklassen im Fachdatenmodell des Kernsystems

Gesamtübersicht Fachdatenmodell Kernsystem

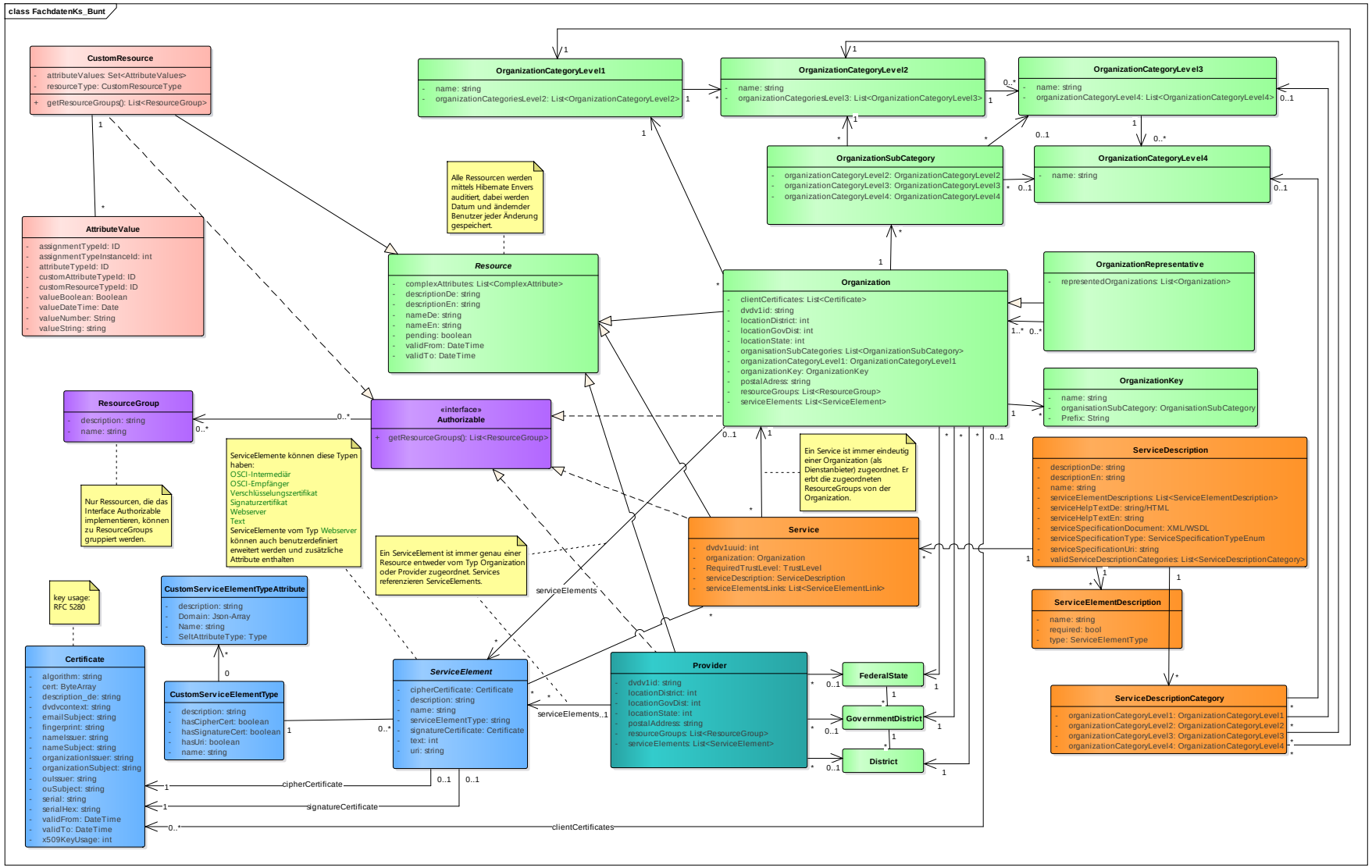


Abbildung 7: Gesamtübersicht Fachdatenmodell Kernsystem

Allgemeine Ressourcen

Die Ressource ist die Basis für alle Fachdaten, wie Dienste, Organisationen, Behörden, Behördenstellvertreter und Provider sowie benutzerdefinierte Ressourcen.

Durch diese Konstruktion haben alle Fachdaten ein identisches Set an Basisattributen. Diese sind:

- Name und Beschreibung der Ressource in deutscher und englischer Sprache
- Gültigkeitszeitraum
- Vorläufig eingetragen?
- Änderungshistorie umgesetzt durch Hibernate Envers

Organisationen (=Behörden) und Stellvertreter

Organisationen sind spezielle Ressourcen, sie haben zusätzlich zu den Eigenschaften einer allgemeinen Ressource einige weitere Attribute:

- Vierstufige Kategorisierung
- Organisationsschlüssel
- Ortsangaben (Bundesland, Regierungsbezirk, Kreis)
- Postadresse
- Dvdv1Id
- Organisationen können Eigentümer von Dienstelementen sein.

Stellvertreter von Organisationen (z.B. Behördenstellvertreter) sind spezielle Organisationen, die zusätzlich zu den Metadaten der Organisation noch eine Liste von Referenzen auf die vertretenen Organisationen halten.

Die Kategorisierung von Organisationen ist über vier Stufen vorgesehen:

- OrganizationCategoryEbene1
- OrganizationCategoryEbene2
- OrganizationCategoryEbene3
- OrganizationCategoryEbene4

Die konkreten Kategorien müssen fachlich festgelegt und abgestimmt werden, sie werden zentral im Admin-Client gepflegt. Die Kategorisierung über diese vier Stufen ist baumartig aufgebaut. Beispielsweise legt die Auswahl einer OrganizationCategoryEbene1=Behörde die Auswahlmöglichkeiten für OrganizationCategoryEbene2 fest auf z.B. Ausländerbehörde, Bundesbehörde, Gesundheitsbehörde, Passbehörde, Gewerbeamt, Justiz. Es ist nicht notwendig für alle Organisationen / Behörden die vierstufige Kategorisierung auszunutzen. Zwingend vorgeschrieben ist eine zweistufige Kategorisierung über OrganizationCategoryEbene1 und OrganizationCategoryEbene2. Die Angabe von weiteren Unterkategorien ist optional. insbesondere wird die Ebene 4 für zukünftige Anwendungsfälle vorgehalten und findet bislang keine Anwendung.

Organisationsschlüssel sind fachliche Schlüsselwerte, die innerhalb der Kategorie eindeutig sind und deren Bildung von der Fachlichkeit in den Eintragungskonzepten vorgegeben ist. Das Tupel aus Kategorie und Organisationsschlüssel ist eindeutig.

Für alle Organisationen sind Ortsangaben im DVDV zu erfassen, es handelt sich hierbei um eine Pflichtangabe.

Das Datum Dvdv1Id wurde eingefügt, um nicht mehr relevante Informationen aus DVDV1 übernehmen zu können und den Pflegenden Stellen als Suchkriterium bereitzustellen. Es kann für beliebige Kriterien verwendet werden, nach denen eine Pflegende Stelle filtern möchte.

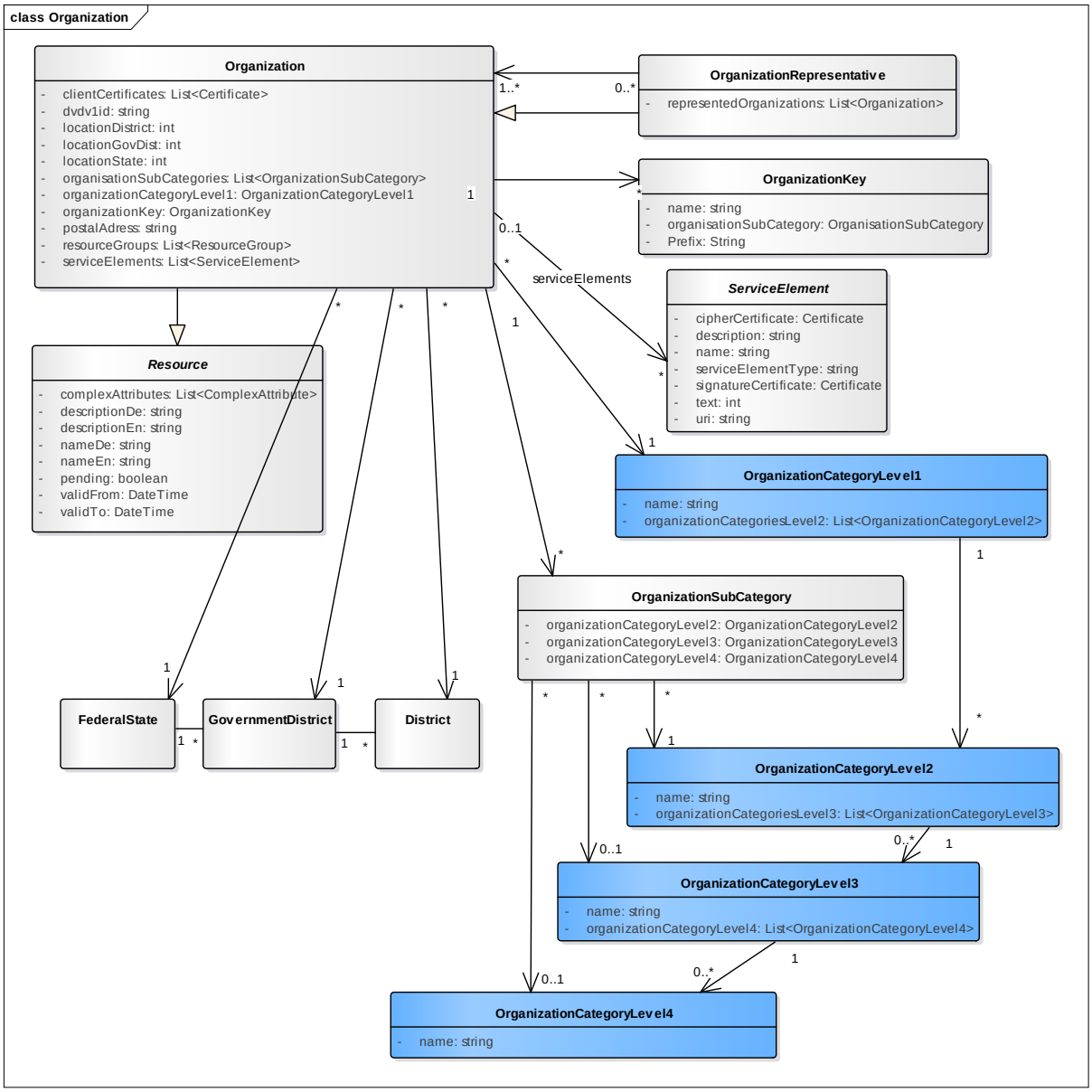


Abbildung 8: Organisationen, Behörden und Behördenstellvertreter

Dienste und Dienstbeschreibungen

Dienstbeschreibungen werden durch ein Spezifikationsdokument spezifiziert und beschrieben. Dieses Spezifikationsdokument wird als XML-Datei bereitgestellt (für XÖV-Dienste als WSDL) und beschreibt den Dienst-Typ vollständig. Für das Anlegen einer neuen Dienstbeschreibung für einen Dienst-Typ reicht die Angabe von Name, Beschreibung, Organisationskategorie und Spezifikationsdokument aus.

Aus dem Spezifikationsdokument generiert das Kernsystem dann die Liste der notwendigen Dienstelemente und hinterlegt sie in den ServiceElementDescriptions sowie den Hilfetext im ServiceHelpText.

Spezifikationsdokumente können unterschiedliche Typen haben, der Typ wird im Attribut serviceSpecification Type angegeben. Für XÖV-Dienste ist der serviceSpecificationType WSDL-OSCI, andere Dienste werden derzeit manuell hinterlegt und nicht durch ein Spezifikationsdokument in einem definierten Format.

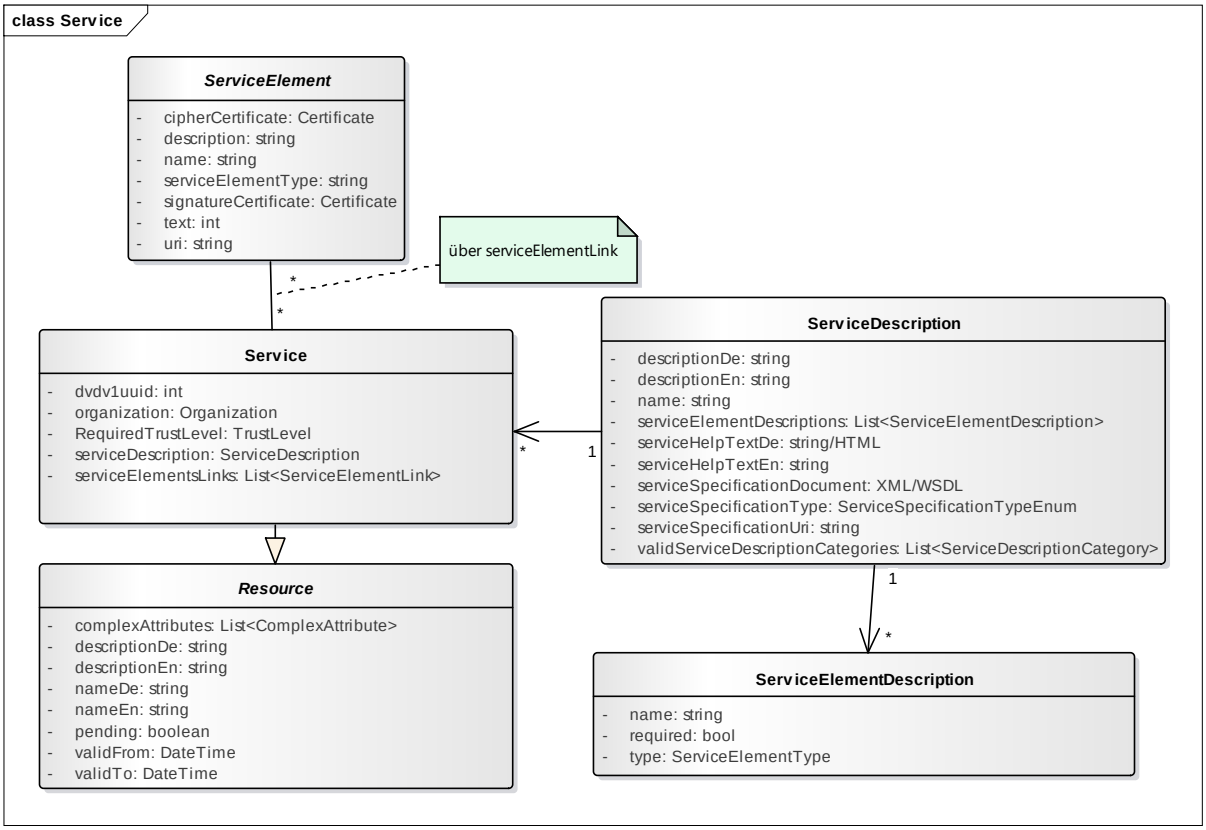


Abbildung 9: Dienste und Dienstbeschreibungen

Dienstelemente

Ein Dienstelement ist immer genau einem Element (einer Ressource) vom Typ Organization oder Provider eindeutig zugeordnet. Diese eindeutig zugeordneten Dienstelemente können dann von beliebig vielen Diensten referenziert werden. Es gibt Dienstelemente in sechs vorgegebenen Ausprägungen:

1. Verschlüsselungszertifikat
2. Signaturzertifikat
3. OSCI-Intermediär
4. OSCI-Empfänger
5. Text
6. Webserver

Neben diesen vorgegebenen Ausprägungen können die Nutzer auch Dienstelemente frei definieren. Hier können die Nutzer einen eigenen Namen vergeben und beliebige Datenfelder vorgeben. Die Konfiguration von benutzerdefinierten Dienstelement-Typen und ihren Attributen wird in den Klassen CustomServiceElementType und CustomServiceElementTypeAttribute abgebildet.

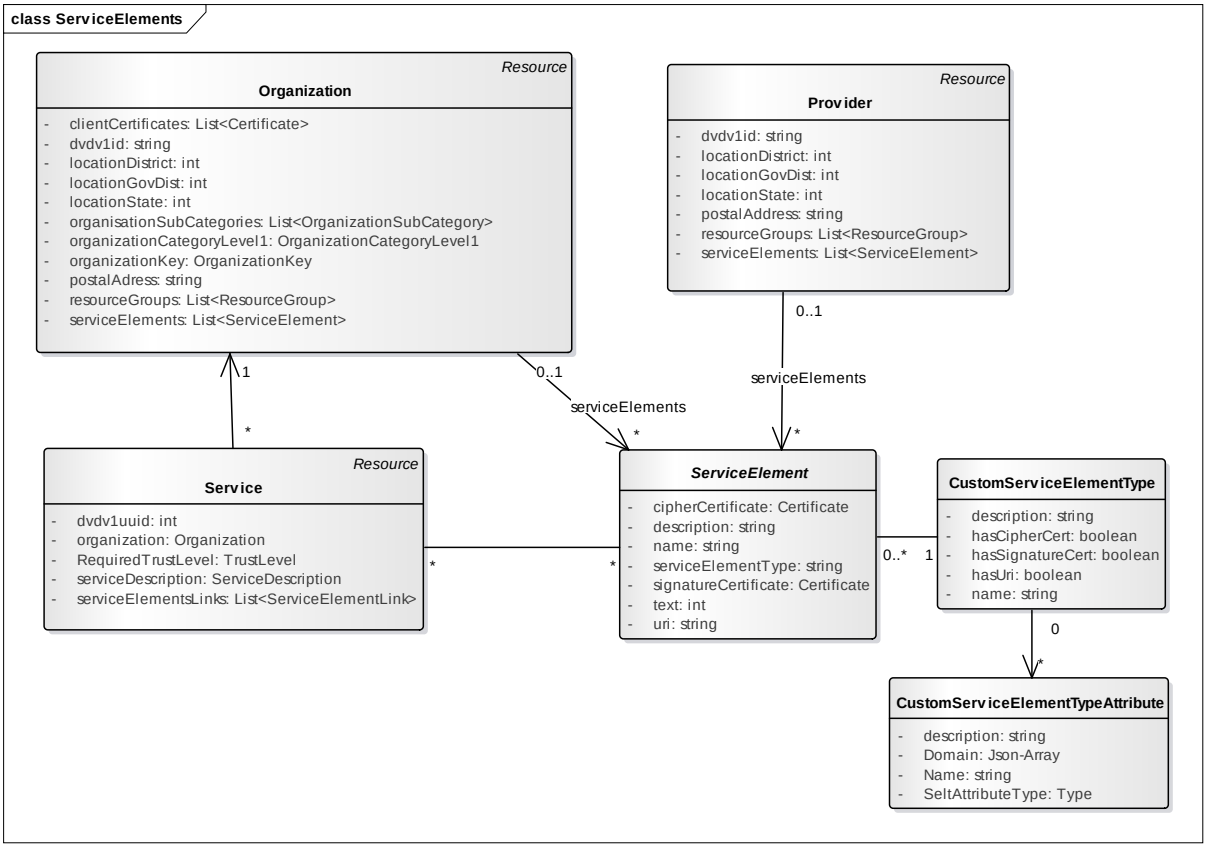


Abbildung 10: Dienstelemente

Provider

Provider sind IT-Dienstleister für die öffentliche Verwaltung, die Infrastruktur und Zertifikate im DVDV-Kontext betreiben und bereitstellen. Sie werden als spezielle Ressourcen der ResourceCategory „Provider“ gespeichert.

Diese speziellen Ressourcen haben eigene Metadaten, die im Objekt „Provider“ enthalten sind. Spezielle Metadaten sind die Ortsangaben (Bundesland, Regierungsbezirk, Kreis). Provider können Eigentümer von Dienstelementen sein.

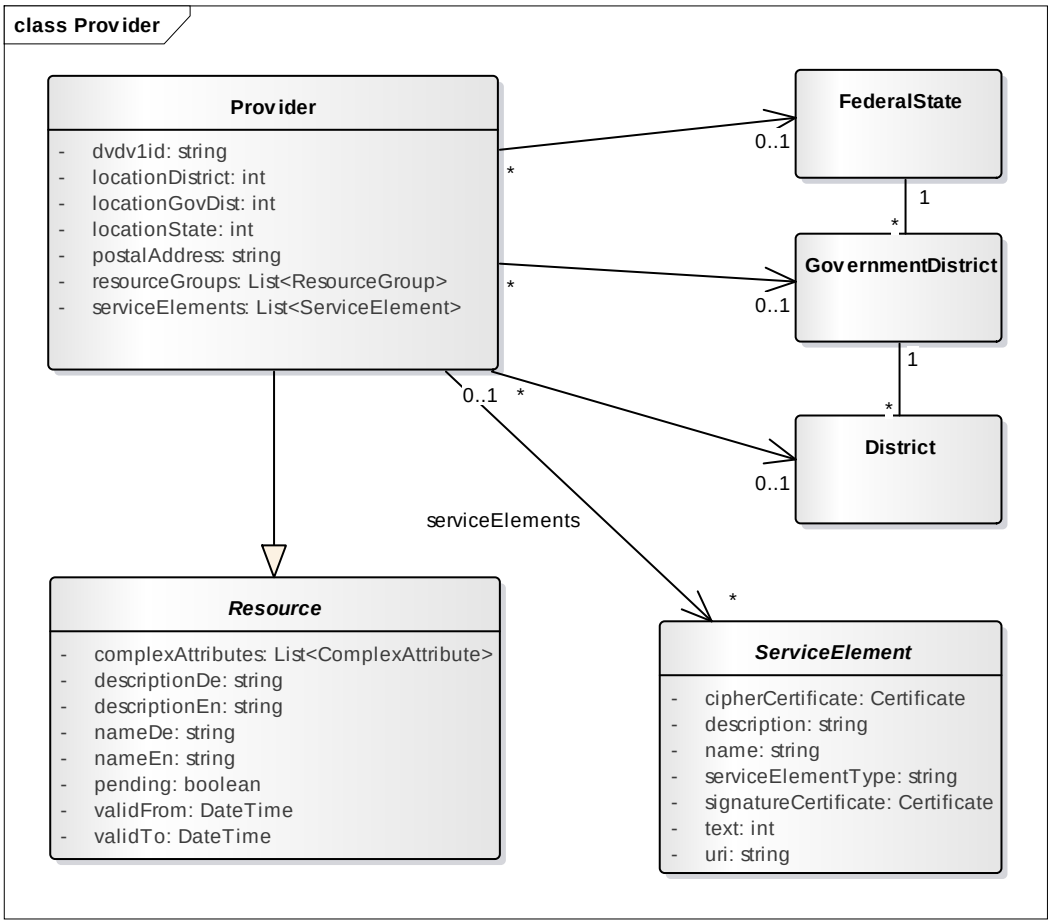


Abbildung 11: Provider

Zertifikate

Zertifikate werden in einer eigenen Datenbanktabelle verwaltet. Die Zertifikat-Daten zum Herausgeber, Antragsteller, Seriennummer, Algorithmus, Fingerprint und Gültigkeit werden beim Erzeugen des Zertifikates für eine bessere Suchbarkeit automatisch befüllt und in der Datenbank abgelegt.

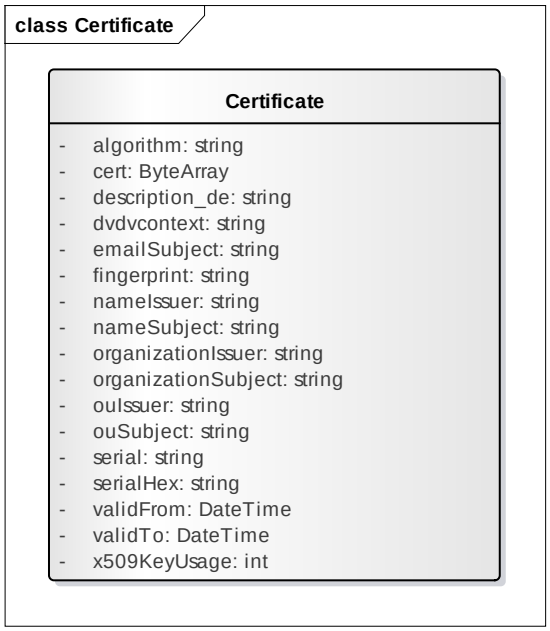


Abbildung 12: Zertifikate

Favoriten und Vorlagen

Benutzer können in DVDV Favoriten, Gruppen von Favoriten und Vorlagen hinterlegen, die ihre tägliche Arbeit erleichtern.

1. Favoriten – Favoriten dienen der schnellen Navigation zu einer bestimmten Ressource, setzen also eine Lesezeichen-Funktionalität um.
2. Favoritengruppen - Favoritengruppen gruppieren mehrere Favoriten und können einerseits für die schnelle Navigation, andererseits aber auch für eine gemeinsame Bearbeitung der gruppierten Favoriten genutzt werden.
3. Vorlagen – Dies sind Vorbefüllungen für bestimmte Masken, z.B. Suchmasken oder Dienstelemente. Die entsprechenden Masken können mit den Default-Werten vorbelegt werden.

Aufgrund der Ähnlichkeit werden Favoriten, Favoritengruppen und Vorlagen in einer gemeinsamen Klasse Bookmarks verwaltet. Die in dieser Klasse verwalteten Daten können je nach Anwendungsfall und Nutzung zum Sprung in einen Use-Case verwendet werden sowie auch für die Vorbefüllung von Masken.

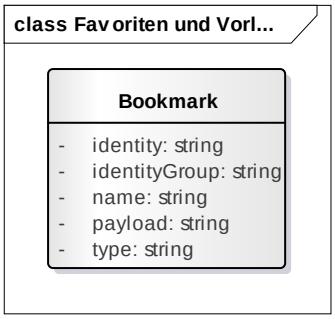


Abbildung 13: Favoriten und Vorlagen

Fachklasse	Beschreibung
Bookmark	Speichert einen Favoriten, eine Favoritengruppe oder eine Vorlage. Die Daten werden in „payload“ in einem passenden Format abgelegt. Bookmarks und Ressourcen werden einer Identity oder IdentityGroup (=Pflegegruppe) zugeordnet. Diese wird im DVDV-IAM angelegt und gehalten. Dem Kernsystem werden bei der Benutzeranmeldung die Identity und alle IdentityGroups mitgeteilt, denen die Identity zugeordnet ist. Um einen Favoriten zu speichern, müssen auch die aktuelle Identity oder eine IdentityGroup gespeichert werden, damit der Favorit entsprechend zugeordnet werden kann.

Tabelle 49: Bookmark - Fachklasse für Favoriten und Vorlagen

Benutzerdefinierte Ressourcen und Attribute

In DVDV können benutzerdefinierte Attribute festgelegt werden, um Ressourcen um eigene Metadaten zu erweitern und auch neue, benutzerdefinierte Ressourcentypen zu gestalten.

In den Klassen mit dem Suffix „Type“ wird die Struktur der benutzerdefinierten Attribute festgelegt (`CustomAttributeType`) und genutzt, um benutzerdefinierte Ressourcentypen auszugestalten (`CustomResourceType`). Für diese benutzerdefinierten Ressourcen können dann neue Metadaten erfasst werden (`AttributeValue`), für jedes Metadatum wird eine Instanz dieser Klasse angelegt.

Hat eine Ressource also z.B. ein benutzerdefiniertes Attribut vom Typ „Person“ mit den Einzelattributen „Name“ und „Geburtsdatum“, dann werden diese Attribute in zwei separaten Instanzen der Klasse `AttributeValue` gehalten.

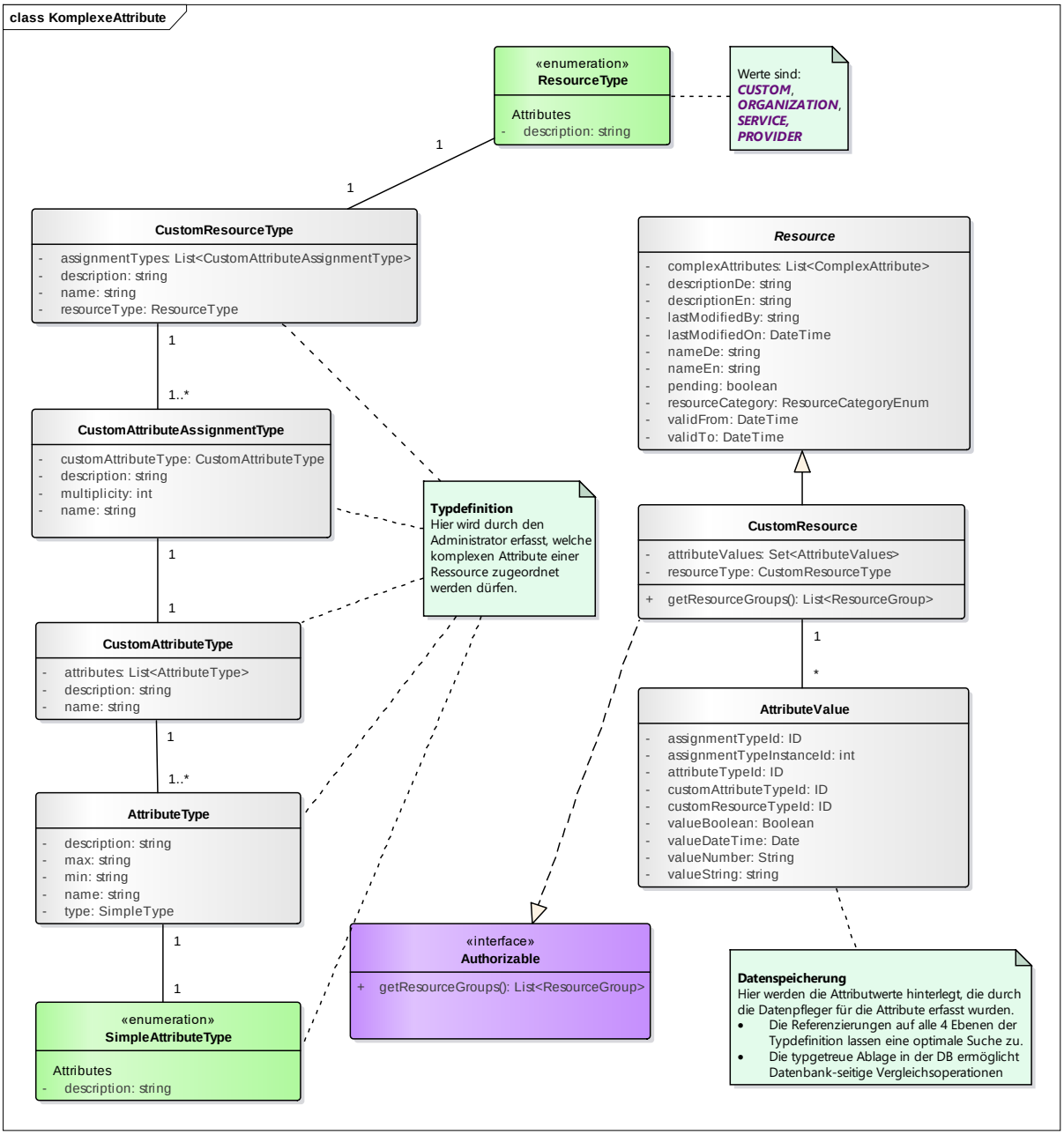


Abbildung 14: Benutzerdefinierte Ressourcen und Attribute

Fachklasse	Beschreibung
CustomResourceType	Typdefinition für eine benutzerdefinierte Ressource. Diese legt fest, welche benutzerdefinierten Attribute für Ressourcen von diesem Typ erstellt werden können (z.B. Ressourcentyp SLA hat die benutzerdefinierten Attribute Verträge und Vertragspartner).
ResourceType	Enum zur Kategorisierung von Ressourcen. Neben den Default-Ressourcenkategorien Organisation, Dienst und Provider können weitere Custom-Ressourcenkategorien administrativ erstellt werden (z.B. neuer Ressourcentyp SLA).
CustomAttributeAssignmentType	Zuordnung eines CustomAttributeType zu einem CustomResourceType (z.B. das benutzerdefinierte Attribut Vertragspartner ist eine Liste von max. 5 benutzerdefinierten Attributen vom Typ Person)
CustomAttributeType	Typdefinition für ein benutzerdefiniertes Attribut. Ein benutzerdefiniertes Attribut kann aus einer Menge einzelner Attribute bestehen (z.B. Person mit Name, Geburtsdatum, Geburtsort).
AttributeType	Typdefinition für ein einzelnes Attribut innerhalb eines benutzerdefiniertes Attributes (z.B. Name, Geburtsdatum, Geburtsort)
SimpleAttributeType	Einfacher Datentyp, zugelassen sind die Standardtypen: int, string, boolean, datetime (z.B. string für Name und Geburtsort, datetime für Geburtsdatum)
Resource	Basisklasse für alle Ressourcentypen, erweiterbar um benutzerdefinierte Attribute
CustomResource	Klasse für konkrete Instanzen von benutzerdefinierten Ressourcen
AttributeValue	Hier werden die konkreten Datenwerte der benutzerdefinierten Attribute einer erfassten Ressource abgelegt (z.B. es wird ein konkreter SLA angelegt und die Vertragspartner werden mit Name und Geburtsdatum erfasst, dann wird ein Datensatz vom Typ Resource erstellt mit einer Menge von Datensätzen vom Typ AttributeValue; diese halten die Attributwerte zu dem neu erfassten SLA).

Tabelle 50: Liste der Fachklassen für Benutzerdefinierte Ressourcen und Attribute

Fachliche Protokollierung

Im DVDV Kernsystem werden alle Änderungen an Ressourcen protokolliert und die komplette Historie der Versionsstände ist jederzeit abrufbar. Die protokollierten Ressourcen und Datenobjekte sind:

- Organisationen und Stellvertreter
- Dienste und Dienstelemente
- Provider
- Zertifikate

Die fachliche Protokollierung wird mit dem Java-Framework Hibernate Envers[14] umgesetzt. Envers führt die Versionierung und das Auditing von Datensätzen direkt innerhalb von Hibernate durch, die Datenänderung und die Fortschreibung der Audit-Tabelle erfolgen immer innerhalb einer Transaktion.

Um Envers einzusetzen, wird für jede Datenbanktabelle, die zu auditierende Fachdaten enthält, eine weitere Audit-Tabelle erstellt. In dieser werden alle Änderungen an den Fachdaten protokolliert. Die Audit-Tabelle wird durch das Suffix „_AUD“ kenntlich gemacht, z.B. gibt es neben der Tabelle „ORGANIZATION“, die Organisationen enthält, die Audit-Tabelle „ORGANIZATION_AUD“. Hier hinein werden alle Änderungen an den Daten geschrieben. Es wird automatisch bei jeder Änderung ein neuer Datensatz geschrieben, der auf seine Vorversion verweist, ein Löschen findet nicht statt.

Für jede Änderung werden zusätzlich zur Vorversion des Datensatzes ein Zeitstempel und der Benutzername des angemeldeten Benutzers gespeichert. Damit lässt sich jederzeit nachvollziehen, welcher Nutzer wann eine Änderung der Daten veranlasst hat.

[14] http://hibernate.org/orm/envers/

8.5.2 Fachdatenmodell des IAM

Das Fachdatenmodell gliedert sich in die Bereiche:

- Benutzer und Anmeldeinformationen
- Benutzergruppen
- Rollen, Rechte und Vertreterregelungen
- Clients

Die Daten liegen in einer gemeinsamen Datenbank, getrennt von den Fachdaten des Kernsystems.

Fachklasse	Beschreibung
User	Ein Benutzer, der sich am IAM-System authentifizieren kann. Enthält neben Benutzerattributen auch • Benutzerinformationen, wie Name, E-Mailadresse, etc. • Beliebige Benutzerattribute, erweiterbar • Zuordnung zu Anmeldeinformationen • Zuordnung zu Benutzergruppen • Zuordnung zu Rollen und Stellvertretungen
Credential	Die Anmeldeinformationen eines Benutzers: • Sichere Speicherung eines Passworts (Hash mit Salt und Hash-Iterationen etc.) • Authentisierungszertifikate • Fehlversuche bei der Anmeldung
IdentityGroup	Eine Gruppe von Benutzern (Identitäten), kurz Benutzergruppe. Benutzergruppen können hierarchisch geordnet werden (über parentGroup). • Beliebige Gruppenattribute, erweiterbar • Zuordnung zu Benutzern
Role	Eine Rolle, die zu Autorisierungsentscheidungen verwendet werden kann: • Zuordnung zu Rechten • Zuordnung zu Ressourcengruppe, auf die sich die Rechte beziehen • Zuordnung zu Benutzergruppe, auf die sich die Rechte beziehen
Substitute (Representation)	Eine Stellvertreterregelung eines Benutzers. Diese enthält: • den Stellvertreter • den stellvertretenen User • die in Stellvertretung übergebene Benutzergruppenmitgliedschaft. Hierüber werden Rollen übergeben. • den Gültigkeitszeitraum der Stellvertretung
Client	Ein dezentrales Fachverfahren / ein Dienstnutzer, der sich am IAM-System authentisieren kann. • Zuordnung zu Rollen • Ein Authentisierungszertifikat / eine Referenz auf ein Authentisierungszertifikat

Tabelle 51: Liste der Fachklassen im Fachdatenmodell des IAM-Systems

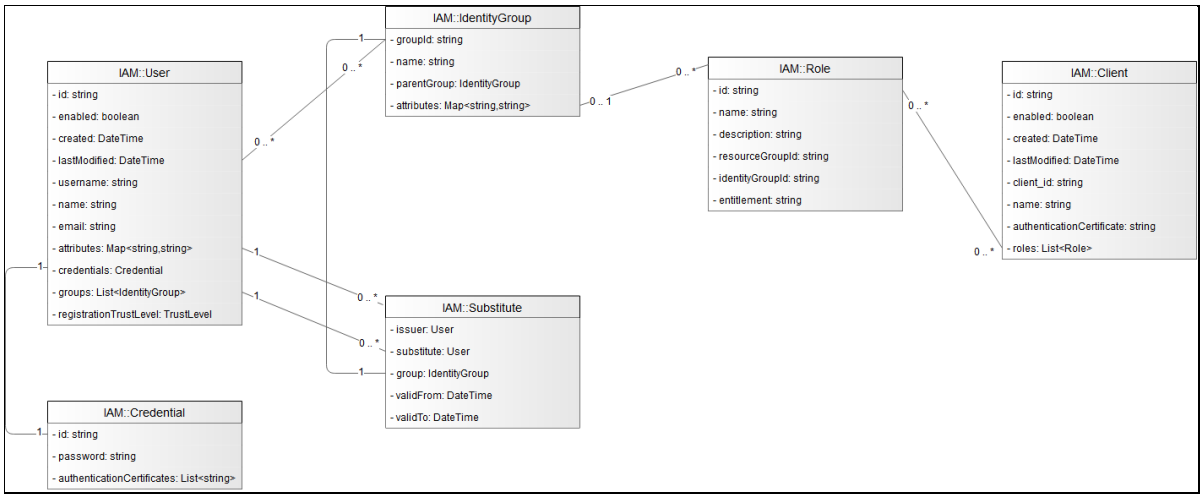


Abbildung 15: Grafische Darstellung der Fachklassen des IAM-Systems

Dieses Datenmodell stimmt weitgehend mit dem existierenden Keycloak-Datenmodell überein. Um den Anpassungsbedarf in Keycloak und den daraus resultierenden Pflegeaufwand bei der Migration auf neuere Keycloak-Versionen zu minimieren, werden projektspezifische Anforderungen so weit möglich mit den bestehenden Datenstrukturen abgebildet. Dies führt dazu, dass

- eine generische Umsetzung einer Domänen-spezifischen Umsetzung vorgezogen wird. Beispielsweise wird das geforderte User-Attribut Description nicht in der Tabelle „USER_ENTITY“ als eigene Tabellenspalte modelliert, sondern über die Tabelle „USER_ATTRIBUTE“.
- Domänen-spezifische Daten in bestehenden Daten kodiert werden, die dadurch eine semantische Bedeutung bekommen. Da bspw. Keycloak-Rollen keine Entitlements und Verweise auf Ressourcengruppe/Identitätsgruppe haben, werden diese im Rollennamen kodiert (so etwa Rolle „Create_RS_Certificates“).

Als einzig notwendige Erweiterung am Keycloak-Datenmodell müssen dann die Vertreterregelungen durch eine neue Tabelle „SUBSTITUTE“ modellieren werden.

Das folgende Diagramm zeigt die Abbildung des obigen Datenmodells auf das Datenbank-Schema von Keycloak. Die notwendige Erweiterung (neue Tabelle) ist gelb hinterlegt.

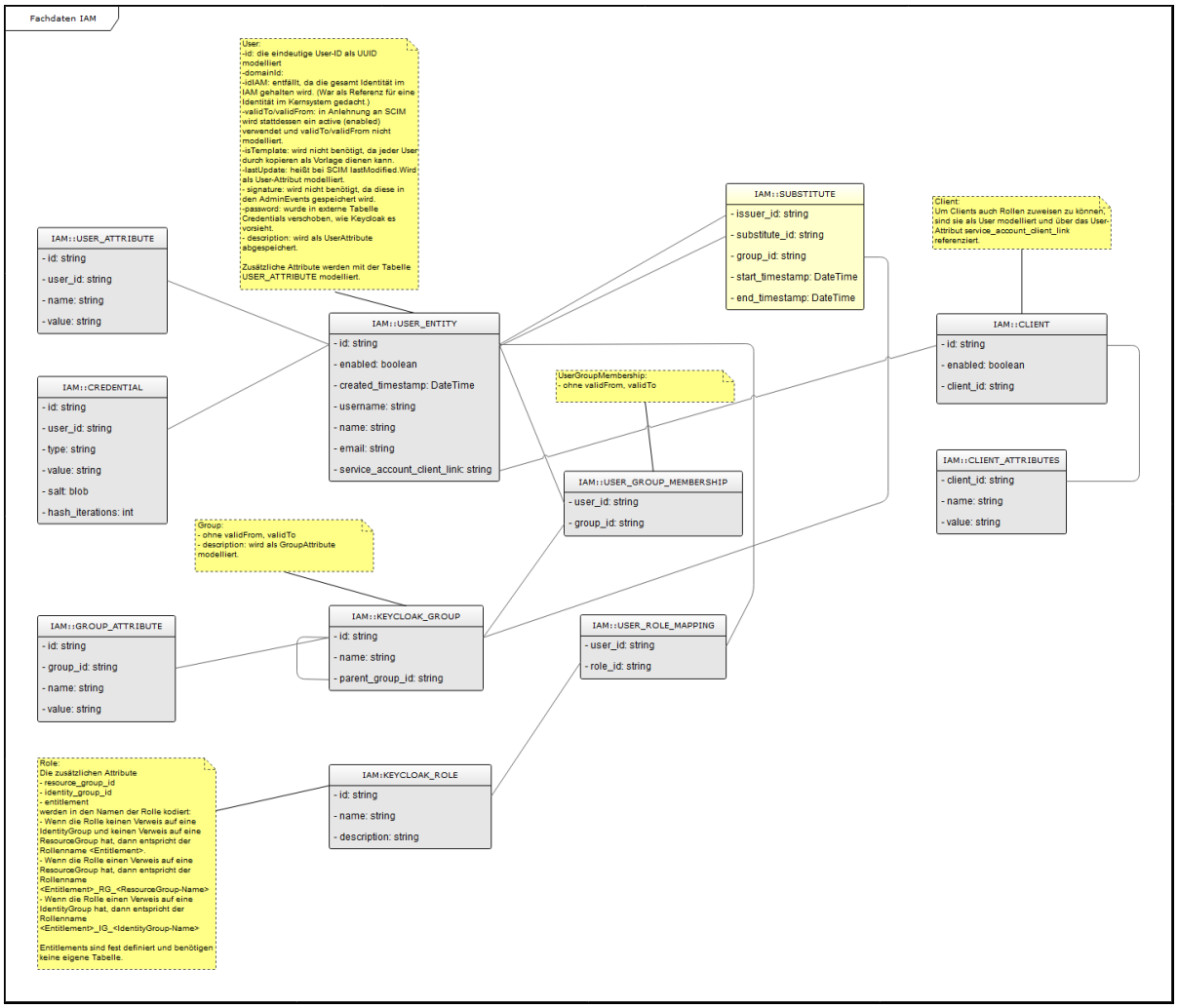


Abbildung 16: Datenmodell des IAM-Systems

8.6 Dienstbeschreibungen als XML / WSDL

Der wesentliche Teil der im DVDV hinterlegten Dienste stammt aus dem XÖV/OSCI-Umfeld. Die Beschreibung dieser Behördendienste mittels WSDL hat sich etabliert. Durch den Upload dieser WSDL-Templates werden die Dienstbeschreibungen im DVDV hinterlegt. Derzeit sind WSDL-Dateien der einzige Weg, Dienstbeschreibungen im DVDV zu hinterlegen.

Es ist zu erwarten, dass mittelfristig andere Dienst-Typen im DVDV hinterlegt werden sollen. Für diese muss ggf. eine abweichende Repräsentation für die Dienstbeschreibungen definiert und umgesetzt werden. Dienstbeschreibungen für neue Dienst-Typen können allerdings erst dann festgelegt werden, wenn die konkreten Anforderungen und Kommunikationsszenarien feststehen. Möglich wird damit z.B. die zukünftige Unterstützung von REST-Services oder AS2/AS4-Diensten.

8.7 Architektur

8.7.1 Architektur des Kernsystems

8.7.1.1 Aufbau des Kernsystems

Das Kernsystem ist auf oberster Ebene untergliedert in die Fachdomänen der Applikation. Innerhalb der Fachdomänen sind die Paketstrukturen weitgehend einheitlich. Exemplarisch wird an dieser Stelle die Fachdomäne de.dataport.dvdv2.core.organization dargestellt.

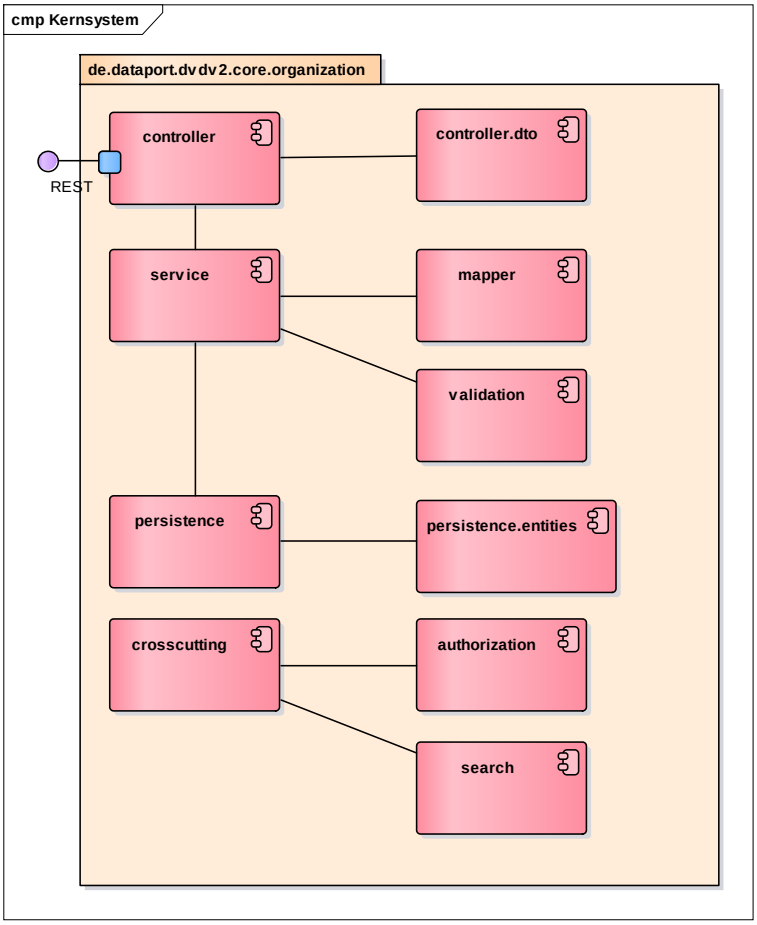


Abbildung 17: Aufbau des Kernsystems

Komponente	Beschreibung
controller	Das Package controller bietet die Rest-Schnittstelle an. Zur Erstellung wird das RESTEasy-Framework verwendet. Der Controller erhält die Datenobjekte im DTO-Format.
controller.dto	Datenobjekte, die im REST-Body an das Kernsystem übergeben werden, werden ins DTO serialisiert.
service	Das Package service beinhaltet die Geschäftslogik und steuert den Ablauf der weiteren Verarbeitung und ruft dabei Methoden der Pakete • mapper • authorization • validation

	• search auf. Nach einem erfolgreichen Durchlauf übergibt es die Daten an die Persistenz.
mapper	Das Package mapper wandelt die DTO-Transferobjekte um in Fachklassen aus dem Package persistence.entities.
validation	Das Package validation führt die Validierung auf den Fachklassen durch. Dazu erhält es die angeforderten Änderungen an den Fachklassen. Anhand dieser Informationen wird ermittelt, ob die übergebenen Daten valide sind. Die Validierung wird durch Bean-Validation an den Fachklassen umgesetzt.
persistence	Die Persistenz nimmt Fachdaten an und persistiert diese in die Datenbank. Dazu wird das Hibernate-Framework verwendet.
persistence.entities	Das Fachdatenmodell der Fachdomäne
authorization	Das Package authorization führt die Autorisierung zentral für alle extern erreichbaren Ressourcen durch. Dazu erhält es die angeforderten Änderungen an den Fachklassen sowie das Authentisierungstoken. Im Authentisierungstoken sind alle Informationen für die Autorisierung enthalten, insbesondere eine Auflistung von Rollen, also ResourceGroups mit den Entitlements auf diesen ResourceGroups. Anhand dieser Informationen wird ermittelt, ob die angemeldete Identität berechtigt ist, die angeforderte Änderung durchzuführen.
search	Das Package search setzt die flexible Suche von Ressourcen nach dem SCIM-Standard[15] zentral für alle Ressourcen um.

Tabelle 52: Liste der Komponenten im Kernsystem

8.7.1.2 Schnittstellen des Kernsystems

Die Schnittstellen des Kernsystems werden nach dem REST-Designprinzipien entwickelt. Damit wird ein Erstellen, Lesen, Ändern, Löschen (CRUD) für alle Ressourcen ermöglicht. Da für Ressourcen auch einfache und komplexe Suchen vorgesehen sind, wird eine Suche von Ressourcen durch Angabe eines Filter-Strings ermöglicht.

An dieser Stelle wird nur eine kurze Übersicht der verfügbaren Schnittstellen gegeben. Die detaillierte Schnittstellendokumentation wird mittels des Swagger[16]-Frameworks direkt aus dem entwickelten Code generiert und in einem separaten Dokument[17] ausgeliefert. Damit ist sichergestellt, dass Dokumentation und Software stets einen identischen Stand aufweisen.

Das Kernsystem bietet drei APIs für unterschiedliche Zwecke und Nutzerkreise an:

1. Directory-API für den Zugriff durch Fachverfahren oder Nachrichtenbroker zum Datenabruf aus dem DVDV. Die hier angebotenen Schnittstellen sind alle performance-optimiert und für Massenzugriffe geeignet. Die Legacy-Facade bietet drei der Schnittstellen, wie bei DVDV 1 üblich, auch über eine OSCI-Kommunikation an.

[15] RFC 7644, System for Cross-domain Identity Management (SCIM): Protocol, September 2015 (https://tools.ietf.org/html/rfc7644)

[16] https://swagger.io/

[17] dvdv2-backend-handbuch-2.x.x.pdf, liegt jeder Auslieferung bei

2. Token-API zum Bezug eines JWT-Token für die Standalone-Authentifizierung einer Organisation am Kernsystem. Auch diese Schnittstelle wird von den Fachverfahren verwendet.
3. Client-API für die Abfrage der Daten durch die Clients Auskunfts-Client, Pflege-Client und Admin-Client. Die hier angebotenen Schnittstellen sind für die interne Nutzung durch die DVDV-Clients vorgesehen und nicht für Massennutzung geeignet.

Schnittstellen der Directory-API

Die Schnittstellen für die Datenabrufe durch Fachverfahren und Clearingstellen sind einer besonders hohen Abfragelast ausgesetzt. Sie sind daher optimiert auf Performance und hohen Durchsatz. Sie werden insbesondere bei den DVDV-Servern genutzt; die Anfragen werden durch die DVDV-Bibliotheken an diese Schnittstellen gestellt. Hier sind über die Legacy-Facade auch die aus DVDV1 bekannten Abfrageschnittstellen umgesetzt.

Schnittstelle der Token API

Um einen Betrieb der DVDV-Server unabhängig vom DVDV-Bundesmaster durchzuführen, kann das DVDV-Kernsystem im Authentifizierungsablauf „Client Credentials Flow“ die Rolle des OAuth2-Authorization Servers einnehmen (vgl. Abschnitt 8.2.2.2). Das Fachverfahren muss sich dabei mit einem Client-Zertifikat einer im DVDV gespeicherten Organisation am Kernsystem authentifizieren. Auf Basis dieses Zertifikates stellt das Kernsystem an dieser Schnittstelle dem Fachverfahren ein Access-Token aus, welches dieses als Mitglied der Organisation ausweist und für Zugriffe auf das Kernsystem berechtigt.

Schnittstellen der Client-API

Die Client-API bietet unter anderem REST-Schnittstellen für die Provisionierung von Ressourcen und anderen Fachdaten des Kernsystems an. Die hier angebotenen Schnittstellen sind für die interne Nutzung durch die DVDV-Clients vorgesehen und nicht für Massennutzung geeignet. Insbesondere werden CRUD-Schnittstellen angeboten für:

- Organisationen (=Behörden / Behördenstellvertreter)
  Über diese Schnittstelle wird auch der XML-Export und -Import umgesetzt, das Nachrichtenformat JSON oder XML für Aufruf oder Rückgabe wird über den MIME-Type angegeben, default ist JSON. Die Organizations-Schnittstelle deckt die Suche nach den Fachklassen Organization und OrganizationRepresentative gleichermaßen ab, so dass eine gemeinsame Suche nach Behörden und Behördenstellvertretern möglich ist.
- Organisationskategorien
- Provider
  Über diese Schnittstelle wird auch der XML-Export und Import umgesetzt, das Nachrichtenformat JSON oder XML für Aufruf oder Rückgabe wird über den MIME-Type angegeben, default ist JSON.
- Dienste
- Dienstbeschreibungen
- Benutzerdefinierte Ressourcen
- Ressourcengruppen
- Zertifikate (nur Datenabruf, da Zertifikate immer im Kontext einer Organisation oder eines Providers stehen und mit diesen gemeinsam angelegt werden)

- Lesezeichen und Vorlagen
- Statistische Funktionen (nur Datenabruf)
- Ortsangaben (nur Datenabruf)
- Ressourcenübergreifende Suche über alle Ressourcen (nur Datenabruf)

Datenabruf über die Client-API

Die Datenabruf-Schnittstellen der Client-API sind mit besonderen Features für die Filterung und Sortierung ausgestattet.

Rückgabe von (Teil-)Listen

Um einer Überlastung von Kernsystem und Schnittstellen vorzubeugen, ist eine Maximallänge von Listen im Kernsystem konfigurierbar. Diese Maximallänge bezieht sich auf alle Ressourcen, die als Liste über die Schnittstelle abgerufen werden können. Wird die Maximallänge überschritten, liefert das Kernsystem eine Fehlermeldung mit dem Hinweis, die Anfrage weiter einzuschränken.

Für eine Einschränkung der Listen werden die Parameter `count` und `startindex` angeboten:

Beispiel: `GET /organizations?startindex=40&count=20`

Dieser Aufruf überträgt eine Liste von 20 Organisationen, beginnend mit der 41. Organisation in der Liste.

Sortierung

Der Aufruf von Teillisten ist nur dann sinnvoll einsetzbar, wenn die Teillisten bei jedem Aufruf die gleiche Sortierung aufweisen, die Sortierung also auf dem Server stattfindet. Dazu werden die Parameter `sortBy` (nach einem Attributnamen) und `sortOrder` (mit den erlaubten Attributwerten `ascending` und `descending`, default ist `ascending`) angeboten:

Beispiel: `GET /organizations?sortBy=nameDe&sortOrder=ascending`

Filterung

Des Weiteren wird eine Filterung zur Einschränkung der Organisationen angeboten:

Beispiel: `GET /organizations?filter=validfrom le "2018-06-15T12:00:00Z" and validto gt "2018-06-15T12:00:00Z"`

liefert alle Organisationen, die am 15.6.2018 um 12:00 Uhr gültig sind.

Die Syntax des Filter-Strings orientiert sich am SCIM-Standard[18] (3.4.2.2. Filtering), der für die Pflege und Suche von Identitäten im IAM-System vorgegeben ist. Die SCIM-Filter-Syntax ist nicht komplett, aber zum großen Teil umgesetzt. Implementiert sind insbesondere:

- UND-Verknüpfung von Filterregeln
- ODER-Verknüpfung von Filterregeln
- Negierung mit dem NOT-Operator
- Verwendung von Klammerung
- Suche nach Teilstrings
- Folgende Operatoren:

`eq`	Equal

[18] RFC 7644, System for Cross-domain Identity Management (SCIM): Protocol, September 2015 (https://tools.ietf.org/html/rfc7644)

ne	not equal
co	Contains
sw	starts with
ew	ends with
pr	present (has value)
gt	greater than
ge	greater than or equal to
lt	less than
le	less than or equal to

Tabelle 53: Liste der Operatoren bei der Filterung

Stapelverarbeitung

Für die Ausführung mehrerer Datenänderungen in einer gemeinsamen Transaktion werden bei den Ressourcentypen Bulk-Schnittstellen zur Stapelverarbeitung vorgesehen. Hier können mehrere Datenänderungen in einem einzigen REST-Aufruf gebündelt und gemeinsam ausgeführt werden.

Alle Aufrufe werden in einer gemeinsamen Transaktion ausgeführt, bei einem Fehler in der Ausführung einer Datenänderung wird keine der Datenänderungen durchgeführt. Sollten mehrere der Datenänderungen fehlgeschlagen sein, wird eine Liste aller aufgetretenen Fehler zurückgemeldet.

8.7.2 Architektur des DVDV-IAM

8.7.2.1 Aufbau und Subkomponenten des DVDV-IAM

Die Architektur des DVDV-IAM folgt der Architektur von Keycloak[19]. Die SCIM-Schnittstelle und der User-Self-Service werden als separate Module implementiert.

[19] Siehe https://www.keycloak.org/docs/latest/server_development/

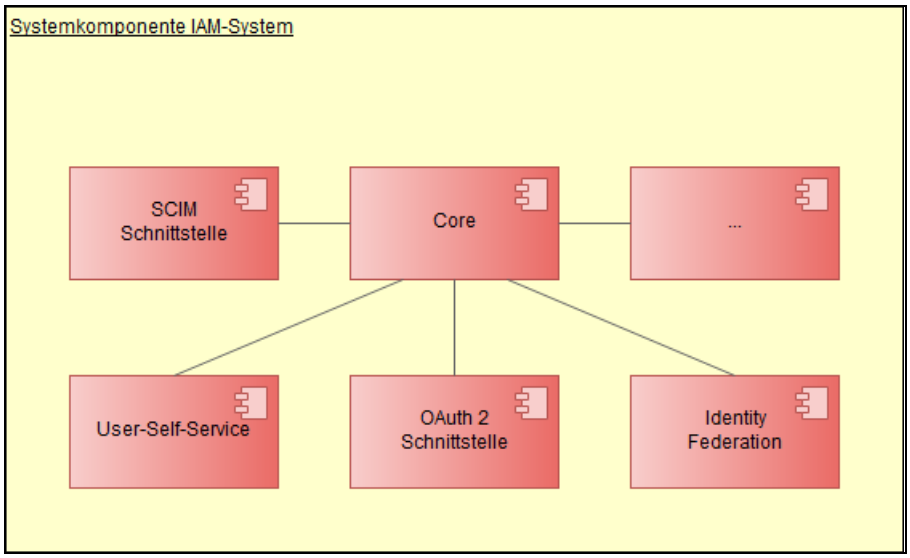


Abbildung 18: Systemkomponenten DVDV-IAM

8.7.2.2 Schnittstellen des DVDV-IAM

Die Schnittstellen des IAM-Systems werden als REST-Schnittstelle nach der SCIM-Spezifikation entwickelt. Damit wird ein Erstellen, Lesen, Ändern, Löschen (CRUD) für alle Objekte des DVDV-IAM ermöglicht. Da für Objekte des IAM-Systems auch einfache und komplexe Suchen vorgesehen sind, wird eine Suche durch Angabe eines Filter-Strings ermöglicht.

Die Umsetzung der Filter-String und das Einschränken der Listengröße erfolgen analog zu den Ausführungen im vorigen Abschnitt. Wie dort, wird an dieser Stelle nur eine kurze Übersicht der verfügbaren Schnittstellen gegeben.

Der Zugriff auf diese Schnittstellen erfolgt authentisiert und autorisiert. Wie bereits beschrieben, ist die Änderungshistorie der User über die Keycloak-Admin-Konsole im Admin-Eventlog einsehbar.

Insbesondere werden CRUD-Schnittstellen angeboten für:

- Benutzer
- Identitätsgruppen
- Rollen
- Stellvertreter
- Keycloak-Clients
- Me (die Benutzerdaten des authentisierten Benutzers)

Stapelverarbeitung

Diese Schnittstelle ist gemäß der Bulk-Schnittstelle im SCIM-Standard[20] (Abschnitt 3.7) für das gleichzeitige Bearbeiten von Objekten modelliert. Die Option failOnErrors ist in der Schnittstelle fest mit dem Wert 0 implementiert, d.h. entweder es tritt kein Fehler auf und alle Operationen werden umgesetzt oder es tritt ein Fehler auf und gar keine Operation wird ausgeführt. Die Bulk-Schnittstelle wird für alle IAM-Objekte (User, Group, Role, Substitute und Client) umgesetzt, um das gleichzeitige Anlegen, Ändern und Löschen und Lesen zu ermöglichen.

[20] RFC 7644, System for Cross-domain Identity Management (SCIM): Protocol, September 2015 (https://tools.ietf.org/html/rfc7644)

8.7.3 Schnittstelle zwischen IAM und Kernsystem beim DVDV-Bundesmaster

Die Systeme IAM-System und das Kernsystem des DVDV-Bundesmasters sind weitgehend unabhängig voneinander. Für einige wenige Anforderungen muss das Kernsystem auf Daten des IAM zugreifen.

8.7.3.1 Rollen für ResourceGroups

Wie in Abschnitt 8.3 ausgeführt, werden Autorisierungsentscheidungen auf Basis von Rollen und damit einer Zuordnung von Identitäten zu ResourceGroups getroffen. ResourceGroups werden im Kernsystem angelegt und gepflegt. Rollen werden im IAM-System angelegt und gepflegt. Hier ist eine enge Verzahnung von DVDV-IAM und DVDV-Bundesmaster notwendig.

Diese Verzahnung wird nicht durch direkten Zugriff zwischen den beiden Systemen realisiert, sondern mittels AdminClient. Im AdminClient werden ResourceGroups angelegt, geändert und gelöscht. Der AdminClient führt zeitgleich auch das Anlegen, Ändern und Löschen der korrespondierenden Rollen im IAM durch.

8.7.3.2 Authentifizierungszertifikate für Organisationen

Organisationen treten im DVDV in zwei fachlichen Rollen auf:

1. **Dienstanbieter** von Diensten, die im DVDV hinterlegt sind
2. **Dienstnutzer** von Diensten, die im DVDV hinterlegt sind und damit Abfrager von DVDV-Diensteinträgen

Organisationen im DVDV können eine dieser Rollen wahrnehmen oder auch beide.

Für die Rolle „Dienstnutzer“ für Dienste an der Directory-API ist bei Zugriff aus dem Internet im DVDV eine Authentisierung am Kernsystem oder am DVDV-IAM notwendig. Um eine Authentifizierungsentscheidung für einen Dienstnutzer zu treffen, muss im jeweiligen System ein Authentifizierungszertifikat des Dienstnutzers geprüft werden. Eine Schnittstelle der Systeme IAM und Kernsystem für den Abgleich von Authentifizierungszertifikaten existiert nicht.

Authentifizierung am Kernsystem

Tritt eine Organisation im DVDV in beiden Rollen „Dienstnutzer“ und „Dienstanbieter“ auf, dann ist ihr Authentifizierungszertifikat als Client-Zertifikat in den meisten Fällen bereits als Client-Zertifikat im DVDV hinterlegt. Um eine doppelte Pflege dieser Zertifikate im IAM und Kernsystem oder alternativ eine weitere Schnittstelle zwischen diesen Systemen zu vermeiden, ist auch am Kernsystem ein Token-Endpunkt umgesetzt. Eine solche Organisation, die in der Rolle Dienstnutzer eine Information vom DVDV abfragen möchte, kann ihr Authentifizierungstoken von diesem Endpunkt beziehen und damit unabhängig vom DVDV-IAM auf die Daten zugreifen.

Authentisierung am IAM

Im DVDV-IAM werden Identitäten von Dienstnutzern abweichend von „normalen“ Identitäten behandelt und als Clients modelliert (da der Dienstnutzer bei OAuth 2 die Rolle des Clients einnimmt). Dienstnutzer sind an eine Benutzergruppe gebunden und lassen sich daher von einer Pflegenden Stelle unabhängig von einer Organisation, einem Provider oder einem Dienst anlegen. Im IAM hinterlegte Dienstnutzer werden im Admin-Client angelegt und verwaltet.

Will nun ein Dienstnutzer Dienstinformationen am DVDV abrufen, authentisiert er sich mit seinem Authentifizierungszertifikat am DVDV-IAM. Das IAM kann das Zertifikat prüfen, da es in der Client-Konfiguration hinterlegt ist. Mit diesem Zertifikat kann es die Authentifizierungsentscheidung treffen und authentifiziert den Dienstnutzer.

8.7.3.3 Identitätengruppen für Favoritenpflege

Eine Identitätengruppe oder IdentityGroup gruppiert eine Menge von Identitäten. Das Kernsystem benötigt die IdentityGroups zur Pflege von gemeinsamen Favoriten für alle Mitglieder einer IdentityGroup.

Das Kernsystem bekommt mit dem Authentifizierungstoken die Identität des angemeldeten Nutzers mitgeteilt. Damit für das Kernsystem eine Zuordnung dieser Identität zu IdentityGroups bekannt ist, werden in diesem Token auch alle IdentityGroups mitgeteilt, denen diese Identität angehört. Ein Benutzer ist damit in der Lage, Favoriteneinträge sowohl für die eigene Identität, als auch für beliebige IdentityGroups, denen er zugeordnet ist, zu erstellen.

Eine Transaktionalität ist für diese Schnittstelle daher nicht vorgesehen. Sollten im Kernsystem des DVDV-Bundesmasters Bookmarks für eine mittlerweile im DVDV-IAM gelöschte IdentityGroup existieren, so reicht die periodische Löschung mit einem zeitgesteuerten Löschservice aus. Dieser Job muss am DVDV-IAM eine Schnittstelle aufrufen, die ihm alle aktuell gepflegten IdentityGroups übermittelt.

8.8 Versionierung der Komponenten und Releasezyklus

8.8.1 DVDV-Bundesmaster und DVDV-Server

8.8.1.1 Releasezyklus von DVDV-Bundesmaster und DVDV-Server

Die Auslieferung der DVDV-Serversoftware findet derzeit regelmäßig viermal im Jahr statt: Sie ist terminlich an die Auslieferung der Oracle Critical Patch Updates (CPUs) der MySQL-Datenbank gekoppelt, damit die Betreiber der Software beide Updates in einem gemeinsamen Software-Change bearbeiten können. Falls erforderlich, können Hotfixes auch zwischen diesen Terminen eingespielt werden.

Für den DVDV-Bundesmaster und den DVDV-Server werden standardmäßig zip-Pakete ausgeliefert.

Die Pakete für den **DVDV-Bundesmaster** enthalten die folgenden Artefakte:

- Softwarepakete zur Installation im jeweiligen Application-Server im Format rpm, jeweils für die Komponenten:
    - Kernsystem
    - DVDV-IAM
    - Pflege-Client
    - Admin-Client
    - Auskunfts-Client
    - Legacy-Facade

  Die rpm-Pakete enthalten jeweils war-Archive zur Installation im Application–Server und die dazugehörigen Installationsskripte.
- Änderungshistorie
- Benutzerhandbuch DVDV-Bundesmaster
- Update-Anleitung für eine Installation als Update von der Vorversion
- Verwundbarkeitsanalyse

- Handbücher für Admin-Client, Pflege-Client, Auskunfts-Client mit und ohne erweiterte Suche
- Schnittstellendokumentation der Directory-Schnittstelle
- Komponente Betreibertest für einen schnellen Test der Directory-Schnittstelle

Die Pakete für den **DVDV-Server** enthalten die folgenden Artefakte:

- Softwarepakete zur Installation im jeweiligen Application-Server im Format rpm, jeweils für die Komponenten:
    - Kernsystem
    - Auskunfts-Client
    - Legacy-Facade

  Die rpm-Pakete enthalten jeweils war-Archive zur Installation im Application–Server und die dazugehörigen Installationsskripte.
- Änderungshistorie
- Benutzerhandbuch DVDV-Server
- Update-Anleitung für eine Installation als Update von der Vorversion
- Handbücher für Auskunfts-Client mit und ohne erweiterte Suche
- Schnittstellendokumentation der Directory-Schnittstelle
- Komponente Betreibertest für einen schnellen Test der Directory-Schnittstelle

8.8.1.2 Versionierung von DVDV-Bundesmaster und DVDV-Server

Die in einer Auslieferung gemeinsam ausgelieferten Komponenten erhalten dabei grundsätzlich eine einheitliche, gemeinsame Versionsnummer mit folgendem Aufbau:

- Hauptversionsnummer (major)
- Nebenversionsnummer (minor)
- Revisionsnummer (patch)

Beispiel: Kernsystem Version 2.10.0

Die gemeinsame Auslieferung aller Softwarekomponenten impliziert, dass alle Komponenten, die untereinander kommunizieren, die gleiche Major- und Minor-Versionsnummer haben müssen, also aus einer gemeinsamen Auslieferung stammen.

Die Major-Versionsnummer wird ausschließlich bei grundlegenden Änderungen an der DVDV-Software hochgezählt, die z.B. die Architektur der Software ändern und damit z.B. bei den Betreibern wesentliche Änderungen im Betrieb verursachen.

Die Minor-Versionsnummer wird für die quartalsweisen Auslieferungen in der Regel um eins erhöht. Üblicherweise beinhalten diese Updates neu implementierte fachliche Features und Änderungen der internen API, die zur Kommunikation zwischen den Komponenten genutzt werden. Es kann nicht davon ausgegangen werden, dass z.B. Kernsystem und Pflege-Client mit unterschiedlichen Minor-Versionsnummern gemeinsam lauffähig sind.

Die Patch-Versionsnummer erhöht sich jeweils durch Änderungen, die zwischen den geplanten Auslieferungen als HotFix stattfinden und üblicherweise keine neuen Fachlichkeiten oder Features beinhalten, z.B. Optimierungen, Bug Fixes etc. Üblicherweise betreffen solche Fixes

nur einzelne Komponenten der Software, diese werden dann ohne die anderen Softwareteile ausgeliefert. Es kann davon ausgegangen werden, dass z.B. Kernsystem und Pflege-Client mit identischen Minor-Versionsnummern und unterschiedlichen Patch-Versionsnummern gemeinsam lauffähig sind.

Für alle Backend-Komponenten kann die Versionsinformation über die Ressource „/version“ (via REST-Schnittstelle) abgerufen werden (siehe dazu auch Kapitel 9). Als Response wird ein JSON geliefert.

Beispiel-JSON: `{"version":"2.1.12"}`

Frontend-Komponenten zeigen die Versionsnummer jeweils in der Fußzeile der Webseite.

Zusätzlich werden diese Informationen im MANIFEST.MF innerhalb des gepackten Pakets (EAR/WAR) abgelegt, so dass diese ohne Aufrufe des Codes kontrolliert werden können.

Die Informationen werden automatisch vom Buildprozess eingefügt. Somit hat der Betrieb verschiedene Möglichkeiten, die korrekten Versionen zu kontrollieren, was die Betreibbarkeit der Anwendung erhöht.

8.8.2 DVDV-Bibliotheken und Beispiele

8.8.2.1 Releasezyklus der DVDV-Bibliotheken

Die zum DVDV bereitgestellten Bibliotheken und Beispiele haben einen von den DVDV-Auslieferungen unabhängigen, unregelmäßigen Releasezyklus. Neue Releases werden im FITKO-Entwicklungsportal veröffentlicht und über eine Mailingliste angekündigt.

8.8.2.2 Versionierung der DVDV-Bibliotheken

Aufgrund des unabhängigen Releasezyklus werden die Bibliotheken daher unabhängig von den Serversystemen versioniert, der Aufbau der Versionsnummer mit major.minor.patch ist dabei identisch zur Serversoftware.

Üblicherweise wird versucht, die Bibliotheken abwärtskompatibel umzusetzen, so dass auch ältere Bibliotheken nach einem Update der Serversoftware weiterhin funktionieren. Sollte dies einmal nicht möglich sein, dann wird dieses durch eine Änderung der Major-Versionsnummer angezeigt.

Die Major-Versionsnummer wird ausschließlich bei grundlegenden Änderungen an den Bibliotheken hochgezählt, insbesondere bei solchen Fällen, in denen die Abwärtskompatibilität nicht gewährleistet ist und eine Bibliothek mit einem Server-Update gewechselt werden muss.

Die Minor-Versionsnummer wird für Auslieferungen in der Regel um 1 erhöht. Üblicherweise beinhalten diese Updates neu implementierte fachliche Features oder die Unterstützung von neuen Schnittstellen am Kernsystem zum Datenabruf.

Die Patch-Versionsnummer erhöht sich jeweils durch Änderungen, die zwischen den geplanten Auslieferungen als HotFix stattfinden und üblicherweise keine neuen Fachlichkeiten oder Features beinhalten, z.B. Optimierungen, Bug Fixes etc. Eine Änderung in der Patch-Nummer hat keine Änderungen der Kompatibilität der Bibliothek zum DVDV-Server zur Folge.

Die Versionsnummern von .NET und Java-Bibliothek werden üblicherweise gleich gehalten, Bibliotheken mit identischen Versionsnummern unterstützen dabei identische Features. Üblicherweise zählt eine neue Auslieferung der Bibliotheken die Minor-Versionsnummer um eins hoch. Mit den Auslieferungen wird in einer Kompatibilitätsmatrix veröffentlicht, mit welchen DVDV-Servern eine DVDV-Bibliothek jeweils kompatibel ist.

8.9 Fremdbibliotheken und Lizenzen

Eine Übersicht der im Projekt verwendeten Fremdbibliotheken und deren Lizenzen wird über das Build-Management-Tool Apache Maven generiert. Dazu wird das Apache Maven Project Info Reports Plugin mit dem Goal „dependencies“ genutzt: project-info-reports:dependencies[21]

Der generierte Report löst alle direkten und transitiven Abhängigkeiten auf und listet die verwendeten Bibliotheken mit den zugehörigen Lizenzmodellen. Der Report wird als der Systemdokumentation beigelegt.

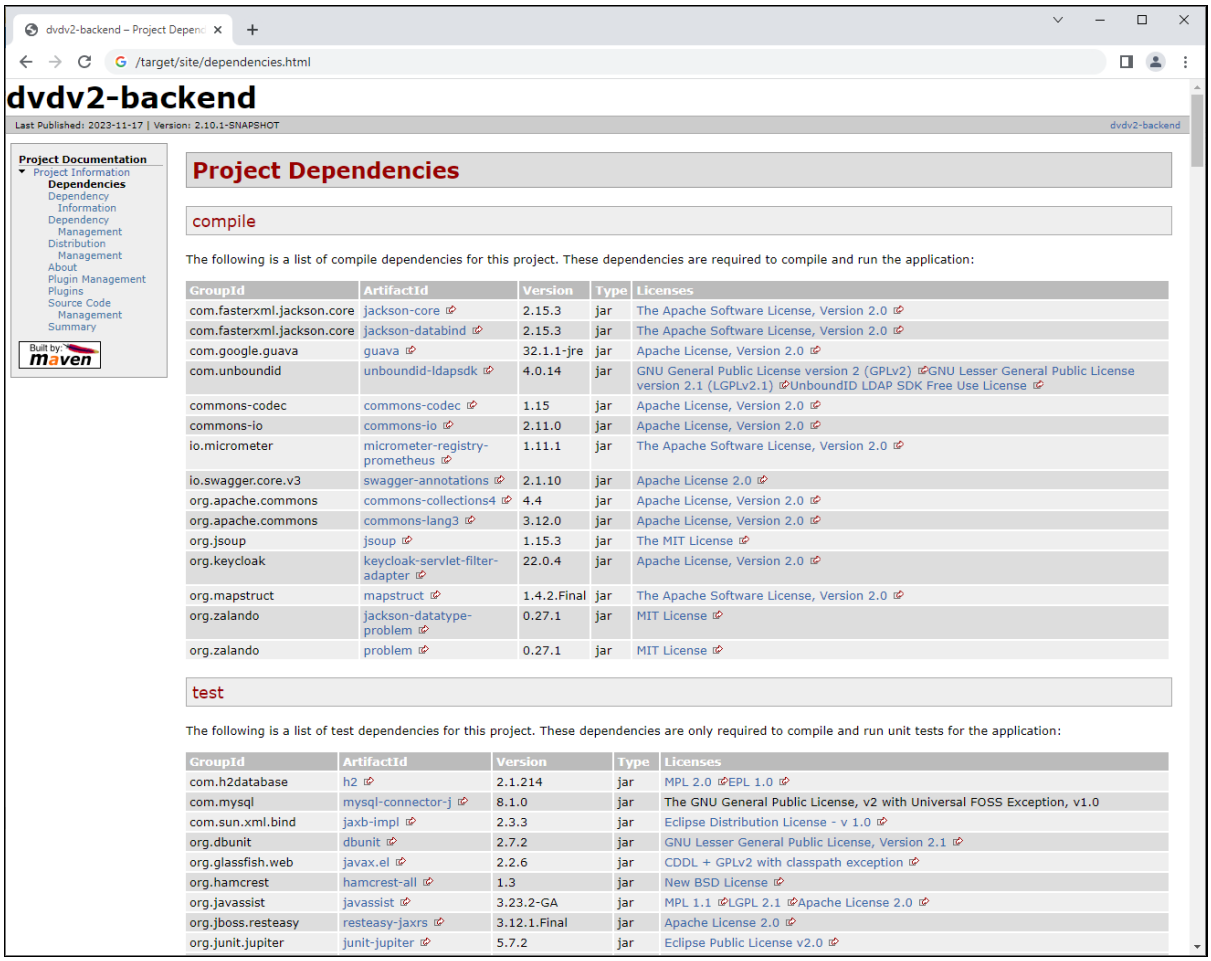


Abbildung 19: Ausgabebericht der Abhängigkeiten

8.10 Quellcodeverwaltung und Build Management

Zur Unterstützung der gemeinsamen Entwicklung und zur Codeintegration wird der Programmcode auf GitHub nicht-öffentlich im Bereich der Fa. Governikus gepflegt und zusammengeführt.

Mit entsprechenden Zugriffsrechten kann der Code unter diesen URLs abgerufen werden:

- https://github.com/Governikus/DVDV2_Admin-Client
- https://github.com/Governikus/DVDV2_Bundesmaster
- https://github.com/Governikus/DVDV2_Pflege-Client

[21] https://maven.apache.org/plugins/maven-project-info-reports-plugin/dependencies-mojo.html

- https://github.com/Governikus/keycloak-scim-management-parent
- https://github.com/Governikus/DVDV2_Kernsystem
- https://github.com/Governikus/DVDV2_Legacyfacade
- https://github.com/Governikus/DVDV2_DotNet_SDK
- https://github.com/Governikus/DVDV2_Java_SDK
- https://github.com/Governikus/dvdv-java-controlfile
- https://github.com/Governikus/dvdv-java-simple
- https://github.com/Governikus/dvdv-dotnet-controlfile

Zur Steigerung der Softwarequalität wird die Software auf einer CI-Strecke kontinuierlich gebaut und geprüft. Dazu wird die Software GitLab bei Dataport eingesetzt. Diese führt bei jeder Änderung im Repository alle Unit-Tests aus, zudem wird der Quellcode hinsichtlich verschiedener Qualitätsbereiche analysiert.

Das Deployment der Software wird auf den Testservern bei Governikus und Dataport ohne Automatisierung durchgeführt.

Automatisierte Integrationstests sind mit der Software Selenium umgesetzt und testen alle Bereiche der Software, auch Oberflächen der Clients, Directory-Schnittstellen und die Legacy-Facade. Die Tests sind im Projekt https://github.com/Governikus/DVDV2_selenium0 abgelegt und werden von den Entwicklern mindestens vor den Software-Releases auf den Testsystemen ausgeführt.

8.11 Codequalität

Codequalität ist ein bedeutender Teilaspekt von Softwarequalität und somit ein wichtiger Teil der Qualitätsziele für DVDV. Zum Erreichen des Qualitätsziels werden im Rahmen des Projektes organisatorische und technische Maßnahmen ergriffen.

8.11.1 Kodierrichtlinien

Für die Erstellung des Quellcodes wurden im Vorfeld konkrete Regeln festgelegt. Diese Regeln betreffen verschiedene Aspekte der Programmierung und verbessern im Wesentlichen die Verständlichkeit und Wartbarkeit der Software:

- Strukturierung des Codes (Quelltextformatierung)
- Anwendung von Entwurfsmustern
- Benennung von Klassen, Methoden (s. Abschnitt 8.15.2)
- Kommentierung (s. Abschnitt 8.15.4)
- Zentrale Speicherung von Literalen (s. Abschnitt 8.15.6)
- Festlegung von Standardkomponenten

8.11.2 Code Reviews

Code Reviews zur regelmäßigen Prüfung der Codequalität durch Entwickler sind ein fester Bestandteil des Jira-Workflows in DVDV und führen zu einer deutlichen Reduktion von Fehlern, z.B.:

- Abweichung von Standards (z.B. Namenskonventionen)
- fehlerhafte Umsetzung der Schnittstellenspezifikation
- fehlerhafte Umsetzung der Anforderungen

- Designfehler
- unzureichende Wartbarkeit

8.11.3 Statische Codeanalyse

Mit Hilfe von Tools zur statischen Codeanalyse ist es schon in der Entwicklungsphase möglich, Probleme mit der Codequalität zu erkennen und direkt zu beheben:

- Spotbugs22: Identifikation von kritischen Codestellen und potenziellen Fehlern
- Checkstyle23: Überprüfung der Einhaltung von syntaktischen Kodierrichtlinien

8.11.4 Verwendung einer Integrationsplattform zur Darstellung und Auswertung verschiedener Codeanalysen

Als Tool zur kontinuierlichen Überwachung und grafischen Darstellung der Codequalität wird SonarQube[24] eingesetzt. Neben der Einbindung der Tools zur statischen Codeanalyse werden durch das Tool folgende Qualitätsbereiche geprüft:

- doppelter Code
- Testabdeckung
- Komplexität des Codes
- Kodierrichtlinien
- Kommentierung

8.12 Unterstützte Browser

Die Webanwendungen Admin-Client, Pflege-Client und Auskunfts-Client unterstützen die folgenden Browser in der jeweils aktuellen Version:

- Mozilla Firefox
- Microsoft Edge
- Google Chrome

8.13 Performanz

Wie in Abschnitt 7.1 erwähnt, wird die Hauptlast des Systems an der Directory-Schnittstelle der DVDV-Server erwartet. Hier ist von einer sehr hohen Anfragelast auszugehen. Alle anderen Komponenten des Systems haben nur eine geringere Last zu erwarten. Die Directory-Schnittstelle wurde daher mit einem besonderen Augenmerk auf hoher Performanz und gutem Durchsatz entwickelt.[25]

Die Performanz einer Software muss für alle Hauptphasen des Lebenszyklus betrachtet werden.

---

22 https://spotbugs.github.io/

23 http://checkstyle.sourceforge.net/

24 https://www.sonarqube.org/

25 Genaue Lastzahlen wurden in einem aufwändigen Last- und Performancetest in 2022 ermittelt. Es konnte nachgewiesen werden, dass die Grenzlast eines DVDV-Servers bei 150 Anfragen pro Sekunde liegt.

8.13.1 Analyse/Entwurfsphase

Maßgeblich für den Entwurf eines performanten Systems sind die Systemarchitektur, das Schnittstellendesign und die Datenbank-Optimierung. Für die Sicherstellung einer performanten Systemarchitektur stützen sich sämtliche Java-Serverkomponenten konsequent auf nebenläufige, statuslose Services, die eine optimale Ressourcenausnutzung gewährleisten. Alle DVDV-Services und insbesondere die Directory-Schnittstelle werden über eine RESTful-API zur Verfügung gestellt.

Um die Performanz eines Systems zur Entwicklungszeit sicherzustellen, werden Profiling-Werkzeuge eingesetzt. Diese Tools erlauben Optimierungen zur Entwicklungszeit. Langsame oder umständlich umgesetzte Codeteile werden identifiziert und damit auch punktgenau die Methoden und Klassen, in denen die meiste Ausführungszeit benötigt wird. Diese werden dann gezielt optimiert und beschleunigt. Zentrale Metriken für die Optimierung der Performanz sind weiterhin

- die Speicherauslastung im Java Heap,
- die Prozessorauslastung sowie Anzahl der Threads und das Thread-Pooling,
- der Netzwerk-Traffic sowie das Connection-Pooling der HTTP-Verbindungen,
- konkurrierende Datenbankzugriffe und geeignetes Connection-Pooling der Datenbankverbindungen.

Basierend auf diesen Metriken lassen sich typische Flaschenhälse für die Performanz schon bei der Entwicklung vermeiden. Durch die Speicherüberwachung lassen sich die exzessive Speichernutzung einzelner Codeteile oder auch Memory-Leaks feststellen und gezielt beheben. Der Netzwerkverkehr wird durch einen geeigneten Zuschnitt der Services und Schnittstellen optimiert.

Neben der Code-Optimierung wird zur Entwicklungszeit auch eine Datenbank-Optimierung durchgeführt. Hierzu werden die folgenden Maßnahmen insbesondere für die Zugriffe über die Directory-Schnittstelle eingesetzt:

1. Eine Statistik-Analyse mit Tools, wie z.B. JProfiler, zur Identifikation von inperformanten SQL-Anfragen für eine gezielte Optimierung.
2. Optimierung langsamer Zugriffe durch Anpassung des Datenbank-Schemas und umfassende Indizierung aller Datenbank-Tabellen.
3. Zuschnitt transaktionaler Schreiboperationen, so dass ein gegenseitiges Blockieren konkurrierender Zugriffe möglichst nicht eintritt.
4. Nutzung von durch den JPA-Provider bereitgestellten Hilfsmitteln, wie die Steuerung des Zugriffstyps, der Caching-Strategie oder die gezielte Optimierung komplexer Abfragen durch den Einsatz einer geeigneten Abfragemethodik, wie z.B. „Named Queries“.

8.13.2 Lasttest

Um das Erreichen der Performanz-Ziele hinsichtlich Durchsatz und Antwortzeit belegen zu können, wurden Last-Tests an der entwickelten Software auf einem realistischen Testsystem durchgeführt.

In 2022 wurde mit einem aufwendigen Last-Test die Performanz der Directory-Schnittstelle des Systems nachgewiesen und die Einhaltung der Anforderungen in unterschiedlichsten Lastszenarien belegt. Testaufbau und Ergebnisse sind in einem eigenen Dokument festgehalten.

8.13.3 Betriebsphase / Pflege / Wartung

Für das betriebliche Monitoring ist der spätere Betreiber der Lösung zuständig und wird auf etablierte Technologien zugreifen, um typische Performanz-Flaschenhälse zu überwachen, wie z.B. die Auslastung des verfügbaren Arbeits- und Festplattenspeichers und des Prozessors.

Um eine Ermittlung von aussagekräftigen Performanz-Kennzahlen zu unterstützen, werden dem Betreiber neben den statistischen Auswertungen auch Performanz-Informationen in den Log-Dateien zur Verfügung gestellt. Diese können, abhängig von den jeweiligen Erfordernissen, über die Konfiguration aktiviert bzw. deaktiviert werden.

8.14 Ausnahmebehandlung

DVDV nutzt eine zentrale Ausnahmebehandlung, basierend auf dem standardisierten Java Exception-Mechanismus, der automatisch von einer Komponente beim Auftreten eines Fehlers aufgerufen wird. Anhand der internen Fehlerkennung wird ein Fehlerobjekt erzeugt und selbiges für die weitere Verarbeitung in einer Ausnahme an den Aufrufer übergeben.

Damit ist eine zentrale Instanz für die Fehlerbehandlung vorhanden, welche die korrekte Beschreibung und eine angemessene Reaktion auf den Fehler ermöglicht. Es erfolgt in jedem Fall eine strukturierte Ausnahmebehandlung (SEH), das heißt der Programmcode zur Ausnahmebehandlung ist vom normalen Anwendungscode getrennt.

Um im DVDV 2.0-Kontext stets sinnvolle Reaktionen auf die Fehlerszenarien zu ermöglichen, finden die Ausnahmebehandlung zentral an der Systemgrenze (RESTful-API) statt. Es wird der ExceptionMapper aus dem javax.ws.rs-Package (RESTEasy-Framework) genutzt. Damit ist es möglich, selektiv auf die möglichen Fehlerszenarien zu reagieren und Exceptions direkt in Response-Objekte zu mappen.

Im Fehlerfall wird von der REST-API (Backend) eine Fehlerresponse gemäß RFC 7807 erzeugt. Dieser RFC beschreibt eine Response mit einem passenden HTTP-Statuscode, Media-Type `application/problem+json` und einem standardisierten Fehlerobjekt im http-Body. Zusätzlich wird auf dem jeweils erforderlichen Log-Level ein Eintrag in die Log-Datei geschrieben.

Fachliche (Plausibilitäten) und technische Fehler werden an der Schnittstelle grundsätzlich gleich behandelt und sind anhand des HTML-Statuscodes (vom Client) zu unterscheiden.

Für die verschiedenen Fehlerszenarien wurden eigene Exception-Handler entwickelt, die für die angepassten Logausgaben und auch für den Inhalt der Fehlerresponse gemäß RFC 7807 verantwortlich sind.

Texte für Fehlerbeschreibungen werden aus einer lokalisierten Ressourcendatei geladen.

Die verwendeten HTTP-Statuscodes im Fehlerfall entsprechen den allgemeinen Standards nach RFC 7231, Abschnitt 6.1.

8.14.1 Verwendete HTTP-Status-Codes (Beispiele)

Code	Nachricht	Bedeutung
400	Bad Request	fehlerhafter Aufbau des Requests (Parameter, Request-Objekt), fachliche Fehler in den Daten (z.B. bei fehlgeschlagenen Plausibilitätsprüfungen)
401	Unauthorized	Authentifizierung fehlgeschlagen
403	Forbidden	Autorisierung fehlgeschlagen bzw. HTTPS erforderlich
404	Not Found	Die angeforderte Ressource wurde nicht gefunden.
409	Conflict	Die Ressource wurde zwischenzeitlich verändert (Optimistic Lock).
500	Internal Server Error	Internal Server Error (unerwarteter Fehler)

Tabelle 54: Liste der HTTP-Status-Codes

8.14.2 Aufbau des Fehlerinfoobjektes

Im Ausnahmefall wird vom Backend ein fest definiertes Responseobjekt im JSON-Format erzeugt. Dieses Objekt enthält einen Container (Liste) der Fehlerinfoobjekte:

Schlüssel	Typ	Bedeutung
resourceIdentifier	String	Schlüsselwert der Ressource (notwendig für Bulk-Operationen)
propertyIdentifier	String	Schlüsselwert (z.B. UUID) des betroffenen Attributs der Ressource (notwendig für Maskenvalidierung)
infoText	String	Fehlerbeschreibung für den Benutzer
additionalInfoText	String	detaillierte Fehlerbeschreibung (wird nicht dem Benutzer angezeigt)

Tabelle 55: Attribute des Fehlerinfoobjektes

8.15 Programmierrichtlinien

8.15.1 Programmiersprache

Die Programmiersprache für alle zu entwickelnden Komponenten ist Java. Damit alle Komponenten auch in einem gemeinsamen Application Server und damit in einer gemeinsamen JVM lauffähig sind, muss die unterstützte Java Version für alle Komponenten einheitlich sein. Die Java-Version wird mit jeder neuen Software-Auslieferung getestet und freigegeben.

8.15.2 Benennungsregeln

Pakete, Klassen und Methoden, Variablen und Konstanten werden nach einem einheitlichen System benannt. Dabei wird grundsätzlich den allgemeinen „Code Conventions for the Java

Programming Language“ gefolgt. Zur Verbesserung der Lesbarkeit des Programmcodes wurden zusätzliche Benennungsregeln für einige Elemente festgelegt:

Paketstruktur

- Komplett in Kleinschrift (lower case)
- Startpaket für alle Komponenten ist „de.dataport.dvdv2“

Klassen

- Klassennamen sind Nomen im Singular, beginnend mit einem großen Buchstaben, jedes weitere Wort im Klassennamen beginnt ebenfalls mit einem Großbuchstaben. Diese Art der Schreibweise wird auch als „upper camel case“ bezeichnet.
- Datentransferobjekte (DTO) enden auf „DTO“ (Beispiel: „KundeDTO“).
- Serviceklassen enden auf „Service“ (Beispiel: „KundeService“).
- REST-Services enden auf „RestService” (Beispiel: „KundeRestService”).
- Data Access Objects (DAO) enden auf „DAO“ (Beispiel: „KundeDAO“).
- Testklassen werden nach der zu testenden Klasse und der Endung „Test“ benannt (Beispiel: „KundeDAOTest“).

Methoden

- Methodennamen sind Verben, beginnend mit einem kleinen Buchstaben, jedes weitere Wort im Namen beginnt mit einem Großbuchstaben. Diese Art der Schreibweise wird auch als „lower camel case“ bezeichnet.
- Testmethoden lassen an ihrem Namen erkennen, was genau getestet wird (betrifft auch Negativtests).

Variablen

- Variablennamen beginnen mit einem kleinen Buchstaben, jedes weitere Wort im Namen beginnt mit einem Großbuchstaben. Diese Art der Schreibweise wird auch als „lower camel case“ bezeichnet.
- Aussagekräftige Benennung, Ausnahme: Temporäre Variablen (in Schleifen) können die Länge 1 haben (i, j, k...)

Konstanten

- Konstantennamen sind in Großbuchstaben, Einzelworte werden durch Unterstriche getrennt (Beispiel „MAX_VALUE“).

8.15.3Logging

Für das Loggen von Anwendungsmeldungen und Fehlern wird in DVDV die vom Application-Server bereitgestellte Logging-Schnittstelle `slf4j` verwendet. Dadurch wird die Log-Ausgabe der DVDV-Software in die Logs des Application-Servers integriert.

Das Logging-Verhalten kann entsprechend den Logging-Richtlinien des Betreibers durch Konfiguration des Application-Servers angepasst werden, um z.B. Periodic-Rotating-File-Handler oder auch Syslog-Handler frei zu definieren.

In der Konfigurationsdatei kann die Ausgabe je nach Wichtigkeit der Nachrichten gefiltert werden. Der Ausgabe-Umfang umfasst alle Nachrichten der Stufe selbst, sowie aller noch dringenderen Stufen.

Es werden in der DVDV-Software folgende Stufen unterschieden:

Log-Level	Bedeutung
TRACE	ausführliches Debugging
DEBUG	allgemeines Debugging zum Auffinden von Fehlern
INFO	allgemeine Informationen zum Programmablauf (Modul gestartet, Modul beendet etc.)
WARN	Auftreten einer unerwarteten, jedoch nicht kritischen Situation
ERROR	Fehler / Ausnahme (REST-API erzeugt HTTP-Fehlercode)

Tabelle 56: Liste der Log-Level

Sensitive und vertrauliche Daten, wie zum Beispiel Passwörter, werden nicht geloggt.

8.15.4Kommentierung

Mit Kommentaren werden Klassen, Methoden und Strukturen kurz beschrieben, so dass Betrachter des Quellcodes ein besseres Verständnis für die Funktion der Anwendung erlangen können. Dies erhöht die Lesbarkeit des Codes und ist ein wichtiges Mittel für die Erreichung des DVDV-Qualitätsziels der Codequalität.

Kommentare sind grundsätzlich in deutscher Sprache verfasst und nutzen die Javadoc-Syntax. Javadoc ist ein Dokumentationswerkzeug, das aus Java-Quelltexten automatisch HTML-Dokumente erstellt. Javadoc ist ein fester Bestandteil des Java Development Kits (JDK).

Die Programmcode-Kommentierung in DVDV umfasst:

- Klassen: Kommentar beschreibt den Zweck und die Aufgabe der Klasse
- Schnittstellen: Kommentar beschreibt den Zweck und die Aufgabe der Schnittstelle und auch die Semantik
- Öffentliche Methoden („public“): Kommentar beschreibt den Zweck und die Aufgabe der Methode, die Übergabeparameter und den Rückgabewert
- Komplexere private Methoden („private“), die nicht selbsterklärend aus dem Namen sind

8.15.5Test

Testen ist ein wesentlicher Teil des Qualitätsmanagements innerhalb von DVDV. Für die Komponententests ist das Testziel der Nachweis der technischen Lauffähigkeit und korrekter fachlicher (Teil-) Ergebnisse.

Da Komponenten (Units bzw. Module) meist nur eine begrenzte Komplexität aufweisen und über klar definierte Schnittstellen aktiviert werden, können sie mit relativ wenigen Testfällen weitgehend vollständig getestet werden. Die Unit-Tests werden von den Softwareentwicklern selbst erstellt.

Zur Umsetzung der Komponententests wird in DVDV das JUnit-Framework eingesetzt. Es ermöglicht das automatisch wiederholbare Testen der einzelnen Units und eine nahtlose Integration in den Buildprozess. Zusätzlich werden Erweiterungen des Frameworks eingesetzt, wie z.B. DBunit zur Unterstützung der Datenbankentwicklung.

Zusätzlich werden automatisierte Integrationstests mit dem Selenium-Framework umgesetzt. Diese werden als Regressionstests mindestens vor den Auslieferungen und nach umfangreicheren Softwareänderungen ausgeführt. Sie decken wesentliche Teile der Anwendung ab und testen insbesondere Schnittstellen und Clients inkl. derer Masken im Zusammenspiel mit dem Kernsystem.

8.15.6 Zentrale Speicherung von Text-Literalen

Literale, im Allgemeinen Texte für Benutzerhinweise, Fehlermeldungen und Beschriftungen, werden nicht direkt im Quellcode hinterlegt, sondern zentral in Ressourcendateien ausgelagert. Die eigentlichen Texte werden jeweils einem hierarchischen und eindeutigen Schlüssel zugeordnet (Key-Value Paare).

Beispiel

```
suche.dienste.no.result = Für den Suchbegriff wurde kein Eintrag gefunden.
```

Literale, die zur Steuerung der Anwendung dienen (zum Beispiel Konfigurationsparameter), werden in sogenannten Property-Dateien verwaltet. Die darin enthaltenen Literale bestehen aus einem hierarchischen Schlüssel und dem zugehörigen Wert.

Beispiel

```
dvdv2.rest.url = https://host.dataport.de:8443/ks/rest

dvdv2.job.logging.cleanup.crontab = 0 0 4 1-5 * * *
```

Durch die separate, zentrale Speicherung können diese Informationen weitgehend unabhängig vom übrigen Programmcode gepflegt werden und lassen sich einfach austauschen (zum Beispiel für verschiedene Stages).

Dies wirkt sich positiv auf die Wartbarkeit und Übertragbarkeit als wichtigem Qualitätskriterium für DVDV aus.

8.16 Barrierefreiheit

Eine barrierefreie Benutzeroberfläche ist im Rahmen von DVDV ein wichtiges Qualitätsziel. Zur Gewährleistung der Barrierefreiheit entsprechend den Anforderungen[26] wurde in der Entwicklungsphase kontinuierlich die Anwendung gegen die Liste der Prüfschritte[27] der BITV (Barrierefreie Informationstechnik-Verordnung) abgeglichen.

8.16.1 Umgang mit Grafiken und Objekten

DVDV ist eine Anwendung zur Datenpflege. Grafiken und Objekte stellen somit keinen zentralen Bestandteil der Anwendung dar und werden daher nur sehr sparsam verwendet. An den Stellen, an denen grafische Elemente verwendet werden (bspw. auf Schaltflächen), werden mit HTML-Mitteln entsprechende textuelle Alternativen angeboten.

[26] mindestens 90 Punkte in einem BITV-Test für die folgenden drei Webseiten: Startseite, Suchergebnisseite, eine beliebige Hilfeseite

[27] https://testen.bitv-test.de

8.16.2 Kontraste und Farben

Die Auswahl des Farbschemas erfolgte anhand der Kriterien der BITV, die ein Kontrastverhältnis vom Vorder- zum Hintergrund von mindestens 4,5:1 vorgibt. Somit ist gewährleistet, dass auch Anwender mit verschiedenen Arten von Farbenschwäche DVDV nutzen können.

8.16.3 Skalierbarkeit

Die Skalierbarkeit der Anwendung wird über die entsprechenden integrierten Funktionalitäten der Webbrowser sichergestellt:

- Mit der Zoom-Funktion des Browsers kann das gesamte Layout proportional zur Schriftgröße vergrößert werden.
- Mit der Text-Vergrößerung im Webbrowser können der Text und die Schriftgröße verändert werden.

8.16.4 Navigation und Orientierung

Entsprechend der Vorgabe VL9 folgt die Navigation innerhalb vom DVDV dem Styleguide der Bundesregierung.

Konsistente Navigationsebenen zeigen den Nutzern jederzeit, an welcher Stelle der Anwendung sie sich befinden. Alle Menüs und Eingabefelder der Anwendung werden in einer definierten Fokus-Reihenfolge durchlaufen, was die reine Bedienung mit der Tastatur ermöglicht und die geforderte Geräteunabhängigkeit sicherstellt.

8.17 Formatfestlegungen

8.17.1 Encoding

Alle Texte in der gesamten Anwendung sind mit UTF-8 ohne BOM encodiert. Von der Anwendung werden alle Zeichen des Standards „Lateinische Zeichen in UNICODE“ v1.1.1 unterstützt.

Zeilenumbrüche werden entsprechend der UNIX-Konvention mit LF encodiert.

8.17.2 Datumsformate

Folgende Festlegungen gelten in der gesamten Anwendung:

- Alle Zeiten in der Datenhaltung und im Kernsystem werden immer in UTC abgelegt und auch in UTC über die HTTP-Schnittstellen des Kernsystems ausgeliefert. Für die Konvertierung in die Systemzeit ist die jeweilige Clientanwendung zuständig.
- Die Entwicklung nutzt die DateTime-API aus Java 8.
- An allen Schnittstellen, insbesondere bei der JSON-Serialisierung, werden DateTime-Objekte immer im Format ISO8601 mit Z (also in UTC) angegeben, also „2014-01-01T23:28:56.782Z“.
- In der Datenbank werden Datumsangaben immer im Typ `datetime` abgelegt.

9 Anhang

9.1 Glossar

Term	Beschreibung
Behörde	Eine Behörde ist eine Organisation vom Typ „Behörde“.
Behördenschlüssel	Ein Behördenschlüssel ist der Schlüssel einer Organisation vom Typ „Behörde“. Dieser ist eindeutig innerhalb der Organisationskategorie (=Behördenkategorie).
Dienst	Fachlicher Dienst, der im DVDV verzeichnet ist.
DVDV-IAM	Komponente DVDV Identity and Access Management
Identität	Nutzer des Kernsystems, der sich am System anmelden kann (entspricht nicht der Definition in der Ausschreibung)
NdB	„Netz des Bundes”, firmierte zuvor unter „DOI-Netz“ (Deutschland-Online Infrastruktur)
Organisation	Eine Organisation ist eine juristische Person, die Dienste anbieten kann (ehemals Behörde).
Organization Representative	Eine OrganizationRepresentative ist eine Organisation, die Dienste im Namen von anderen Organisationen in Stellvertretung anbieten kann (ehemals Behördenstellvertreter).
OrganizationKey	Ein Organisationsschlüssel ist der Schlüssel einer Organisation. Dieser ist eindeutig innerhalb der Organisationskategorie.
Provider	IT-Dienstleister für die öffentliche Verwaltung, die Infrastruktur und Zertifikate im DVDV-Kontext betreiben und bereitstellen.
Registry	Verzeichnis zur Speicherung von Diensten
Repository	Verzeichnis zur Speicherung von Ressourcen, die keine Dienste sind
Ressource	Oberbegriff für alle pflegbaren Fachdaten in DVDV, insbesondere Organisationen, Dienste, Provider, Zertifikate, benutzerdefinierte Ressourcen

9.2 Abbildungs- und Tabellenverzeichnis