DVDV

B14.25 – 0200/14: 1

Verfahrensbeschreibung

Dokumenten-Version: 2.02 vom 26.03.2024

Status: in Fortschreibung

Inhaltsverzeichnis

1 Über dieses Dokument

Das Deutsche Verwaltungsdiensteverzeichnis (DVDV) ist eine fach- und verwaltungsübergreifende Infrastrukturkomponente des E-Government in Deutschland. 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 elektronische Fachverfahren und Online-Dienste, keine menschlichen Nutzer.[1]

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. Das DVDV ist darauf ausgerichtet, im laufenden Betrieb weitere Dienste und Systeme anzubinden und im Backend größerer Verbundsysteme die rechtssichere Kommunikation über standardisierte Verfahren mittels standardisierter Kommunikationsszenarien zu ermöglichen.

Im Zuge der stetig voranschreitenden Digitalisierung der Verwaltungsleistungen wird die Bedeutung des DVDV in den kommenden Jahren voraussichtlich erheblich wachsen. Es entstehen derzeit sowohl im europäischen als auch im nationalen Kontext zahlreiche neue Anforderungen, in deren Kontexten das DVDV eine gewichtige Rolle spielen soll. Diese Herausforderungen betreffen nicht nur eine Ausweitung der Nutzer- und Transaktionszahlen inklusive des damit einhergehenden Datenpflegeaufwands, sondern es werden Dienstleistungen und Dienstleister in völlig neuen Anwendungssituationen verzeichnet und neue Protokollstandards in neuen Netzen unterstützt und verzeichnet.

Das vorliegende Dokument soll allen Personen, die sich eingehender mit dem DVDV auseinandersetzen möchten, den Einstieg in dieses Thema erleichtern und einen ersten Überblick der organisatorischen und technischen Aspekte vermitteln. Aus Gründen der Übersichtlichkeit müssen in diesem Dokument viele Einzelheiten ausgeblendet bleiben, die zum Gesamtverständnis des DVDV nicht unbedingt erforderlich sind und den Lesefluss eher beeinträchtigen würden. Selbstverständlich existieren für sämtliche Aspekte der Realisierung detaillierte Beschreibungen, etwa eine Architekturdokumentation, je ein Benutzerhandbuch für DVDV-Bundesmaster und DVDV-Server, Handbücher für sämtliche Clients, diverse Eintragungskonzepte für die verzeichneten Behördenkategorien usw. Sollten Sie als Leser:in Bedarf an vertiefenden Informationen haben, wenden Sie sich bitte an die beim ITZBund eingerichtete Koordinierende Stelle DVDV[2] (dvdv@itzbund.de).

1.1 Ausgangslage und Zielsetzung

Die Idee des Deutschen Verwaltungsdiensteverzeichnisses reicht zurück bis zum Jahr 2002. Die damalige Novellierung des Melderechtsrahmengesetzes (MRRG)[3] sah eine elektronische Datenübermittlung zwischen Meldebehörden zwingend vor. Das war Anlass, über eine zentrale Infrastrukturkomponente für den automatisierten Austausch von Verbindungsdaten über das Internet nachzudenken. Diese sollte an zentraler Stelle technische Adress- und Protokollinformationen von E-Government-Fachverfahren (Applikationen) zwischen unterschiedlichen Verwaltungsträgern in Bund, Ländern und Kommunen bereitstellen, so dass kein Verfahren ein eigenes Adressverzeichnis pflegen und bereitstellen muss.

---

1 Quelle: https://www.it-planungsrat.de/DE/Projekte/Anwendungen/DVDV_2_0/dvdv_2_0_node.html

2 Weitere Informationen zur Koordinierenden Stelle DVDV entnehmen Sie bitte Kapitel 4.

3 Siehe dazu Melderechtsrahmengesetz vom 16.08.1980 – neu gefasst durch Bekanntmachung vom 19.04.2002 (BGBl I 2002, S. 1342).

Eine weitere zentrale Anforderung an das DVDV war und ist, dass es die Voraussetzungen für die rechtssichere und vertrauenswürdige Adressierung hoheitlicher Dienste im Sinne von Verwaltungsleistungen auf höchstem Sicherheits-, Validitäts- und Integritätsniveau schafft. Dies geschieht einerseits organisatorisch, indem ausschließlich durch die Verwaltung beauftragte, sog. Pflegende Stellen schreibenden Zugriff auf die im DVDV hinterlegten Daten haben. Andererseits sorgt die Verfahrensarchitektur dafür, dass Datenreplikationen innerhalb des DVDV-Systems nur auf gesicherten Netzen des Bundes stattfinden und die beteiligten Kommunikationspartner beim lesenden Zugriff eindeutig authentifiziert werden.

Schnell kam die Idee auf, diese Lösung nicht nur zwischen Meldebehörden, sondern auch fachoffen für andere (Online-)Dienste zu nutzen. Bund, Länder und kommunale Spitzenverbände einigten sich im Kooperationsausschuss Automatisierte Datenverarbeitung (KoopA ADV) auf das DVDV als gemeinsame Infrastrukturkomponente.

War das System initial auf den Datenaustausch zwischen Behörden der Innenverwaltung ausgelegt, entwickelte sich das DVDV seitdem stetig weiter und nahm insbesondere seit 2018 durch die steigenden Anforderungen aus Bund und Ländern neue XÖV-Fachdomänen auf.

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.

Im Jahr 2019 wurde die Codebasis des DVDV komplett modernisiert und unter der Bezeichnung „DVDV 2.0“ funktional wesentlich erweitert. Dies sollte die Zukunftssicherheit des Systems gewährleisten. Zentrale Motive waren 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 vom vorhergehenden auf das neue System erfolgte im Oktober 2019 ohne Einschränkung oder gar Unterbrechung der Nutzerverfügbarkeit.

1.2 Aktuelle Anforderungen aus SDG, RegMoG, OZG und OOP

Die Welt und die Anforderungen an das DVDV veränderten sich nach 2019 weiter und sind heute sogar noch dynamischer geworden. Zahlreiche Projekte und Initiativen rund um die Digitalisierung der Dienstleistungen der öffentlichen Verwaltung nehmen derzeit Fahrt auf oder stehen „in den Startlöchern“, neue Einsatzszenarien unter DVDV-Beteiligung konkretisieren sich.

Als ein Stichwort sei an dieser Stelle die Umsetzung des Onlinezugangsgesetzes (OZG) genannt, welches Bund, Länder und Gemeinden verpflichtet, den Bürgerinnen und Unternehmen viele ihrer Verwaltungsleistungen zukünftig auch in elektronischer Form über Portale anzubieten. Damit verwoben sind die Anforderungen, die sich aus der Befolgung des Once-Only-Principle (OOP) ergeben. Das OOP zielt auf die Verringerung des Verwaltungsaufwands, indem Antragsteller von Behördenleistungen bestimmte Standardinformationen nur noch einmal mitteilen müssen. Weitere Behörden, die diese Angaben ebenfalls benötigen, nutzen diese einmal gemachten Angaben nach – sofern der Antragsteller diesem Verfahren zustimmt.

Eine weitere Initiative, die sich potenziell der bereits existierenden Infrastrukturkomponente DVDV bedienen könnte, ist das Single Digital Gateway (SDG). Dieses wurde 2018 vom Europäischen Parlament und dem Europäischen Rat als einheitliches und EU-weites Zugangsportal für Verwaltungsleistungen beschlossen. Die daraus entstandene SDG-Verordnung ist Bestandteil der OZG-Umsetzung in Deutschland und kann im Sinne des Once-Only-Principle nur über zentrale Komponenten gelingen. Auch hier kann das DVDV einen wesentlichen Beitrag liefern.

Große Herausforderungen stellen die spezifischen SDG-Anforderungen dar, insbesondere die noch zu klärenden Schnittstellen, Identifizierungen und Authentifizierungen und nicht zuletzt

die Verpflichtung zur Mehrsprachigkeit. Für das DVDV wäre eine entsprechende Konzeption und Anpassung auf diese Anforderungen notwendig.

Einen Baustein für die konsequente Umsetzung der Ziele des SDG und des OZG bildet das „Koordinierungsprojekt Registermodernisierung“ des IT-Planungsrats. Mit dem gleichnamigen Gesetz (RegMoG) hat die Bundesregierung 2021 den Grundstein für die flächendeckende Modernisierung der bestehenden Registerlandschaft gelegt. Die logische Verknüpfung der Register der öffentlichen Verwaltung unter Beachtung optimaler technischer, rechtlicher und organisatorischer Funktionalität gewährleistet hohe Datenqualität und -aktualität und damit einen schnellen, unkomplizierten Datenaustausch.

Das Projekt Registermodernisierung verfolgt als eines seiner zentralen Nutzenversprechen die Förderung einer effizienten Verwaltung durch Once-Only-Verwaltungsleistungen. Voraussetzung für die konsequente Anwendung des OOP ist eine grundsätzlich engere Vernetzung zwischen den Behörden und die Kenntnis, welche Daten wo abgelegt sind. Hier dient das DVDV wiederum als zentrales Verzeichnis für die Adressierung der Anbieter von Verwaltungsdienstleistungen.

Für das DVDV ergeben sich aus der Registermodernisierung unterschiedliche Herausforderungen: Es ist sowohl von einer signifikanten Erhöhung der Zahl der Anfragen, als auch von einer erheblichen Zunahme der im System hinterlegten Dienste und Behörden auszugehen, auch werden weitere Arten der Anfragen hinzukommen. Nicht zuletzt müssen unterschiedliche technische Verbindungsparameter für die unterschiedlichen Kommunikationsszenarien innerhalb der grundlegenden Referenzarchitektur implementiert werden.

Mit Blick auf den dynamischen Zuwachs des zwischenbehördlichen Datenaustausches in Deutschland ist davon auszugehen, dass sich das DVDV auch in den nächsten Jahren weiterentwickeln und anpassen muss.

1.3 DVDV als Produkt des IT-Planungsrats

Inzwischen ist aus dem Projekt DVDV ein Produkt des IT-Planungsrats (IT-PLR) geworden. Dieses Gremium folgte 2010 dem KoopA ADV nach und dient der Koordinierung der Zusammenarbeit von Bund und Ländern in Fragen der Informationstechnik. Der IT-PLR besteht aus dem/der Beauftragten der Bundesregierung für Informationstechnik (BfIT) sowie einem/einer für Informationstechnik zuständigen Vertreter/in jedes Bundeslandes.

Produkte des IT-PLR sind dauerhaft betriebene Dienste, die den im Staatsvertrag genannten Zweck des „informations- und kommunikationstechnisch unterstützten Regierens und Verwaltens“ erfüllen. Hierzu zählen u. a. technische Schnittstellen, Kommunikationsdienste, zentrale Anwendungen und Methoden.

Weitere Produkte des IT-Planungsrats

- 115 - Einheitliche Behördennummer
- Behördenfinder Deutschland (BFD)
- eGov-Campus – Plattform für digitale Lehrangebote auf dem Gebiet e-Government/ Verwaltungsinformatik
- Föderales Informationsmanagement (FIM) - liefert standardisierte Informationen für Verwaltungsleistungen
- FIT-Store – Angebotsplattform zur Nach-/Mitnutzung digitalisierter Onlinedienste
- GovData – nationales Metadatenportal, über das Bund, Länder und Kommunen ihre Verwaltungsdaten auffindbar und zugänglich machen

- Governikus (genauer „Anwendung Governikus des IT-Planungsrats“) - ermöglicht den gesetzeskonformen und sicheren Austausch vertrauenswürdiger Daten und Dokumente über das Internet
- Governikus MultiMessenger (genauer „Anwendung Governikus MultiMessenger [GMM] des IT-Planungsrates“) – fungiert als zentrale Multikanalkommunikationsplattform
- Online-Gateway Portalverbund (PVOG) - verknüpft die Verwaltungsportale der Länder und des Bundes
- Online-Sicherheitsprüfung (OSiP) - Verfahren zur automatisierten und weitestgehend medienbruchfreien Beteiligung von Stellen der personenbezogenen Sicherheits- und Zuverlässigkeitsprüfungen

Die Federführung des DVDV oblag bis Mitte 2021 dem Bundesministerium des Innern, für Bau und Heimat (BMI) und wurde durch das Produktmanagement DVDV der Föderalen IT-Kooperation AöR (FITKO) abgelöst. Die FITKO ist eine vom IT-Planungsrat geschaffene Organisation, die mit operativen Planungs-, Steuerungs- und Koordinierungsaufgaben die effektive Umsetzung der Beschlüsse des IT-Planungsrats befördert. Dazu koordiniert und vernetzt sie die Akteur:innen, fördert und entwickelt gemeinsame Lösungen und Kooperationen und bietet Raum für neue Wege der Zusammenarbeit.

1.4 Aktuelle Nutzungszahlen

Um sich ein Bild von den Größenordnungen machen zu können, hier ein paar Zahlen zur Nutzung des DVDV. Zum Zeitpunkt der Erstellung des Dokumentes sind im DVDV die Zugangsparameter von mehr als 32.000 Behörden und Einrichtungen der öffentlichen Verwaltung oder zu diesem Zweck tätigen Organisationen eingetragen. Für diese sind ca. 58.000 konkrete Dienste verzeichnet.

Transaktionszahlen sind wegen der verteilten Natur des Systems nur sehr schwer zu ermitteln. Nach einer im Sommer 2020 vorgenommenen Erhebung erscheint für das Gesamtsystem eine Zahl von etwa einer Million Zugriffen pro Tag realistisch, Tendenz steigend.

2 Aufbau des DVDV

Das Deutsche Verwaltungsdiensteverzeichnis ist als verteiltes System umgesetzt und stellt eine Infrastruktur aus mehreren Komponenten zur Verfügung, die für unterschiedliche Aufgaben ausgelegt sind. In diesem Kapitel werden Aufbau, Funktionsweise, Schnittstellen und Zusammenwirken der einzelnen DVDV-Komponenten dargestellt.

2.1 Grundzüge der Architektur

Das DVDV ist als verteiltes System und Verbundverfahren aufgebaut und besteht aus einem sog. DVDV-Bundesmaster sowie mehreren DVDV-Servern in verschiedenen Bundesländern, die sich paarweise vertreten. Diese Architektur eignet sich besonders zur Bewältigung der hohen Anforderungen an die Performanz und gewährleistet über die Georedundanz eine hohe Verfügbarkeit des DVDV-Systems.

Den Kern der verteilten Infrastruktur bildet dabei der *DVDV-Bundesmaster*, der den führenden Datenbestand des Gesamtsystems hält. Sämtliche schreibenden Zugriffe auf den Datenbestand werden ausschließlich hier und nur durch berechtigte „Pflegende Stellen“ über einen „Pflege-Client“ vorgenommen. Eine der Aufgaben des DVDV-Bundesmasters ist das sog. „Identity and Access Management“ (IAM), mit dem z.B. Rollen und Rechte von Benutzern, wie etwa den Pflegenden Stellen, gesteuert werden können.

Lesende Zugriffe, also Anfragen an das DVDV, richten sich immer an die sogenannten DVDV-Server, niemals an den DVDV-Bundesmaster. Die DVDV-Server werden dezentral von mehreren Ländern über ganz Deutschland verteilt betrieben, meist von IT-Dienstleistern, z.B. Landesdatenzentralen (siehe Kap. 2.3.1).

Auf den DVDV-Servern befindet sich jeweils eine Kopie des DVDV-Datenbestands, die quasi permanent über die sicheren Netze des Bundes (NdB) mit dem DVDV-Bundesmaster abgeglichen wird. Änderungen am zentralen Datenbestand beim DVDV-Bundesmaster werden i.d.R. innerhalb weniger Sekunden auf sämtliche DVDV-Server repliziert. Falls aus irgendeinem Grunde die Verbindung zwischen einem DVDV-Server und dem DVDV-Bundesmaster unterbrochen werden sollte, können die Anfragen der Fachverfahren in den angebundenen Systemen von dem betroffenen DVDV-Server auch ohne aktuelle Replikation weiter beantwortet werden. Wenn hingegen ein DVDV-Server ausfallen bzw. seine Verbindung zum Internet gestört sein sollte, übernimmt für diese Zeit ein designierter anderer DVDV-Server seine Vertretung.

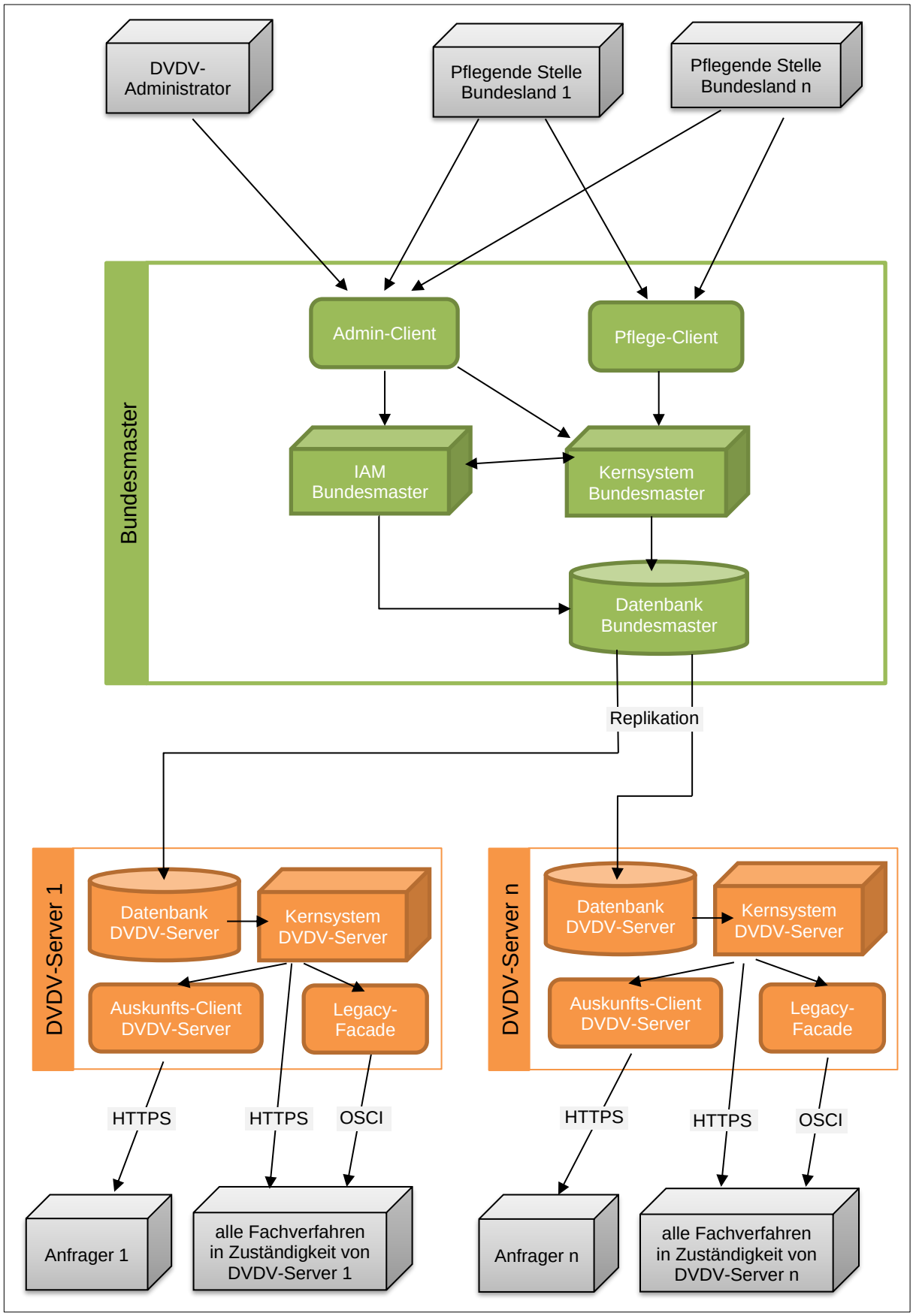

Abbildung 1: DVDV als Verbundverfahren

2.2 DVDV-Bundesmaster

Die wichtigste Komponente des DVDV ist der zentrale DVDV-Bundesmaster, der vom ITZ-Bund betrieben wird. Er besteht aus dem sog. Kernsystem und der Master-Datenbank, dem IAM sowie Admin- und Pflege-Client.

Der DVDV-Bundesmaster stellt das DVDV-Referenzsystem dar, sämtliche schreibende Zugriffe auf das DVDV erfolgen ausschließlich an diesem zentralen System durch dazu berechtigte „Pflegende Stellen“. Diese verwenden für Datenänderungen einen als Web-Anwendung konzipierten Pflege-Client. Zur Verwaltung der Zugriffsrechte und Rollen innerhalb des Systems dient eine weitere Komponente, der sog. Admin-Client. Diese Rechte werden im IAM hinterlegt und von diesem zur Authentifizierung von Benutzern verwendet.

Der DVDV-Bundesmaster ist nur an die Netze des Bundes (NdB) angeschlossen, nicht jedoch an das Internet.

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

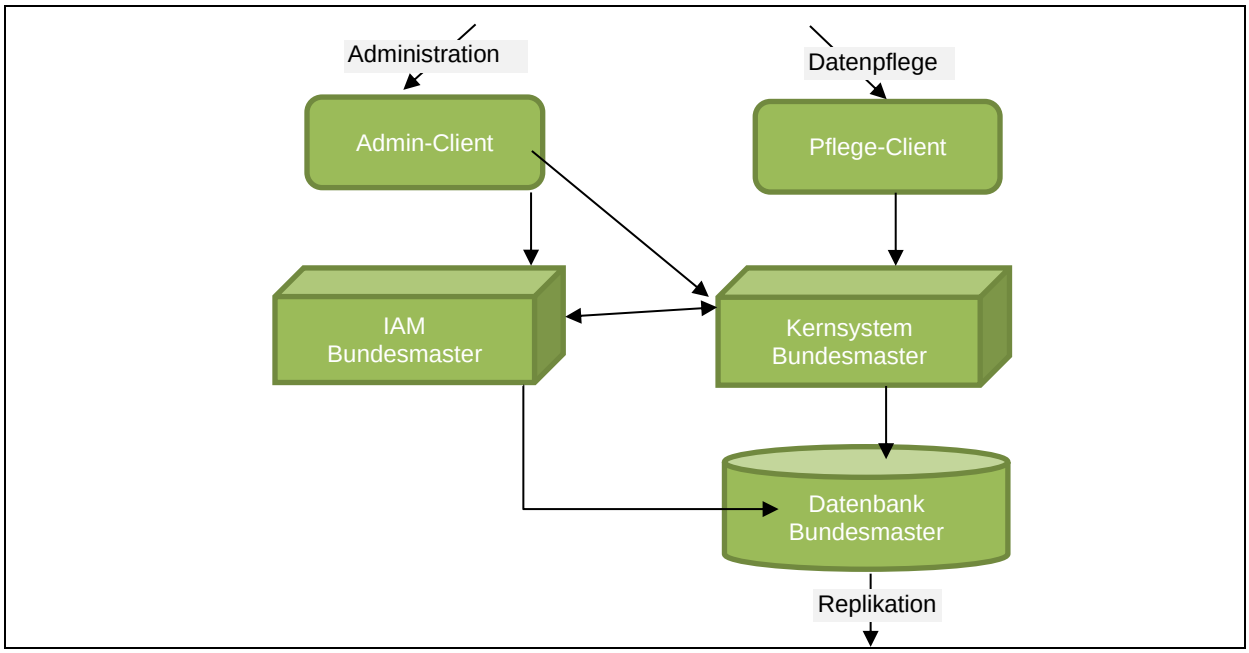

Abbildung 2: Aufbau des DVDV-Bundesmasters

2.2.1 Kernsystem DVDV-Bundesmaster

Über das Kernsystem werden alle fachlichen Daten des DVDV-Systems langfristig abgelegt und bereitgestellt. Dabei handelt es sich etwa um:

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

Das DVDV-Kernsystem ist als reine Serverkomponente ausgeprägt, der Zugriff erfolgt ausschließlich über die angebotene Directory-Schnittstelle.

Der DVDV-Bundesmaster hat die folgenden Schnittstellen zu anderen Systemen und Nutzern:

- Schnittstelle zum Pflege-Client für die Erfassung, Änderung und Löschung der im DVDV hinterlegten Organisationen und Dienste
- Schnittstelle zum Admin-Client für die Verwaltung der Metadaten des Systems, etwa Benutzerrechte, Rollen, Dienstbeschreibungen, Ressourcentypen, aber auch Anpassungen am Datenmodell.
- Schnittstelle zu den DVDV-Servern, über die die Replikation des Datenbestands durchgeführt wird.

2.2.2 Pflege-Client

Der Pflege-Client ist eine Browser-basierte Webapplikation und wird ausschließlich durch das ITZBund betrieben. Er dient der Datenpflege im DVDV und wird von den Pflegenden Stellen über die Netze des Bundes (NdB) genutzt.

Mit dem Pflege-Client können die im DVDV gehaltenen Datenobjekte, wie Organisationen, Provider, Dienste, Dienstbeschreibungen, Zertifikate und Favoriten, angelegt, geändert oder gelöscht werden. Dazu kann der Datenbestand über den Pflege-Client durchsucht, gefiltert und angezeigt werden. Darüber hinaus kann der Pflege-Client auch Statistiken und Änderungshistorien der Daten erzeugen und darstellen. Zum Funktionsumfang des Pflege-Clients gehört ein integriertes Benutzerhandbuch. Die Screenshots vermitteln einen Eindruck von der Benutzungsoberfläche des Pflege-Clients.

Abbildung 3: Oberstes Auswahlmenü des Pflege-Client

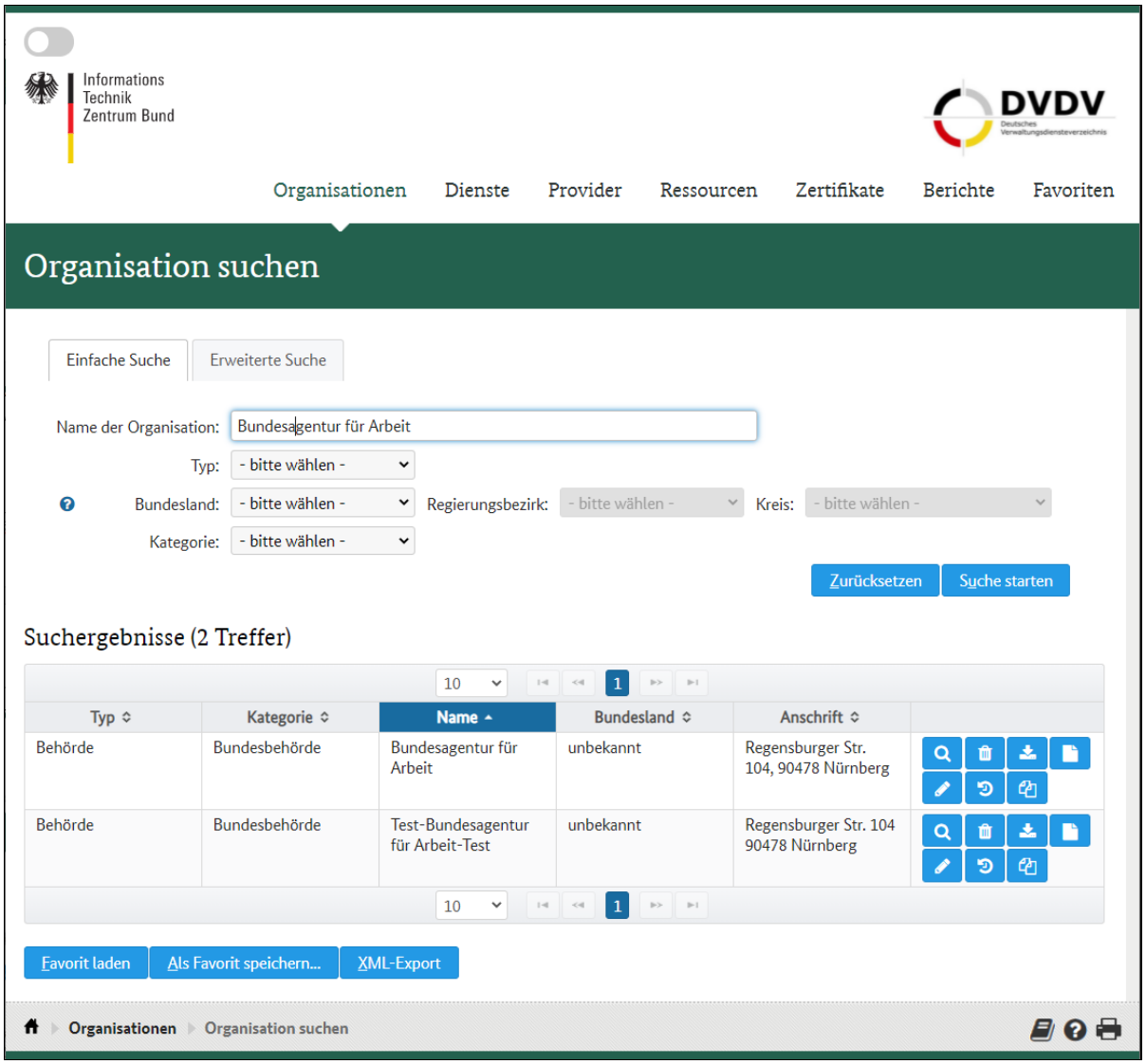

Abbildung 4: Funktion „Organisation suchen“ im Pflege-Client

2.2.3 Admin-Client

Neben dem zuvor beschriebenen Pflege-Client ist auch der Admin-Client ein Bestandteil der vom ITZBund zentral betriebenen DVDV-Bundesmaster-Infrastruktur. Während der Pflege-Client zur Erfassung, Änderung oder Löschung fachlicher Daten dient, werden über den ebenfalls Browser-basierten Admin-Client die notwendigen Metadaten gepflegt, z.B. Benutzer und Benutzergruppen, Stellvertreterregelungen, Rollen und Rechte und Ressourcengruppen für die Steuerung der Authentisierung und Autorisierung.

Des Weiteren sind administrative Tätigkeiten rund um die Ressourcenpflege im Admin-Client möglich. Dazu gehören etwa die Anlage neuer Dienst-Typen, z.B. durch Upload einer entsprechenden Dienstbeschreibung, die Erstellung neuer Ressourcen-Typen und die Pflege von Organisationskategorien. Über den Admin-Client kann in einem gewissen Umfang auch das Datenmodell flexibel angepasst werden, sofern neu entstehende Anforderungen dies sinnvoll erscheinen lassen.

Der Admin-Client kommuniziert mit den beiden angebundenen Komponenten Kernsystem und Identity and Access Management (IAM). Die administrativen Änderungen werden im DVDV-Kernsystem dauerhaft gespeichert („persistiert“), alle die Authentifizierung betreffenden Daten werden im angebundenen DVDV-IAM gespeichert.

Der nachfolgende Screenshot stammt vom obersten Auswahlmenü des Admin-Clients, über das die Hauptfunktionen ausgewählt werden. Wie auch beim Pflege-Client, bietet der Admin-Client für die berechtigten Nutzer ein integriertes Benutzerhandbuch.

Abbildung 5: Oberstes Auswahlmenü des Admin-Client

2.2.4 DVDV-IAM

Zum DVDV-Bundesmaster gehört außerdem eine zentrale Komponente „Identity and Access Management“ (IAM). Das IAM realisiert das Benutzer- und Zugriffskontrollmanagement auf das DVDV-Gesamtsystem. Zum Benutzermanagement gehören dabei die Pflege von Benutzern (Identitäten), Benutzergruppen und deren Anmeldeinformationen sowie die Pflege von Rollen, Rechten und Vertreterregelungen.

Das IAM gewährleistet, dass nur die dafür autorisierten Benutzer und Client-Systeme in dem vorgesehenen Umfang Zugriff auf die Clients des DVDV-Bundesmasters sowie bestimmte Funktionen der DVDV-Server erhalten. Das DVDV-IAM authentifiziert die Zugriffe auf das DVDV, insbesondere auf den Pflege- und Admin-Client beim DVDV-Bundesmaster sowie auf die Auskunfts-Clients bei den DVDV-Servern.

Das IAM-System im DVDV basiert auf dem Produkt Keycloak, welches um zusätzlich benötigte Fähigkeiten erweitert wurde. Das IAM nutzt eine MySQL-Datenbank.

Im Zusammenhang mit den seit 2022 möglichen DVDV-Anfragen über die Directory-Schnittstelle (siehe Kap. 3.4.1.2) ist das IAM außerdem technisch dafür ausgelegt, Berechtigungstoken auszustellen und zu validieren, die angebundene Systeme (insb. Fachverfahren) benötigen, um sich bei Anfragen auf den DVDV-Servern zu authentifizieren. In der Praxis wird diese Methode derzeit nicht verwendet, sondern die Authentifizierung findet am Kernsystem statt.

Das DVDV-IAM hat die folgenden Schnittstellen zu anderen Systemen und DVDV-Nutzern:

- Schnittstelle zum Admin-Client, über die das IAM administriert wird. Damit werden DVDV-Nutzer und angebundene Systeme zur Durchführung von Anfragen berechtigt, sowie die Berechtigung der Pflegenden Stellen zur Dateneingabe verwaltet.
- Schnittstelle zur Token-Ausgabe, über die das IAM den DVDV-Verfahrensbeteiligten auf Anfrage in den folgenden Situationen Token ausstellt:
  - für Administratoren bei Authentifizierung per Zertifikat
  - für Pflegende Stellen bei Authentifizierung per Zertifikat
  - für Nutzer des Auskunfts-Client bei Authentifizierung per Benutzername/Passwort
  - für angebundene Systeme, die Anfragen auf das DVDV über die Directory-Schnittstelle durchführen, bei Authentifizierung per Zertifikat

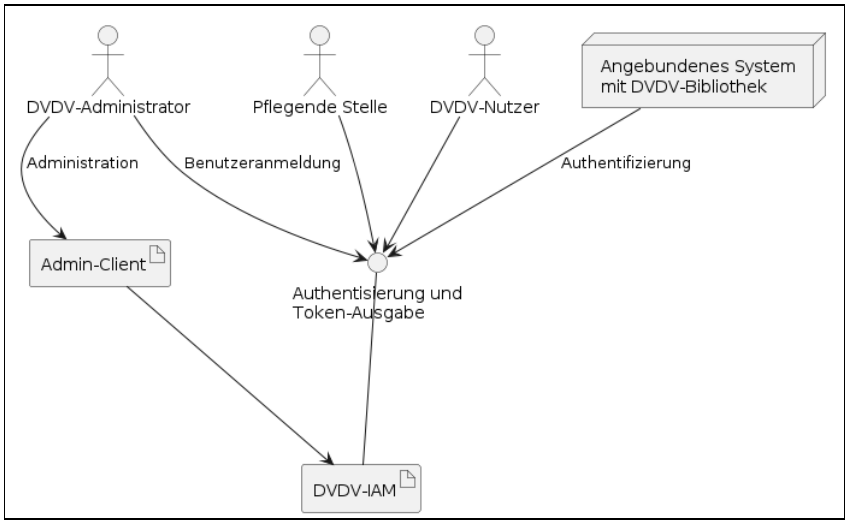

Abbildung 6: Schnittstellen des DVDV-IAM

2.3 DVDV-Server

Neben dem DVDV-Bundesmaster stellen die DVDV-Server die zweite Hauptkomponente des DVDV dar. Über die DVDV-Server gehen sämtliche Anfragen an das DVDV-System ein und werden von ihnen beantwortet. Ähnlich dem DVDV-Bundesmaster, besteht ein DVDV-Server aus einem Kernsystem („Backend“) und einem nachgelagerten MySQL-Datenbankserver. Zusammen mit dem eigentlichen DVDV-Server werden dort der Auskunfts-Client und eine Legacy-Facade-Komponente betrieben.

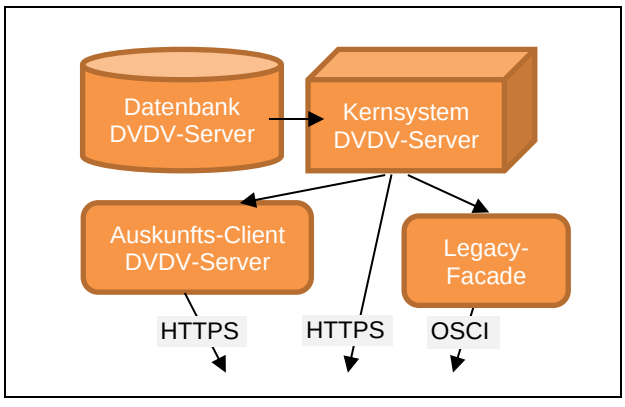

Abbildung 7: Aufbau eines DVDV-Servers

2.3.1 Betreiber

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. Schließlich werden auch DVDV-Server betrieben, die für mehrere Bundesländer zuständig sind.

Innerhalb des Verbundverfahrens teilen sich zum Zeitpunkt der Erstellung dieses Dokuments folgende Instanzen der DVDV-Server die Anfragelast:

Bundesland/Organisation	**Betreiber**
zentrale Komponenten	
DVDV-Bundesmaster	ITZBund
DVDV-IAM	ITZBund
DVDV-Server der Bundesländer	
Baden-Württemberg	Komm.ONE
Bayern	Landesamt für Digitalisierung, Breitband und Vermessung Bayern (LDBV)
Berlin	IT-Dienstleistungszentrum Berlin (ITDZ)
Brandenburg	Brandenburgischer IT-Dienstleister (ZIT-BB)
Bremen	Dataport
Hamburg	Dataport
Hessen I	ekom21 (KGRZ Kassel)
Hessen II	ekom21 (KGRZ Gießen)
Mecklenburg-Vorpommern	Dataport
Niedersachsen	Kommunale Datenverarbeitung Oldenburg (KDO)
Nordrhein-Westfalen I	citeq
Nordrhein-Westfalen II	Kommunales Rechenzentrum Niederrhein (KRZN)
Rheinland-Pfalz	Landesbetrieb Daten und Information (LDI)
Saarland	citeq
Sachsen	Staatsbetrieb Sächsische Informatik Dienste (SID)
Sachsen-Anhalt	Dataport
Schleswig-Holstein	Dataport
Thüringen	Thüringer Landesrechenzentrum (TLRZ)

Tabelle 1: Betreiber von DVDV-Bundesmaster und DVDV-Servern der Bundesländer

2.3.2 Zuständigkeit

Wie zuvor beschrieben, herrscht im Verbundverfahren DVDV eine Arbeitsteilung, nach der schreibende Zugriffe ausschließlich über den DVDV-Bundesmaster und lesende Zugriffe ausschließlich über die in der ganzen Republik verteilten DVDV-Server durchgeführt werden. Anfragen von Fachverfahren richten sich somit immer an einen der DVDV-Server, niemals an den zentralen DVDV-Bundesmaster.

Alle DVDV-Server sind jeweils nur für die Anfragen bestimmter, dazu berechtigter Nutzer zuständig. Das sind in der Regel die Anfragen von Fachverfahren (oder vorgeschalteten Clearingstellen) aus dem eigenen Bundesland des DVDV-Server-Betreibers sowie Anfragen aus anderen Bundesländern, mit denen der Betreiber eine entsprechende Vereinbarung geschlossen hat. So ist etwa die Dataport AöR mit Sitz in Altenholz, Schleswig-Holstein für den DVDV-Server-Betrieb von gleich fünf Bundesländern (Bremen, Hamburg, Mecklenburg-Vorpommern, Sachsen-Anhalt und Schleswig-Holstein) zuständig, während es andererseits in Hessen und Nordrhein-Westfalen jeweils zwei DVDV-Server in ein und demselben Bundesland gibt.

2.3.3 Vertreterregelung

Das DVDV hat den Anspruch möglichst hoher Verfügbarkeit. Aus diesem Grund ist es üblich, dass die Betreiber eines DVDV-Servers einen anderen DVDV-Server vertraglich als Vertreter verpflichten. Dieser Vertreter übernimmt bei Ausfall des eigentlich zuständigen DVDV-Servers, z.B. durch technische Störungen, Überlast oder während geplanter Wartungsfenster, die Beantwortung der während dieser Zeit eingehenden Anfragen. Vertretungen müssen dabei nicht unbedingt gegenseitig erfolgen, sondern können auch gestaffelt oder asymmetrisch sein, also z.B. Server A vertritt B, B vertritt C und C vertritt A oder Server A vertritt B und C, C vertritt A.

Ausgelöst wird die Nutzung des Vertretungsservers, wenn ein anfragendes Fachverfahren nach einer vorgegebenen Zeit keine Antwort des zunächst kontaktierten, primär zuständigen DVDV-Servers erhalten hat. Es kann dann in einer erneuten Anfrage die im Fachverfahren hinterlegten Daten des Vertretungsservers verwenden. Prinzipiell können im DVDV beliebig viele Vertreter benannt werden, in der Praxis gibt es derzeit jedoch immer genau einen designierten Vertreter für jeden DVDV-Server. Die Implementierung eines entsprechenden Failover-Mechanismus innerhalb des DVDV-Clients des anfragenden Fachverfahrens obliegt den Fachverfahrensherstellern. Die für das DVDV bereitgestellten Bibliotheken unterstützen dies mit passenden Methoden (siehe Kap. 3.4.2).

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. Der Ausfall eines oder gar mehrerer DVDV-Server darf nicht dazu führen, dass auf das DVDV insgesamt nicht mehr zugegriffen werden kann. Der Ausfall des zentralen DVDV-Bundesmasters und des IAM kann für einen gewissen Zeitraum toleriert oder durch bestimmte, redundant angelegte Verfahren (siehe Kap. 2.3.6) kompensiert werden, ohne dass die Performanz des Gesamtsystems gravierend leidet.

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

2.3.4 Datenreplikation

Änderungen am Datenbestand werden, wie geschildert, mit Hilfe des Pflege- oder des Admin-Clients ausschließlich auf dem Datenbestand des DVDV-Bundesmasters vorgenommen. Über einen Replikationsmechanismus überprüfen alle DVDV-Server permanent, ob ihr Datenbestand noch mit dem Datenbestand auf dem DVDV-Bundesmaster übereinstimmt. Bei einer Veränderung werden die durchgeführten Modifikationen über sicheren Netze des Bundes (NdB) an alle DVDV-Server übertragen und in deren Datenbank übernommen, so dass anschließend DVDV-Server und der DVDV-Bundesmaster wieder über denselben Datenbestand verfügen.

2.3.5 Schnittstellen der DVDV-Server

Damit die DVDV-Verfahrensbeteiligten ihre Anfragen an das DVDV-System stellen können, sind die DVDV-Server im Internet verfügbar. Für die Anfragen stellen die DVDV-Server zwei unterschiedliche Schnittstellen zur Verfügung, nämlich die Legacy Facade mit ihrer OSCI-

Schnittstelle sowie die Directory-Schnittstelle. Zusätzlich gibt es eine Tokenausgabe-Schnittstelle. Details zur Nutzung der Schnittstellen finden sich in Kapitel 3.4.1.

2.3.6 Kernsystem DVDV-Server

Das Kernsystem der DVDV-Server gleicht grundsätzlich dem Kernsystem des DVDV-Bundesmasters, wie es in Kap. 2.2.1 beschrieben ist.

2.3.7 Auskunfts-Client

Während die im DVDV hinterlegten Daten zu Organisationen und deren angebotenen Diensten bislang nur von den verbundenen Systemen in automatisierten Verfahren bzw. von Pflegenden Stellen über den Pflege-Client abgerufen werden konnten, eröffnet der Auskunfts-Client nun auch natürlichen Personen einen Zugriff – sofern sie dazu berechtigt sind. Er dient damit insbesondere den Dienstanbietern und Dienstnutzern (d.h. den eingetragenen Organisationen) zur Verifikation der gespeicherten Dienstinformationen.

Der Auskunfts-Client wird an den DVDV-Servern betrieben und ist über das Internet erreichbar. Auch der Auskunfts-Client ist eine Browser-basierte Webapplikation und ist in der äußeren Gestaltung und Funktionalität dem Pflege-Client sehr ähnlich, mit dem Unterschied, dass er nur lesende Zugriffe ermöglicht.

Die nachfolgenden Screenshots aus der Benutzeroberfläche zeigen das oberste Auswahlmenü mit den Hauptfunktionen sowie ein Beispiel für die Darstellung eines Suchergebnisses im Auskunfts-Client. Im Vergleich zu der in Abbildung 4 gezeigten Benutzeroberfläche des Pflege-Client fällt auf, dass er entsprechend seiner Aufgabe keine schreibenden Zugriffe zulässt. Zum Funktionsumfang des Auskunfts-Clients gehört ein integriertes Benutzerhandbuch.

Abbildung 8: Oberstes Auswahlmenü des Auskunfts-Clients

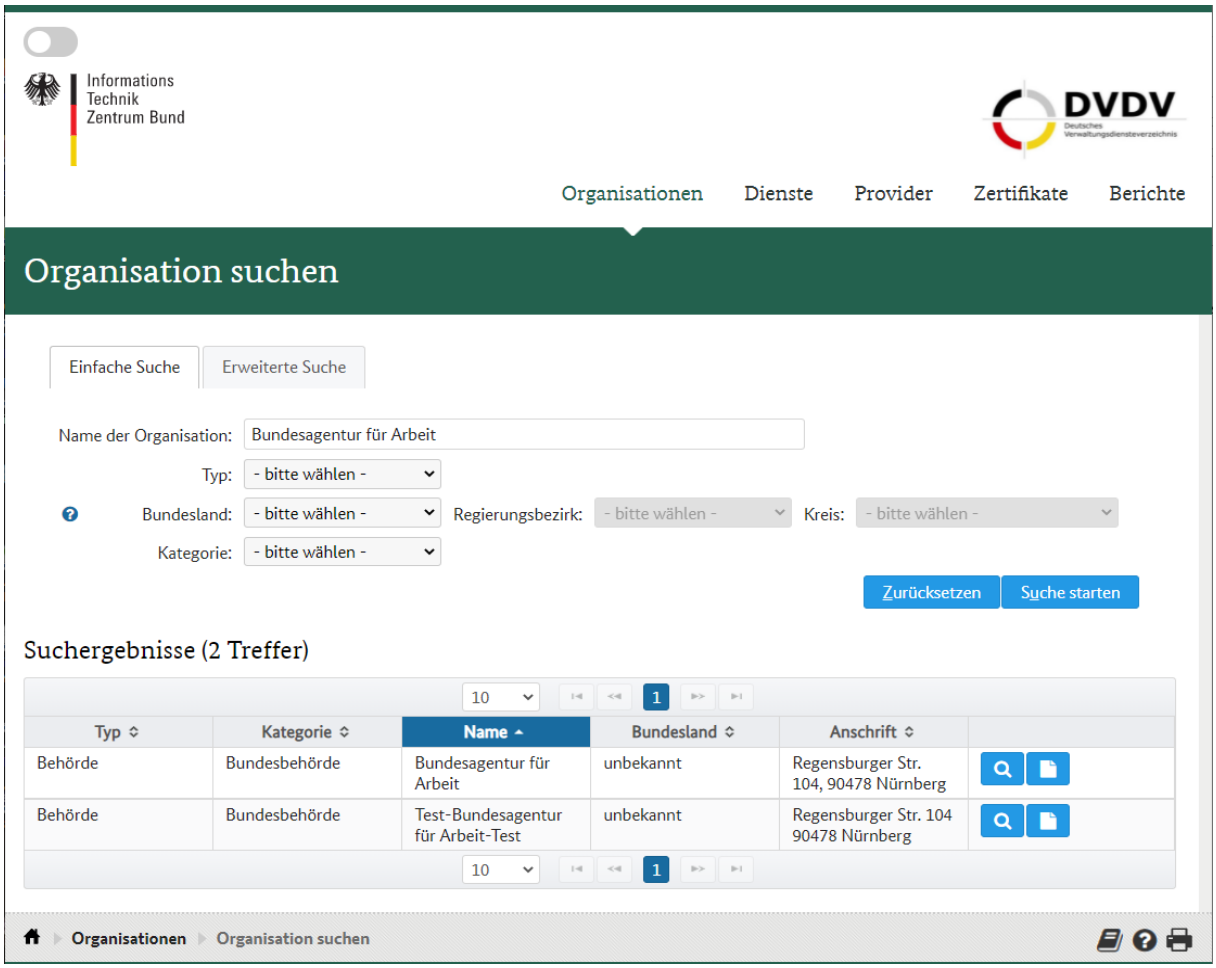

Abbildung 9: Benutzeroberfläche des Auskunfts-Clients

2.3.8 Legacy Facade

Eine weitere bei den DVDV-Servern betriebene Komponente ist die sog. „Legacy-Schnittstelle“ (auch „Legacy Facade“). Diese ermöglicht den anfragenden Fachverfahren bis auf Weiteres die Verwendung der bereits in DVDV 1 genutzten OSCI-Schnittstellen (siehe Kap. 3.4.1.1). Intern verwendet das Kernsystem von DVDV 2.0 bereits seit seiner Einführung im Oktober 2019 die Directory-Schnittstelle für die Datenanfragen; diese verwendet das HTTP-Protokoll. Details hierzu finden sich in Kap. 3.4.1.2

Die Legacy Facade sorgt dafür, dass die im OSCI-Format eingehenden Anfragen auf dem DVDV-Server intern auf die Directory-Schnittstelle umgesetzt werden. Damit wurde die Umstellung der DVDV-Komponenten von der Umstellung der Fachverfahren auf die neuen Schnittstellen entkoppelt. Die Fachverfahrenshersteller können in ihren Anwendungen die bisherigen Schnittstellen ohne Anpassung an DVDV 2.0 zunächst weiter nutzen. Langfristig erfolgt nach einer Umstellungszeit der Wechsel auf die neue Directory-Schnittstelle. Die Legacy Facade-Komponente wird dann nicht mehr betrieben.

3 Nutzung des DVDV

Dieses Kapitel beschreibt, welche Daten mit ihrer Struktur im DVDV verzeichnet sind, wie sie dort hingelangen und abgerufen werden können.

3.1 Datenstruktur

Die Architekturdokumentation beschreibt detailliert das dem DVDV zugrundeliegende, komplexe Datenmodell. Die nachfolgende Abbildung beschränkt sich aus Gründen der Übersichtlichkeit auf die Darstellung der wichtigsten Datenobjekte, ihre Felder und deren Bedeutung, soweit sie zum Verständnis des Gesamtsystems DVDV erforderlich sind.

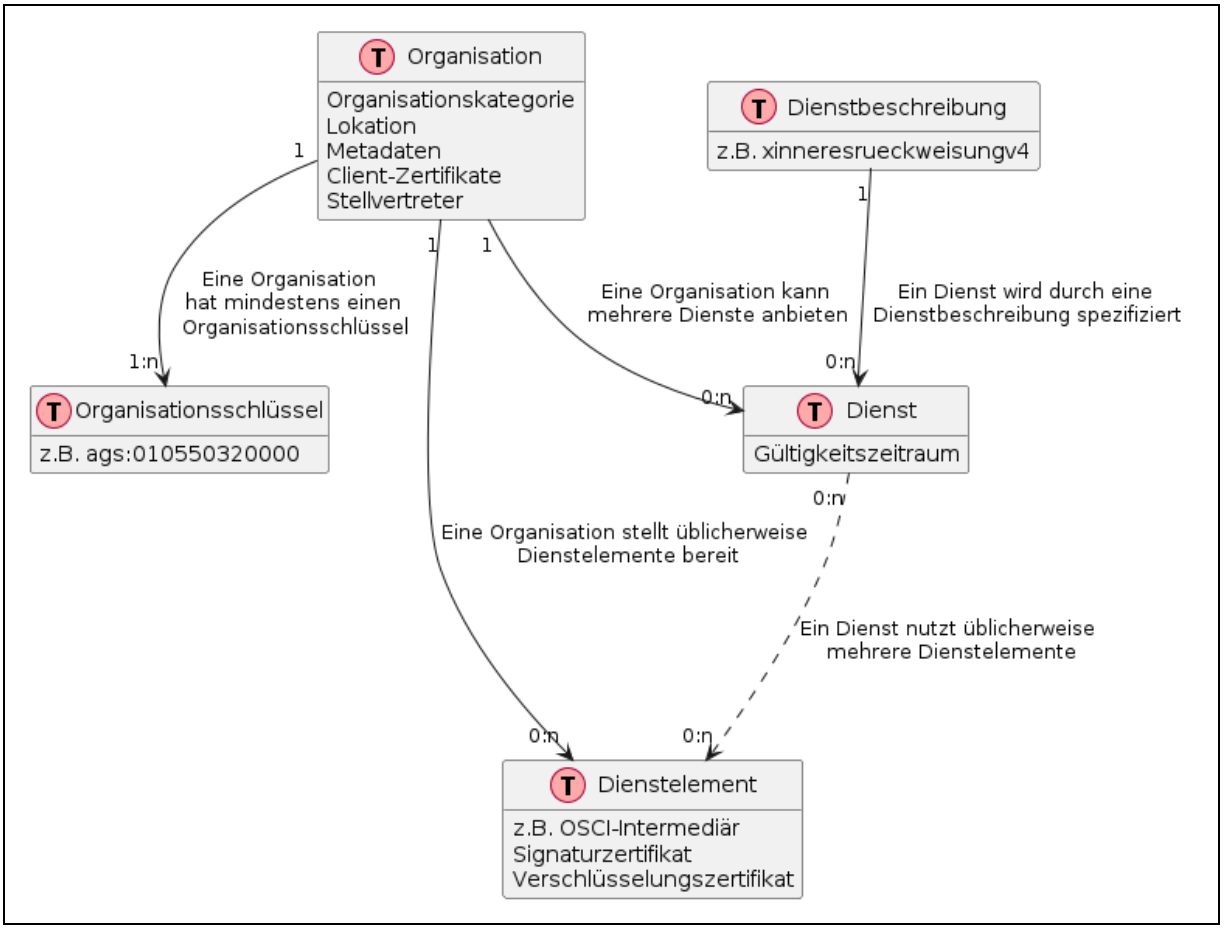

Abbildung 10: Daten im DVDV-Kernsystem

3.1.1 Organisationen

Unter „Organisationen“ werden im DVDV Behörden, Privatunternehmen sowie sonstige Organisationen verstanden, die hoheitliche Aufgaben übernehmen. Organisationen sind die Kommunikationspartner in den unterschiedlichen Fachszenarien, die Dienste anbieten und/oder verwenden („konsumieren“), die wiederum andere Organisationen anbieten. Zu diesem Zweck sind folgende Daten einer Organisation im DVDV hinterlegt:

- *Organisationskategorien* (siehe Kap. 3.1.1.1)
- *Lokation* der Organisation, d.h. die Zuordnung zu einem Bundesland und, falls vorhanden, zum Regierungsbezirk und Kreis, für den die Organisation tätig ist. Für Bundesbehörden oder Kreis-übergreifende Organisationen sind diese Angaben optional.

- *Metadaten,* z.B. der Name der Organisation, die Postadresse oder Felder mit Beschreibungstexten.
- *Client-Zertifikate* der Organisation, welche im DVDV-Kontext zur Authentifizierung der Organisation genutzt werden. Dies hat zwei Facetten:
  - „Standalone-Authentifizierung“ von DVDV-Anfragen (siehe Kap. 2.3.6): Eine Organisation, die mit Client-Zertifikaten im DVDV verzeichnet ist, kann diese verwenden, um sich für DVDV-Anfragen zu authentifizieren. Jede so verzeichnete Organisation ist damit zur Anfrage von DVDV-Daten berechtigt.
  - Autorisierung von Anfragen auf fachliche Dienste einer Organisation: Ein Dienstanbieter fragte dabei beim DVDV an, ob seine Organisationskategorie mit der Kategorie einer anfragenden Organisation übereinstimmt.
- *Stellvertreter von Organisationen.* Darunter werden im DVDV-Kontext spezielle Organisationen verstanden, die stellvertretend die Kommunikation für angeschlossene Organisationen übernehmen können. Je nach fachlichem Bereich werden Stellvertreter auch als „Clearingstelle“, „Vermittlungsstelle“ o.ä. bezeichnet. Ein Stellvertreter vertritt immer eine Reihe von im DVDV hinterlegten Organisationen. Daher ist für die Stellvertreter zusätzlich zu den Metadaten noch eine Liste von Referenzen auf die von ihnen jeweils vertretenen Organisationen hinterlegt.
- Zugeordneter *Organisationsschlüssel* (siehe Kap. 3.1.1.2)
- Zugeordnete *Dienste* und zugeordnete *Dienstelemente* (siehe Kap. 3.1.2)

3.1.1.1 Organisationskategorien

Den Organisationen und Dienstbeschreibungen werden im DVDV Organisationskategorien zugeordnet, die bis zu vier Ebenen tief verschachtelt und in einer festgelegten Baumstruktur aufgebaut sind. Die in einer übergeordneten Ebene getroffene Zuordnung einer Organisation bestimmt, welche Zuordnungen auf der jeweils darunterliegenden Ebene möglich sind.

Beispiele für Organisationskategorien der ersten Ebene sind etwa Behörde, Kammer, Portal, Privatwirtschaft usw. Auf der zweiten Ebene finden sich u.a. Bauaufsichtsbehörde, Finanzamt, Meldebehörde, Standesamt, Wohngeldbehörde etc. Die Zuordnung der obersten beiden Kategorien-Ebenen ist für sämtliche Organisationen obligatorisch, die Zuweisung einer dritten und vierten Ebene ist dagegen optional und wird derzeit in der Praxis auch nicht verwendet.

Änderungen an der Kategorienstruktur können bei Bedarf, z.B. bei der Aufnahme neuer Dienste in das DVDV, durch die Koordinierende Stelle DVDV über den Admin-Client (siehe Kap. 2.2.3) eingepflegt werden.

Im Downloadbereich der Koordinierende Stelle DVDV[4] findet sich eine aktuelle Übersichtsliste der Kategorien und Dienste.

3.1.1.2 Organisationsschlüssel

Jeder im DVDV verzeichneten Organisation wird zu ihrer Identifikation ein *Organisationsschlüssel* zugeordnet. Der Aufbau des Organisationsschlüssels variiert je nach Fachstandard und Organisationskategorie und wird in einem sog. „Eintragungskonzept“ definiert (siehe dazu Kap. 3.3.1). Ein Organisationsschlüssel setzt sich immer folgendermaßen zusammen:

- Ein vorangestelltes Präfix besteht i.d.R. aus drei Kleinbuchstaben (keine Umlaute) und identifiziert die Fachlichkeit und i.d.R. auch, d.h. die Organisationskategorie.
- Danach kommt als Trennzeichen ein Doppelpunkt „:“.

[4] siehe https://www.itzbund.de/DE/itloesungen/standardloesungen/dvdv/downloads/downloads.html

- Schließlich folgt die Organisations-ID als Abfolge von Ziffern, deren Anzahl und Bedeutung im jeweiligen Eintragungskonzept festgelegt wird.

Ein korrekter DVDV-Organisationsschlüssel ist zum Beispiel *ags:01055032.* Dieser Schlüssel steht tatsächlich für die Meldebehörde von Neustadt in Holstein. Das Präfix „ags“ stellt den Bezug zum Meldewesen her. Dessen Eintragungskonzept schreibt fest, dass für die nachfolgende ID der achtstellige amtliche Gemeindeschlüssel zu verwenden ist. Die ersten beiden Stellen des Gemeindeschlüssels bezeichnen dabei das Bundesland (hier „01“ für Schleswig-Holstein), die nächsten drei Stellen den Landkreis bzw. die kreisfreie Stadt, der die betreffende Gemeinde angehört (hier „055“ für den Kreis Ostholstein). In Bundesländern mit Regierungsbezirken kann dieser über die dritte Stelle des Gemeindeschlüssels identifiziert werden. Die sechste bis achte Stelle unterscheidet dann die Gemeinden innerhalb eines Landkreises (hier ist das die „032“).

Neue Organisationsschlüssel werden i.d.R. im Zusammenhang mit der Aufnahme neuer Fachlichkeiten bzw. Kommunikationsszenarien in das DVDV vergeben. Dazu ist vorher ein Antrag bei der Koordinierenden Stelle DVDV erforderlich, der nach Prüfung der Expertengruppe DVDV zur Entscheidung vorgelegt wird. Entscheidet sich die Expertengruppe DVDV für die Zulassung der neuen Fachlichkeit in das DVDV, ist für die Schlüsselvergabe die im Eintragungskonzept genannte Stelle („Dienstprovider“) verantwortlich.

Wichtiger Hinweis: Die hier verwendeten Organisationsschlüssel dienen nur zur Katalogisierung von Verfahrenskennungen im DVDV. Es handelt sich dabei keinesfalls um formale oder amtliche Behördenschlüssel der Behörden oder Verwaltungen in Deutschland.

Hier sei noch einmal auf die stets aktuelle Übersichtsliste der Dienste und Kategorien inklusive der vergebenen Präfixe im Downloadbereich der Koordinierenden Stelle DVDV verwiesen.

3.1.2 Dienste

3.1.2.1 Dienste und Dienstbeschreibungen

Dienste sind die zentralen Elemente der im DVDV verzeichneten Daten. Organisationen bzw. deren Stellvertreter bieten Dienste an oder fragen diese an („konsumieren“). Dienste sind im DVDV verzeichnet, um von angebundenen Systemen angefragt zu werden und sind damit der Kern des Deutschen Verwaltungsdiensteverzeichnis.

Im DVDV sind zu einem konkreten, von einer Organisation angebotenen Dienst alle Daten verzeichnet, die für die Dienstnutzung notwendig sind. Dies sind:

- Metadaten wie Name und Beschreibung,
- Verweis auf die zugehörige Dienstbeschreibung,
- angebundene Dienstelemente (siehe Kap. 3.1.2.2) und
- eindeutiger Dienstbezeichner.

Jeder konkret von einer Organisation im DVDV angebotene Dienst gehört zu einer bestimmten Dienstbeschreibung, die ihn eindeutig identifiziert und jede Dienstbeschreibung ist wiederum in der Regel mindestens einem Fachstandard zugeordnet, z.B. XBau, XFamilie, XInneres usw. Die Dienstbeschreibungen werden textlich in einem Eintragungskonzept (siehe Kap. 3.3.1) beschrieben und tragen häufig für Außenstehende mehr oder weniger kryptische Abkürzungen, z.B. *XBau22-ANZ-BH2BAB*, *xinneresrueckweisungv4* oder *xorganspende100passausweisstelle2ogr*. Einzelheiten hierzu finden sich in Kapitel 3.3.2.

3.1.2.2 Dienstelemente

Dienstelemente enthalten Informationen, die die Ausprägung eines Dienstes eindeutig beschreiben und den Dienstnutzern Verbindungsparameter zur Adressieren des Dienstanbieters liefern. Insbesondere sind dies konkrete Infrastrukturkomponenten, wie Intermediäre, URLs,

Zertifikate und Ähnliches. Ein Dienstelement wird immer von genau einer Organisation bereitgestellt. Diese bereitgestellten Dienstelemente können dann in beliebig vielen Diensten verwendet werden. Auch umgekehrt können Dienste grundsätzlich beliebig viele Dienstelemente benutzen, sofern diese in der entsprechenden Dienstbeschreibung vorgesehen sind. Sowohl Dienste als auch Organisationen (siehe Kap. 3.1.1) besitzen dazu im DVDV-Datenmodell Referenzen auf Dienstelemente.

Dienstelemente gibt es zum Zeitpunkt der Erstellung dieses Dokuments in den folgenden Ausprägungen:

- OSCI-Intermediär,
- OSCI-Empfänger,
- Signaturzertifikat,
- Verschlüsselungszertifikat,
- Text,
- Webserver,
- Bezahldienstserver,
- benutzerdefinierte Dienstelemente mit eigenem Namen und beliebigen Datenfeldern.

Weitergehende Informationen über die Verwendung von Zertifikaten in Dienstelementen finden Sie in Kap. 3.2.3.1.

3.2 Zertifikate

Dieses Kapitel informiert darüber, welche Arten von elektronischen Signaturen bzw. Zertifikaten bei den DVDV-Verfahrensbeteiligten zum Einsatz kommen. Es soll ferner ein Verständnis zur Funktionsweise von Zertifikaten im DVDV-Kontext vermitteln. Ein gewisses Grundverständnis zum Aufbau von X.509-Zertifikaten wird an dieser Stelle vorausgesetzt.

Im Rahmen des DVDV-Gesamtprozesses werden alle Informationen elektronisch übermittelt, dabei werden auch offene Netzwerke, wie das Internet, genutzt. Damit die zu übertragenden Daten sicher ausgetauscht werden können, sind definierte Standards einzuhalten. Zum einen müssen die Empfänger der Daten zweifelsfrei feststellen können, wer der Absender ist (Authentizität), zum anderen muss eine unbemerkte Manipulation oder Verfälschung der Daten durch die Beteiligten oder durch Dritte ausgeschlossen werden können (Integrität).

Aus diesem Grund werden alle Nachrichten, die die im DVDV verzeichneten Organisationen untereinander austauschen, mit Hilfe von verfahrensspezifischen Zertifikaten signiert und verschlüsselt.

In den nachfolgenden Abschnitten wird erläutert, wie die Kommunikation im Rahmen des DVDV abläuft, welche Sicherheitsmechanismen eingesetzt werden und welche Zertifikate an welcher Stelle benötigt werden.

3.2.1 Verfahrensbeteiligte

Im DVDV-Kontext werden verschiedene Verfahrensbeteiligte unterschieden:

- „*Organisationen*“ bzw. ihre *Stellvertreter* oder auch „*DVDV-Nutzer*“ sind alle Kommunikationspartner, die an einem elektronischen Datenaustausch teilnehmen, also Daten rechtssicher senden und empfangen.
- „*Provider*“ im Sinne von DVDV sind Institutionen, die zur Realisierung von Onlinediensten die notwendigen Infrastruktursysteme betreiben.[5] Bei einem Provider kann es sich handeln um…

[5] Bitte nicht verwechseln mit den „Dienstprovidern“, die für die Erstellung von Eintragungskonzepten verantwortlich sind und als Dienstbetreiber der jeweiligen Fachstandards fungieren (siehe Kap. 3.3.1).

  - den Betreiber einer oder mehrerer Clearingstellen,
  - ein kommunales Rechenzentrum, das die Infrastruktur für einen Teil der Organisationen bzw. ihrer Stellvertreter bereitstellt,
  - den Betreiber eines Intermediärs oder einer anderen Transport-Infrastrukturkomponente.
- „*Pflegende Stelle*“ sind für jedes Bundesland vorgesehen. Sie sind berechtigt, die Daten für das jeweilige Bundesland im Auftrag zu verändern (siehe Kap. 3.3.3).
- „*Abfrageberechtigte*“ bzw. „Data Consumer“ sind bspw. die Fachverfahren der DVDV-Nutzer, die ggf. unter Nutzung der DVDV-Bibliothek, Daten aus dem DVDV abfragen. Zu den Abfrageberechtigten zählen auch Personen, die über den Auskunfts-Client Daten einsehen können (siehe Kap. 2.3.7).

3.2.2 Verwendete Zertifikatstypen im DVDV

Folgende Zertifikatstypen werden im Kontext des DVDV-Gesamtsystems eingesetzt:

- *Software*-Zertifikate: Für den Nachrichtenaustausch werden spezielle Software-Zertifikate benötigt. Bei diesen Zertifikaten handelt es sich um fortgeschrittene Signaturen im Sinne der eIDAS-Verordnung, die zum Signieren und Verschlüsseln verwendet werden können. Der Verwendungszweck ist also vielfältig. Hierbei wird unterschieden in:
  - Personenbezogene Zertifikate und
  - Gruppen-/Funktions-Zertifikate.
- *TLS-Server-Zertifikate* Haupteinsatzgebiet von TLS (Transport Layer Security) ist das Internet, wenn beispielsweise eine verschlüsselte Verbindung zu einem Server aufgebaut werden soll. TLS-Serverzertifikate kommen vorrangig bei den Hauptkomponenten DVDV-Bundesmaster und DVDV-Server für die Absicherung der Verbindung zwischen Client und Server zum Einsatz. Eine tiefergehende Erläuterung zur Funktionsweise ist an dieser Stelle nicht vorgesehen.

Für beide Typen gilt der nachfolgende Zyklus eines Zertifikats:

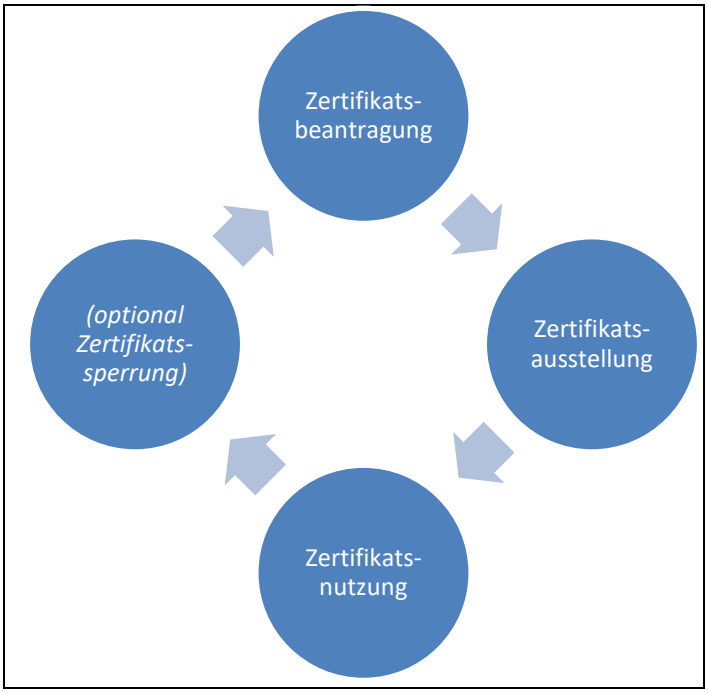

Abbildung 11: Zertifikatszyklus

Im Folgenden werden die einzelnen Phasen kurz beschrieben:

Phase	Beschreibung
Zertifikatsbeantragung	Der Antragsteller beantragt einen der beiden Zertifikatstypen bei einem Trustcenter. Hierzu gehört auch die Identifikation des Antragstellers gegenüber einer Registrierungsstelle im Auftrag des Trustcenters.
Zertifikatsausstellung	Das Trustcenter stellt nach erfolgreich Beantragung das Softwarezertifikat aus. Der Schlüsselverantwortliche kann sich das Schlüsselpaar (privater + öffentlicher Schlüssel) herunterladen.
Zertifikatsnutzung	Zur Zertifikatsnutzung gehört unter anderem das Signieren und Verschlüsseln von Nachrichten im DVDV-Kontext.
Zertifikatssperrung	Im Falle von Kompromittierung oder Diebstahl des privaten Schlüssels muss das Zertifikat vom Schlüsselverantwortlichen gesperrt werden.

Tabelle 2: Phasen des Zertifikatszyklus

Bei den Verfahrensbeteiligten kommen folgende Typen von Softwarezertifikaten zum Einsatz:

Verfahrensbeteiligte	personenbezogene Zertifikate	Gruppen- /Funktions-Zertifikate
Organisationen bzw. Stellvertreter		x
Provider		x
Pflegende Stellen	x	
Abfrageberechtigte		x

Tabelle 3: Verwendete Typen von Softwarezertifikaten

Wie der Tabelle zu entnehmen ist, werden im DVDV hauptsächlich Gruppen- bzw. Funktionszertifikate verwendet. Eingesetzt werden diese Zertifikate vor allem in Fachverfahren zum Ver- und Entschlüsseln von Fachnachrichten.

Zum einen werden die Zertifikate nicht nur von *einer* (natürlichen) Person verwendet und zum anderen dient das Zertifikat einer speziellen Funktion (z.B. Transport von Gewerbemitteilungen im OSCI-Kontext).

Pflegende Stellen nutzen im Gegensatz dazu immer personenbezogene Zertifikate, u.a. um die Nachweisbarkeit der von ihnen im DVDV durchgeführten Änderungen gewährleisten zu können.

3.2.3 Einsatz von Softwarezertifikaten im DVDV-Kontext

Im DVDV werden Softwarezertifikate entweder bei Dienstelementen oder bei Organisationen und deren Stellvertretern durch die Pflegenden Stellen hinterlegt.

3.2.3.1 Einsatz in Dienstelementen

Bei den in Kap. 3.1.2.2 aufgelisteten Dienstelementen kommen stellenweise ebenfalls Gruppen- bzw. Funktions-Softwarezertifikate zum Einsatz. Die relevanten Dienstelemente werden im Folgenden näher beschrieben:

Dienstelement	Beschreibung
OSCI-Empfänger	Das Zertifikat dient im Rahmen von OSCI-Transport zur Verschlüsselung der Auftragsdaten (sog. „innerer Umschlag“ bzw. ContentContainer). Hier wird unter anderem der öffentliche Schlüssel der Organisation bzw. des Organisations-Stellvertreters im DVDV hinterlegt.
OSCI-Intermediär	Bei diesem Dienstelement dient das Zertifikat zur Verschlüsselung der OSCI-Transport-Daten („äußerer Umschlag“). Die Entschlüsselung der Transport-Daten findet auf dem OSCI-Intermediär statt.
Verschlüsselungszertifikat	Dieses Zertifikat dient der Verschlüsselung der OSCI-Inhaltsdaten auf der Ebene XML Encryption und dient als zusätzliches Sicherheitsmerkmal.
Signaturzertifikat	Dieses Zertifikat wird benötigt, um die Authentizität von signierten Antworten eines fachlichen Dienstes verifizieren zu können. Die zusätzliche Signatur der Inhaltsdaten wird nicht für alle Kommunikationsszenarien benötigt. Ob sie im jeweiligen Dienst obligatorisch ist, legt der Dienst-Provider im Eintragungskonzept fest.

Tabelle 4: Einsatz von Software-Zertifikaten in Dienstelementen

3.2.3.2 Einsatz bei den Organisationen bzw. Organisations-Stellvertretern

Ein weiterer Einsatzbereich von Softwarezertifikaten im DVDV ist ihre Verwendung als sogenannte *Client-Zertifikate* zur Authentifizierung von Organisationen und Organisations-Stellvertretern. In Kap. 3.1.1 finden Sie dazu eine detaillierte Beschreibung.

3.2.4 Relevante DVDV-Prozesse

In diesem Abschnitt sollen die DVDV-Prozesse hinsichtlich ihrer Zertifikatsverwendung näher beleuchtet werden. Allgemein unterscheidet man folgende Teil-Prozesse:

- Pflege der Daten
- Replikation von Daten
- Anfrage an den DVDV-Server
- Übermittlung von Nachrichten

3.2.4.1 *Prozess „Pflege der Daten“*

Dieser Prozess stellt über Pflege- und -Admin-Client einen schreibenden Zugang auf den DVDV-Bundesmaster zur Verfügung.

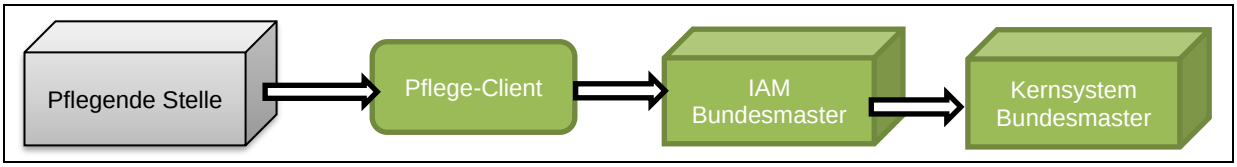

Abbildung 12: Prozess „Pflege der Daten“

Eine Pflegende Stelle ruft über einen Web-Browser die URL des Pflege-Clients auf und wird aufgefordert, sich mit ihrem personenbezogenen Softwarezertifikat zu authentifizieren.

Das funktioniert allerdings nur, sofern (u.a.) der öffentliche Teil dieses Zertifikats auf dem DVDV-IAM beim DVDV-Bundesmaster hinterlegt ist. Der private Schlüssel muss außerdem auf Client-Seite (also bei der Pflegenden Stelle) korrekt im Zertifikatsspeicher konfiguriert sein.

Nach erfolgreicher Authentifizierung und Anmeldung am Pflege-Client können Daten am Kernsystem des DVDV-Bundesmaster verändert werden.

3.2.4.2 *Prozess „Replikation von Daten“*

Änderungen am DVDV-Bundesmaster (Pflege der Daten) werden mittels MySQL-Replikation auf die angebundenen DVDV-Server repliziert (siehe Kap. 2.3.4). Die Replikation erfolgt über einen mittels TLS-Zertifikat abgesicherten Tunnel.

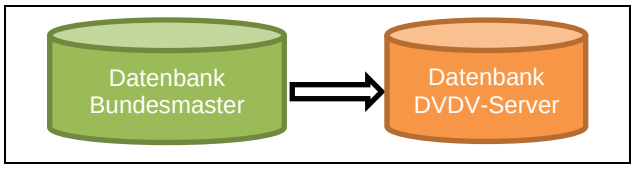

Abbildung 13: Prozess „Replikation von Daten“

3.2.4.3 *Prozess „Anfrage an den DVDV-Server“*

In diesem Prozess geht es um die Anfrage einer Organisation bzw. eines Organisations-Stellvertreters an den jeweils zuständigen DVDV-Server. Die anfragende Organisation erhält von dem DVDV-Server die aktuellen Transport-Parameter der gesuchten Empfänger-Organisation.

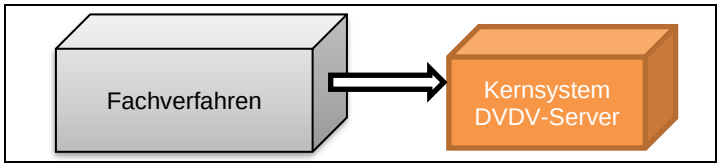

Abbildung 14: Prozess „Anfrage an den DVDV-Server“

Das Fachverfahren der anfragenden Organisation bzw. des Organisations-Stellvertreters kommuniziert mit dem Kernsystem des DVDV-Servers über eine abgesicherte TLS-Verbindung. Außerdem wird jede Anfrage mittels OAuth abgesichert. Nähere Details finden Sie in Kap. 3.2.5.

3.2.4.4 Prozess „Übermittlung von Nachrichten“

Mit Hilfe der vom DVDV-Server zurückgemeldeten Transportparameter generiert das anfragende Fachverfahren eine verschlüsselte Nachricht an die zuständige Transportinfrastruktur-Komponente der gesuchten Organisation. Derzeit handelt es sich dabei i.d.R. um Kommunikation mittels OSCI-Transport, das DVDV ist aber nicht auf diese allein festgelegt. Um einem gelegentlichen Missverständnis vorzubeugen: Das DVDV selbst ist nicht an der eigentlichen Nachrichtenübermittlung beteiligt, sondern liefert nur die notwendigen Parameter; die Nachrichtenübermittlung ist Aufgabe des Fachverfahrens der anfragenden Organisation.

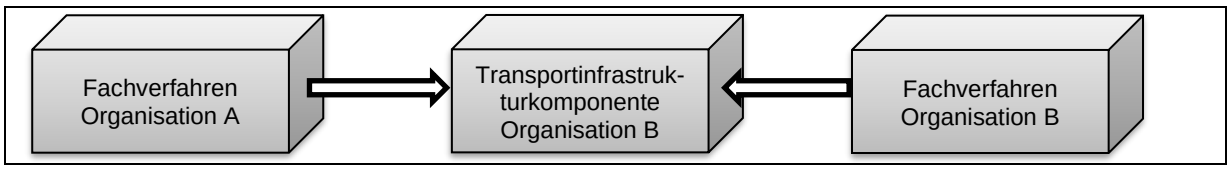

Abbildung 15: Prozess „Übermittlung von Nachrichten“

3.2.5 Detaillierter Blick auf den Prozess „Anfrage an den DVDV-Server“

Ergänzend zu den technischen Ausführungen in Kap. 3.4.1.2 soll an dieser Stelle der Ablauf zur Anfrage eines Fachverfahrens an den DVDV-Server nochmal Schritt für Schritt beschrieben werden.

Folgendes Szenario soll als Beispiel dienen: Das Standesamt von Musterstadt A übermittelt Todesfallbescheinigungen an eine Gesundheitsbehörde von Musterstadt B.

1. Das Fachverfahren des Standesamtes der Musterstadt A verwendet den lokal hinterlegten *privaten Schlüssel*, um sich mit Hilfe der DVDV-Bibliothek an der Token-Schnittstelle des zuständigen DVDV-Servers anzumelden.
2. Das Kernsystem des zuständigen DVDV-Servers sucht ein passendes Client-Zertifikat (*öffentlicher Schlüssel*) im replizierten Datenbestand.
3. Das Kernsystem findet ein passendes Client-Zertifikat des Standesamts der Musterstadt A. Aus Sicht des Kernsystems ist es an dieser Stelle unerheblich, an welcher Organisation dieses Client-Zertifikat durch die DVDV-Pflegende Stelle hinterlegt wurde. Entscheidend ist, dass es zum Fingerprint passt und noch nicht abgelaufen ist.
4. Das Kernsystem stellt einen Zugriffstoken aus und liefert diesen über die DVDV-Bibliothek an das Fachverfahren des Standesamtes der Musterstadt A zurück. Die Authentifizierung war erfolgreich.
5. Mit Hilfe des Tokens darf das Fachverfahren nun Abfragen beim jeweiligen DVDV-Server stellen und dort die benötigten technischen Parameter der Gesundheitsbehörde der Musterstadt B anfragen.
6. Mit den von der DVDV-Bibliothek zur Verfügung gestellten Methoden erhält das Fachverfahren die notwendigen Parameter und kann die Nachricht anschließend an den Empfänger versenden.

3.3 Eintragung von DVDV-Daten

Nach den weiter oben beschriebenen, wichtigen Datenobjekten soll folgend beschrieben werden, wie diese Daten in das DVDV gelangen.

Die Verzeichnung von Diensten und Organisationen im DVDV liegt in der Verantwortung der jeweiligen Fachlichkeit. Die fachlich zuständige Organisation stellt dazu in Abstimmung mit der Koordinierenden Stelle DVDV ein textuelles *Eintragungskonzept* für ihren Fachstandard sowie eine formale, technische *Dienstbeschreibung* für jeden einzelnen im DVDV verzeichneten

Diensttyp bereit. Die eigentliche Eintragung der Behörden und Organisationen, die die betroffenen Dienste für Anfragen bereitstellen, übernehmen dann die Pflegenden Stellen.

3.3.1 Eintragungskonzepte

Eintragungskonzepte beziehen sich in den meisten Fällen auf eine bestimmte Fachlichkeit (genauer: eine konkrete Version eines Fachstandards) und beschreiben textuell, wie die zugehörigen Dienste im DVDV verzeichnet werden sollen. Bei Fortschreibungen eines zugrundeliegenden Fachstandards sind entsprechende Update-Versionen der jeweils korrespondierenden Eintragungskonzepte erforderlich.

Verantwortlich für die Erstellung der Eintragungskonzepte sind die Dienstbetreiber des jeweiligen Fachstandards, im DVDV-Kontext auch als „Dienstprovider“ bezeichnet. Es ist durchaus üblich, dass der Dienstprovider einen geeigneten Dienstleister mit der Erstellung des Eintragungskonzepts beauftragt. Oftmals wird ein neuer Fachstandard zunächst im Rahmen eines Pilotierungsvorhabens erprobt, in dessen Verlauf auch eine erste Version des Eintragungskonzepts für das DVDV entsteht.

Neue bzw. aktualisierte Eintragungskonzepte müssen vor ihrer Verwendung freigegeben werden. In der Regel kontaktiert dazu der jeweilige Dienstprovider bereits in der Erstellungsphase die Koordinierende Stelle DVDV und klärt in einem iterativen Prozess die offenen Fragen. Anschließend wird das fertige Eintragungskonzept der Expertengruppe DVDV (siehe Kap. 4) zur Genehmigung vorgelegt.

Die DVDV-Eintragungskonzepte haben einen festgelegten Aufbau, der Antworten auf folgende Fragen liefern soll:

- *Fachliche Beschreibung des Dienstes:* Wer kommuniziert mit wem zu welchem Zweck?
- *Ausgangslage:* Fachliche Beschreibung des Vorhabens. Wie erfolgte die Kommunikation bisher? Gibt es gesetzliche Grundlagen / Fristen?
- *Standard:* Beruht das Vorhaben auf einem XÖV-Standard? Wenn ja: benennen und kurz ausführen, wenn nicht: Vorhaben näher beschreiben.
- *Systematik zur Vergabe der Organisationskategorien und Präfixe:* Werden neue Organisationskategorien benötigt? Welche bestehenden Kategorien kommen hier zum Einsatz? Jede neue Kategorie erfordert ein eindeutiges Präfix, bestehend aus möglichst drei Kleinbuchstaben.
- *Organisationsschlüssel-Systematik* (siehe auch Kap. 3.1.1.2): Kann eine bestehende Systematik verwendet werden? Alternativ ist darzustellen, dass durch die neue Systematik eine eindeutige Schlüsselvergabe sichergestellt werden kann. Hier werden auch Angaben dazu erwartet, wie die Daten in die entsprechende Codeliste im XRepository[6] gepflegt werden.
- *Dienste:* Beschreibung der Dienste inkl. der Dienstnamen sowie Nennung der zulässigen Dienstnutzer und –anbieter.
- *Zertifikate:* Angaben zu den Zertifikaten, die zum Einsatz kommen dürfen bzw. müssen.
- *Technische Aspekte:* Handelt es sich um synchrone oder asynchrone Nachrichtenübertragungen? Erfolgt die Datenübermittlung per OSCI?
- *Organisatorische Aspekte:* Der Dienst-Provider (fachlich zuständige Stelle) ist mit Behörde, Ansprechpartner, E-Mail (Postfach) und Telefonnummer zu benennen.

[6] Die Plattform *XRepository* (https://www.xrepository.de/) wird im Auftrag des IT-Planungsrats durch die Koordinierungsstelle für IT-Standards (KoSIT) betrieben und stellt allen eGovernment-Vorhaben eine verlässliche Drehscheibe zur Bereitstellung und zum Bezug XÖV-konformer Standards und Codelisten zur Verfügung.

- *Pflegende Stellen:* Übernehmen alle im DVDV-Kontext benannten Pflegenden Stellen oder einzelne, konkret zu benennende Pflegende Stellen die Pflege der Daten im DVDV?
- *DVDV-Server:* Soll auf alle DVDV-Server oder nur auf einzelne, konkret zu benennende DVDV-Server lesend zugegriffen werden?
- *Intermediäre:* Sollen nur bestimmte Intermediäre verwendet werden dürfen oder sind diese frei wählbar?

Die Koordinierende Stelle DVDV stellt in ihrem Downloadbereich[7] eine stets aktuelle Übersichtsliste der Dienste bereit, die auch sämtliche aktuell genutzten Kategorien, vergebenen Präfixe und die jeweils zuständigen Dienstprovider enthält.

Bei neu hinzukommenden Diensten informiert die Koordinierende Stelle DVDV nach deren Bereitstellung per Mail alle Pflegenden Stellen DVDV. Dazu gehören insbesondere die Informationen über Dienstname, Fachstandard und Version, Gültigkeitszeitraum (gültig ab, gültig bis), Präfix und Kategorie (siehe Kap. 3.1.1.2 bzw. 3.1.1.1), Detailinformationen zum Dienstanbieter sowie Informationen, ob der Dienst bundesweit verbindlich oder optional ist.

3.3.2 Dienstbeschreibungen

Neben dem Eintragungskonzept ist zusätzlich eine rein technische, formale Spezifikation jedes im DVDV verwendeten Dienstes erforderlich, die sog. „Dienstbeschreibung“. Die Dienstbeschreibung wird von den Dienstprovidern an die Koordinierende Stelle DVDV geliefert. Derzeit wird hierfür die Beschreibungssprache Web Service Description Language (WSDL[8]) verwendet. Dazu gib es eine DVDV-spezifische Erweiterung, die die Abbildung aller für OSCI-Transport erforderlichen Parameter ermöglicht.

Die Dienstbeschreibung liefert in der WSDL-Struktur Informationen über:

- Namen, HTML-Beschreibung und Kategorie(n) des zu beschreibenden Dienstes,
- Datenstrukturen der Inhaltsdaten (XML-Schema),
- Aufbau der zu übermittelnden Nachrichten,
- Schnittstellen zum Nachrichtenaustausch,
- Bindung von Protokoll und Schnittstellen inkl. der zu verwendenden Zertifikate,
- Operationen zum Nachrichtenaustausch,
- Endpunkte des Dienstes, z.B. zuständige OSCI-Intermediäre, Zertifikate,
- Hinweise zum Dienstanbieter.

Ganz besonders wichtig sind dabei die Angaben zu den obligatorischen und optionalen Dienstelementen, etwa Intermediären und Zertifikaten sowie die am Anfang der WSDL im Segment „Documentation“ untergebrachte HTML-Dienstbeschreibung. Anhand des Namens und des definierten „targetNamespace“ kann jede Dienstbeschreibung eindeutig identifiziert werden.

Die WSDL-Datei mit einer oder mehreren Dienstbeschreibungen wird über den Admin-Client (siehe Kap. 2.2.3) im DVDV hinterlegt und in die DVDV-Datenstruktur übernommen. Sobald dies erfolgt ist, generiert das DVDV daraus die Liste der für einen Diensttypen notwendigen Dienstelemente (siehe Kap. 3.1.2.2) sowie den Hilfetext für den Pflege-Client (siehe Kap. 2.2.2). Anschließend können die Pflegenden Stellen diese neuen oder geänderten Diensttypen verwenden und im Rahmen der Datenpflege den Organisationen zuordnen, die Dienste dieses Typs anbieten.

Wegen ihrer großen Bedeutung im DVDV-Kontext finden sich im Anhang 1 das Schema der DVDV-WSDL-Erweiterung, ein darauf basierendes Template für eine OSCI-WSDL-Dienstbe-

[7] siehe https://www.itzbund.de/DE/itloesungen/standardloesungen/dvdv/downloads/downloads.html

[8] WSDL ist eine Plattform-, Programmiersprachen- und Protokoll-unabhängige, XML-basierte Beschreibungssprache des W3C für Webservices und dient zum Austausch von XML-Nachrichten.

schreibung sowie als Beispiel die WSDL eines konkreten XÖV-OSCI-Dienstes. Über die Koordinierende Stelle DVDV kann bei Interesse ein Template für eine derartige Dienstbeschreibung im WSDL-Format bezogen werden.[9]

Prinzipiell sind auch andere Formate für die Dienstbeschreibungen möglich, was im Einzelfall geprüft werden muss.

3.3.3 Pflegende Stellen

Während die Bereitstellung von neuen Diensten im DVDV Aufgabe der Koordinierenden Stelle DVDV ist, erfolgt die Neuanlage, Änderung oder Löschung von Diensten bzw. der Dienst-anbietenden Organisationen ausschließlich durch die Pflegenden Stellen. Nur diese sind berechtigt und technisch in der Lage, Änderungen am DVDV-Datenbestand durchzuführen.

Die Tätigkeiten und die Zusammenarbeit der Pflegenden Stellen der Länder sind grundsätzlich in einer von der Koordinierenden Stelle DVDV herausgegebenen Policy festgelegt. Im Detail gestalten sich die Abläufe aufgrund der föderalen Struktur des DVDV nicht immer einheitlich, da es unterschiedliche landesspezifische Regelungen und Beauftragungen gibt, die beachtet werden müssen.

Jedes Bundesland bestimmt genau eine Stelle, deren Mitarbeiterinnen und Mitarbeiter für die Pflege der Organisationen und Dienste dieses Bundeslands verantwortlich sind. Es ist damit sichergestellt, dass jeder Organisationseinheit auf Kommunal- und Landesebene im DVDV eine zuständige Pflegende Stelle zugeordnet ist. Dabei kann es durchaus sein, dass mehrere Bundesländer dieselbe Pflegende Stelle nutzen, z.B. Dataport für die Länder Bremen, Hamburg, Sachsen-Anhalt und Schleswig-Holstein.

Bei der Pflege bundesweit zuständiger Organisationseinheiten, wie der Bundesdruckerei, dem Kraftfahrtbundesamt, dem Bundesamt für Migration und Flüchtlinge usw., ist entscheidend, in welchem Bundesland die Organisation ihren (Haupt-)Sitz hat. Beispielsweise ist für den Beitragsservice ARD ZDF Deutschlandradio die Pflegende Stelle von Nordrhein-Westfalen zuständig, da der Beitragsservice in Köln residiert.

Funktional erfolgt die Dienst-Pflege mit Hilfe des in Kapitel 2.2.2 beschriebenen Pflege-Client.

3.4 Anfrage der Daten am DVDV

Nachdem es in den vorangegangenen Kapiteln darum ging, welche Daten im DVDV verzeichnet sind und auf welchem Weg sie dort hinkommen, soll es folgend um die Berechtigung und die Methoden zum „Konsum“ der Daten gehen.

3.4.1 Schnittstellen der DVDV-Server

Mit Ausnahme der Anfragen aus dem Auskunfts-Client (siehe Kap. 2.3.7), stammen sämtliche Anfragen aus entsprechenden DVDV-Clients eines bei der anfragenden Organisation verwendeten Fachverfahrens. Die Fachverfahrens-Clients müssen eine der beiden angebotenen Schnittstellen unterstützen:

- Bereits seit DVDV 1 wird eine *OSCI-Schnittstelle* verwendet. Dabei werden die Anfragen im OSCI-Format an einen dafür designierten OSCI-Intermediär geschickt, der sie über die sog. Legacy Facade (siehe Kap. 2.3.8) an den zuständigen DVDV-Server weiterleitet und die Rückantwort wiederum im OSCI-Format bereitstellt. Diese Schnittstelle wird nur noch für eine begrenzte Zeit unterstützt. Weitere Details finden sich in Kap. 3.4.1.1.

[9] Die Koordinierungsstelle für IT-Standards (KoSIT) stellt mit dem *XGenerator* ein Werkzeug zur automatisierten Prüfung von XÖV-Fachmodellen und zur Erzeugung der zu einem XÖV-Standard gehörenden Bestandteile bereit. Siehe https://www.xoev.de/xoev/xoev-produkte/xgenerator-11551

- Seit Sommer 2022 gibt es parallel zur OSCI-Schnittstelle auch die performantere sog. *Directory-Schnittstelle*. Hier werden die Anfragen von den Fachverfahrens-Clients direkt an die zuständigen DVDV-Server gerichtet und von diesen ohne Umweg über eine Legacy Facade-Komponente oder einen OSCI-Intermediär beantwortet. Weitere Details finden sich in Kap. 3.4.1.2.

Die OSCI-Schnittstelle wurde 2023 abgekündigt, d.h. nach einer Umstellungsphase wird nur noch die Directory-Schnittstelle unterstützt werden. In der Zwischenzeit werden beide Schnittstellen von den DVDV-Servern parallel angeboten, was den Fachverfahrensherstellern Zeit geben soll, ihr jeweiliges Produkt umzustellen und im Rahmen des üblichen Release-Zyklus ein aktualisiertes Update an die Kunden - die anfragenden Organisationen - auszuliefern.

3.4.1.1 OSCI-Schnittstelle

Bereits seit 2007 werden Anfragen an das DVDV über die OSCI-Schnittstelle gesendet. Der Fachverfahrens-Client richtet dabei Anfragen im OSCI-Nachrichten-Format an einen vom DVDV-Server-Betreiber bereitgestellten OSCI-Intermediär, der sie an das Kernsystem des DVDV-Servers (siehe Kap. 2.3.8 und 2.3.6) weiterleitet. Damit die anfragenden Fachverfahrens-Clients diese Methode auch nach der Umstellung auf DVDV 2.0 im Jahr 2019 weiter nutzen konnten, wurde seinerzeit die Legacy Facade implementiert, die die „Übersetzungsarbeit“ zwischen Fachverfahren und Kernsystem erledigt. Tatsächlich nutzt die Legacy Facade bereits seit 2019 systemintern die Directory-Schnittstelle (siehe Kap. 2.3.8). Seit 2022 ist die Directory-Schnittstelle auch direkt für Fachverfahren erreichbar.

OSCI sieht standardmäßig eine Transportverschlüsselung vor, daher werden Anfrage und Antwort verschlüsselt übertragen. Zur Absicherung des Dialoges kommen zudem Verschlüsselungen im Rahmen des Challenge/Response-Verfahrens von OSCI-Transport zum Einsatz.

Grundsätzlich kann jedes Fachverfahren Anfragen über die OSCI-Schnittstelle an einen DVDV-Server stellen. Aus diesem Grund kann der DVDV-Server die anfragenden Fachverfahrens-Clients nicht kennen und auch keine Authentizitätsprüfungen vornehmen; Anfragen werden daher nicht elektronisch signiert. Aus Sicht des anfragenden Fachverfahrens stellt der DVDV-Server eine vertrauenswürdige Instanz dar. Um die Integrität und Authentizität des Antwortdokumentes zusichern zu können, werden die XML-Dokumente auf Ebene der Inhaltsdaten vom DVDV-Server signiert. Da die Antwort-Dokumente die Daten der Anfragen mit beinhalten, ist dem anfragenden Fachverfahrens-Client garantiert, dass er die zur Anfrage passende Antwort erhalten hat.

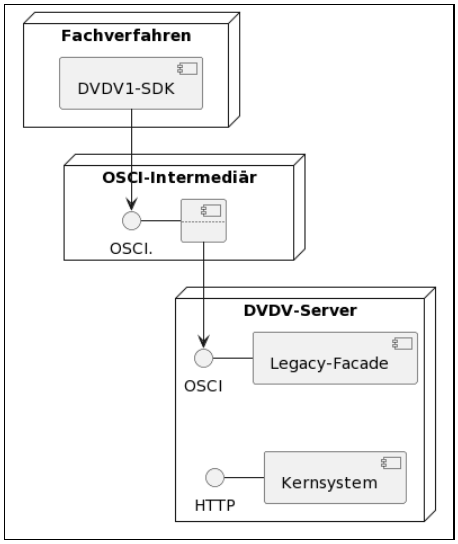

Abbildung 16: Anfragen über die OSCI-Schnittstelle

Die anfragenden Fachverfahrens-Clients müssen mit ihrem sog. Client-Zertifikat auf dem Intermediär verzeichnet sein. Durch dieses werden sie authentifiziert, wenn sie mit dem Intermediär kommunizieren, etwa um die in ihrem Intermediärs-Postfach eingegangenen Nachrichten mit den Rückantworten des DVDV-Systems abzurufen.

3.4.1.2 Directory-Schnittstelle

Seit 2022 können Fachverfahrens-Clients für ihre Anfragen an das DVDV alternativ zur OSCI-Schnittstelle auch die Directory-Schnittstelle (z.T. auch „REST-Schnittstelle genannt) nutzen, die sich direkt am Kernsystem des DVDV-Servers befindet. Damit entfällt die Notwendigkeit zur Nutzung eines OSCI-Intermediärs. Für den Zugriff auf die Directory-Schnittstelle wird das HTTP-Protokoll[10] verwendet. Die dafür erforderliche DVDV-Bibliothek (siehe Kap. 3.4.2) kann kostenlos über das Entwicklungsportal der FITKO[11] bezogen und durch Fachverfahrenshersteller in ihren Produkten verbaut werden.

Voraussetzung der praktischen Nutzung der Directory-Schnittstelle im Echtbetrieb ist die Freigabe durch den jeweiligen DVDV-Server-Betreiber. Nach einer definierten Übergangszeit, in der die Fachverfahren von deren Herstellern umzustellen sind, werden die Legacy Facade-Komponenten an allen DVDV-Servern abgeschaltet und das DVDV nimmt nur noch HTTP-Anfragen über die Directory-Schnittstelle entgegen.

Anfragen über die Directory -Schnittstelle sind mit dem OAuth-Protokoll abgesichert und erfordern stets die Authentifizierung des jeweiligen DVDV-Nutzers mit Hilfe eines Tokens, welches die DVDV-Nutzer über die *Tokenausgabe-Schnittstelle des Kernsystems* auf jedem DVDV-Server beziehen können (sog. „Standalone-Authentifizierung“).

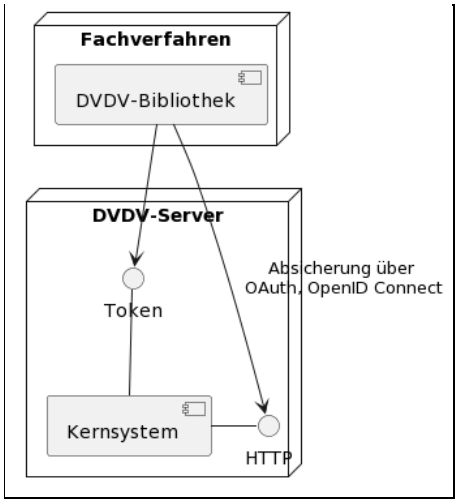

Abbildung 17: Anfragen über die Directory-Schnittstelle

Als Alternative zur Authentifizierung am Kernsystem wurde auch eine Tokenausgabe-Schnittstelle am zentralen DVDV-IAM des DVDV-Bundesmasters (siehe Kap. 2.2.4) implementiert, die jedoch bislang in der Praxis wenig Relevanz hat, da die Standalone-Authentifizierung aufgrund des verteilten Betriebs zu bevorzugen ist.

3.4.2 DVDV-Bibliotheken

Um die Softwareentwickler von Fachverfahren oder Anwendungsprogrammen bei der Integration von Anfragen über die OSCI-Schnittstelle an das DVDV zu unterstützen, werden für beide

[10] Die Directory-Schnittstelle nutzt das HTTP-Protokoll und unterstützt eine TLS-Verschlüsselung (Transport Layer Security). Nach Vorgabe im Betriebshandbuch ist die Directory-Schnittstelle durch den Betreiber des DVDV-Servers mit einem TLS-Zertifikat abzusichern, so dass in der Praxis ein https-Endpunkt angeboten wird.

[11] Sie finden den Einstieg zum DVDV-Entwicklungsportal der FITKO unter: https://docs.fitko.de/dvdv/register

Schnittstellen DVDV-Bibliotheken bereitgestellt. Diese bieten Funktionalitäten in Form von Klassen und -Methoden, um möglichst komfortabel Anfragen an das DVDV zu formulieren und dessen Antworten auszuwerten. Die Bibliotheken entlasten die Softwareentwickler, so weit möglich, von der Entwicklung der Kommunikationsinfrastruktur oder Nachrichtenformaten. Es werden sowohl Einzelanfragen als auch eine Stapel-Verarbeitung unterstützt.

Die DVDV-Bibliotheken können entweder als direkt nutzbare Programmierschnittstelle unverändert verwendet werden oder die Quellen der Implementierung können ganz oder in Teilen als Muster für die eigene Integrationsprogrammierung dienen. Die Programmierschnittstellen machen keine Vorgaben hinsichtlich der Laufzeit-Architektur der nutzenden Programme.

Die Bibliotheken können zusammen mit der erforderlichen Dokumentation sowie einigen Beispielen kostenlos über das Entwicklungsportal der FITKO bezogen werden.

3.4.2.1 Bibliothek für die OSCI-Schnittstelle

Die Kommunikation von Fachverfahren oder Anwendungsprogrammen mit der OSCI-Schnittstelle des DVDV erfolgt über OSCI-Transport 1.2. Zu diesem Zweck stützt sich die DVDV-Bibliotheksimplementierung auf die OSCI-Bibliothek der IT-Planungsratsanwendung Governikus.[12]

SDK mit der DVDV-Bibliothek zur Nutzung der OSCI-Schnittstelle sind für Java und .Net-Umgebungen verfügbar. Sie unterstützen drei definierte Anfragen an das DVDV, nämlich:

- *find.ServiceDescription:* Diese DVDV-Anfrage dient dazu, alle notwendigen Informationen zu ermitteln, die ein anfragender Fachverfahrens-Client benötigt, um den angebotenen Dienst einer Behörde nutzen zu können. Primär sind dies technische Verbindungsparameter, wie Netzwerkadressen und Zertifikate der Infrastruktursysteme, aber ggf. auch Schemata zu Inhaltsdaten, Anforderungen an das Signaturniveau usw.
- *find.AuthorityDescription:* Mit Hilfe dieser Anfrage erhält ein Fachverfahrens-Client nähere Informationen zu einer im DVDV verzeichneten Organisation, z.B. allgemeine Daten zu der Behörde und deren Stellvertretern, wie Name, postalische Anschrift, Behördenschlüssel und identifizierende Client-Zertifikate sowie eine Auflistung aller von der Behörde und deren Stellvertretern angebotenen Diensten.
- *verify.Category:* Diese Anfrage wird von Fachverfahrens-Clients in der Rolle Dienstanbieter gestellt, d.h. von Behörden, die einen fachlichen Dienst implementiert und im DVDV publiziert haben. Mit Hilfe der *verifyCategory*-Anfrage kann ein Dienstanbieter überprüfen lassen, ob das den Dienst anfragende Fachverfahren einer bestimmten Behördenkategorie zugeordnet ist (siehe auch Kap. 3.1.1.1) und damit eine Autorisierungsentscheidung stützen.

Alle drei genannten Anfragen sind vom DVDV-Server implementiert als OSCI-Transport-Services des Kommunikationstyps *request/response*. Sowohl die Anfrage als auch die Antwort werden in Form von XML-Dokumenten als Inhalt eines OSCI-Inhaltcontainers transportiert.

3.4.2.2 Bibliothek für die Directory-Schnittstelle

Auch für die Nutzung der Directory-Schnittstelle wird den Softwareentwicklern von Fachverfahren oder Anwendungsprogrammen eine DVDV-Bibliothek in den Varianten Java und .Net angeboten. Sie wird zusammen mit einer Dokumentation und lauffähigen Beispielen zur Nutzung veröffentlicht. In der Bibliothek sind die folgenden Features umgesetzt:

- *Authentifizierung* entweder am DVDV-IAM/Keycloak (siehe Kap. 2.2.4) oder direkt am DVDV-Server mittels zertifikatbasierter Authentifizierung

[12] https://www.governikus.de/service/osci-bibliothek/

- *Failover* (Vertreterregelung) zur Nutzung von mehreren DVDV-Servern. Ist ein Server nicht erreichbar, dann wird der nächste Server in der Kette verwendet. In regelmäßigen Abständen wird die Erreichbarkeit des primären Servers erneut geprüft und auf diesen zurückgeschwenkt, sobald die Verbindung wieder etabliert ist. Details zur Vertreterregelung finden sich in Kap. 2.3.1.
- Aufruf der nachfolgend beschriebenen *Anfragen* an das DVDV und Aufbereitung der Antworten in einem dedizierten Datenmodell.

Folgende DVDV-Anfragen können am Interface „DVDVManager“ der DVDV-Bibliothek verwendet werden:

- *findOrganizationDescription:* Diese DVDV-Anfrage dient der Suche nach einer Organisation oder einem Stellvertreter mit Hilfe von Organisationsschlüssel und Kategorie der gesuchten Organisation. Sie ist vergleichbar mit der Methode *find.AuthorityDescription* aus dem DVDV-SDK, Kap. 3.4.2.1.
- *findServiceDescription:* Mit Hilfe dieser DVDV-Anfrage kann über den Organisationsschlüssel und die URI der Dienstbeschreibung nach einem Dienst zu einer Organisation gesucht werden. Sie ist vergleichbar mit der entsprechenden Methode *find.ServiceDescription* aus dem DVDV-SDK.
- *verifyCategory:* Diese Anfrage wird zur Überprüfung verwendet, ob das einen Dienst anfragende Fachverfahren einer bestimmten Behördenkategorie zugeordnet ist. Sie ist vergleichbar mit der Anfrage *verify.Category* aus dem DVDV-SDK.
- *findCategories:* Diese Anfrage dient der Ermittlung der Kategorie einer Organisation oder eines Stellvertreters durch Angabe des Organisationsschlüssels und des Fingerprints eines Client-Zertifikats. Zurückgegeben wird eine Liste der Kategorien der gefundenen Organisation bzw. ihrer Stellvertreter.
- *findOrganizationsByServiceElement:* Diese Anfrage dient zur Suche nach Organisationen anhand bestimmter Eigenschaften eines ihrer Dienstelemente.
- *findCertificateByFingerprint:* Die letzte Anfrage liefert bei Angabe des Fingerprints eines Zertifikats das zugehörige, im DVDV hinterlegte Zertifikat.

3.4.3 DVDV-Nutzer

3.4.3.1 anfrageberechtigte Organisationen

Grundsätzlich sind alle Behörden der deutschen öffentlichen Verwaltung auf Bundes-, Länder- und Kommunalebene zur Nutzung des DVDV berechtigt, also auch zur Anfrage der dort hinterlegten Daten.

Neben den o.g. Organisationen aus der öffentlichen Verwaltung sind auch Unternehmen unabhängig von ihrer Rechtsform als juristische Personen nutzungsberechtigt, wenn mindestens eine der folgenden Bedingungen zutrifft:

- Es existiert eine gesetzliche Grundlage, aus der hervorgeht, dass das Unternehmen mit der Erfüllung hoheitlicher Aufgaben betraut, beliehen oder verpflichtet ist.
- Das Unternehmen wird zu mindestens 50% aus Mitteln der öffentlichen Hand finanziert.
- Im Rahmen der OZG-Umsetzungen und Bereitstellung von LeiKa-Leistungen kann in begründeten Ausnahmefällen von dieser Regelung abgewichen werden, sofern die Expertengruppe DVDV (siehe Kap. 4) dies beschließt.

3.4.3.2 Clearingstellen

In vielen Fällen laufen die DVDV-Anfragen über sog. Clearingstellen. Das sind Dienstleister, die im Auftrag ihrer Kunden, meist Organisationen aus der Öffentlichen Verwaltung, als zentrale Vermittlungsstelle („Nachrichtenbroker“) handeln. Sie unterstützen, bündeln und optimieren die Kommunikationsvorgänge der Fachverfahren ihrer Auftraggeber sowohl in technischer als auch organisatorischer Hinsicht.

Zu den Aufgaben einer Clearingstelle gehören allgemein:

- Bereitstellung von sicheren Kommunikationsdiensten,
- Daten- und Formatkonvertierungen,
- Anbindung von Verzeichnisdiensten, wie etwa dem DVDV,
- Routing in verteilten DV-Verbünden.

Die Clearingstellen wirken aber auch entgegengesetzt in Richtung derjenigen im DVDV verzeichneten Organisationen, die Dienste bereitstellen. Hier haben die Clearingstellen die Aufgabe, die technische Erreichbarkeit der angefragten Dienste ihrer Auftraggeber innerhalb standardisierter Informationsverbünde sicherzustellen und eingehende Anfragen ggf. zu konvertieren und im Zielformat an die angefragte Organisation zu routen.

3.4.3.3 Fachverfahrenshersteller

Zur Unterstützung der Fachverfahrenshersteller bei der Implementierung passender Clients werden vom DVDV die in Kap. 3.4.2 beschriebenen Bibliotheken kostenlos bereitgestellt und sind über die Koordinierende Stelle DVDV zu beziehen:

- für die OSCI-Schnittstelle je eine Bibliothek für .Net und Java,
- für die Directory-Schnittstelle je eine Bibliothek für .Net und Java.

Es ist die Aufgabe der Fachverfahrenshersteller, in ihren Produkten etwaige Änderungen der Schnittstellen anzupassen. Für die OSCI-Schnittstelle hat sich die Änderungshäufigkeit zuletzt auf ca. ein neues SDK-Release pro Jahr eingependelt. Für die neue Directory-Schnittstelle ist perspektivisch von einem ähnlichen Release-Zyklus auszugehen.

3.4.4 DVDV-Testsystem

Um die Nutzung des DVDV weiter zu fördern und technische Hindernisse zur Verknüpfung mit anderen Systemen so früh wie möglich auszuräumen, hat das DVDV-Produktmanagement die Einrichtung eines DVDV-Testsystems bei der Governikus GmbH & Co. KG beauftragt. Dieses kann grundsätzlich kostenlos genutzt werden, befindet sich technisch stets auf dem aktuellsten Versionsstand und bietet den Zugriff sowohl per OSCI- als auch über die Directory-Schnittstelle (siehe Kap. 3.4.1) an.

Das DVDV-Testsystem richtet sich primär an Fachverfahrenshersteller und soll die Erprobung der Anbindung ihrer Anwendungen an das DVDV in einer geschützten Umgebung und ohne Beeinträchtigung des operativen Betriebs ermöglichen. Berechtigt zur Nutzung des DVDV-Testsystems sind alle Organisationen, die bereits auf das operative DVDV zugreifen oder künftig zugreifen wollen, insbesondere Hersteller von Fachverfahren.

Die Koordinierende Stelle DVDV gilt als erste Anlaufstelle und regelt den organisatorischen Zugang zum DVDV-Testsystem.

4 DVDV-Aufbauorganisation

In den vorangegangenen Kapiteln ging es um den Aufbau des DVDV als Gesamtsystem und auf Komponentenebene sowie um die Strukturierung, Pflege und die Anfrage von Daten. Das Dokument soll mit einer Darstellung der verschiedenen Akteure schließen, welche die übergeordnete Produktverantwortung tragen und die kontinuierliche Weiterentwicklung sicherstellen.

Produktmanagement DVDV

Das Produktmanagement für das DVDV liegt bei der Föderalen IT-Kooperation AöR (FITKO). Zu seinen Aufgaben gehören 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.

Koordinierende Stelle DVDV

Die Koordinierende Stelle DVDV (KS) 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 die Mitglieder der Expertengruppe DVDV, für Pflegende Stellen, für DVDV-Serverbetreiber, für Fachverfahrensverantwortliche und für die Auftragnehmer.

Fachgruppe DVDV

Der Bund und die Länder bringen sich über eine Fachgruppe und eine Expertengruppe beim DVDV ein. Die beiden Gremien repräsentieren die Bedarfsträger, also die Behörden und anderen Organisationen der öffentlichen Verwaltung, und stellen sicher, dass die Interessen der Nutzer:innen während des Betriebs einbezogen und das DVDV fachlich und technisch anforderungsgetrieben weiterentwickelt wird.

Die Fachgruppe DVDV übernimmt die Rolle des Lenkungsausschusses. Die Länder sowie der Bund benennen jeweils eine Person für dieses Gremium.

Expertengruppe DVDV

Die Expertengruppe DVDV fungiert als Arbeitsgruppe, die Vorentscheidungen zum Betrieb sowie zur fachlichen und technischen Ausrichtung des DVDV trifft. Außerdem bereitet sie Entscheidungen von strategischer Bedeutung für die Fachgruppe DVDV vor.

Auftragnehmer

Die Auftragnehmer sind für die Pflege und Weiterentwicklung der Software der DVDV-Komponenten zuständig. Sie formulieren, konzeptionieren und kalkulieren Änderungsanträge („Change Requests“) und arbeiten diese nach Beauftragung ab. Außerdem betreiben sie das DVDV-Testsystem für Fachverfahrenshersteller (siehe Kap. 3.4.4).

Auftragnehmer im DVDV-Kontext sind derzeit die Governikus GmbH & Co. KG in Bremen sowie die Dataport AöR mit Sitz in Altenholz.

5 Verzeichnisse

5.1 Abkürzungsverzeichnis

Abkürzung	Bedeutung
AGS	Amtlicher Gemeindeschlüssel
API	Application Programming Interface
BfIT	Beauftragte(r) der Bundesregierung für Informationstechnik
BMI	Bundesministerium des Innern, für Bau und Heimat
BSI	Bundesamt für Sicherheit in der Informationstechnik
DVDV	Deutsches Verwaltungsdiensteverzeichnis
eIDAS	electronic Identification, Authentication and Trust Services, Verordnung Nr. 910/2014 des Europäischen Parlaments
FITKO	Föderale IT-Kooperation
HTTP	Hypertext Transfer Protocol
IAM	Identity and Access Management
ITZBund	Informationstechnikzentrum Bund
IT-PLR	IT-Planungsrat
KoopA ADV	Kooperationsausschuss Automatisierte Datenverarbeitung Bund/Länder/Kommunaler Bereich
KoSIT	Koordinierungsstelle für IT-Standards
LeiKa	Leistungskatalog der öffentlichen Verwaltung
NdB	Netze des Bundes
OAuth2	Open Authorization 2
OOP	Once Only Principle
OSCI	Online Services Computer Interface
OZG	Onlinezugangsgesetz
RegMoG	Registermodernisierungsgesetz
REST	Representational State Transfer
SDG	Single Digital Gateway
SDK	Software Development Kit
SQL	Structured Query Language
URL	Uniform Resource Locator
WSDL	Web Services Description Language
W3C	World Wide Web Consortium
XML	Extensible Markup Language
XÖV	XML in der öffentlichen Verwaltung

5.2 Abbildungsverzeichnis

5.3 Tabellenverzeichnis

Anhang 1: WSDL-Dienstbeschreibungen

Anhang 1.1: Schema der DVDV-WSDL-Extension für OSCI-Transport

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema targetNamespace="http://www.osci.de/2006/07/wsdl/"
    xmlns:tns="http://www.osci.de/2006/07/wsdl/"
    xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/"
    xmlns:xs="http://www.w3.org/2001/XMLSchema"
    xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
    xmlns:osci="http://www.osci.de/wsdl/"
    elementFormDefault="qualified" attributeFormDefault="unqualified">
    <xs:import namespace="http://schemas.xmlsoap.org/wsdl/"/>
    <xs:import namespace="http://www.w3.org/2000/09/xmldsig#"
    schemaLocation="http://www.w3.org/TR/2001/CR-xmldsig-core-20010419/xmldsig-core-schema.xsd"/>
    <xs:complexType name="extensibilityElementType" abstract="true">
        <xs:attribute ref="wsdl:required" use="optional"/>
    </xs:complexType>
    <xs:element name="binding" type="osci:bindingType">
        <xs:annotation>
            <xs:documentation>Kennzeichnet Bindung an OSCI-Transport und gibt Default-Ausprägungen für alle
            Operationen an</xs:documentation>
        </xs:annotation>
    </xs:element>
    <xs:element name="operation" type="osci:operationType">
        <xs:annotation>
            <xs:documentation>Beschreibt Ausprägung der OSCI-Kommunikation einer
            Operation</xs:documentation>
        </xs:annotation>
    </xs:element>
    <xs:element name="address" type="osci:addressType">
        <xs:annotation>
            <xs:documentation>Bündelt die Informationen zu den Endpunkten des Services, den Intermediären und
            Empfängern</xs:documentation>
        </xs:annotation>
    </xs:element>
    <xs:element name="container" type="osci:containerType">
        <xs:annotation>
            <xs:documentation>Repräsentiert einen verschlüsselten oder unverschlüsselten
            Datencontainer</xs:documentation>
        </xs:annotation>
        <!--
        <xs:keyref name="contentRef" refer="wsdl:part">
            <xs:selector xpath="osci:content"/>
            <xs:field xpath="@part"/>
        </xs:keyref>
        <xs:keyref name="attachmentRef" refer="wsdl:part">
            <xs:selector xpath="osci:attachment"/>
            <xs:field xpath="@part"/>
        </xs:keyref> -->
    </xs:element>
    <xs:simpleType name="communicationTypeChoice">
        <xs:annotation>
            <xs:documentation>Aufzählung für die vier OSCI-Transport-Kommunikationstypen</xs:documentation>
        </xs:annotation>
        <xs:restriction base="xs:string">
            <xs:enumeration value="one-way-active"/>
            <xs:enumeration value="one-way-passive"/>
            <xs:enumeration value="request-response"/>
            <xs:enumeration value="request-response-noprotocol"/>
        </xs:restriction>
```

```
</xs:simpleType>
<xs:simpleType name="signatureLevelChoice">
    <xs:annotation>
        <xs:documentation>Aufzählung für die Signaturniveaus</xs:documentation>
    </xs:annotation>
    <xs:restriction base="xs:string">
        <xs:enumeration value="none"/>
        <xs:enumeration value="advanced"/>
        <xs:enumeration value="qualified"/>
    </xs:restriction>
</xs:simpleType>
<xs:attributeGroup name="kryptoAttributesGroup">
    <xs:annotation>
        <xs:documentation>Fasst Angaben über Signatur- und Verschlüsselungsanforderungen
        zusammen</xs:documentation>
    </xs:annotation>
    <xs:attribute name="signatureLevel" type="osci:signatureLevelChoice" use="optional" default="none"/>
    <xs:attribute name="encrypted" type="xs:boolean" use="optional" default="false"/>
</xs:attributeGroup>
<xs:complexType name="bindingType">
    <xs:annotation>
        <xs:documentation>Kennzeichnet Bindung an OSCI-Transport und gibt Default-Ausprägungen für alle
        Operationen an</xs:documentation>
    </xs:annotation>
    <xs:complexContent>
        <xs:extension base="tns:extensibilityElementType">
            <xs:sequence>
                <xs:choice>
                    <xs:element name="author" type="osci:X509DataType" minOccurs="0"/>
                    <xs:element name="reader" type="osci:X509DataType" minOccurs="0"/>
                </xs:choice>
            </xs:sequence>
            <xs:attributeGroup ref="osci:kryptoAttributesGroup"/>
        </xs:extension>
    </xs:complexContent>
</xs:complexType>
<xs:complexType name="operationType">
    <xs:annotation>
        <xs:documentation>Repräsentiert ein spezifiziertes, fachliches
        Kommunikationsszenario</xs:documentation>
    </xs:annotation>
    <xs:complexContent>
        <xs:extension base="tns:extensibilityElementType">
            <xs:attribute name="communicationType" type="osci:communicationTypeChoice" use="required"/>
            <xs:attributeGroup ref="osci:kryptoAttributesGroup"/>
            <xs:attribute name="subject" type="xs:string"/>
        </xs:extension>
    </xs:complexContent>
</xs:complexType>
<xs:complexType name="contentType">
    <xs:annotation>
        <xs:documentation>Repräsentiert einen beliebigen Inhalt innerhalb von OSCI-
        Inhaltsdaten</xs:documentation>
    </xs:annotation>
    <xs:complexContent>
        <xs:extension base="tns:extensibilityElementType">
            <xs:attribute name="part" type="xs:QName"/>
        </xs:extension>
    </xs:complexContent>
</xs:complexType>
<xs:complexType name="attachmentType">
    <xs:annotation>
```

```
            <xs:documentation>Repräsentiert einen Anhang innerhalb von OSCI-Inhaltsdaten</xs:documentation>
        </xs:annotation>
        <xs:complexContent>
            <xs:extension base="tns:extensibilityElementType">
                <xs:attribute name="part" type="xs:QName"/>
                <xs:attribute name="mimetype" type="xs:string"/>
            </xs:extension>
        </xs:complexContent>
    </xs:complexType>
    <xs:complexType name="containerType">
        <xs:annotation>
            <xs:documentation>Repräsentiert einen verschlüsselten oder unverschlüsselten
            Datencontainer</xs:documentation>
        </xs:annotation>
        <xs:complexContent>
            <xs:extension base="tns:extensibilityElementType">
                <xs:sequence>
                    <xs:choice>
                        <xs:element name="readerRef" type="osci:X509DataTypeRef" minOccurs="0"/>
                        <xs:element name="authorRef" type="osci:X509DataTypeRef" minOccurs="0"/>
                    </xs:choice>
                    <xs:element name="container" type="osci:containerType" minOccurs="0"
                    maxOccurs="unbounded"/>
                    <xs:element name="part" minOccurs="0" maxOccurs="unbounded">
                        <xs:complexType>
                            <xs:sequence>
                                <xs:element name="content" type="osci:contentType" minOccurs="0"
                                maxOccurs="unbounded"/>
                                <xs:element name="attachment" type="osci:attachmentType" minOccurs="0"
                                maxOccurs="unbounded"/>
                            </xs:sequence>
                            <xs:attribute name="minOccurs" type="xs:nonNegativeInteger" use="optional"
                            default="1"/>
                            <xs:attribute name="maxOccurs" type="xs:nonNegativeInteger" use="optional"
                            default="1"/>
                            <xs:attribute name="maxSize" type="xs:nonNegativeInteger" use="optional"/>
                        </xs:complexType>
                    </xs:element>
                </xs:sequence>
                <xs:attributeGroup ref="osci:kryptoAttributesGroup"/>
                <xs:attribute name="name" type="xs:ID" use="optional"/>
                <xs:attribute name="required" type="xs:boolean" use="optional" default="true"/>
            </xs:extension>
        </xs:complexContent>
    </xs:complexType>
    <xs:complexType name="addressType">
        <xs:annotation>
            <xs:documentation>Spezialisierung von wsdl:port. Bündelt die Informationen zu den Endpunkten des
            Services, den Intermediären und Empfängern</xs:documentation>
        </xs:annotation>
        <xs:complexContent>
            <xs:extension base="tns:extensibilityElementType">
                <xs:sequence>
                    <xs:choice>
                        <xs:element name="intermediary" type="osci:intermediaryType"/>
                        <xs:element name="intermediaryRef" type="osci:intermediaryTypeRef"/>
                    </xs:choice>
                    <xs:choice>
                        <xs:element name="addressee" type="osci:addresseeType"/>
                        <xs:element name="addresseeRef" type="osci:addresseeTypeRef"/>
                    </xs:choice>
                </xs:sequence>
```

```
            <xs:attribute name="alternative" type="xs:boolean" use="optional" default="false"/>
        </xs:extension>
    </xs:complexContent>
</xs:complexType>
<xs:complexType name="addresseeType">
    <xs:annotation>
        <xs:documentation>Enthält Verbindungsdaten zum Empfänger des
        Servicerequests</xs:documentation>
    </xs:annotation>
    <xs:complexContent>
        <xs:extension base="tns:extensibilityElementType">
            <xs:all>
                <xs:element name="cipherCertificate" type="ds:X509DataType" minOccurs="0"/>
            </xs:all>
            <xs:attribute name="uri" type="xs:anyURI" use="optional"/>
            <xs:attribute name="name" type="xs:ID" use="required"/>
        </xs:extension>
    </xs:complexContent>
</xs:complexType>
<xs:complexType name="addresseeTypeRef">
    <xs:annotation>
        <xs:documentation>Referenziert den Datentyp addresseeType</xs:documentation>
    </xs:annotation>
    <xs:attribute name="ref" type="xs:IDREF" use="required"/>
</xs:complexType>
<xs:complexType name="intermediaryType">
    <xs:annotation>
        <xs:documentation>Enthält Verbindungsdaten des Intermediärs als Endpunkt des
        Services</xs:documentation>
    </xs:annotation>
    <xs:complexContent>
        <xs:extension base="tns:extensibilityElementType">
            <xs:all>
                <xs:element name="signatureCertificate" type="ds:X509DataType"/>
                <xs:element name="cipherCertificate" type="ds:X509DataType"/>
            </xs:all>
            <xs:attribute name="uri" type="xs:anyURI" use="required"/>
            <xs:attribute name="name" type="xs:ID" use="required"/>
        </xs:extension>
    </xs:complexContent>
</xs:complexType>
<xs:complexType name="intermediaryTypeRef">
    <xs:annotation>
        <xs:documentation>Referenziert den Datentyp intermediaryType</xs:documentation>
    </xs:annotation>
    <xs:attribute name="ref" type="xs:IDREF" use="required"/>
</xs:complexType>
<xs:complexType name="X509DataType">
    <xs:annotation>
        <xs:documentation>Reichert den Datentyp aus Digital Signature um ein Namensattribut
        an</xs:documentation>
    </xs:annotation>
    <xs:complexContent>
        <xs:extension base="ds:X509DataType">
            <xs:attribute name="name" type="xs:ID" use="required"/>
        </xs:extension>
    </xs:complexContent>
</xs:complexType>
<xs:complexType name="X509DataTypeRef">
    <xs:annotation>
        <xs:documentation>Referenziert den Datentyp X509DataType</xs:documentation>
    </xs:annotation>
```

```
        <xs:attribute name="ref" type="xs:IDREF" use="required"/>
    </xs:complexType>
</xs:schema>
```

Anhang 1.2: Beispiel eines OSCI-WSDL-Template

```
<?xml version="1.0" encoding="UTF-8"?>
<!-- Service -->
<definitions name="myService" targetNamespace="http://www.myDomain.de/myService.wsdl"
    xmlns="http://schemas.xmlsoap.org/wsdl/"
    xmlns:tns="http://www.myDomain.de/myService.wsdl"
    xmlns:msg="http://www.myDomain.de/myMessageType"
    xmlns:tpl="http://www.dvdv.de/dvdv/template/"
    xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/"
    xmlns:osci="http://www.osci.de/2006/07/wsdl/"
    xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
    xmlns:xs="http://www.w3.org/2001/XMLSchema"
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
    <documentation>
        <tpl:categories><tpl:category>Meine Kategorie</tpl:category></tpl:categories>
        <![CDATA[<html>
            <head><title>Meine Dienstbeschreibung</title> </head>
            <body>
                <h1>Meine Dienstbeschreibung</h1>
                Dies ist die vollständige und präzise Beschreibung meines Dienstes
            </body>
        </html>]]>
    </documentation>

    <!-- Datenstrukturen -->
    <types>
        <!-- XML-Schema der Inhaltsdaten -->
        <xs:schema targetNamespace="http://www.myDomain.de/myMessageTypes">

            <xs:element name="myRequestElement">
                <xs:complexType>
                    <xs:sequence>
                        <xs:element name="Field1" type="xs:string"/>
                        <xs:element name="Field2" type="xs:string"/>
                    </xs:sequence>
                </xs:complexType>
            </xs:element>

            <xs:element name="myResponseElement">
                <xs:complexType>
                    <xs:sequence>
                        <xs:element name="Answer" type="xs:string"/>
                    </xs:sequence>
                </xs:complexType>
            </xs:element>

            <xs:element name="myFaultElement">
                <xs:complexType>
                    <xs:sequence>
                        <xs:element name="Text" type="xs:string"/>
                        <xs:element name="Number" type="xs:int"/>
                    </xs:sequence>
                </xs:complexType>
            </xs:element>
        </xs:schema>
    </types>
```

```
<!-- Nachrichten mit Parts -->
<message name="serviceRequest">
    <part name="serviceRequestPart" element="msg:myRequestElement"/>
    <part name="documentPart" type="xs:base64Binary"/>
</message>
<message name="serviceResponse">
    <part name="serviceResponsePart" element="msg:myResponseElement"/>
</message>
<message name="fault">
    <part name="faultPart" element="msg:myFaultElement"/>
</message>

<!-- Interface -->
<portType name="myInterface">
    <operation name="myMessageExchange">
        <input message="tns:serviceRequest"/>
        <output message="tns:serviceResponse"/>
        <fault message="tns:fault" name="fault"/>
    </operation>
</portType>

<!-- Bindung von Protokoll und Interface -->
<binding name="osciBinding" type="tns:myInterface">
    <osci:binding signatureLevel="none" encrypted="none">
        <osci:reader name="myRequestReader">
            <tpl:certificate/>
        </osci:reader>
        <osci:author name="myResponseAuthor">
            <tpl:certificate/>
        </osci:author>
    </osci:binding>

    <!-- Operation -->
    <operation name="myMessageExchange">
        <osci:operation communicationType="request-response" signatureLevel="none" encrypted="true"/>
        <input>
            <osci:container required="true">
                <osci:readerRef ref="myRequestReader"/>
                <osci:part>
                    <osci:content part="tns:serviceRequestPart"/>
                </osci:part>
                <osci:part>
                    <osci:attachment part="tns:documentPart" mimetype="application/pdf"/>
                </osci:part>
            </osci:container>
        </input>
        <output>
            <osci:container signatureLevel="advanced" encrypted="true" required="true">
                <osci:authorRef ref="myResponseAuthor"/>
                <osci:part>
                    <osci:content part="tns:serviceResponsePart"/>
                </osci:part>
            </osci:container>
        </output>
    </operation>
</binding>

<!-- Endpoints des Services -->
<service name="myService">

    <!-- OSCI Infrastrukturserver -->
```

```
        <osci:devices>
            <osci:intermediary uri="" name="myIntermediary">
                <osci:signatureCertificate>
                    <tpl:certificate/>
                </osci:signatureCertificate>
                <osci:cipherCertificate>
                    <tpl:certificate/>
                </osci:cipherCertificate>
            </osci:intermediary>
            <osci:addressee name="myAddressee" uri="">
                <osci:cipherCertificate>
                    <tpl:certificate/>
                </osci:cipherCertificate>
            </osci:addressee>
        </osci:devices>

        <!-- Service Endpoint -->
        <port name="myOSCIPort" binding="tns:osciBinding">
            <osci:address>
                <osci:intermediaryRef ref="myIntermediary"/>
                <osci:addresseeRef ref="myAddressee"/>
            </osci:address>
        </port>
    </service>

</definitions>
```

Anhang 1.3: WSDL eines konkreten XÖV-OSCI-Dienstes

```
<?xml version="1.0" encoding="UTF-8"?>
<!-- Service -->
<definitions name="myService"  targetNamespace="http://www.myDomain.de/myService.wsdl"
    xmlns="http://schemas.xmlsoap.org/wsdl/"
    xmlns:tns="http://www.myDomain.de/myService.wsdl"
    xmlns:msg="http://www.myDomain.de/myMessageType"
    xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/"
    xmlns:osci="http://www.osci.de/2006/07/wsdl/"
    xmlns:dvdv="http://www.dvdv.de/messages/1.0/query"
    xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
    xmlns:xs="http://www.w3.org/2001/XMLSchema"
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
    <documentation>
        <tpl:categories><tpl:category>Meine Kategorie</tpl:category></tpl:categories>
        <![CDATA[<html>
            <head><title>Meine Dienstbeschreibung</title> </head>
            <body>
                <h1>Meine Dienstbeschreibung</h1>
                Dies ist die vollständige und präzise Beschreibung meines Dienstes!
            </body>
        </html>]]>
    </documentation>

    <!-- Datenstrukturen -->
    <types>
        <!-- XML-Schema der Inhaltsdaten -->
        <xs:schema targetNamespace="http://www.myDomain.de/myMessageTypes">
            <xs:element name="myRequestElement">
                <xs:complexType>
                    <xs:sequence>
                        <xs:element name="Field1" type="xs:string"/>
                        <xs:element name="Field2" type="xs:string"/>
```

```
            </xs:sequence>
        </xs:complexType>
    </xs:element>

    <xs:element name="myResponseElement">
        <xs:complexType>
            <xs:sequence>
                <xs:element name="Answer" type="xs:string"/>
            </xs:sequence>
        </xs:complexType>
    </xs:element>

    <xs:element name="myFaultElement">
        <xs:complexType>
            <xs:sequence>
                <xs:element name="Text" type="xs:string"/>
                <xs:element name="Number" type="xs:int"/>
            </xs:sequence>
        </xs:complexType>
    </xs:element>
  </xs:schema>
</types>
<!-- Nachrichten -->
<message name="serviceRequest">
  <part name="serviceRequestPart" element="msg:myRequestElement"/>
  <part name="documentPart" type="xs:base64Binary"/>
</message>
<message name="serviceResponse">
  <part name="serviceResponsePart" element="msg:myResponseElement"/>
</message>
<message name="fault">
  <part name="faultPart" element="msg:myFaultElement"/>
</message>

<!-- Interfaces -->
<portType name="myInterface">
  <operation name="myMessageExchange">
    <input message="tns:serviceRequest"/>
    <output message="tns:serviceResponse"/>
    <fault message="tns:fault" name="fault"/>
  </operation>
</portType>

<!-- Bindung von Protokoll und Interface -->
<binding name="osciBinding" type="tns:myInterface">
  <osci:binding signatureLevel="none" encrypted="none">
    <osci:reader name="myRequestReader">
      <ds:X509Certificate>
      MIIEfTCCA2WgAwIBAgIKC87gyAAAAAAAzDANBgkqhkiG9w0BAQUFADBXMQswCQYDVQQG
      EwJERTERMA8GA1UEChMIRGF0YXBvcnQxEjAQBgNVBAsTCU1hc2NoaW5lbjEhMB8GA1UE
      AxMYU3ViQ0EtRGF0YXBvcnQtSW50MDEtTTAxMB4XDTA2MDgwODEyNDg0MFoXDTExMDg
      wODEyNTg0MFowQTELMAkGA1UEBhMCREUxETAPBgNVBAoTCERhdGFwb3J0MQ0wCwYD
      VQQLEwREVkRWMRAwDgYDVQQDEwd1c2NkdmR2MIGfMA0GCSqGSIb3DQEBAQUAA4GN
      ADCBiQKBgQDIEpp15HMlgkSsSZlcZ94dnbpvJikC+FcWHbO7LizCXiljyNtNN5WDZVnYypsv4fFR
      7FIpvsRH57yFplgPDblkU9JrL8c6VazYb1FmAA8nqohFX7Gcxelp81T5r+fvfzLpmDGK6qtQ/3tCh5v
      gM3j/D67SvPR6A62WjK/nF6DKoQIDAQABo4IB4zCCAd8wDgYDVR0PAQH/BAQDAgTwMBMG
      A1UdJQQMMAoGCCsGAQUFBwMCMB0GA1UdDgQWBBRNmfGKlDDmY7MiLI17+ICrSYVkKT
      BtBgNVHSMEZjBkgBQPBxigTBzFnqy+g5ohoyaTa4o3dqFApD4wPDELMAkGA1UEBhMCREUx
      ETAPBgNVBAoTCERhdGFwb3J0MRowGAYDVQQDExFDQS1EYXRhcG9ydC1JbnQwMYIKYQ
      gARwAAAAAAAjCByAYDVR0fBIHAMIG9MHCgbqBshmpsZGFwOi8veDUwMC5kYXRhcG9ydC5
      kZS9DTj1TdWJDQS1EYXRhcG9ydC1JbnQwMS1NMDEsT1U9TWFzY2hpbmVuLE89RGF0YXB
      vcnQsQz1ERT9DZXJ0aWZpY2F0ZVJldm9jYXRpb25saXN0MEmgR6BFhkNodHRwOi8vd3d3Lm
```

```
                RhdGFwb3J0LmRlL3RydXN0Y2VudGVyL2NybC9TdWJDQS1EYXRhcG9ydC1JbnQwMS1NMD
                EuY3JsMF8GCCsGAQUFBwEBBFMwUTBPBggrBgEFBQcwAoZDaHR0cDovL3d3dy5kYXRhcG
                9ydC5kZS90cnVzdGNlbnRlci9haWEvU3ViQ0EtRGF0YXBvcnQtSW50MDEtTTAxLmNydDANBgk
                qhkiG9w0BAQUFAAOCAQEAgENiEUngx5LR9Hv+ZR2dmpd7jI9oxiT8Nw5NwrktC0uV7VR2utLpg
                yctMENy52nJN3NKu2gu20TDj9hDt8Fo7obR1IGyAz2pv0aTd3cwJHiKTwEBxQRUy97lhvWS2mp0
                /gxyRI7obSvyNuE6kXBMDi9TXdPEXHxsuuqdvnLdZ9BoRjlfYEVftANf5RoKL7t4kmpq+ildaWaQJ5
                C1Vx9RYXaTLbKzOnZHxiLuBvfWnxUoB9M2DMR0PWhXFg/HTRpv1z8BbfGFabhVfesJGgwSN3
                +oX0INsl/Ow7VDVcPXQeHHljt/R4bSVePVp83JYRQEq4HOCMR3apGHei1pBK+8NA
                ==</ds:X509Certificate>
            </osci:reader>
            <osci:author name="myResponseAuthor">
                <ds:X509Certificate>
                MIIEfTCCA2WgAwIBAgIKC87gyAAAAAAAzDANBgkqhkiG9w0BAQUFADBXMQswCQYDVQQG
                EwJERTERMA8GA1UEChMIRGF0YXBvcnQxEjAQBgNVBAsTCU1hc2NoaW5lbjEhMB8GA1UE
                AxMYU3ViQ0EtRGF0YXBvcnQtSW50MDEtTTAxMB4XDTA2MDgwODEyNDg0MFoXDTExMDg
                wODEyNTg0MFowQTELMAkGA1UEBhMCREUxETAPBgNVBAoTCERhdGFwb3J0MQ0wCwYD
                VQQLEwREVkRWMRAwDgYDVQQDEwd1c2NkdmR2MIGfMA0GCSqGSIb3DQEBAQUAA4GN
                ADCBiQKBgQDIEpp15HMlgkSsSZlcZ94dnbpvJikC+FcWHbO7LizCXiljyNtNN5WDZVnYypsv4fFR
                7FlpvsRH57yFplgPDblkU9JrL8c6VazYb1FmAA8nqohFX7Gcxelp81T5r+fvfzLpmDGK6qtQ/3tCh5v
                gM3j/D67SvPR6A62WjK/nF6DKoQIDAQABo4IB4zCCAd8wDgYDVR0PAQH/BAQDAgTwMBMG
                A1UdJQQMMAoGCCsGAQUFBwMCMB0GA1UdDgQWBBRNmfGKlDDmY7MiLl17+ICrSYVkKT
                BtBgNVHSMEZjBkgBQPBxigTBzFnqy+g5ohoyaTa4o3dqFApD4wPDELMAkGA1UEBhMCREUx
                ETAPBgNVBAoTCERhdGFwb3J0MRowGAYDVQQDExFDQS1EYXRhcG9ydC1JbnQwMYIKYQ
                gARwAAAAAAAjCByAYDVR0fBIHAMIG9MHCgbqBshmpsZGFwOi8veDUwMC5kYXRhcG9ydC5
                kZS9DTj1TdWJDQS1EYXRhcG9ydC1JbnQwMS1NMDEsT1U9TWFzY2hpbmVuLE89RGF0YXB
                vcnQsQz1ERT9DZXJ0aWZpY2F0ZVJldm9jYXRpb25saXN0MEmgR6BFhkNodHRwOi8vd3d3Lm
                RhdGFwb3J0LmRlL3RydXN0Y2VudGVyL2NybC9TdWJDQS1EYXRhcG9ydC1JbnQwMS1NMD
                EuY3JsMF8GCCsGAQUFBwEBBFMwUTBPBggrBgEFBQcwAoZDaHR0cDovL3d3dy5kYXRhcG
                9ydC5kZS90cnVzdGNlbnRlci9haWEvU3ViQ0EtRGF0YXBvcnQtSW50MDEtTTAxLmNydDANBgk
                qhkiG9w0BAQUFAAOCAQEAgENiEUngx5LR9Hv+ZR2dmpd7jI9oxiT8Nw5NwrktC0uV7VR2utLpg
                yctMENy52nJN3NKu2gu20TDj9hDt8Fo7obR1IGyAz2pv0aTd3cwJHiKTwEBxQRUy97lhvWS2mp0
                /gxyRI7obSvyNuE6kXBMDi9TXdPEXHxsuuqdvnLdZ9BoRjlfYEVftANf5RoKL7t4kmpq+ildaWaQJ5
                C1Vx9RYXaTLbKzOnZHxiLuBvfWnxUoB9M2DMR0PWhXFg/HTRpv1z8BbfGFabhVfesJGgwSN3
                +oX0INsl/Ow7VDVcPXQeHHljt/R4bSVePVp83JYRQEq4HOCMR3apGHei1pBK+8NA
                ==</ds:X509Certificate>
            </osci:author>
        </osci:binding>
        <!-- Operation -->
        <operation name="myMessageExchange">
            <osci:operation communicationType="request-response-noprotocol"
                signatureLevel="none" encrypted="true"/>
            <input>
                <osci:container required="true">
                    <osci:readerRef ref="myRequestReader"/>
                    <osci:part>
                        <osci:content part="tns:serviceRequestPart"/>
                    </osci:part>
                    <osci:part>
                        <osci:attachment part="tns:documentPart" mimetype="application/pdf"/>
                    </osci:part>
                </osci:container>
            </input>
            <output>
                <osci:container signatureLevel="advanced" encrypted="true" required="true">
                    <osci:authorRef ref="myResponseAuthor"/>
                    <osci:part>
                        <osci:content part="tns:serviceResponsePart"/>
                    </osci:part>
                </osci:container>
            </output>
        </operation>
    </binding>
```

```
<!-- Endpoints des Services -->
<service name="myService">
    <!-- OSCI Infrastrukturserver -->
    <osci:devices>
        <osci:intermediary uri="http://www.domain.de/osciIntermediary" name="myIntermediary">
            <osci:signatureCertificate>
                <ds:X509Certificate>
                MIIEiDCCA3CgAwIBAgIKU1BtXQAAAAAA0DANBgkqhkiG9w0BAQUFADBXMQswCQYDVQQ
                QGEwJERTERMA8GA1UEChMIRGF0YXBvcnQxEjAQBgNVBAsTCU1hc2NoaW5lbjEhMB8
                GA1UEAxMYU3ViQ0EtRGF0YXBvcnQtSW50MDEtTTAxMB4XDTA2MDgyMjEwMDMxM1oX
                DTExMDgyMjEwMTMxM1owTDELMAkGA1UEBhMCREUxETAPBgNVBAoTCERhdGFwb3J
                0MRcwFQYDVQQLEw5UZXN0Z292ZXJuaWt1czERMA8GA1UEAxMIdXNjZ292dGUwgZ8w
                DQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBANHZ4kYVROaz94hZiwjGqbG+cnLDPPD50VZ
                C9F15i4QcpO0nFFKVgvgeAT0PhIFN6hJ9dpHfgj3VXKAwH2LBrFXDKrZFJLglFmFukIXjlEUE
                AkOCR2uU5YZMicB0G1z+zyFTl8SLo8L7f+VrQ5x2haPA7xvxkF78X3dqfDG2e7rBAgMBAAGj
                ggHjMIIB3zAOBgNVHQ8BAf8EBAMCBPAwEwYDVR0lBAwwCgYIKwYBBQUHAwIwHQYDV
                R0OBBYEFPxP/sFG+lCA/FY922DcJdtgrSaXMG0GA1UdIwRmMGSAFA8HGKBMHMWerL6
                DmiGjJpNrijd2oUCkPjA8MQswCQYDVQQGEwJERTERMA8GA1UEChMIRGF0YXBvcnQxGj
                AYBgNVBAMTEUNBLURhdGFwb3J0LUludDAxggphCABHAAAAAAACMIHIBgNVHR8EgcA
                wgb0wcKBuoGyGamxkYXA6Ly94NTAwLmRhdGFwb3J0LmRlL0NOPVN1YkNBLURhdGFwb
                3J0LUludDAxLU0wMSxPVT1NYXNjaGluZW4sTz1EYXRhcG9ydCxDPURFP0NlcnRpZmljYX
                RlUmV2b2NhdGlvbmxpc3QwSaBHoEWGQ2h0dHA6Ly93d3cuZGF0YXBvcnQuZGUvdHJ1c3
                RjZW50ZXIvY3JsL1N1YkNBLURhdGFwb3J0LUludDAxLU0wMS5jcmwwXwYIKwYBBQUHA
                QEEUzBRME8GCCsGAQUFBzAChkNodHRwOi8vd3d3LmRhdGFwb3J0LmRlL3RydXN0Y2V
                udGVyL2FpYS9TdWJDQS1EYXRhcG9ydC1JbnQwMS1NMDEuY3J0MA0GCSqGSIb3DQEB
                BQUAA4IBAQCUcSMl+uhlTS5cZzE2CRJ+1MvMOJWCCdYFzQSBcknZRyN5XQFUoo+fNYs
                3aBpyd6PooTu0AdNi5v9SaGmdna5rnqYFdB7DgMdNfhxhwsNlNoUDjkd840ZpLG8ErvRceBL
                5tFD7TCfJL2+fmHsuJi4uhndxVWKJ9EMutaVZuWCYqJFm9zG3SUyQVksUjTi97iKXYYf0uZo
                C2SRoKoElaFHN5Px/2ZSdkQYsVPROOys++eounN5F1VeDlb1ilVL5CNw63aRyukvLuY77Lw
                DbWFg+M3ROc22pFrzfPUMPfNGikIPIm7Ns60JBHioNttqL1119HNV5Do+KZrdX7C1+yMz8
                </ds:X509Certificate>
            </osci:signatureCertificate>
            <osci:cipherCertificate>
                <ds:X509Certificate>
                MIIEiDCCA3CgAwIBAgIKU1BtXQAAAAAA0DANBgkqhkiG9wBAQUFADBXMQswCQYDVQQ
                GEwJERTERMA8GA1UEChMIRGF0YXBvcnQxEjAQBgNVBAsTCU1hc2NoaW5lbjEhMB8GA
                1UEAxMYU3ViQ0EtRGF0YXBvcnQtSW50MDEtTTAxMB4XDTA2MDgyMjEwMDMxM1oXDT
                ExMDgyMjEwMTMxM1owTDELMAkGA1UEBhMCREUxETAPBgNVBAoTCERhdGFwb3J0M
                RcwFQYDVQQLEw5UZXN0Z292ZXJuaWt1czERMA8GA1UEAxMIdXNjZ292dGUwgZ8wDQ
                YJKoZIhvcNAQEBBQADgY0AMIGJAoGBANHZ4kYVROaz94hZiwjGqbG+cnLDPPD50VZC9
                F15i4QcpO0nFFKVgvgeAT0PhIFN6hJ9dpHfgj3VXKAwH2LBrFXDKrZFJLglFmFukIXjlEUEAk
                OCR2uU5YZMicB0G1z+zyFTl8SLo8L7f+VrQ5x2haPA7xvxkF78X3dqfDG2e7rBAgMBAAGjgg
                HjMIIB3zAOBgNVHQ8BAf8EBAMCBPAwEwYDVR0lBAwwCgYIKwYBBQUHAwIwHQYDVR0
                OBBYEFPxP/sFG+lCA/FY922DcJdtgrSaXMG0GA1UdIwRmMGSAFA8HGKBMHMWerL6Dmi
                GjJpNrijd2oUCkPjA8MQswCQYDVQQGEwJERTERMA8GA1UEChMIRGF0YXBvcnQxGjAY
                BgNVBAMTEUNBLURhdGFwb3J0LUludDAxggphCABHAAAAAAACMIHIBgNVHR8EgcAwgb
                0wcKBuoGyGamxkYXA6Ly94NTAwLmRhdGFwb3J0LmRlL0NOPVN1YkNBLURhdGFwb3J0
                LUludDAxLU0wMSxPVT1NYXNjaGluZW4sTz1EYXRhcG9ydCxDPURFP0NlcnRpZmljYXRlU
                mV2b2NhdGlvbmxpc3QwSaBHoEWGQ2h0dHA6Ly93d3cuZGF0YXBvcnQuZGUvdHJ1c3RjZ
                W50ZXIvY3JsL1N1YkNBLURhdGFwb3J0LUludDAxLU0wMS5jcmwwXwYIKwYBBQUHAQEE
                UzBRME8GCCsGAQUFBzAChkNodHRwOi8vd3d3LmRhdGFwb3J0LmRlL3RydXN0Y2VudG
                VyL2FpYS9TdWJDQS1EYXRhcG9ydC1JbnQwMS1NMDEuY3J0MA0GCSqGSIb3DQEBBQ
                UAA4IBAQCUcSMl+uhlTS5cZzE2CRJ+1MvMOJWCCdYFzQSBcknZRyN5XQFUoo+fNYs3a
                Bpyd6PooTu0AdNi5v9SaGmdna5rnqYFdB7DgMdNfhxhwsNlNoUDjkd840ZpLG8ErvRceBL5tF
                D7TCfJL2+fmHsuJi4uhndxVWKJ9EMutaVZuWCYqJFm9zG3SUyQVksUjTi97iKXYYf0uZoC2
                SRoKoElaFHN5Px/2ZSdkQYsVPROOys++eounN5F1VeDlb1ilVL5CNw63aRyukvLuY77LwDb
                WFg+M3ROc22pFrzfPUMPfNGikIPIm7Ns60JBHioNttqL1119HNV5Do+KZrdX7C1+yMz8
                </ds:X509Certificate>
            </osci:cipherCertificate>
        </osci:intermediary>
        <osci:addressee name="myAddressee" uri="/myAddressees/sampleAddressee">
```

```
            <osci:cipherCertificate>
                <ds:X509Certificate>
                MIIEfTCCA2WgAwIBAgIKC87gyAAAAAAAzDANBgkqhkG9w0BAQUFADBXMQswCQYDVQQ
                QGEwJERTERMA8GA1UEChMIRGF0YXBvcnQxEjAQBgNVBAsTCU1hc2NoaW5lbjEhMB8
                GA1UEAxMYU3ViQ0EtRGF0YXBvcnQtSW50MDEtTTAxMB4XDTA2MDgwODEyNDg0MFoX
                DTExMDgwODEyNTg0MFowQTELMAkGA1UEBhMCREUxETAPBgNVBAoTCERhdGFwb3J
                0MQ0wCwYDVQQLEwREVkRWMRAwDgYDVQQDEwd1c2NkdmR2MIGfMA0GCSqGSIb3D
                QEBAQUAA4GNADCBiQKBgQDIEpp15HMlgkSsSZlcZ94dnbpvJikC+FcWHbO7LizCXiljyNtN
                N5WDZVnYypsv4fFR7FIpvsRH57yFplgPDblkU9JrL8c6VazYb1FmAA8nqohFX7Gcxelp81T5r+
                fvfzLpmDGK6qtQ/3tCh5vgM3j/D67SvPR6A62WjK/nF6DKoQIDAQABo4IB4zCCAd8wDgYDV
                R0PAQH/BAQDAgTwMBMGA1UdJQQMMAoGCCsGAQUFBwMCMB0GA1UdDgQWBBRN
                mfGKlDDmY7MiLl17+ICrSYVkKTBtBgNVHSMEZjBkgBQPBxigTBzFnqy+g5ohoyaTa4o3dqFA
                pD4wPDELMAkGA1UEBhMCREUxETAPBgNVBAoTCERhdGFwb3J0MRowGAYDVQQDEx
                FDQS1EYXRhcG9ydC1JbnQwMYIKYQgARwAAAAAAAjCByAYDVR0fBIHAMIG9MHCgbqBs
                hmpsZGFwOi8veDUwMC5kYXRhcG9ydC5kZS9DTj1TdWJDQS1EYXRhcG9ydC1JbnQwMS
                1NMDEsT1U9TWFzY2hpbmVuLE89RGF0YXBvcnQsQz1ERT9DZXJ0aWZpY2F0ZVJldm9jY
                XRpb25saXN0MEmgR6BFhkNodHRwOi8vd3d3LmRhdGFwb3J0LmRlL3RydXN0Y2VudGVyL
                2NybC9TdWJDQS1EYXRhcG9ydC1JbnQwMS1NMDEuY3JsMF8GCCsGAQUFBwEBBFMw
                UTBPBggrBgEFBQcwAoZDaHR0cDovL3d3dy5kYXRhcG9ydC5kZS90cnVzdGNlbnRlci9haW
                EvU3ViQ0EtRGF0YXBvcnQtSW50MDEtTTAxLmNydDANBgkqhkiG9w0BAQUFAAOCAQEAg
                ENiEUngx5LR9Hv+ZR2dmpd7jI9oxiT8Nw5NwrktC0uV7VR2utLpgyctMENy52nJN3NKu2gu20
                TDj9hDt8Fo7obR1IGyAz2pv0aTd3cwJHiKTwEBxQRUy97lhvWS2mp0/gxyRI7obSvyNuE6kXB
                MDi9TXdPEXHxsuuqdvnLdZ9BoRjlfYEVftANf5RoKL7t4kmpq+ildaWaQJ5C1Vx9RYXaTLbKz
                OnZHxiLuBvfWnxUoB9M2DMR0PWhXFg/HTRpv1z8BbfGFabhVfesJGgwSN3+oX0INsl/Ow7
                VDVcPXQeHHljt/R4bSVePVp83JYRQEq4HOCMR3apGHei1pBK+8NA
                ==</ds:X509Certificate>
            </osci:cipherCertificate>
        </osci:addressee>
    </osci:devices>

    <!-- Service Endpoint -->
    <port name="myOSCIPort" binding="tns:osciBinding">
        <osci:address>
            <osci:intermediaryRef ref="myIntermediary"/>
            <osci:addresseeRef ref="myAddressee"/>
        </osci:address>
    </port>
</service>

<!--- Hinweise zum Dienstanbieter -->
<dvdv:supplier>
    <dvdv:authorityKey>dvdv:myProvider</dvdv:authorityKey>
    <dvdv:timestamp>2007-10-31T15:30:00.800</dvdv:timestamp>
</dvdv:supplier>

</definitions>
```