Nationales Once-Only-Technical-System (NOOTS) Technical Design Documents (TDDs)

Version 0.9

Stand 15. Dezember 2022

Inhaltsverzeichnis

1 HIGH-LEVEL-ARCHITECTURE 5

1.1 Management Summary 5

1.2 Überblick 5

1.3 Anforderungen 6

1.3.1 Rechtliche Grundlagen und Rahmenbedingungen 6
1.3.2 Kontext 6
1.3.3 Ziele 13
1.3.4 Scope 13
1.3.5 Nachweise 15
1.3.6 Abgrenzungen 17

1.4 High-Level-Architecture Beschreibung 18

1.4.1 Übergreifende Entwurfsentscheidungen 18
1.4.2 Use-Cases 22
1.4.3 Ausblick und weiterführende Aspekte 68

1.5 Ausblick & Weiterführende Aspekte 83

1.5.1 Sequenzdiagramm zu Use-Case 3 83
1.5.2 Sequenzdiagramm zu Use-Case 4 83

2 <PLATZHALTER KAPITEL 2> 85

3 NOOTS KOMPONENTEN BESCHREIBUNG 86

3.1 Registerdatennavigation 86

3.1.1 Management Summary 86
3.1.2 Einleitung 86
3.1.3 Kontext 87
3.1.4 Annahmen und Rahmenbedingungen 91
3.1.5 Fachliche Anforderungen 93
3.1.6 Facharchitektur 110
3.1.7 Technische Aspekte 124
3.1.8 Ausblick & Weiterführende Aspekte 129

3.2 Preview 146

3.3.1 Überblick 146
3.3.2 Annahmen & Rahmenbedingungen 146
3.3.3 Fachliches Konzept 147
3.3.4 Facharchitektur 151
3.3.5 Technisches Konzept 154
3.3.6 Ausblick & Weiterführende Aspekte 154

3.4 IAM für Behörden ... *156*
3.4.1 Überblick ... 156
3.4.2 Annahmen & Rahmenbedingungen ... 158
3.4.3 Fachliches Konzept (inkl. Facharchitektur) ... 159
3.4.4 Technisches Konzept ... 170
3.4.5 Ausblick & Weiterführende Aspekte ... 184
3.5 V-PKI Infrastruktur ... *186*
3.5.1 Überblick ... 186
3.5.2 Annahmen und Rahmenbedingungen ... 191
3.5.3 Fachliches Konzept (inkl. Facharchitektur) ... 192
3.5.4 Umsetzung ... 208
3.5.5 Ausblick & Weiterführende Aspekte ... 209
3.6 IDM Unternehmen (Basisregister für Unternehmen) ... *210*
3.6.1 Überblick ... 210
3.6.2 Fachliches Konzept ... 211
3.6.3 Technisches Konzept ... 212
3.6.4 Ausblick & Weiterführende Aspekte ... 213
3.7 IDM Personen (IDA) ... *214*
3.7.1 Überblick ... 214
3.7.2 Annahmen & Rahmenbedingungen ... 215
3.7.3 Fachliches Konzept ... 216
3.7.4 Technisches Konzept ... 221
3.7.5 Ausblick & Weiterführende Aspekte ... 223
3.8 Datenschutzcockpit ... *224*
3.8.1 Überblick ... 224
3.8.2 Fachliches Konzept ... 225
3.8.3 Technisches Konzept ... 230
3.8.4 Ausblick & Weiterführende Aspekte ... 231
3.9 Vermittlungsstellen ... *232*
3.9.1 Überblick ... 232
3.9.2 Annahmen & Rahmenbedingungen ... 234
3.9.3 Fachliches Konzept ... 235
3.9.4 Ausblick & Weiterführende Aspekte ... 245
3.10 Intermediäre Plattformen ... *251*
3.10.1 Management Summary ... 251
3.10.2 Überblick ... 252
3.10.3 Kontext ... 254

3.10.4 Fachliches Konzept (Anforderungen & Architektur) 261
3.10.5 Technische Aspekte 295
3.10.6 Zentrale Evidence Provider/Data Provider für die Anbindung an EU-OOTS und NOOTS 299
3.10.7 Ausblick & Weiterführende Aspekte 301
3.11 Data Consumer (Evidence Requestor) *304*
3.11.1 Überblick 304
3.11.2 Anschlussbedingungen NOOTS Komponenten 305
3.12 Data Provider (Evidence Provider) *310*
3.12.1 Überblick 310
3.12.2 Anschlussbedingungen NOOTS Komponenten 310
4 GENERISCHER NACHWEISABRUFSTANDARD 317
5 ANHANG 318
5.1 Quellenverzeichnis *318*
5.2 Tabellenverzeichnis *325*
5.3 Abbildungsverzeichnis *329*
5.4 Glossar & Abkürzungsverzeichnis *331*
5.4.1 Glossar 331
5.4.2 Abkürzungsverzeichnis 5

1 High-Level-Architecture

1.1 Management Summary

Das Projekt Gesamtsteuerung Registermodernisierung hat die Aufgabe, gemäß IT-Planungsratsbeschluss 2022/06, eine validierte Fassung des Architekturzielbilds der Registermodernisierung bis Ende 2022 vorzulegen. Das vorliegende Dokument beschreibt den aktuellen Konzeptions- und Umsetzungsstand des nationalen Once-Only-Technical-Systems (NOOTS) und orientiert sich, aus Zwecken der Wiedererkennung, inhaltlich und strukturell an den Technical-Design-Documents (TDDs) der Europäischen Kommission. Das NOOTS ist ein System aus technischen Komponenten, Schnittstellen und Standards sowie organisatorischen und rechtlichen Regelungen, das öffentlichen Stellen den rechtskonformen Abruf von elektronischen Nachweisen aus den Registern der deutschen Verwaltung ermöglicht. Über einen Anschluss an das europäische Once-Only-Technical-System (EU-OOTS) wird ein Austausch von Nachweisen mit dem EU-Ausland ermöglicht. Das vorliegende Dokument wird rechtliche und fachliche Grundlagen, daraus abgeleitete Anforderungen und die Use-Cases der Registermodernisierung detailliert darstellen. Zu den zentralen Komponenten des Zielbilds werden zudem detaillierte konzeptionelle Beschreibungen und Umsetzungsstände geliefert. Auch wird in diesem Dokument ein Nachweisabrufstandard spezifiziert, der einen entscheidenden Mehrwert für den behördlichen Nachweisabruf darstellen wird.

1.2 Überblick

Zielsetzung, Zielgruppe und Ergebnisse der High-Level-Architecture (HLA) des NOOTS.

Zielsetzung

- Validierung des Architekturzielbilds der Registermodernisierung.
- Beschreibung des übergreifenden Zusammenwirkens der NOOTS-Komponenten in nationalen und europäischen Use-Cases.

Zielgruppe

- Entscheidungsträger und Fachexperten im Projekt Gesamtsteuerung Registermodernisierung
    - IT-Planungsrat (IT-PLR), Lenkungskreis (LK) Registermodernisierung, Transformationseinheit (TE) Registermodernisierung, Kompetenzteams (KT)

- Architekten und Umsetzungsverantwortliche im Projekt Gesamtsteuerung Registermodernisierung
    - Verantwortliche für NOOTS-Komponenten, Fachverfahren (Data Consumer), Registerführende Behörden (Data Provider)

Aufbau

- Darstellung der zentralen Vorarbeiten und IT-Planungsratsbeschlüsse sowie nationalen und europäischen Gesetze und Verordnungen
- Beschreibung von Zielen und Aufbau des NOOTS
- Modellierung von nationalen und europäischen Use-Cases
- Darstellung des Konzeptions- und Umsetzungsstands der zentralen Komponenten des NOOTS
- Formulierung von NOOTS-Anschlussbedingungen an Data Consumer und Data Provider
- Spezifizierung des nationalen EDM-Standards für Nachweisabrufe

1.3 Anforderungen

1.3.1 Rechtliche Grundlagen und Rahmenbedingungen

Gesetzestexte und Verordnungen, aus denen sich die rechtlichen Rahmenbedingungen des NOOTS und der Anschluss an das EU-OOTS ergeben, sind im Anhang unter dem Quellenverzeichnis aufgeführt.

Weitere Rahmenbedingungen aus den folgenden Bereichen sind ebenfalls im Quellenverzeichnis aufgeführt. Dies sind insbesondere:

- Beschlüsse des IT-Planungsrats
- Entscheidungen des IT-Planungsrats
- Dokumente der Europäischen Kommission zur SDG-Umsetzung
- Sonstige weiterführende Dokumente

1.3.2 Kontext

Die Registermodernisierung ist ein zentrales Vorhaben im Rahmen der Verwaltungsmodernisierung und Digitalisierungsvorhaben von Bund, Ländern und

Kommunen. Digitale und vernetzte Register sind notwendig, um Verwaltungsleistungen vollständig digital anbieten und Verwaltungsprozesse effizient gestalten zu können. Die gesetzliche Grundlage der Registermodernisierung bildet das Registermodernisierungsgesetz (Quelle: [RGR-01]), welches am 06. April 2021 verkündet wurde.

Um das Vorhaben umzusetzen, wurde im Juni 2021 vom IT-Planungsrat das Projekt "Gesamtsteuerung Registermodernisierung" initiiert. Die Umsetzung des Once-Only-Prinzips ist ein wesentliches Ziel der Registermodernisierung. Demnach sollen staatliche Stellen bereits vorhandene Daten und Nachweise selbst abrufen, sofern das Einverständnis der Bürgerinnen und Bürger vorliegt. Dies bedeutet, dass Informationen durch Bürgerinnen und Bürger nur noch einmalig übermittelt werden müssen. Darüber hinaus ist das Once-Only-Prinzip auch für die Umsetzung des Onlinezugangsgesetzes (OZG) wesentlich, um den Reifegrad 4 des OZG-Reifegradmodells zu erreichen. Des Weiteren ist die Umsetzung des Once-Only-Prinzips auch europarechtlich im Rahmen der Single Digital Gateway (SDG) Verordnung gefordert. (Quelle: [SQ-04]) Die Europäische Kommission verpflichtet die Mitgliedsstaaten nach EU-Verordnung 2018/1724, ausgewählte Verfahren (nach Anhang II SDG-VO) bis Dezember 2023 in die Lage zu versetzen, grenzüberschreitende digitale Nachweise nach dem Once-Only-Prinzip ausstellen zu können. Für die Komponenten im NOOTS bedeutet das, dass sie für eine Verwendung im EU-OOTS geeignet sein müssen oder so zu gestalten sind, dass der Anschluss an ein entsprechendes Gegenstück im EU-OOTS möglich ist (Quelle: [RGR-05]). Schließlich soll mithilfe der Registermodernisierung auch ein registerbasierter Zensus etabliert werden. Dadurch entfallen sonst notwendige Direktbefragungen, sodass hier Kosten- und Aufwandseinsparungen erzielt werden können. (Quelle: [SQ-04])

Das Projekt „Gesamtsteuerung Registermodernisierung“ unter Federführung des Bundes (Bundesministerium des Innern und für Heimat (BMI)) sowie der Länder Baden-Württemberg, Bayern, Hamburg und Nordrhein-Westfalen soll im Rahmen eines übergreifenden Programmmanagements die Realisierung des Zielbilds der Registermodernisierung voranbringen. (Quelle: [IT-PLR-B-05])

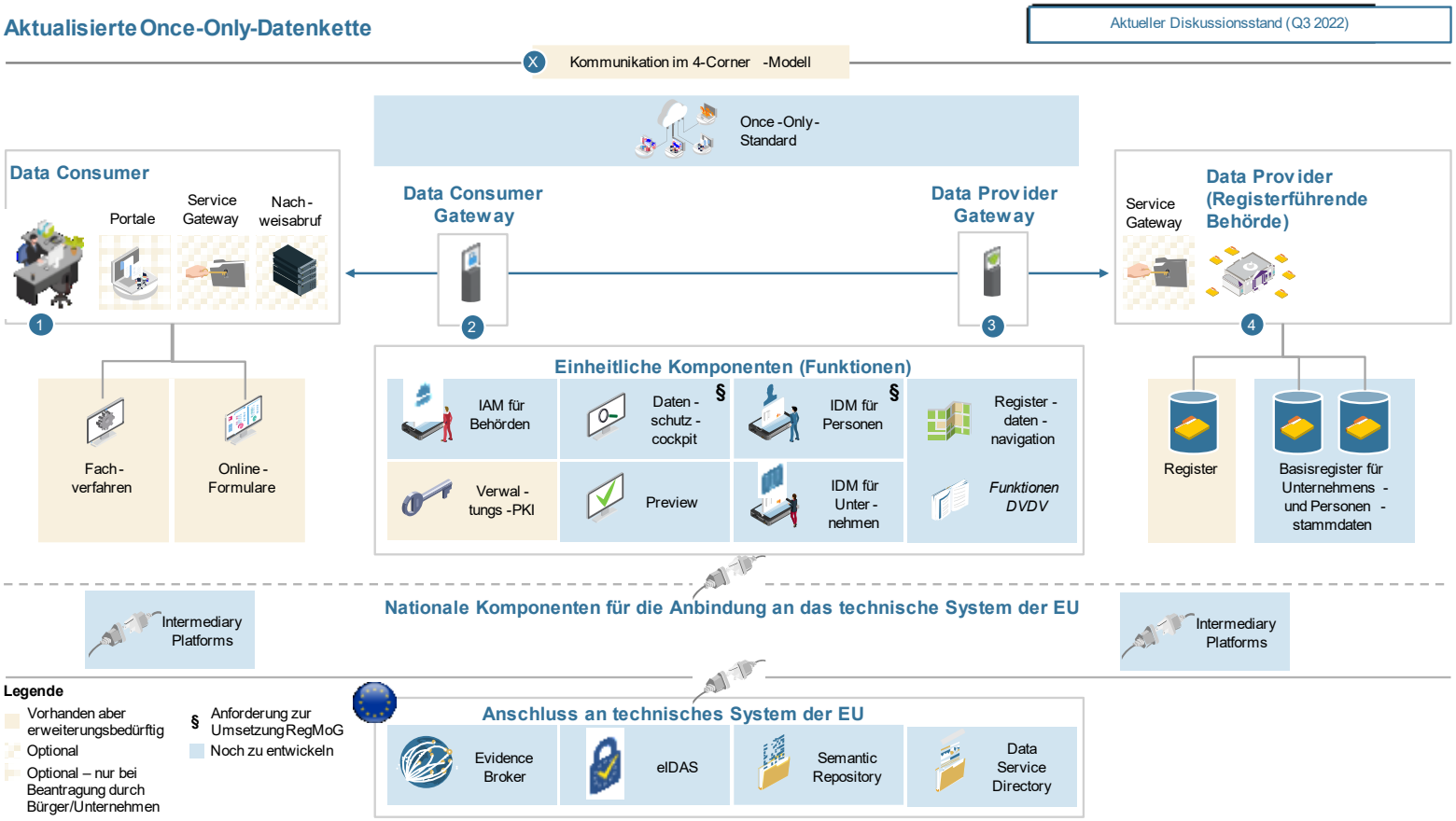


Abbildung 1: Übersicht NOOTS Komponenten und Umfeld

Tabelle 1: Komponentenübersicht und Aufgabenbeschreibung NOOTS

Komponente	Kurzform	Aufgabe	Konzeption
Data Consumer	DC	Data Consumer im Sinne des Zielbilds sind Fachverfahren für Behörden, die Nachweise ohne Beteiligung der Antragstellenden abrufen oder Online-Dienste (z.B. Portale), die eine Schnittstelle zwischen Antragssteller und Fachverfahren herstellen. Antragssteller können natürliche Personen und Unternehmen sein, die das NOOTS zum Zweck der Beantragung einer Verwaltungsleistung verwenden. Der Data Consumer verantwortet die Authentifizierung der Antragstellenden und Protokollierung der Nutzerfreigabe zum Datenaustausch (Consent). Dieser Vorgang ist gesetzlich gefordert und stellt die notwendige Voraussetzung für jeden durch Bürgerinnen und Bürger initiierten und die Identifikationsnummer verwendenden behördlichen Datenaustausch dar.	Kapitel 3.10 Data Consumer
Data Provider	DP	Data Provider sind registerführende Behörden oder Basisregister für Unternehmens- und Personendaten und haben die Aufgabe, Daten in Form von Nachweisen bereitzustellen. Data Provider sind gesetzlich verpflichtet, Datenzugriffe zu protokollieren und diese, wie auch die über eine Person oder ein Unternehmen geführten Bestandsdaten, bei Bedarf an ein Datenschutzcockpit zu übermitteln	Kapitel 3.11 Data Provider
Datenschutz-cockpit	DSC	Das Datenschutzcockpit (DSC), nach Artikel 2 des Registermodernisierungsgesetzes (RegMoG), hat die Aufgabe, Datenübermittlungen unter Verwendung der Identifikationsnummer (IDNr.) anzuzeigen. Mit der Einführung des DSC werden Bürgerinnen und Bürger die Möglichkeit erhalten, einfach und digital nachvollziehen zu können, welche öffentlichen Stellen Daten, zu welchem Zeitpunkt und zu welchem Zweck unter Verwendung der IDNr. ausgetauscht haben. Das DSC fördert demnach Transparenz und den Abbau von Vorbehalten gegen die Einführung der IDNr. Das DSC selbst darf keine Daten über Personen speichern. Das Datenschutzcockpit übernimmt	Kapitel 3.7 Datenschutz-cockpit

		im Nachweisabrufprozess selbst keine Funktion, sondern dient der nachträglichen Rückverfolgbarkeit von Nachweisabrufen unter Verwendung der Identifikationsnummer. Dazu greift das DSC auf die Protokolldaten der Register zu. Datenabrufe, die ohne Verwendung der IDNr. stattfinden, also in der Behörden-zu-Behörden-Kommunikation ohne Bürgerbeteiligung oder im EU-Kontext, können deshalb im DSC nicht eingesehen werden.	
Vorschau-funktion	Preview	Die Preview soll Bürgerinnen und Bürger ermöglichen, die bei einem Nachweisabruf zwischen Behörden der öffentlichen Verwaltung ausgetauschten Nachweise vorab einsehen und über die weitere Verwendung entscheiden zu können. Eine Nutzung dieser Daten für die Erbringung von Verwaltungsleistungen ist somit erst dann zulässig, wenn die betroffene Person eine explizite Zustimmung gegeben hat. Für europäische Nachweisabrufe ist festgelegt, dass die Preview im Mitgliedsstaat des Evidence Providers erbracht werden muss. Im NOOTS wird die Preview dementsprechend durch die Data Consumer für nationale Nachweisabrufe und durch die Intermediären Plattformen für europäische Nachweisabrufe erbracht werden.	Kapitel 3.2 Preview
Identity Management für Personen	IDM für Personen	Das Identity Management (IDM) für Personen verantwortet die Bereitstellung der Identifikationsnummer und personenbezogener Basisdaten, die zur zweifelsfreien Identifikation von Bürgerinnen und Bürgern benötigt werden. Damit wird eine zentrale Grundlage für den automatisierten Nachweisabruf geschaffen.	Kapitel 3.6 Identity Management für Personen
Identity Management für Unternehmen	IDM für Unternehmen	Das Identity Management (IDM) für Unternehmen verantwortet die Bereitstellung der Wirtschafts-Identifikationsnummer und unternehmensbezogener Basisdaten, die zur zweifelsfreien Identifikation von Unternehmen benötigt werden. Damit wird eine zentrale Grundlage für den automatisierten Nachweisabruf geschaffen.	Kapitel 3.5 Identity Management für Unternehmen

Registerdaten-navigation	RDN	Die Registerdatennavigation (RDN) ist der zentrale Routingdienst im NOOTS. Auf Anfrage liefert die RDN einem Data Consumer die Information, von welchem technischen Dienst dieser einen gewünschten Nachweis abrufen kann, welche Behörde diesen Dienst betreibt und welche Verbindungsparameter für einen Abruf erforderlich sind. Die RDN wird sowohl für nationale Abrufe als auch für Abrufe aus dem EU-Ausland verwendet.	Kapitel 3.1 Registerdaten-navigation
Identity and Accessmanagement für Behörden	IAM für Behörden	Das Identity- and Accessmanagement (IAM) für Behörden ermöglicht die sichere Authentifizierung und Autorisierung von öffentlichen Stellen beim Zugriff auf Register und die technischen Komponenten des NOOTS. Dazu stellt das IAM für Behörden die Einhaltung der Governance für eine gesetzeskonforme Erteilung von Identitäten sowie berechtigungsrelevanten Informationen (Behördenkategorie) sicher, protokolliert und überwacht die Zugriffe. Das IAM für Behörden ist ausschließlich auf nationale Identitäts- und Berechtigungsprüfungen beschränkt. Für Abrufe aus dem EU-Ausland sind derzeit keine IAM-Komponenten vorgesehen. Die Authentifizierung von Nutzenden des NOOTS (z.B. Bürgerinnen und Bürger oder Unternehmen) liegt hingegen außerhalb des Scope des IAM für Behörden.	Kapitel 3.3 IAM für Behörden
Verwaltungs-Public-Key-Infrastructure	V-PKI	Die Verwaltungs-Public-Key-Infrastructure (V-PKI) der deutschen Verwaltung wird seit 2001 vom BSI betrieben und ist für die Ausstellung von Zertifikaten (zertifizierte Schlüsselpaare) für öffentliche Stellen und im Auftrag der öffentlichen Verwaltung tätiger Unternehmen (z.B. Handelskammer) zuständig, die als digitaler Ausweis dienen und zur Identifikation, Verschlüsselung und elektronischen Signaturerstellung eingesetzt werden können. Die Ausstellung von Zertifikaten für Privatpersonen ist keine Aufgabe der V-PKI. Die V-PKI dient ausschließlich der Authentifizierung auf Ebene der öffentlichen Stellen. Die von der V-PKI ausgestellten Zertifikate werden von allen technischen Komponenten des NOOTS benötigt.	Kapitel 3.4 V-PKI

Data Consumer Gateway / Data Provider Gateway	Vermittlungs-stellen	Vermittlungsstellen, nach §7 des Identifikationsnummerngesetzes (IDNrG.), werden durch öffentliche Stellen betrieben, führen eine abstrakte Berechtigungsprüfung durch und Protokollierung die Abrufe von Nachweisen. Vermittlungsstellen müssen diese Aufgabe ohne Kenntnis der Nachrichteninhalte durchführen. Sofern eine Berechtigungsprüfung negativ ausfällt, müssen Vermittlungsstellen den Nachweisabruf abbrechen	Kapitel 3.8 Vermittlungs-stellen
Intermediäre Plattformen	IP	Um der Once-Only-Verpflichtung der SDG-VO zum grenzüberschreitenden Nachweisaustausch mit dem EU-Ausland nachzukommen, setzt Deutschland auf den Einsatz von Intermediären Plattformen. Diese vermitteln zwischen dem NOOTS und dem EU-OOTS, indem Nachweisabfragen aus dem EU-Ausland in nationale Abfragen umgewandelt werden und umgekehrt. Durch den Einsatz Intermediärer Plattformen (IP) können Funktionen für grenzüberschreitenden Nachrichtenaustausch gebündelt werden, die sonst durch die Data Consumer und Data Provider selbst erbracht werden müssten.	Kapitel 3.9 Intermediäre Plattformen

1.3.3 Ziele

Im Zielbild der Registermodernisierung vom Januar 2021 hat der IT-Planungsrat folgende Ziele formuliert. Die weitere Erläuterung der Ziele kann [IT-PLR-B-04] entnommen werden. Für das NOOTS sind alle genannten Ziele relevant. Es gibt jedoch Unterschiede in der Dringlichkeit. Derzeit werden daher nur die Ziele explizit adressiert, die entweder 2023 oder 2025 relevant sind. Die weiteren Ziele werden erst in einer späteren Iteration des NOOTS adressiert. In diesem Dokument werden die in der folgenden Tabelle eingeführten Kurzbezeichnungen verwendet, wenn auf die Ziele der Registermodernisierung Bezug genommen wird.

Tabelle 2: Übersicht IT-PLR Ziele Registermodernisierung 2023/2025

Ziel	Kurzbezeichnung	Bereit-stellung
Einfache, digitale Once-Only-Verwaltungsleistungen	Once-Only	Ende 2025
Aufwandsarmer und aktueller registerbasierter Zensus	Registerzensus	offen
Effizienter und sicherer zwischenbehördlicher Datenaustausch	Verwaltungs-digitalisierung	Ende 2025
Hohe Anschlussfähigkeit an das europäische technische System (SDG-VO)	SDG-VO	Ende 2023
Sekundärnutzung der Registerdaten durch die Wissenschaft	Wissenschaft	offen
Hoher Datenschutzstandard und erweiterte Transparenz	Datenschutz	Ende 2023

1.3.4 Scope

Das NOOTS ist ein System aus technischen Komponenten, Schnittstellen und Standards sowie organisatorischen und rechtlichen Regelungen, das öffentlichen Stellen den rechtskonformen Abruf von elektronischen Nachweisen aus den Registern der deutschen Verwaltung ermöglicht. Zu diesem Zweck stellt das NOOTS einheitliche Komponenten

bereit und formuliert Anschlussbedingungen an Data Consumer und Data Provider. Über einen Anschluss an das EU-OOTS wird ein Austausch von Nachweisen mit dem EU-Ausland ermöglicht. Die Nachweisaustausche erfolgen dabei teilweise über das NOOTS und teilweise über das EU-OOTS.

Die folgende Grafik zeigt das NOOTS und alle Systeme, die mit ihm interagieren, sowohl im nationalen als auch im grenzübergreifenden Kontext. Der Scope des NOOTS umfasst dabei nicht nur die Komponenten und Standards, die das NOOTS mitbringt. Es formuliert auch Anschlussbedingungen an die Systeme, die daran angeschlossen werden. Die Data Consumer und Data Provider selbst gehören jedoch nicht zum Scope des NOOTS. Dasselbe gilt für Datenverarbeitung oder Datenübermittlung, die nach dem Nachweisabruf durch den Data Consumer erfolgen. Insbesondere gehört auch die Weiterleitung des Nachweises im Zuge der Antragseinreichung nicht zum Scope des NOOTS.

Datenaustausche zum Zweck des Registerzensus oder wissenschaftlicher Auswertungen werden in dieser Version des NOOTS noch nicht explizit adressiert. Sie sind daher nur ausgegraut dargestellt.

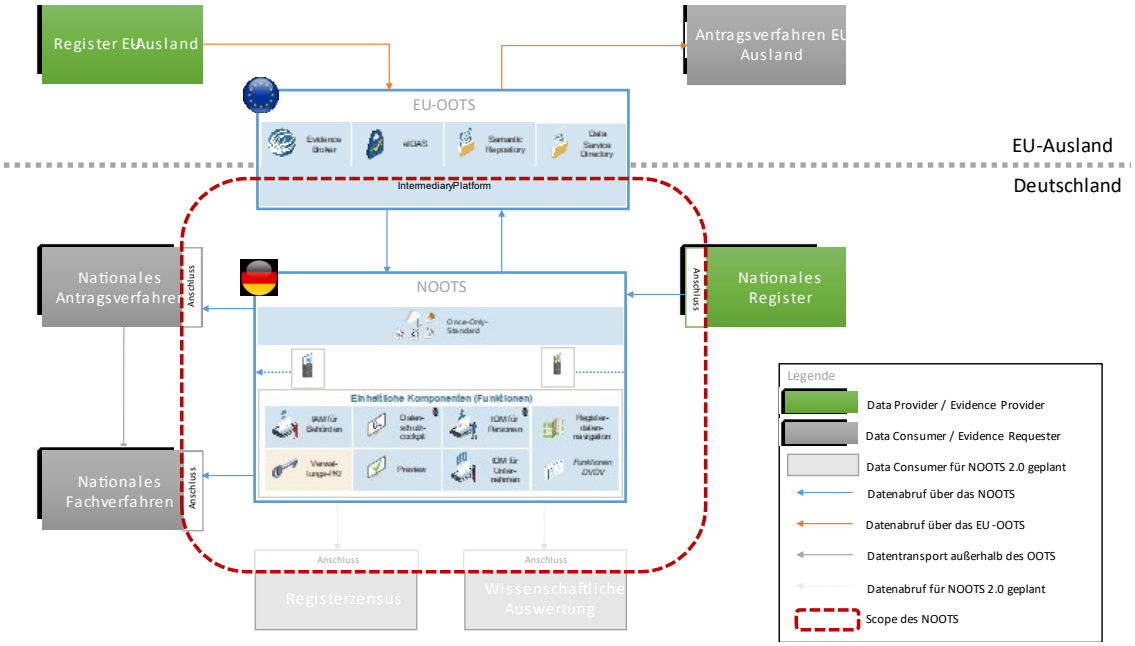


Abbildung 2: Scope High-Level-Architecture

1.3.5 Nachweise

Der Begriff "Nachweis" spielt im NOOTS sowie in EU-OOTS eine zentrale Rolle. In diesem Kapitel wird er zunächst definiert und dann näher differenziert.

Definition

In Artikel 3 der SDG-VO werden Nachweise beschrieben als "alle Unterlagen oder Daten, einschließlich Text-, Ton-, Bild- oder audiovisuelle Aufzeichnungen, unabhängig vom verwendeten Medium, die von einer zuständigen Behörde verlangt werden, um Sachverhalte oder die Einhaltung der in Artikel 2 Absatz 2 Buchstabe b genannten Verfahrensvorschriften nachzuweisen." (Quelle: [RGR-05])

Gemäß dieser Definition sind Nachweise nicht durch technische Merkmale definiert, sondern durch ihre Verwendung zum Nachweis eines Sachverhalts. Das Maß, in dem ein Nachweis elektronisch verarbeitet werden kann, hat dabei erhebliche Auswirkungen auf den Nutzen, den der Nachweisabruf für die Verwaltungsdigitalisierung stiften kann. Daher definiert das folgende Reifegradmodell unterschiedliche Digitalisierungsgrade von Nachweisabrufen.

Reifegradmodell Nachweisabruf

Das Reifegradmodell definiert vier Stufen der Digitalisierung von Nachweisabrufen. In der niedrigsten Stufe A sind Nachweise nicht digitalisiert. Das ist in vielen Fällen der Ausgangszustand. In der höchsten Stufe sind Nachweise elektronisch übermittelbar, elektronisch auswertbar und bedarfsgerecht auf ihren Verwendungszweck zugeschnitten. Das ist der Zielzustand. Dieser erfordert aber nicht nur technologische, sondern auch organisatorische und rechtliche Anforderungen. Es ist daher nicht davon auszugehen, dass dieser Reifegrad im ersten Schritt erreicht wird. Gemäß IT-PLR-Beschluss 2022/22 AL 2 strebt die Registermodernisierung die Erreichung von mindestens Reifegrad C an. Das Ziel, Reifegrad D zu erreichen, bleibt davon unbenommen. (Quelle: [IT-PLR-E-01])

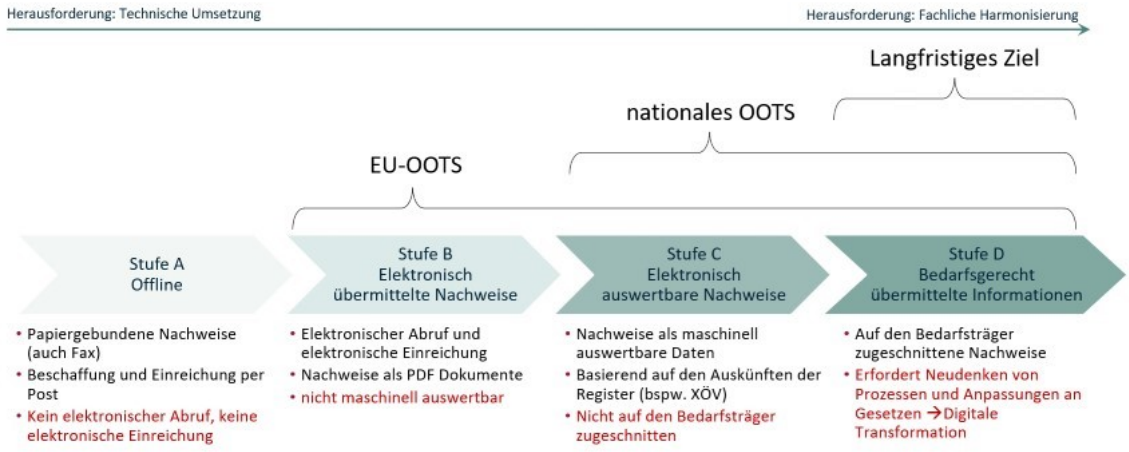


Abbildung 3: Reifegradmodell Registermodernisierung

- **Stufe A – Offline:** Nachweise werden ausschließlich in papiergebundener Form bereitgestellt, ein elektronischer Abruf ist nicht möglich. Der Austausch dieser Nachweise erfolgt durch Bezug und Einreichung durch Bürgerinnen und Bürger oder durch den direkten Austausch zwischen Data Consumer (Fachverfahren) und Data Provider (registerführenden Behörde) auf postalischem Weg oder Fax. In diesem Reifegrad ist eine automatisierte Verarbeitung im Online- oder Fachverfahren nicht möglich. Diese Stufe entspricht weitestgehend dem Status quo in der Verwaltung.
- **Stufe B – Elektronische übermittelte Nachweise:** Nachweise liegen in einem Format vor, das eine elektronische Datenübermittlung ermöglicht, beispielsweise im PDF- bzw. JPEG-Format. Eine maschinelle Auswertung zum Zweck der Datenübernahme in das Antragsformular im Online- oder Fachverfahren ist in diesem Reifegrad noch nicht möglich. Dies entspricht dem durch die Europäische Kommission festgelegten Mindestzustand für die Anbindung an das EU-OOTS.
- **Stufe C – Elektronische auswertbare Nachweise:** Nachweise können elektronisch in strukturierter Form abgerufen werden, sind aber oft den papiergebundenen Nachweisen aus Stufe A und B nachempfunden, bspw. Geburtsurkunden oder Meldeauskünften. Die elektronische Repräsentation orientiert sich an bestehenden Fachstandards, wie sie heute in Registerauskünften genutzt werden, bspw. XMeld oder XPersonenstand. Der Vorteil dieser Reifegradstufe ist, dass Nachweise mindestens in maschinenlesbarer Form

übermittelt werden, was eine automatisierte Datenübernahme im Online- oder Fachverfahren ermöglicht.

- **Stufe D – Bedarfsgerecht übermittelte Informationen:** Diese Reifegradstufe sieht vor, dass Informationen zielgerichtet elektronisch abgerufen werden können. Statt eines Nachweises, der heute auch immer personenbezogene Daten enthält, die für die eigentliche Nachweiserbringung unerheblich sind, werden lediglich ein oder mehrere auf den konkreten Bedarf zugeschnittene Informationen ausgetauscht. Damit wird kein vollständiger Nachweis, sondern lediglich ein maschinenlesbarer Datensatz ausgetauscht, der vom Data Consumer benötigt wird. Auch wäre es in diesem Reifegrad möglich, eine konkrete Frage zur Prüfung eines Sachverhalts zu verschicken, die dann durch die registerführende Behörde beantwortet wird. Würde beispielsweise eine Prüfung auf Volljährigkeit im Antragsprozess notwendig sein, könnte eine registerführende Behörde diesen Sachverhalt dann mit einem "Ja" oder "Nein" beantworten.

1.3.6 Abgrenzungen

1.3.6.1 Standardisierung der Nachweistypen

Damit Nachweise automatisiert verarbeitet werden können, muss Einigkeit unter allen beteiligten Akteuren über Struktur, Syntax und Semantik der Nachweise bestehen. Das betrifft nicht nur Data Provider und Data Consumer. Bei Online-Antragsverfahren ist bspw. auch das Fachverfahren, in dem der Antrag verarbeitet wird, betroffen. Dazu ist eine fachliche Standardisierung aller Nachweistypen erforderlich. Diese Standardisierung ist nicht im Scope des NOOTS. Für die Erreichung der Ziele der Registermodernisierung ist sie jedoch zwingen erforderlich. Dabei sollten bestehende nationale Standard, bspw. DSMeld für das Meldewesen, und zu erwartende Standardisierungsbemühungen auf europäischer Ebene einbezogen werden.

1.3.6.2 Befähigung der Register

Die Register müssen nicht nur technisch an das NOOTS angebunden werden. Sie müssen auch befähigt werden, Nachweise in angemessener Zeit zu liefern. Dazu gehören bspw.

- die Einspeicherung der IDNr.,
- die Bereinigung des Datenbestands, z.B. durch Auflösen von Doubletten,

- durch Digitalisierung der Nachweise als strukturierte Daten, sofern dies noch nicht vollständig der Fall ist,
- die Schaffung technischer Voraussetzungen, um Verfügbarkeit und Antwortzeit zu gewährleisten.

Im Einzelfall ergeben sich daraus weitere Herausforderungen, bspw. wenn das Register keine Datenhoheit über den eigenen Datenbestand hat (bspw. Spiegelregister). Die Steuerung und Umsetzung dieser Maßnahmen liegen nicht im Scope des NOOTS. Das NOOTS definiert lediglich Anschlussbedingungen, die einen Nachweisabruf über das NOOTS technisch grundsätzlich möglich machen.

1.3.6.3 Begriff Registerdatenabruf

Der Abruf von Registerdaten erfolgt nur in Antragsverfahren zur Umsetzung des Once-Only Prinzips oder der SDG-VO zum Zweck des Nachweises von Sachverhalten. In anderen Kontexten (Verwaltungsdigitalisierung, Registerzensus, Wissenschaft) werden dieselben Daten zu einem anderen Zweck benötigt. Da der Nachweisbegriff hier nicht einschlägig ist, wird in diesen Fällen von Registerdatenabrufen gesprochen. Technisch existiert kein Unterschied zwischen Registerdaten und Nachweisen. Auch das Reifegradmodell kann auf Registerdaten angewendet werden.

1.4 High-Level-Architecture Beschreibung

1.4.1 Übergreifende Entwurfsentscheidungen

Die folgenden Entwurfsentscheidungen sind von übergreifender Relevanz für die Gesamtarchitektur.

Tabelle 3: Übergreifende Entwurfsentscheidungen

Entscheidung	Erläuterung	Beschlussreferenz
Entscheidung zur Umsetzung eines NOOTS	Im Validierung des Architekturzielbilds der Registermodernisierung wurde festgestellt, dass bestehende nationale Anforderungen z.B. zur Einführung der Identifikationsnummer nach dem IDNrG und der Wirtschaftsnummer nach dem UBRegG, zur Umsetzung eines Datenschutzcockpit gemäß § 10 OZG oder zur Gewährleistung einer durchgängigen Ende-zu-Ende-Sicherheit perspektivisch nicht durch das bei der Europäischen Kommission (EU-KOM) in Entwicklung befindliche EU-OOTS nach Art. 14 SDG-Verordnung (VO (EU) 2018/1724) abgedeckt werden können. Aus diesem Grund wurde entschieden, dass ein NOOTS umgesetzt werden muss. Um die Anschlussfähigkeit an das EU-OOTS sicherzustellen, dürfen Abweichungen zwischen den nationalen und europäischen Lösungen nur dann erfolgen, wenn diese für die Umsetzung der nationalen Anforderungen zwingend erforderlich sind. Der Anschluss an die EU soll zusätzlich durch eine zentral entwickelte technische Lösung unterstützt werden, den sogenannten „SDG-Connector“.	IT-PLR Beschluss 2022/06
Synchrone und asynchrone Nachweisabrufe	Im Zielbild der Registermodernisierung werden sowohl synchrone und asynchrone Prozesse vorgesehen. Die Begriffe "synchron" und "asynchron" sind dabei nicht in einem technischen Sinne zu verstehen, sondern entsprechend der Eignung für einen Nachweisabruf unter Beteiligung von Bürgern und Unternehmen. Um die für den Nachweisabruf notwendige Nutzerinteraktion zu ermöglichen, muss ein Nachweis synchron, also innerhalb weniger Sekunden, für die Weiterverarbeitung bereitstehen. In asynchronen Prozessen hingegen könnte die Zeit mehrere Minuten, Stunden oder Tage betragen, was sich für einen Nachweisabruf mit Nutzerinteraktion nicht eignet. Dies entspricht auch den Anforderungen des EU-OOTS, in dem ausschließlich synchrone, "automatisiert austauschbare" Nachweisabrufe unterstützt werden. Entsprechend wurde im IT-PLR-Beschluss 2022/22 festgelegt, dass wenn der Data Consumer ein Online-Dienst ist (z. B. ein Portal oder ein Formularmanagementsystem) ist, nur fachlich synchrone	IT-PLR Beschluss 2022/22 - Entscheidung asynchrone Prozesse

Entscheidung	Erläuterung	Beschlussreferenz
	Nachweisabrufe möglich sein sollen. Für die Behörde-zu-Behörde-Kommunikation, in denen keine Nutzerinteraktion notwendig ist, sollen auch fachlich asynchrone Nachweisabrufe möglich sein. Dies ermöglicht die Anbindung von Registern, die noch nicht in der Lage sind, synchron zu antworten.	
Generischer Nachweisabrufstandard	Für die Umsetzung des Once-Only-Prinzips wird es erforderlich sein, eine Vielzahl heterogener IT-Systeme für den Nachweisabruf zu ertüchtigen und miteinander zu verbinden. Um den Abruf und die Übermittlung von Nachweisen zu standardisieren, hat der IT-Planungsrat entschieden, einen generische Nachweisabrufstandard zu entwickeln. Um Vorteile gleichermaßen im nationalen wie auch europäischen Kontext zu erzeugen und die SDG-Umsetzung zu fördern, soll dieser Standard auf Grundlage des Exchange-Data-Model (EDM) des EU-OOTS entwickelt werden und nur dann von dieser abweichen, wenn es im NOOTS zwingend erforderlich ist. Im Folgenden wird dieser Standard auch als DE-EDM-Standard bezeichnet.	IT-PLR Beschluss 2022/22 - Entscheidung Nachweisabrufstandard
Anschluss an dezentrale Register über Spiegelregister oder Abrufportale	Sowohl das EU-OOTS als auch das NOOTS stellen eine Vielzahl unterschiedlicher Anforderungen, sogenannte Anschlussbedingungen, die beim Anschluss an die nationale oder europäische Infrastruktur umgesetzt werden müssen. Während es zentralen Registern voraussichtlich mit akzeptablem Aufwand möglich sein wird, diese Anforderungen zu erfüllen, gestaltet sich die Situation bei dezentralen Registern deutlich komplexer. Insbesondere dann, wenn sich die Dezentralität bis auf kommunale Ebene erstreckt, kann nicht davon ausgegangen werden, dass die notwendigen Ressourcen zur Anbindung an das OOTS vorhanden sind. Auf technischer Ebene ist daher in diesen Fällen überlegenswert, ob der Anschluss an die Systeme zum Nachweisabruf als Anlass genommen werden kann, auch hier zentrale Strukturen wie Spiegelregister oder Abrufportale zu schaffen und diesen dann die Rolle als Data Provider zu übertragen.	IT-PLR Beschluss 2022/34 - Entscheidung NOOTS-Registeranbindung

Entscheidung	Erläuterung	Beschlussreferenz
Anschluss an das EU-OOTS über Intermediäre Plattformen	Um die Aufwände und Belastungen für die verantwortlichen Stellen zur Anbindung der Register und Online-Services an das EU-OOTS möglichst gering zu halten, sollen im Rahmen der Registermodernisierung Aufgaben und Funktionen zur Umsetzung der Anschlussbedingungen soweit möglich und sinnvoll von zentralen Strukturen übernommen werden. Das EU-OOTS erlaubt gemäß Artikel 1 Nr. 6 der Durchführungsverordnung (DVO) für den Anschluss an das System die indirekte Anbindung über Intermediäre Plattformen, die von den Mitgliedstaaten ausgestaltet werden können. Dadurch kann verhindert werden, dass spezifische Funktionalitäten, die nur für die EU-Anbindung benötigt werden, in einer Vielzahl von dezentralen Registern und Online-Services implementiert werden müssen. Der Anschluss öffentlicher Stellen an das technische System gemäß Artikel 14 SDG-VO soll daher verpflichtend über Intermediäre Plattformen (technische Komponenten i.S.v. Art. 1 Nr. 6 DVO zu Art. 14 SDG-VO) erfolgen.	IT-PLR Beschluss 2022/34 - Entscheidung EU-OOTS

1.4.2 Use-Cases

In diesem Kapitel werden die zentralen Use-Cases der Registermodernisierung beschrieben. Jedes Ziel aus Kapitel 1.3.3 Ziele wird durch mindestens einen Use-Case (UC) adressiert. Nicht adressiert werden die Ziele Registerzensus und Wissenschaft. Diese Use-Cases werden in späteren Iterationen dieses Dokuments untersucht.

Die Modellierung erfolgt in Anlehnung an die Prozessmodellierung der europäischen Technical Design Documents unter Verwendung der ArchiMate-Notation. (Quelle: [EU-02]).

Tabelle 4: Überblick Use-Cases

UC	Ziel	Initiator	Data Consumer	Data Provider
1a	Once-Only	Natürliche Person	Deutsches Antragsverfahren	Deutsches Register
1b	Once-Only	Juristische Person	Deutsches Antragsverfahren	Deutsches Register
2	Verwaltungs-digitalisierung	Nationale Behörde	Deutsches Fachverfahren	Deutsches Register
3	SDG-VO	Natürliche oder juristische Person	Verwaltungs-verfahren im EU-Ausland	Deutsches Register
4	SDG-VO	Natürliche oder juristische Person	Deutsches Antragsverfahren	Register im EU-Ausland

Hinweis

Die Ziele "Registerzensus" und "Wissenschaft" werden in dieser Version des NOOTS noch nicht explizit adressiert. Das Ziel "Datenschutz" ist übergreifender Natur und wird durch alle Use-Cases adressiert.

1.4.2.1 Use-Case 1a: Bürgerinitiierter Nachweisabruf im NOOTS

Der Use-Case beschreibt den von einer Bürgerin oder Bürger initiierten Abruf nationaler Nachweise aus nationalen Registern. Der Abruf erfolgt aus nationalen Antragsverfahren heraus. Dabei wird unterstellt, dass das Antragsverfahren Kenntnis darüber hat, welche Nachweistypen es benötigt und welche Routinginformation es von den Nutzenden abfragen muss, um das für den Nachweis zuständige Register zu ermitteln. Diese Informationen können nach Ermessen des Antragsverfahrens auch schon beim Ausfüllen des Antrags erhoben und von dort übernommen werden.

In der Regel werden für einen Antrag mehrere Nachweise benötigt. Dann müssen die Prozessschritte UC1a-05 bis UC1a-12 mehrfach durchlaufen werden.

Zweck des Nachweisabrufs ist es, den Nachweis zusammen mit dem Antrag bei der dafür zuständigen Behörde einzureichen. Das Antragsverfahren liegt nicht im Scope des NOOTS. Daher wird hier weder das Ausfüllen des Antrags noch das Einreichen des Antrags beschrieben.

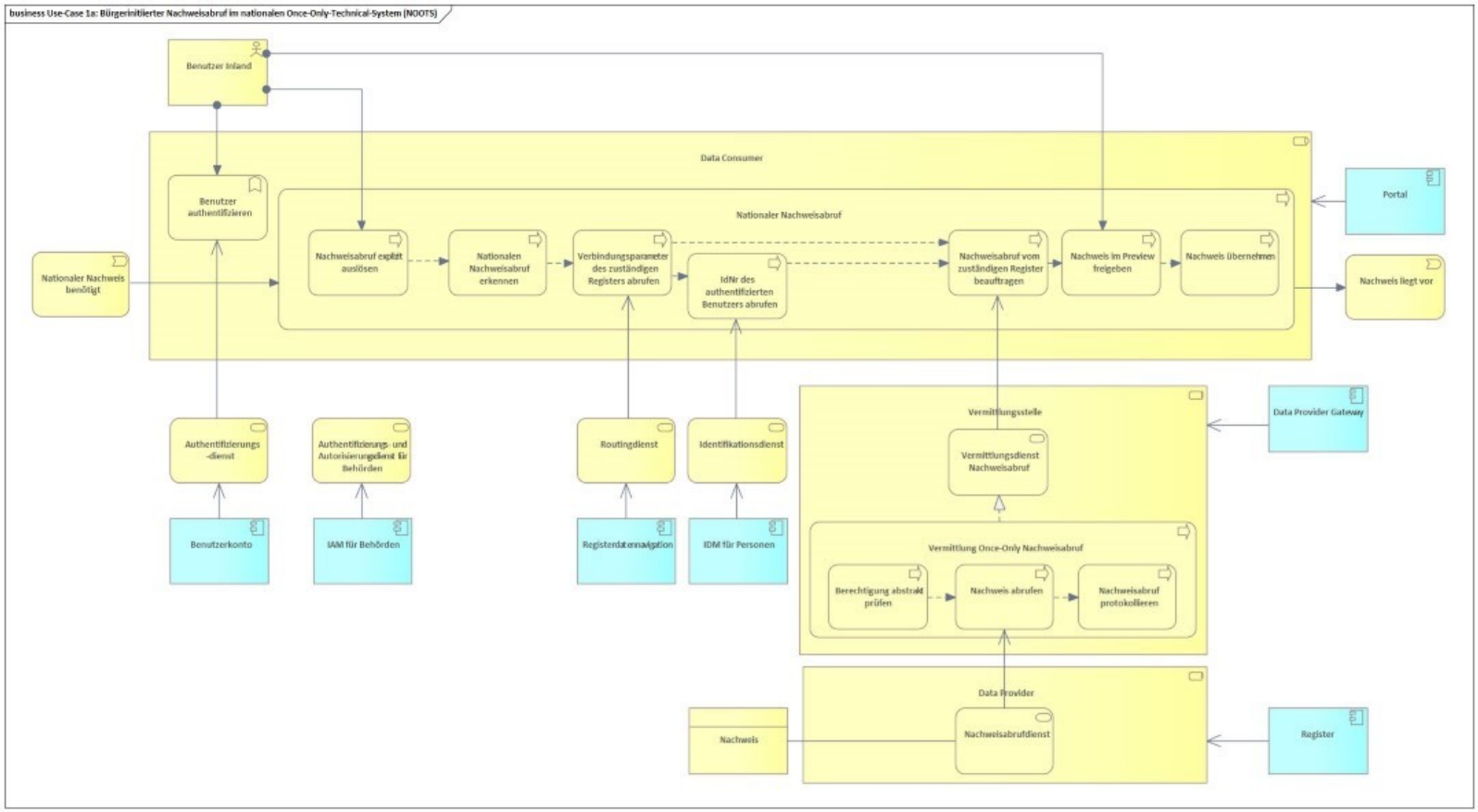


Abbildung 4: Use-Case 1a: Bürgerinitiierter Nachweisabruf

Tabelle 5: Prozessschritte Use-Case 1a: Bürgerinitiierter Nachweisabruf im NOOTS

Prozessschritt	Element	Beschreibung	Anmerkung
[UC1a-01]	• Benutzer Inland • Nutzende authentifizieren • Authentifizierungs-dienst • Benutzerkonto	• Für den Bezug einer Verwaltungsleistung müssen sich Nutzende bei einem nationalen Data Consumer anmelden. • Der Data Consumer ist verpflichtet, die Authentizität der Nutzenden durch geeignete Maßnahmen sicherzustellen	• Für ein hohes Vertrauensniveau muss eine Authentifizierung mit der eID erfolgen. • Prozesse innerhalb der Portale / Online-Dienste werden hier nicht im Detail betrachtet
[UC1a-02]	• Benutzer Inland • Nationaler Nachweis benötigt • Nachweisabruf explizit auslösen	• Damit ein Data Consumer einen Nachweis für eine Verwaltungsleistung abrufen darf, müssen Nutzende einen Nachweisabruf veranlassen ("explicit Request").	
[UC1a-03]	• Nationalen Nachweisabruf erkennen	• Da sich der nationale und der europäische Nachweisabruf grundlegend unterscheiden, muss der Data Consumer zunächst prüfen, ob es sich um einen nationalen oder europäischen Nachweisabruf handelt. • Im vorliegenden Prozess stellt der Data Consumer fest, dass es sich um einen nationalen Nachweisabruf handelt.	• Die Prüfung kann durch den Data Consumer selbst oder durch eine Komponente erfolgen, die den Nachweisabruf steuert.

Prozessschritt	Element	Beschreibung	Anmerkung
[UC1a-04]	• IDNr. des authentifizierten Nutzenden abrufen • Identifikations-dienst • IDM für Personen	• Damit Bürgerinnen oder Bürger im Data Provider zweifelsfrei identifiziert werden kann, greift der Data Consumer auf einen Identifikations-Dienst zurück. • Der Identifikations-Dienst wird von der Komponente IDM für Personen bereitgestellt. • Der Identifikations-Dienst liefert anhand von übergebenen Basisdaten (z.B. aus der eID), die einer Person zugehörige Identifikationsnummer.	• Die Identifikationsnummer wird nur dann benötigt, wenn der Data Provider zu der Auswahl von nachweislieferndem Register gehört, die anhand des Registermodernisierungs-gesetzes definiert sind und damit die Identifikationsnummer einspeichern dürfen. Anderenfalls muss der Nachweisabruf ohne Identifikationsnummer durchgeführt werden.
[UC1a-05]	• Verbindungsparame ter des zuständigen Registers abrufen • Routingdienst • Registerdatennaviga tion	• Um den für einen Nachweis zuständigen Data Provider festzustellen, greift der Data Consumer auf einen Routingdienst zurück. • Der Routingdienst wird von der Registerdatennavigation bereitgestellt. • Der Routingdienst liefert die für einen Nachweisabruf notwendigen Verbindungsparameter zum technischen Dienst einer Behörde, von der ein Nachweis ausgestellt wird.	• Im Fall eines nationalen Nachweisabruf kann davon ausgegangen werden, dass dem Data Consumer bekannt ist, ○ welcher Nachweistyp benötigt wird und ○ welche Routingparameter zur Bestimmung des

Prozessschritt	Element	Beschreibung	Anmerkung
			Nachweistyps benötigt werden.
[UC1a-06]	• Nachweisabruf vom zuständigen Register beauftragen	• Sobald alle notwendigen Parameter ermittelt wurden, generiert der Data Consumer einen DE-EDM-Request. • Der Data Consumer verschlüsselt personenbezogene Inhaltsdaten, sodass nur der Data Provider diese einsehen kann. • Im Request werden der gesuchte Nachweistyp, die ermittelten Verbindungsparameter, die ermittelte Identifikationsnummer und weitere Routingparameter übergeben. • Der Data Consumer übermittelt den Request an eine Vermittlungsstelle.	
[UC1a-07]	• Vermittlungsdienst Nachweisabruf	• Die Vermittlungsstelle empfängt den DE-EDM-Request von einem Data Consumer.	
[UC1a-08]	• Berechtigung abstrakt prüfen	• Die Vermittlungsstelle führt, gemäß §7 Identifikationsnummerngesetz, eine abstrakte Berechtigungsprüfung durch. • Im Prozess der abstrakten Berechtigungsprüfung wird ermittelt, ob die beteiligten Kommunikationspartner	• Unter einer abstrakten Berechtigungsprüfung wird verstanden, dass die Prüfung ohne Kenntnis des Nachrichteninhalts und damit insbesondere ohne

Prozessschritt	Element	Beschreibung	Anmerkung
		berechtigt sind, Nachweise zu einem bestimmten Zweck auszutauschen. • Die Prüfung erfolgt anhand von Metadaten aus dem DE-EDM-Request. • Fällt die Prüfung positiv aus, kann der Nachweisabruf fortgesetzt werden. Bei einer negativen Prüfung hat die Vermittlungsstelle die Aufgabe, den Nachweisabruf zu unterbinden.	Kenntnis der betroffenen Person erbracht werden muss.
[UC1a-09]	• Nachweis abrufen	• Im vorliegenden Prozess fällt die Prüfung positiv aus und die Vermittlungsstelle leitet den DE-EDM-Request an den für den Nachweis zuständigen technischen Endpunkt eines Data Provider weiter.	
[UC1a-10]	• Nachweisabruf protokollieren	• Die Vermittlungsstelle führt, gemäß §7 Identifikationsnummerngesetz, eine Protokollierung des Nachweisabrufs durch.	• Die im Identifikations-nummerngesetz geforderte Protokollierung der Vermittlungsstellen wird derzeit nicht durch das Datenschutzcockpit genutzt.
[UC1a-11]	• Nachweisabruf-dienst	• Der Data Provider entschlüsselt die personenbezogenen Inhaltsdaten und ermittelt den gesuchten Nachweis.	

Prozessschritt	Element	Beschreibung	Anmerkung
	• Nachweis	• Der Data Provider generiert eine DE-EDM-Response. • Der Data Provider verschlüsselt den ermittelten Nachweis und weitere sonstige personenbezogene Daten, sodass nur der Data Consumer diese einsehen kann. • Der Data Provider übermittelt die Response an die Vermittlungsstelle.	
[UC1a-12]	• Vermittlungsdienst Nachweisabruf	• Die Vermittlungsstelle empfängt die DE-EDM-Response des Data Providers. • Die Vermittlungsstelle leitet die DE-EDM-Response an den Data Consumer weiter.	
[UC1a-13]	• Nachweis in der Preview freigeben	• Der Data Consumer erhält die DE-EDM-Response und entschlüsselt die personenbezogenen Inhaltsdaten. • Der Data Consumer ist verpflichtet, die übermittelten Nachweisdaten vor der Verwendung im Fachverfahren durch die Nutzenden freigeben zu lassen. • Dazu generiert der Data Consumer eine Preview aus den Nachweisdaten. • Bei einer positiven Entscheidung der Nutzenden können die Daten im Antragsverfahren verwendet werden.	• Die Aufbereitung der Daten ebenso wie die Entscheidung, ob der Antrag auch ohne Nachweise eingereicht werden kann, obliegt dem Data Consumer. • Werden mehrere Nachweise benötigt, ist es aus Gründen der Usability sinnvoll, zunächst alle Nachweise abzurufen. Dazu sind die Schritte UC1a-05 bis UC1a-12

Prozessschritt	Element	Beschreibung	Anmerkung
		• Bei einer negativen Entscheidung dürfen die Daten nicht im Antragsverfahren verwendet werden.	für jeden Nachweis auszuführen. Die Nachweisabrufe können parallel erfolgen.
[UC1a-14]	• Nachweis übernehmen	• Im vorliegenden Prozess fällt die Preview positiv aus. • Die Nachweisdaten werden in den Antragsprozess übernommen.	• Der Data Consumer kann selbst entscheiden, wie die ermittelten Nachweisdaten verwendet werden. Beispielsweise könnte der Data Consumer diese im Antrag nutzen, um Daten zu ergänzen oder aber einen Abgleich mit den Angaben der Nutzenden durchführen.
[UC1a-15]	• Nachweis liegt vor	• Der Nachweisabruf ist abgeschlossen.	

1.4.2.2 Use-Case 1b: Unternehmensinitiierter Nachweisabruf im NOOTS

Der Use-Case beschreibt den von einem Unternehmen initiierten Abruf nationaler Nachweise aus nationalen Registern. Der Abruf erfolgt aus nationalen Antragsverfahren aus. Dabei wird unterstellt, dass das Antragsverfahren Kenntnis darüber hat, welche Nachweistypen es benötigt und welche Routinginformation es von den Nutzenden abfragen muss, um das für den Nachweis zuständige Register zu ermitteln. Diese Informationen können nach Ermessen des Antragsverfahrens auch schon beim Ausfüllen des Antrags erhoben und von dort übernommen werden.

In der Regel werden für einen Antrag mehrere Nachweise benötigt. Dann müssen die Prozessschritte UC1b-05 bis UC1b-12 mehrfach durchlaufen werden.

Zweck des Nachweisabrufs ist es, den Nachweis zusammen mit dem Antrag bei der dafür zuständigen Behörde einzureichen. Das Antragsverfahren liegt nicht im Scope des NOOTS. Daher wird hier weder das Ausfüllen des Antrags noch das Einreichen des Antrags beschrieben.

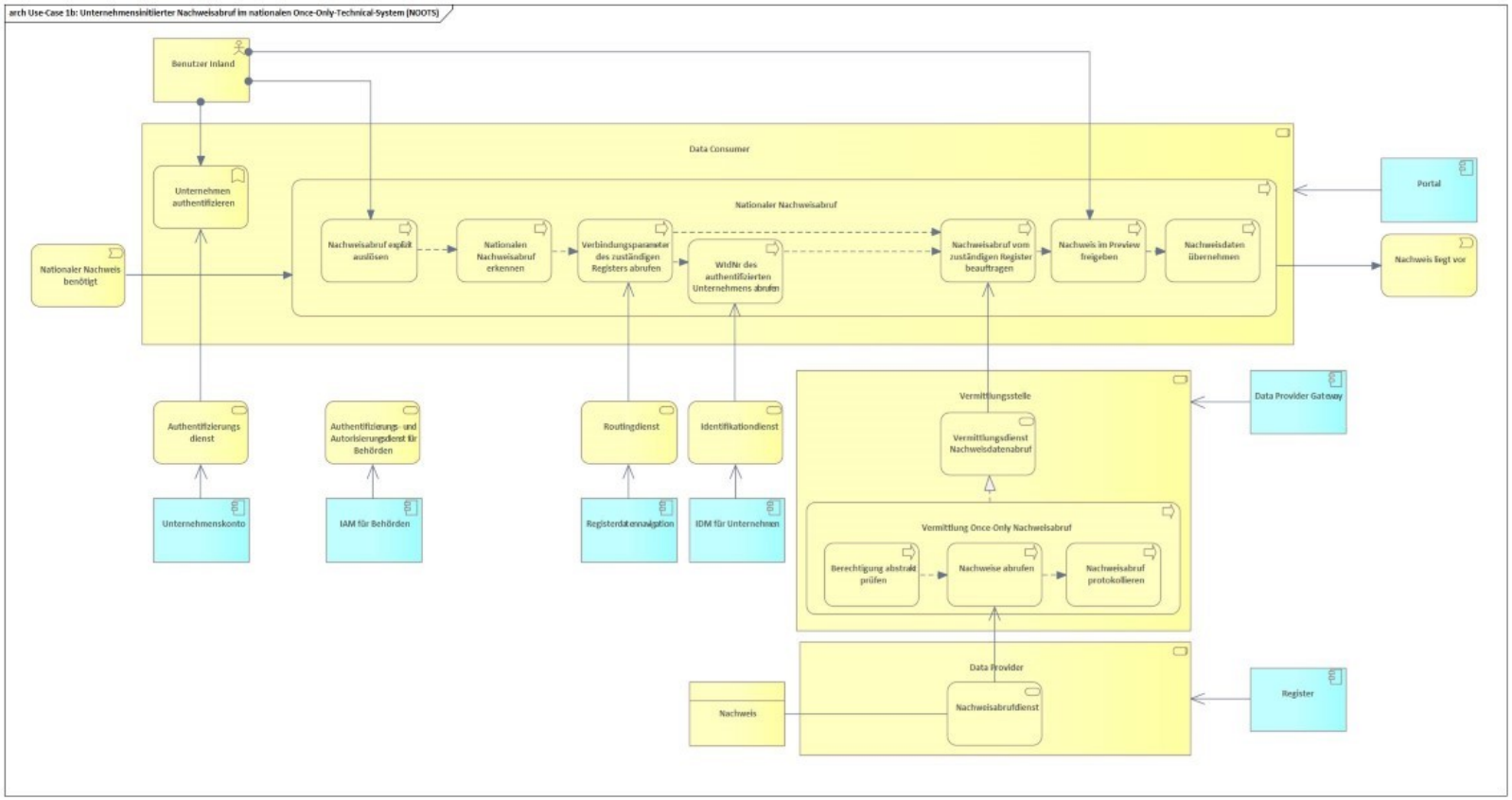


Abbildung 5: Use-Case 1b: Unternehmensinitiierter Nachweisabruf

Tabelle 6: Prozessschritte Use-Case 1b: Unternehmensinitiierter Nachweisabruf

Prozessschritt	Element	Beschreibung	Anmerkung
[UC1b-01]	• Benutzer Inland • Nutzende authentifizieren • Unternehmen authentifizieren • Authentifizierungs-dienst & Unternehmens-konto	• Für den Bezug einer Verwaltungsleistung müssen sich Nutzende, die im Auftrag eines Unternehmens handeln, bei einem nationalen Data Consumer anmelden. • Der Data Consumer ist verpflichtet, die Authentizität der Nutzenden durch geeignete Maßnahmen sicherzustellen. Gleichzeitig muss sichergestellt sein, dass die Nutzenden im Auftrag des Unternehmens handeln dürfen.	• Für ein hohes Vertrauensniveau muss eine Authentifizierung mit der eID erfolgen. • Prozesse innerhalb der Portale / Online-Dienste werden hier nicht im Detail betrachtet.
[UC1b-02]	• Benutzer Inland • Nationaler Nachweis benötigt • Nachweisabruf explizit auslösen	• Damit ein Data Consumer einen Nachweis für eine Verwaltungsleistung abrufen darf, müssen die Nutzenden einen Nachweisabruf veranlassen ("explicit Request").	
[UC1b-03]	• Nationalen Nachweisabruf erkennen	• Der Data Consumer muss prüfen, ob es sich um einen nationalen oder europäischen Nachweisabruf handelt. • Im vorliegenden Prozess stellt der Data Consumer fest, dass es sich um einen nationalen Nachweisabruf handelt.	

Prozessschritt	Element	Beschreibung	Anmerkung
[UC1b-04]	• Verbindungsparameter des zuständigen Registers abrufen • Routingdienst • Registerdaten-navigation	• Um den für einen Nachweis zuständigen Data Provider festzustellen, greift der Data Consumer auf einen Routingdienst zurück. • Der Routingdienst wird von der Registerdatennavigation bereitgestellt. • Der Routingdienst liefert die für einen Nachweisabruf notwendigen Verbindungsparameter zum technischen Dienst einer Behörde, die für die Ausstellung des Nachweises verantwortlich ist.	• Im Fall eines nationalen Nachweisabrufs kann davon ausgegangen werden, dass dem Data Consumer bekannt ist, • welche Nachweistypen für ein Antragsverfahren benötigt werden und • welche Routingparameter zur Bestimmung des Nachweistyps benötigt werden.
[UC1b-05]	• WIDNr. der authentifizierten Nutzenden abrufen • Identifikations-dienst • IDM für Unternehmen	• Damit das Unternehmen im Data Provider zweifelsfrei identifiziert werden kann, greift der Data Consumer auf einen Identifikations-Dienst zurück. • Der Identifikations-Dienst wird von der Komponente IDM für Unternehmen bereitgestellt. • Der Identifikations-Dienst liefert anhand von übergebenen Basisdaten (z.B. aus der eID) die einem Unternehmen zugehörige Wirtschaftsidentifikationsnummer.	•

Prozessschritt	Element	Beschreibung	Anmerkung
[UC1b-06]	• Nachweisabruf vom zuständigen Register beauftragen	• Sobald alle notwendigen Parameter ermittelt wurden, generiert der Data Consumer einen DE-EDM-Request. • Der Data Consumer verschlüsselt personenbezogene Inhaltsdaten, sodass nur der Data Provider diese einsehen kann. • Im Request werden der gesuchte Nachweistyp, die ermittelten Verbindungsparameter, die ermittelte Wirtschaftsidentifikationsnummer und weitere Routingparameter übergeben. • Der Data Consumer übermittelt den Request an eine Vermittlungsstelle.	
[UC1b-07]	• Vermittlungsdienst Nachweisabruf	• Die Vermittlungsstelle empfängt den DE-EDM-Request von einem Data Consumer.	
[UC1b-08]	• Berechtigung abstrakt prüfen	• Die Vermittlungsstelle führt eine abstrakte Berechtigungsprüfung durch. • Im Prozess der abstrakten Berechtigungsprüfung wird ermittelt, ob die beteiligten Kommunikationspartner berechtigt sind, Nachweise zu einem bestimmten Zweck auszutauschen. • Die Prüfung erfolgt anhand von Metadaten aus dem DE-EDM-Request.	

Prozessschritt	Element	Beschreibung	Anmerkung
		• Fällt die Prüfung positiv aus, kann der Nachweisabruf fortgesetzt werden. Bei einer negativen Prüfung hat die Vermittlungsstelle die Aufgabe, den Nachweisabruf zu unterbinden.	
[UC1b-09]	• Nachweis abrufen	• Die Vermittlungsstelle leitet den DE-EDM-Request an den für den Nachweis zuständigen technischen Endpunkt eines Data Provider weiter.	
[UC1b-10]	• Nachweisabruf protokollieren	• Die Vermittlungsstelle führt eine Protokollierung des Nachweisabrufs durch.	
[UC1b-11]	• Nachweisabruf-dienst • Nachweis	• Der Data Provider entschlüsselt die personenbezogenen Inhaltsdaten und ermittelt den gesuchten Nachweis. • Der Data Provider generiert eine DE-EDM-Response. • Der Data Provider verschlüsselt den ermittelten Nachweis und weitere sonstige personenbezogene Daten, sodass nur der Data Consumer diese einsehen kann. • Der Data Provider übermittelt die Response an die Vermittlungsstelle.	

Prozessschritt	Element	Beschreibung	Anmerkung
[UC1b-12]	• Vermittlungsdienst Nachweisabruf	• Die Vermittlungsstelle empfängt die DE-EDM-Response des Data Providers. • Die Vermittlungsstelle leitet die DE-EDM-Response an den Data Consumer weiter.	
[UC1b-13]	• Nachweis in der Preview freigeben	• Der Data Consumer erhält die DE-EDM-Response und entschlüsselt die personenbezogenen Inhaltsdaten. • Der Data Consumer ist verpflichtet, die übermittelten Nachweisdaten vor der Verwendung im Fachverfahren durch die Nutzenden freigeben zu lassen. • Dazu generiert der Data Consumer eine Preview aus den Nachweisdaten. • Bei einer positiven Entscheidung der Nutzenden können die Daten im Antragsverfahren verwendet werden. • Bei einer negativen Entscheidung dürfen die Daten nicht im Antragsverfahren verwendet werden.	
[UC1b-14]	• Nachweis übernehmen	• Im vorliegenden Prozess fällt die Preview positiv aus. • Die Nachweisdaten werden in den Antragsprozess übernommen.	

Prozessschritt	Element	Beschreibung	Anmerkung
[UC1b-15]	• Nachweis liegt vor	• Der Nachweisabruf ist abgeschlossen.	

1.4.2.3 Use-Case 2: Behördeninitiierter Registerdatenabruf im NOOTS

Der Use-Case beschreibt den von einer Behörde initiierten Abruf nationaler Nachweise aus nationalen Registern ohne Beteiligung von Bürgern oder Unternehmen. Der Abruf erfolgt aus nationalen Antragsverfahren aus. Dabei wird unterstellt, dass das Antragsverfahren Kenntnis darüber hat, welche Nachweistypen und welche Routinginformation es benötigt, um das für den Nachweis zuständige Register zu ermitteln.

Werden mehrere Nachweise benötigt, müssen die Prozessschritte UC2-05 bis UC1a-10 mehrfach durchlaufen werden.

Zweck des Nachweisabrufs ist es, den Nachweis direkt im Fachverfahren zu nutzen. Das Fachverfahren liegt nicht im Scope des NOOTS. Daher wird das Einreichen des Antrags hier nicht beschrieben.

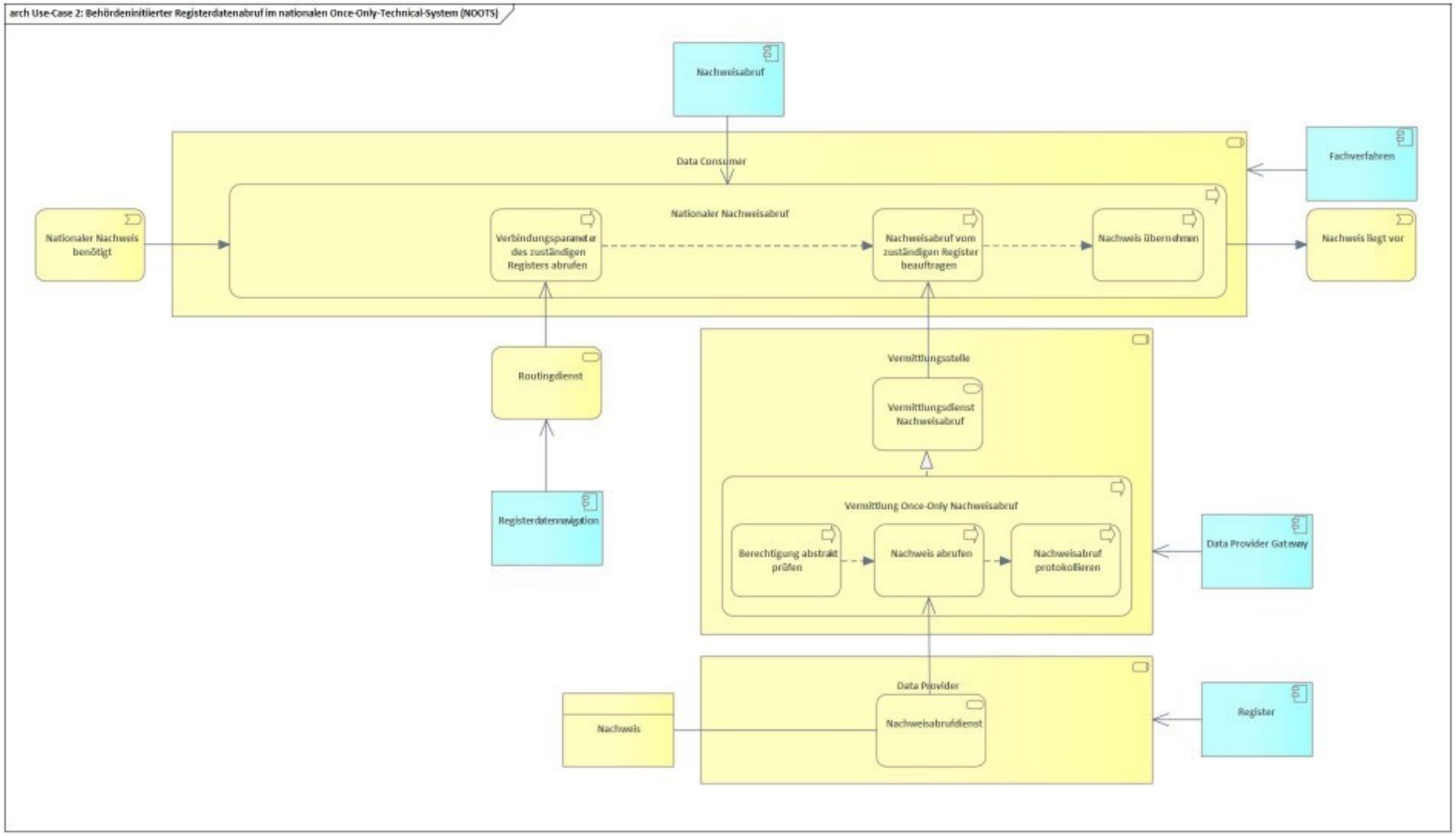


Abbildung 6: Use-Case 2: Behördeninitiierter Registerdatenabruf

Tabelle 7: Prozessschritte Use-Case 2: Behördeninitiierter Registerdatenabruf

Prozessschritt	Element	Beschreibung	Anmerkung
[UC2-01]	• Nationalen Nachweis benötigt • Nachweisabruf explizit auslösen	• Der Abruf eines Nachweises wird durch eine Behörde initiiert.	• Im Unterschied zum bürgerinitiierten Nachweisabruf wird dieser Prozess ohne Beteiligung des Bürgers durchgeführt.
[UC2-02]	• Verbindungsparameter des zuständigen Registers abrufen • Routingdienst • Registerdaten-navigation	• Um den für einen Nachweis zuständigen Data Provider festzustellen, greift der Data Consumer auf einen Routingdienst zurück. • Der Routingdienst wird von der Registerdatennavigation bereitgestellt. • Der Routingdienst liefert die für einen Nachweisabruf notwendigen Verbindungsparameter zum technischen Dienst einer Behörde, die für die Ausstellung des Nachweises verantwortlich sind.	• Im Fall eines nationalen Nachweisabruf kann davon ausgegangen werden, dass dem Data Consumer bekannt ist, • welche Nachweistypen benötigt werden und • welche Routingparameter zur Bestimmung des Nachweistyp benötigt werden.
[UC2-03]	• Nachweisabruf vom zuständigen Register beauftragen	• Sobald alle notwendigen Parameter ermittelt wurden, generiert der Data Consumer einen DE-EDM-Request.	

Prozessschritt	Element	Beschreibung	Anmerkung
		• Der Data Consumer verschlüsselt personenbezogene Inhaltsdaten, sodass nur der Data Provider diese einsehen kann. • Im Request werden der gesuchte Nachweistyp, die ermittelten Verbindungsparameter und weitere Routingparameter übergeben. • Der Data Consumer übermittelt den Request an eine Vermittlungsstelle.	
[UC2-04]	• Vermittlungsdienst Nachweisabruf	• Die Vermittlungsstelle empfängt den DE-EDM-Request von einem Data Consumer.	
[UC2-05]	• Berechtigung abstrakt prüfen	• Die Vermittlungsstelle führt eine abstrakte Berechtigungsprüfung durch. • Im Prozess der abstrakten Berechtigungsprüfung wird ermittelt, ob die beteiligten Kommunikationspartner berechtigt sind, Nachweise zu einem bestimmten Zweck auszutauschen. • Die Prüfung erfolgt anhand von Metadaten aus dem DE-EDM-Request. • Fällt die Prüfung positiv aus, kann der Nachweisabruf fortgesetzt werden.	

Prozessschritt	Element	Beschreibung	Anmerkung
		• Bei einer negativen Prüfung hat die Vermittlungsstelle die Aufgabe, den Nachweisabruf zu unterbinden.	
[UC2-06]	• Nachweis abrufen	• Die Vermittlungsstelle leitet den DE-EDM-Request an den für den Nachweis zuständigen technischen Endpunkt eines Data Provider weiter.	
[UC2-07]	• Nachweisabruf protokollieren	• Die Vermittlungsstelle führt eine Protokollierung des Nachweisabrufs durch.	
[UC2-08]	• Nachweisabruf-dienst • Nachweis	• Der Data Provider entschlüsselt die personenbezogenen Inhaltsdaten und ermittelt den gesuchten Nachweis. • Der Data Provider generiert eine DE-EDM-Response. • Der Data Provider verschlüsselt den ermittelten Nachweis und weitere sonstige personenbezogene Daten, sodass nur der Data Consumer diese einsehen kann. • Der Data Provider übermittelt die Response an eine Vermittlungsstelle.	
[UC2-09]	• Vermittlungsdienst Nachweisabruf	• Die Vermittlungsstelle empfängt die DE-EDM-Response des Data Providers.	

Prozessschritt	Element	Beschreibung	Anmerkung
		• Die Vermittlungsstelle leitet die DE-EDM-Response an den Data Consumer weiter.	
[UC2-10]	• Nachweis übernehmen	• Die Nachweisdaten werden in das Antragsverfahren übernommen.	
[UC2-11]	• Nachweis liegt vor	• Der Nachweisabruf ist abgeschlossen.	

1.4.2.4 Use-Case 3: Abruf von nationalen Nachweisen über das EU-OOTS

Der Use-Case beschreibt den von einer Bürgerin oder Bürger initiierten Abruf nationaler Nachweise aus nationalen Registern über das EU-OOTS. Der Abruf erfolgt aus europäischen Antragsverfahren aus. Das Antragsverfahren hat keine Kenntnis darüber, welche Nachweistypen es benötigt und welche Routinginformation es von den Nutzenden abfragen muss, um das für den Nachweis zuständige Register zu ermitteln. Diese Informationen können erst im Nachweisabrufprozess erhoben werden.

In der Regel werden für einen Antrag mehrere Nachweise benötigt. Dann müssen die Prozessschritte UC3-03 bis UC3-19 mehrfach durchlaufen werden.

Zweck des Nachweisabrufs ist es, den Nachweis zusammen mit dem Antrag bei der dafür zuständigen Behörde einzureichen. Das Antragsverfahren liegt nicht im Scope des NOOTS. Daher wird hier weder das Ausfüllen des Antrags noch das Einreichen des Antrags beschrieben.

Zur besseren Unterscheidbarkeit sind Prozessschritte im Rahmen des EU-OOTS schraffiert hinterlegt:

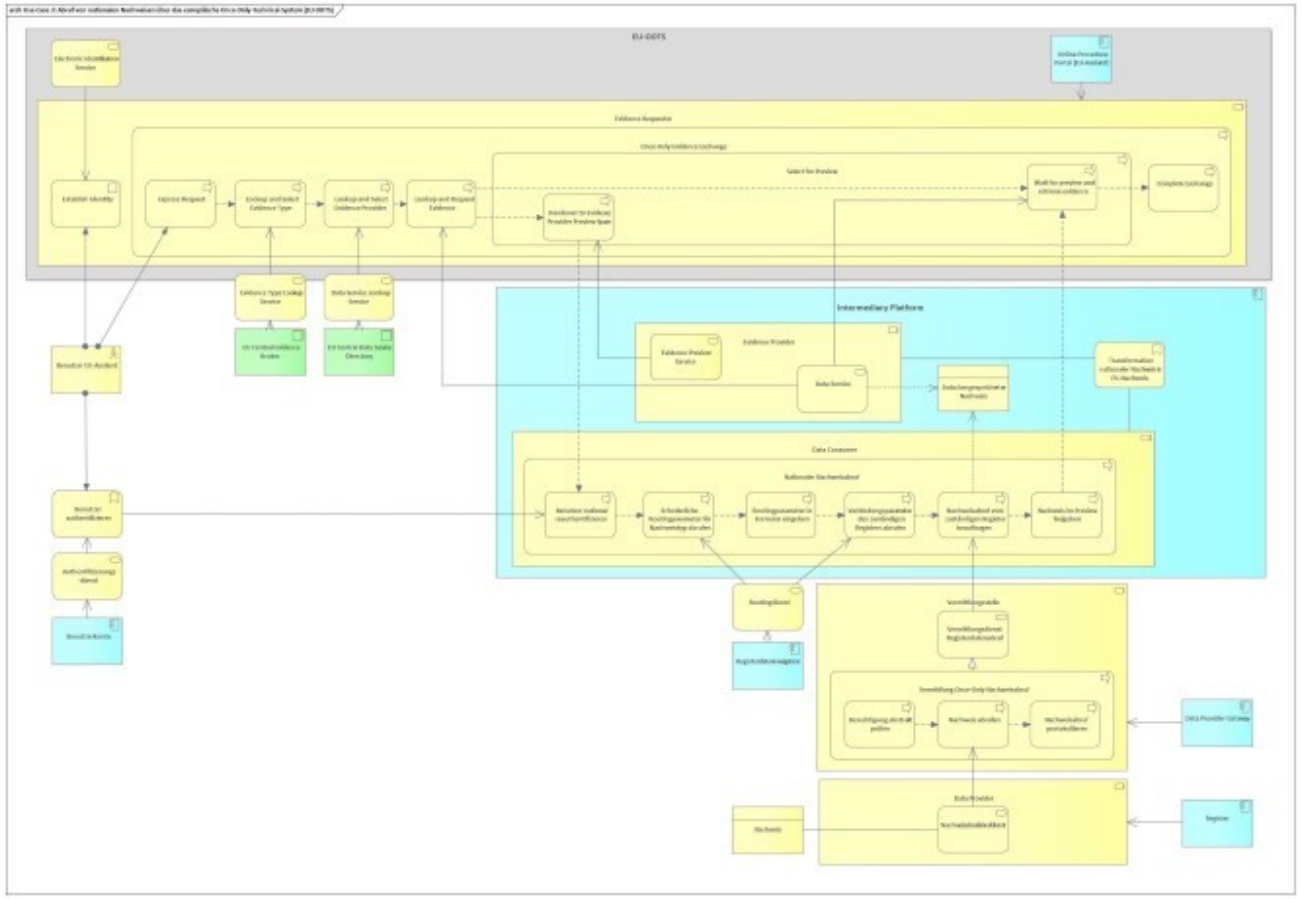


Abbildung 7: Use-Case 3: Abruf von nationalen Nachweisen

Tabelle 8: Prozessschritte Use-Case 3: Abruf von nationalen Nachweisen

Prozessschritt	Element	Beschreibung	Anmerkung
[UC3-01]	• Benutzer EU-Ausland • Electronic Identification Service • Establish Identity	• Für den Bezug einer europäischen Verwaltungsleistung müssen sich Nutzende zunächst bei einem europäischen Evidence Requester anmelden. • Der Evidence Requester ist verpflichtet, die Authentizität der Nutzenden durch geeignete Maßnahmen sicherzustellen. • Zur Authentifizierung wird eIDAS verwendet.	• Prozesse innerhalb der Portale / Online-Dienste werden hier nicht im Detail betrachtet.
[UC3-02]	• Benutzer EU-Ausland • Express Request	• Damit ein Evidence Requester einen Nachweis für eine europäische Verwaltungsleistung abrufen darf, müssen Nutzende einen Nachweisabruf veranlassen ("explicit Request").	
[UC3-03]	• Lookup and Select Evidence Type • Evidence Type Lookup Service • EU Central Evidence Broker	• Um einen europäischen Nachweisabruf durchführen zu können, muss der Evidence Requester zunächst den Evidence Broker des Mitgliedstaats ermitteln, aus dem der Nachweis abgerufen werden soll. • Für Nachweisabrufe aus Deutschland wird der im EU-OOTS zentral bereitgestellte EU Central Evidence Broker verwendet. • Sobald der verantwortliche Evidence Broker ermittelt ist, kann der Evidence Requester abfragen, welcher Nachweistyp	• Dieser Prozess muss für jeden Sachverhalt wiederholt werden. • Wird ein deutscher Nachweis abgerufen, wird der EU Central Evidence Broker verwendet. • Wie mit Auswahllisten verfahren wird, hängt vom jeweiligen Evidence

Prozessschritt	Element	Beschreibung	Anmerkung
		im EU-Mitgliedstaat zu einem zu ermittelnden Sachverhalt (Requirement) zugeordnet ist. • Es ist möglich, dass der Evidence Broker mehr als einen Nachweistypen ermittelt und dem Evidence Requester eine Auswahlliste bereitstellt.	Requester ab und kann unterschiedlich gehandhabt werden.
[UC3-04]	• Lookup and Select Evidence Provider • Data Service Lookup Service • EU Central Data Service Directory	• Zu jedem zuvor ausgewählten Nachweistyp muss der Evidence Requester dann ermitteln, welcher Data Service im Mitgliedsstaat für die Ausstellung des zugehörigen Nachweises zuständig ist. • Dazu muss der Evidence Requester zunächst das Data Service Directory des Mitgliedstaats ermitteln, aus dem der Nachweis abgerufen werden soll. • Für Nachweisabrufe aus Deutschland wird, das im EU-OOTS zentral bereitgestellte EU Central Data Service Directory verwendet. • Sobald das verantwortliche Data Service Directory ermittelt ist, kann der Evidence Requester abfragen, welcher Data Service im EU-Mitgliedstaat einen gesuchten Nachweistyp ausstellt. • Es ist möglich, dass das Data Service Directory mehr als einen Data Service zurück ermittelt und dem Evidence Requester eine Auswahlliste bereitstellt.	• Dieser Prozess muss für jeden Nachweistyp wiederholt werden, für den sich der Evidence Requester zuvor entschieden hat, Nachweise abzurufen. • Wird ein deutscher Nachweis abgerufen, wird das EU Central Data Service Directory verwendet. • Wie mit Auswahllisten verfahren wird, hängt vom jeweiligen Evidence Requester ab.

Prozessschritt	Element	Beschreibung	Anmerkung
		• Bei einem Nachweisabruf aus dem NOOTS kann derzeit davon ausgegangen werden, dass als Antwort immer die Verbindungsparameter eines Data Service zurückgeliefert werden, der durch eine Intermediäre Plattform bereitgestellt wird.	
[UC3-05]	• Lookup and Request Evidence	• Sobald alle notwendigen Parameter ermittelt wurden, generiert der Evidence Requester einen EDM-Request für jeden Nachweisabruf. • Im Request werden der gesuchte Nachweistyp, die ermittelten Verbindungsparameter und weitere Routingparameter übergeben. • Der Evidence Requester übermittelt den Request über Access-Points an die nationale Intermediäre Plattform.	• Im Gegensatz zum nationalen Nachweisabrufprozess muss ein Abruf von Nachweisen der deutschen Verwaltung aus dem EU-Ausland ohne Verwendung der Identifikationsnummer erfolgen. • Stattdessen kommen direkt persönliche Identifikations-daten zum Einsatz.
[UC3-06]	• Data Service	• Da die Intermediäre Plattform zu diesem Zeitpunkt noch nicht weiß, welches Register den Nachweis liefern wird, kann sie diesen nicht unmittelbar abrufen und zurückliefern. • Stattdessen liefert sie eine Exception zurück. Mittels einer darin enthaltenen Preview-URL werden die Nutzenden auf den Preview-Space der Intermediäre Plattform umgeleitet.	• Der Preview-Space ist eine Benutzeroberfläche, die von der Intermediäre Plattform angeboten wird. Er wird verwendet, um direkt mit den Nutzenden zu interagieren, bspw. um Routingparameter zur Ermittlung des

Prozessschritt	Element	Beschreibung	Anmerkung
			zuständigen Registers abzufragen. • Hier findet auch die Preview-Funktion der Nachweise statt.
[UC3-07]	• Handover to Evidence Provider Preview Space	• Der Evidence Requester verarbeitet die Exception und die mitgelieferte URL und leitet die Nutzenden auf den Preview-Space der Intermediäre Plattform durch.	
[UC3-08]	• Nutzende national reauthentifizieren • Nutzende authentifizieren • Authentifizierungs-dienst • Benutzerkonto	• Mit der Weiterleitung der Nutzenden auf den Preview-Space der Intermediären Plattform und damit der Weiterleitung auf die eine Nutzeroberfläche einer NOOTS-Komponente, wird es erforderlich, dass sich die Nutzenden erneut authentifizieren. • Aus nationaler Sicht wird die Intermediäre Plattform, die den Preview-Space bereitstellt, im Folgenden in der Rolle eines nationalen Data Consumer auftreten. • Wie auch bei einem nationalen Nachweisabruf ist es deshalb erforderlich, dass die Intermediäre Plattform die Authentizität der Nutzenden durch geeignete Maßnahmen sicherstellt.	• Für ein hohen Vertrauensniveau muss eine Authentifizierung mit der eID erfolgen. • Prozesse innerhalb der Portale / Online-Dienste werden hier nicht im Detail betrachtet. • Zu klären ist, ob es SSO im NOOTS geben wird, falls mehrere Nachweise abgerufen werden müssen.

Prozessschritt	Element	Beschreibung	Anmerkung
[UC3-9]	• Erforderliche Routingparameter für Nachweistyp abrufen • Routingdienst • Registerdaten-navigation	• Um den für einen Nachweis zuständigen Data Provider festzustellen, greift die Intermediäre Plattform auf einen Routingdienst zurück. • Der Routingdienst wird von der Registerdatennavigation bereitgestellt. • Der Routingdienst liefert der Intermediären Plattform die Information, ob weitere Routingparameter für den Nachweisabruf benötigt werden.	• Für die Nachweisermittlung können unterschiedliche Routingparameter benötigt werden. Der Evidence Requester hat darüber keine Kenntnis, da im Schritt UC3-04 nur Routinginformationen zur Intermediären Plattform abgerufen wurden. • Diese Routingparameter zum eigentlichen Evidence Provider müssen dann von Nutzenden eingegeben werden, um den Nachweisabrufprozess fortsetzen zu können.
[UC3-10]	• Routingparameter in Formular eingeben	• Falls die persönliche Identifikationsdaten aus der Nutzerauthentifizierung nicht ausreichen, einen Nachweisabruf durchzuführen, werden die Nutzenden aufgefordert, die im vorherigen Schritt ermittelten Routingparameter einzugeben.	
[UC3-11]	• Verbindungspara-meter des	• Der Routingdienst liefert im Anschluss die für einen Nachweisabruf notwendigen Verbindungsparameter zum	

Prozessschritt	Element	Beschreibung	Anmerkung
	zuständigen Registers abrufen • Routingdienst • Registerdaten-navigation	technischen Dienst einer Behörde, die für die Ausstellung des Nachweises verantwortlich ist.	
[UC3-12]	• Nachweisabruf-dienst	• Sobald alle notwendigen Parameter ermittelt wurden, generiert die Intermediäre Plattform einen DE-EDM-Request. • Die Intermediäre Plattform verschlüsselt personenbezogene Inhaltsdaten, sodass nur der Data Provider diese einsehen kann. • Im Request werden der gesuchte Nachweistyp, die ermittelten Verbindungsparameter und weitere Routingparameter übergeben. • Die Intermediäre Plattform übermittelt den Request an eine Vermittlungsstelle.	• Bis zu diesem Punkt wurden personenbezogene Inhaltsdaten ohne Ende-zu-Ende-Verschlüsselung über das EU-OOTS ausgetauscht.
[UC3-13]	• Vermittlungsdienst Nachweisabruf	• Die Vermittlungsstelle empfängt den DE-EDM-Request von einem Data Consumer.	• Im Gegensatz zum nationalen Nachweisabrufprozess muss ein europäischer Nachweisabrufprozess ohne Verwendung der

Prozessschritt	Element	Beschreibung	Anmerkung
			Identifikationsnummer erfolgen.
[UC3-14]	• Berechtigung abstrakt prüfen	• Im §7 des Identifikationsnummerngesetz wird beschrieben, dass Vermittlungsstellen die Übermittlungsberechtigung abstrakt prüfen und protokollieren müssen. • Das Identifikationsnummerngesetz gilt ausschließlich für Nachweisabrufe, die unter Verwendung der Identifikationsnummer durchgeführt werden. • Europäische Nachweisabrufe erfolgen grundsätzlich ohne Identifikationsnummer. • Es ist nicht geklärt, ob eine abstrakte Berechtigungsprüfung und Protokollierung durchgeführt werden müssen.	• Die abstrakte Berechtigungsprüfung könnte, wenn auch nicht durch das Identifikationsnummern-gesetz gefordert, dennoch einen Beitrag zur IT-Sicherheit / Datenschutz leisten. • Entsprechend ist zu klären, ob die Vermittlungsstellen bei europäischen Nachweisabrufen dennoch eine abstrakte Berechtigungsprüfung und Protokollierung durchführen sollten.
[UC3-15]	• Nachweisabruf-dienst • Nachweis	• Der Data Provider entschlüsselt die personenbezogenen Inhaltsdaten und ermittelt den gesuchten Nachweis. • Der Data Provider generiert eine DE-EDM-Response.	

Prozessschritt	Element	Beschreibung	Anmerkung
		• Der Data Provider verschlüsselt den ermittelten Nachweis und weitere sonstige personenbezogene Daten, sodass nur der Data Consumer diese einsehen kann. • Der Data Provider übermittelt die Response an eine Vermittlungsstelle.	
[UC3-16]	• Nachweisabruf protokollieren	• Die Vermittlungsstelle empfängt die DE-EDM-Response vom Data Provider. • Die Vermittlungsstelle protokolliert den Nachweisabruf. • Die Vermittlungsstelle leitet die DE-EDM-Response an die Intermediäre Plattform weiter.	
[UC3-17]	• Nachweis in der Preview freigeben	• Die Intermediäre Plattform erhält die DE-EDM-Response und entschlüsselt die personenbezogenen Inhaltsdaten. • Die Intermediäre Plattform ist verpflichtet, die übermittelten Nachweisdaten vor der Weiterleitung an den Evidence Requester durch die Nutzenden freigeben zu lassen. • Dazu generiert die Intermediäre Plattform eine Preview aus den Nachweisdaten. • Die Nutzenden können entscheiden, die in der Preview angezeigten Daten freizugeben. • Bei einer positiven Entscheidung können die Nachweise vom Evidence Requester abgerufen werden. Bei einer negativen	

Prozessschritt	Element	Beschreibung	Anmerkung
		Entscheidung dürfen die Nachweise nicht an den Evidence Requester herausgegeben werden. • Im vorliegenden Fall wird die Preview positiv beschieden. • Die Intermediäre Plattform führt die Nutzenden zurück auf den Preview-Space des Evidence Requester und übermittelt eine Preview-ID, mit der ein Nachweis im Anschluss bei der Intermediären Plattform abgerufen werden kann.	
[UC3-18]	• Wait for preview and retrieve evidence	• Der Evidence Requester erzeugt einen erneuten EDM-Request und übergibt zusätzlich zu den zuvor übermittelten Parametern auch die von der Intermediäre Plattform erhaltene Preview-ID. • Der Evidence Requester übermittelt den Request über Access-Points an den Data Service der Intermediäre Plattform.	
[UC3-19]	• Data Service	• Die Intermediäre Plattform verarbeitet die Preview-ID und erzeugt eine EDM-Response, die den freigegebenen Nachweis beinhaltet. • Die Intermediäre Plattform übermittelt die EDM-Response über Access-Points an den Evidence Requester.	

Prozessschritt	Element	Beschreibung	Anmerkung
[UC3-20]	• Complete Exchange	• Der Nachweisabruf ist abgeschlossen.	• Falls mehrere Nachweise benötigt werden, wird der Prozess ab Schritt UC3-06 für jeden noch fehlenden Nachweis wiederholt.

1.4.2.5 Use-Case 4: Abruf von europäischen Nachweisen über das EU-OOTS

Der Use-Case beschreibt den von einer Bürgerin oder Bürger initiierten Abruf europäischer Nachweise aus europäischen Registern über das EU-OOTS. Der Abruf erfolgt aus deutschen Antragsverfahren heraus. Das Antragsverfahren hat keine Kenntnis darüber, welche Nachweistypen es benötigt und welche Routinginformation es von den Nutzenden abfragen muss, um das für den Nachweis zuständige Register zu ermitteln. Diese Informationen können erst im Nachweisabrufprozess erhoben werden.

In der Regel werden für einen Antrag mehrere Nachweise benötigt. Dann müssen die Prozessschritte UC4-06 bis UC4-19 mehrfach durchlaufen werden.

Zweck des Nachweisabrufs ist es, den Nachweis zusammen mit dem Antrag bei der dafür zuständigen Behörde einzureichen. Das Antragsverfahren liegt nicht im Scope des NOOTS. Daher wird hier weder das Ausfüllen des Antrags noch das Einrichten beschrieben.

Zur besseren Unterscheidbarkeit sind Prozessschritte im Rahmen des EU-OOTS schraffiert hinterlegt:

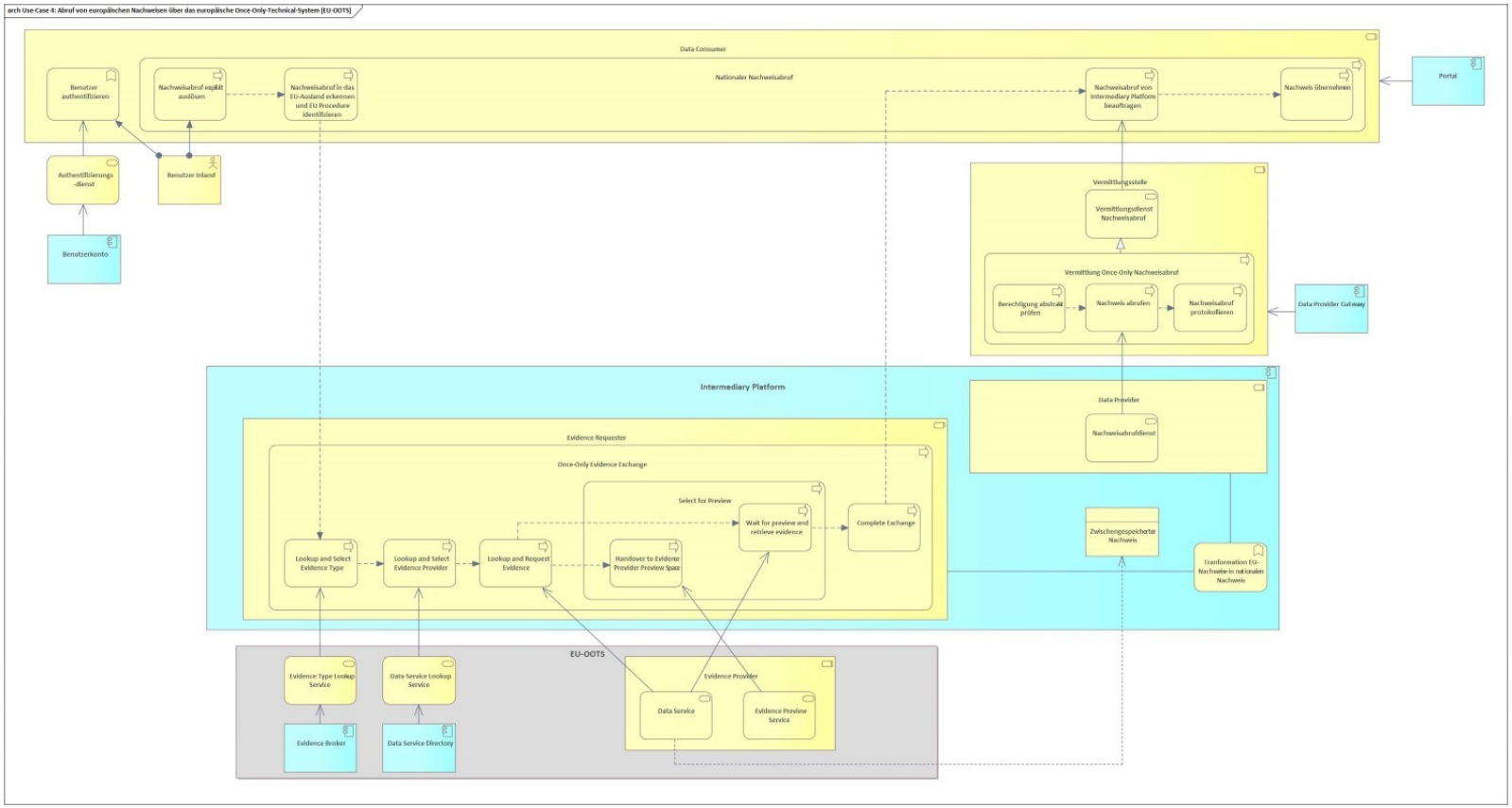


Abbildung 8: Use-Case 4: Abruf von europäischen Nachweisen

Tabelle 9: Prozessschritte Use-Case 4: Abruf von europäischen Nachweisen

Prozessschritt	Element	Beschreibung	Anmerkung
[UC4-01]	• Nutzende Inland • Nutzende authentifizieren • Authentifizierungs-dienst • Benutzerkonto	• Für den Bezug einer Verwaltungsleistung müssen sich Nutzende zunächst bei einem nationalen Data Consumer anmelden. • Der Data Consumer ist verpflichtet, die Authentizität der Nutzenden durch geeignete Maßnahmen sicherzustellen.	• Für ein hohes Vertrauensniveau muss eine Authentifizierung mit der eID erfolgen. • Prozesse innerhalb der Portale / Online-Dienste werden hier nicht im Detail betrachtet.
[UC4-02]	• Benutzer Inland • Nachweisabruf explizit auslösen	• Damit ein Data Consumer einen Nachweis für eine Verwaltungsleistung abrufen darf, müssen Nutzende einen Nachweisabruf veranlassen ("explicit Request").	• Der Begriff "Zustimmung" wurde im Kontext der Consent-Komponente durch das KT Recht & Datenschutz als unpassend eingestuft.
[UC4-03]	• Europäischen Nachweisabruf erkennen	• Der Data Consumer muss prüfen, ob es sich um einen nationalen oder europäischen Nachweisabruf handelt. • Im vorliegenden Prozess stellt der Data Consumer fest, dass es sich um einen europäischen Nachweisabruf handelt. • Aus diesem Grund übergibt der Data Consumer den Nachweisabruf mit einem DE-EDM-Request an die zuständige Intermediäre Plattform.	• Ob die Prüfung durch den Data Consumer selbst oder eine noch zu konzeptionierende Komponente erfolgen wird, die den Nachweisabruf steuert und als "Weiche"

Prozessschritt	Element	Beschreibung	Anmerkung

			fungiert, wird derzeit im KT Architektur untersucht.
			• Klärungspunkte:
			  ○ Bündelung von Nachweisabrufen
			  ○ Identifikation des Requirements
			  ○ Übergabe über 4-Corner?

[UC4-04]	• Lookup and Select Evidence Type • Evidence Type Lookup Service • EU Central Evidence Broker	• Um einen europäischen Nachweisabruf durchführen zu können, muss die Intermediäre Plattform zunächst den Evidence Broker des Mitgliedstaats ermitteln, aus dem der Nachweis abgerufen werden soll. • Sobald der verantwortliche Evidence Broker ermittelt ist, kann der Evidence Requester abfragen, welcher Nachweistyp im EU-Mitgliedstaat zu einem zu ermittelnden Sachverhalt (Requirement) zugeordnet ist. • Es ist möglich, dass der Evidence Broker mehr als einen Nachweistypen ermittelt und dem Evidence Requester eine Auswahlliste bereitstellt.	• Dieser Prozess muss für jeden Sachverhalt wiederholt werden. • Wie mit Auswahllisten verfahren wird, hängt vom jeweiligen Evidence Requester ab und kann unterschiedlich gehandhabt werden.

Prozessschritt	Element	Beschreibung	Anmerkung
		• Diese werden den Nutzenden in einer Auswahlliste angeboten. Die Nutzenden können einen oder mehrere Nachweistypen auswählen.	
[UC4-05]	• Lookup and Select Evidence Provider • Data Service Lookup Service • EU Central Data Service Directory	• Zu jedem zuvor ausgewählten Nachweistyp muss die Intermediäre Plattform dann ermitteln, welcher Evidence Provider im Mitgliedsstaat für die Ausstellung des zugehörigen Nachweises zuständig ist. • Dazu muss die Intermediäre Plattform zunächst das Data Service Directory des Mitgliedstaats ermitteln, aus dem der Nachweis abgerufen werden soll. • Vom verantwortlichen Data Service Directory fragt die Intermediäre Plattform ab, welcher Data Service im EU-Mitgliedstaat einen gesuchten Nachweistyp ausstellt. Falls für die Abfrage weitere Routingparameter erforderlich sind, fordert die Intermediäre Plattform die Nutzenden auf, diese einzugeben. Es ist möglich, dass das Data Service Directory mehr als einen Data Service zurück ermittelt. Diese werden den Nutzenden in einer Auswahlliste angeboten. Die Nutzenden können einen oder mehrere Data Services auswählen.	• Dieser Prozess muss für jeden Nachweistyp wiederholt werden, für den sich die Intermediäre Plattform zuvor entschieden hat, Nachweise abzurufen. • Für die Nachweisermittlung können, abhängig vom Mitgliedsstaat, unterschiedliche Routingparameter benötigt werden, über die der Evidence Requester keine Kenntnis haben kann. • Diese Routingparameter müssen dann von den Nutzenden eingegeben werden, um den Nachweisabrufprozess fortsetzen zu können.

Prozessschritt	Element	Beschreibung	Anmerkung
[UC4-06]	• Lookup and Request Evidence	• Sobald alle notwendigen Parameter ermittelt wurden, generiert die Intermediäre Plattform einen EU-EDM-Request. • Im Request werden der gesuchte Nachweistyp, die ermittelten Verbindungsparameter und weitere Routingparameter übergeben. • Die Intermediäre Plattform übermittelt den Request über Access-Points an einen Evidence Provider.	
[UC4-07]	• Data Service	• Ruft eine Intermediäre Plattform einen Evidence Provider erstmalig im Nachweisabrufprozess auf, ist vorgesehen, dass eine Exception ausgelöst wird. • Die Exception liefert eine URL zurück, die dafür verwendet wird, den Nutzenden auf einen Preview-Space innerhalb des Evidence Provider zu navigieren. • Der Evidence Provider übermittelt die Exception an die Intermediäre Plattform.	• Der Preview-Space wird benötigt, um eine direkte Nutzerinteraktion zu ermöglichen.
[UC4-08]	• Handover to Evidence Provider Preview Space	• Die Intermediäre Plattform verarbeitet die Exception und die mitgelieferte URL und führt einen redirect der Nutzenden auf den Preview-Space des Evidence Provider durch.	• Dieser Vorgang wird für jeden zuvor ausgewählten Nachweistyp erneut (sequenziell) durchgeführt.

Prozessschritt	Element	Beschreibung	Anmerkung
[UC4-9]	• Preview Service	• Der Preview-Service stellt eine Benutzeroberfläche im Mitgliedsstaat des Evidence Providers bereit. In der Regel findet hier eine Reauthentifizierung und eine Preview des Nachweises statt, bevor dieser an den Evidence Requester übermittelt wird. • Der Evidence Requester kann weitere Verarbeitungsschritte und Nutzerinteraktionen implementieren. Diese werden hier nicht weiter spezifiziert. • Bei einer positiven Entscheidung können die Nachweise durch die Intermediäre Plattform abgerufen werden. Bei einer negativen Entscheidung dürfen die Nachweise nicht an die Intermediäre Plattform herausgegeben werden. • Im vorliegenden Fall wird die Preview positiv beschieden. • Der Evidence Provider führt die Nutzenden zurück auf die Intermediäre Plattform und übermittelt eine Preview-ID, mit der ein Nachweis im Anschluss von der Intermediären Plattform abgerufen werden kann.	
[UC4-10]	• Wait for preview and retrieve evidence	• Die Intermediäre Plattform erzeugt einen erneuten EDM-Request und übergibt die vom Evidence Provider erhaltene Preview-ID. • Die Intermediäre Plattform übermittelt den Request über Access-Points an den Data Service des Evidence Providers.	

Prozessschritt	Element	Beschreibung	Anmerkung
[UC4-11]	• Data Service	• Der Evidence Provider verarbeitet den EDM-Request und die Preview-ID und erzeugt eine EDM-Response, die den freigegebenen Nachweis beinhaltet. • Der Evidence Provider übermittelt die EDM-Response über Access-Points an die Intermediäre Plattform.	
[UC4-12]	• Complete Exchange • Zwischen-gespeicherter Nachweis	• Die Intermediäre Plattform verarbeitet die EDM-Response und speichert den Nachweis für den späteren Abruf durch den Data Consumer. • Die Intermediäre Plattform leitet die Nutzenden zurück zum Data Consumer und gibt eine Abruf-ID für den zwischengespeicherten Nachweis zurück.	
[UC4-13]	• Nachweisabruf von Intermediärer Plattform beauftragen	• Der Data Consumer erzeugt einen DE-EDM-Request. • Der Data Consumer verschlüsselt personenbezogene Inhaltsdaten, sodass nur die Intermediäre Plattform diese einsehen kann. Daneben wird auch die Abruf-ID übergeben, die dem Zweck dient, den in der Intermediäre Plattform gespeicherten Nachweis identifizieren zu können. • Der Data Consumer übermittelt den DE-EDM-Request an eine Vermittlungsstelle.	

Prozessschritt	Element	Beschreibung	Anmerkung
[UC4-14]	• Vermittlungsdienst Nachweisabruf	• Die Vermittlungsstelle empfängt die DE-EDM-Request vom Data Consumer. • Die Vermittlungsstelle leitet die DE-EDM-Request an die Intermediäre Plattform weiter.	
[UC4-15]	• Berechtigung abstrakt prüfen	• Im §7 des Identifikationsnummerngesetz wird beschrieben, dass Vermittlungsstellen die Übermittlungsberechtigung abstrakt prüfen und protokollieren müssen. • Das Identifikationsnummerngesetz gilt ausschließlich für Nachweisabrufe, die unter Verwendung der Identifikationsnummer durchgeführt werden. • Europäische Nachweisabrufe erfolgen grundsätzlich ohne Identifikationsnummer. • Es ist nicht geklärt, ob eine abstrakte Berechtigungsprüfung und Protokollierung durchgeführt werden müssen.	
[UC4-16]	• Nachweisabruf-dienst • Nachweis	• Die Intermediäre Plattform entschlüsselt die personenbezogenen Inhaltsdaten und ermittelt den gesuchten Nachweis anhand der Abruf-ID. • Die Intermediäre Plattform generiert eine DE-EDM-Response.	

Prozessschritt	Element	Beschreibung	Anmerkung
		• Die Intermediäre Plattform verschlüsselt den ermittelten Nachweis und weitere sonstige personenbezogene Daten, sodass nur der Data Consumer diese einsehen kann. • Die Intermediäre Plattform übermittelt die Response an eine Vermittlungsstelle.	
[UC4-17]	• Vermittlungsdienst Nachweisabruf	• Die Vermittlungsstelle empfängt die DE-EDM-Response von der Intermediäre Plattform. • Die Vermittlungsstelle leitet die DE-EDM-Response an die Data Consumer weiter.	
[UC4-18]	• Nachweisabruf protokollieren	• Die Vermittlungsstelle empfängt die DE-EDM-Response vom Data Provider. • Die Vermittlungsstelle protokolliert den Nachweisabruf. • Die Vermittlungsstelle leitet die DE-EDM-Response an die Intermediäre Plattform weiter.	
[UC4-19]	• Nachweis in der Preview freigeben	• Der Data Consumer erhält die DE-EDM-Response und entschlüsselt die personenbezogenen Inhaltsdaten sowie den Nachweis.	

Prozessschritt	Element	Beschreibung	Anmerkung
[UC4-20]	• Nachweis übernehmen	• Der Nachweis kann im Antragsverfahren verwendet werden. • Der Nachweisabruf ist abgeschlossen.	

1.4.3 Ausblick und weiterführende Aspekte

Auflistung von relevanten Annahmen, Klärungspunkten und Anforderungen, die bei der Modellierung des Use-Cases aufgezeigt wurden.

- Sachverhalte oder Aspekte der Modellierung die einen Klärungsbedarf beschreiben und in späteren Iterationen dieses Dokuments aufgelöst werden müssen, werden als **Klärungspunkt** festgehalten.
- Sachverhalte oder Aspekte der Modellierung, die im Kompetenzteam Architektur abgestimmt sind und der Verdeutlichung von besonderen Merkmalen dienen, werden als **Annahme** festgehalten.
- Sachverhalte oder Aspekte der Modellierung, die eine besondere Auswirkung auf das Gesamtsystem oder die darin enthaltenen Komponenten haben, werden als **Anforderung** festgehalten.

1.4.3.1 Klärungspunkte aus der Use-Case-Modellierung

Tabelle 10: Klärungspunkte aus der Use-Case Modellierung

ID	Offener Punkt	Erläuterung	Kontext	Arbeitsthese
[KPUC-01]	• Soll der Nachweisbegriff auch außerhalb von Antragsverfahren verwendet werden?	• Der Nachweisbegriff ist nicht einschlägig für alle Use-Cases.	• Die Definition des Nachweisbegriffs stammt aus der SDG-VO.	• Der Nachweisbegriff sollte durchgängig, über alle Use-Cases hinweg, verwendet werden. • Die Anpassung des Nachweisbegriffs ist zu prüfen (Prüffrage an KT Recht & Datenschutz)
[KPUC-02]	• Soll der Abruf eines Nachweises aus einem nationalen Register über eine zusätzliche Komponente "Nachweisabrufdienst" gekapselt werden?	• Der Nachweisabruf aus dem EU-Ausland wird durch die IP gekapselt. Für den Data Consumer gestaltet sich der Abruf trotz hoher Komplexität des EU-OOTS daher sehr einfach. • Für den Abruf aus nationalen Registern existiert derzeit kein	• Ein zentrales Architekturprinzip für das NOOTS sagt aus, dass der Anschluss von Data Consumer und Data Provider so einfach und kostengünstig wie möglich umsetzbar sein soll und dass Data Consumer und Data Provider durch	• Dieses Thema wird in der zweiten Iteration der nationalen TDDs adressiert.

ID	Offener Punkt	Erläuterung	Kontext	Arbeitsthese
		Kapseln. Daher ist die gesamte Komplexität des NOOTS für den Data Consumer sichtbar.	zentrale Komponenten entlastet, werden sollten.	
[KPUC-03]	• Sollte durch das NOOTS vorgeschrieben werden, dass die Kommunikation über Vermittlungsstellen (inkl. der im IDNrG. beschriebenen Funktionen) auch dann erfolgt, wenn beim Nachweisabruf keine IDNr. verwendet wird?	• Die Identifikationsnummer wird nicht verwendet, wenn • die WIDNr. zum Einsatz kommt, z.B. im Unternehmenskontext. • der Nachweisabruf zwischen Behörden ohne Bürgerbeteiligung erfolgt. • die IDNr. vom Register nicht unterstützt wird. • bei Nachweisabrufen im EU-Kontext • Die abstrakte Berechtigungsprüfung könnte, wenn auch nicht durch das Identifikationsnummerng esetz gefordert, dennoch	• Im §7 des Identifikationsnummernge setz wird beschrieben, dass Vermittlungsstellen die Übermittlungs-berechtigung abstrakt prüfen und protokollieren müssen. • Vermittlungsstellen überwachen im nationalen Kontext die Nachweisabrufe zwischen Data Consumer und Data Provider und dienen der fachlichen Absicherung des Nachweisabrufs. • Nach Einschätzung des Kompetenzteam Recht & Datenschutz beschränkt sich der Geltungsbereich des	• Vermittlungsstellen in allen Use-Cases einsetzen, unabhängig vom IDNrG. • Beitrag zur IT-Sicherheit / DatenschutzSchaffung einer einheitlichen nationalen Architektur

ID	Offener Punkt	Erläuterung	Kontext	Arbeitsthese
		einen Beitrag zur IT-Sicherheit / Datenschutz leisten. • Da nationale Register ohnehin an Vermittlungsstellen angeschlossen werden müssen, würde der Einsatz im EU-Kontext keinen zusätzlichen Aufwand bedeuten.	Identifikationsnummerngesetz auf nationale Nachweisabrufprozesse mit Bürgerbeteiligung.	
[KPUC-04]	• Sollte durch das NOOTS vorgeschrieben werden, dass Vermittlungsstellen auch beim Abruf europäischer Nachweise eingesetzt werden?	• Ruft ein deutscher Data Consumer einen Nachweis aus der EU ab, bieten Vermittlungsstellen keinen Mehrwert und erzeugen sogar Komplexität, weil sie eine einheitliche API erzwingen, die für den Anruf aus dem EU-Ausland nicht passt. • Synergieeffekte, die dadurch entstehen, dass bereits Anbindungen aus	• Im §7 des Identifikationsnummerngesetz wird beschrieben, dass Vermittlungsstellen die Übermittlungsberechtigung abstrakt prüfen und protokollieren müssen. • Vermittlungsstellen überwachen im nationalen Kontext die Nachweisabrufe zwischen Data Consumer und Data Provider und dienen der	• Dieses Thema wird in der zweiten Iteration der nationalen TDDs adressiert. • Argumentation 1: o Da Vermittlungsstellen beim Abruf von Nachweisen aus EU-Mitgliedsstaaten keinen Mehrwert bringen (es kann keine abstrakte Berechtigungsprüfung durchgeführt werden),

ID	Offener Punkt	Erläuterung	Kontext	Arbeitsthese
		dem nationalen Kontext existieren, sind hier auch nicht zu erwarten. Es handelt sich um einen Data Provider Gateway speziell für die Intermediäre Plattform. • Wenn dieser Klärungspunkt positiv beschieden wird, müsste festgelegt werden, nach welchen fachlichen Regeln die abstrakte Berechtigungsprüfung durchgeführt werden kann.	fachlichen Absicherung des Nachweisabrufs. • Nach Einschätzung des Kompetenzteam Recht & Datenschutz beschränkt sich der Geltungsbereich des Identifikations-nummerngesetz auf nationale Nachweisab-rufprozesse mit Bürgerbeteiligung.	besteht kein Bedarf auf diese zurückzugreifen. • Argumentation 2: ○ Einheitlichkeit und Pflegbarkeit des Prozesses. ○ Weniger Aufwand für den Data Consumer, wenn er immer die gleiche API (zur Vermittlungsstelle) nutzt. ○ Die Aufgabe der abtstrakten Berechtigungsprüfung fiele hier aber logischerweise weg.
[KPUC-05]	• Wie die Intermediäre Plattform ermitteln, welche persönlichen Identifikationsdaten für den Nachweisabruf benötigt werden?	• Wird die Identifikationsnummer nicht verwendet, muss der Antragssteller anhand von persönlichen Identifikationsdaten ermittelt werden.	• Im Identifikationsnummernge setz (§5) wird der Zweck und die Vergabe der IDNr. beschrieben. • Nach Einschätzung des Kompetenzteam Recht &	• Die IP greift auf einen Exception-Mechanismus zurück, der durch das Register ausgelöst wird, wenn unzureichende Identifikationsdaten übermittelt wurden.

ID	Offener Punkt	Erläuterung	Kontext	Arbeitsthese
		• Die Intermediäre Plattform wird ermitteln müssen, welche persönlichen Identifikationsdaten vom jeweiligen Register erwartet werden.	Datenschutz beschränkt sich der Geltungsbereich des Identifikationsnummerngesetz auf nationale Prozesse mit Bürgerbeteiligung.	
[KPUC-06]	• Wer ist für die Datenpflege des „EU Central Evidence Broker“ verantwortlich?	• Deutschland wird den „EU Central Evidence Broker“ verwenden, um den EU-Mitgliedsstaaten notwendige Informationen zu nationalen Nachweistypen bereitzustellen.	• Für einen EU-Nachweisabruf ist es erforderlich, dass ein Evidence Requester den zu einem Requirement passenden Nachweistyp über den Evidence Broker des Mitgliedstaats ermittelt.	• Auflösung in der Zukunft - Verantwortliche EU-Gremien kümmern sich bereits um diesen Klärungspunkt.
[KPUC-07]	• Wer ist für die Datenpflege des „EU Central Data Service Directory“ verantwortlich?	• Deutschland wird den „EU Central Data Service Directory“ verwenden, um den EU-Mitgliedsstaaten notwendige Informationen zu nationalen Data Services bereitzustellen.	• Für einen EU-Nachweisabruf ist es erforderlich, dass ein Evidence Requester den für die Bereitstellung des Nachweises verantwortlichen Data Service des über das Data	• Auflösung in der Zukunft - Verantwortliche EU-Gremien kümmern sich bereits um diesen Klärungspunkt.

ID	Offener Punkt	Erläuterung	Kontext	Arbeitsthese
			Service Directory des Mitgliedsstaats ermittelt.	
[KPUC-08]	• Ist es erforderlich, dass ein erneuter „explicit Request“ für einen aus dem EU-OOTS initiierten nationalen Nachweisabruf eingeholt wird?	• Für den nationalen Nachweisabruf ist vorgesehen, dass ein „explicit Request“ durch den Antragssteller erfolgt.	• Nachdem ein Antragssteller durch den Evidence Requester an die Preview-Area einer nationalen Intermediäre Plattform weitergeleitet wurde und sich authentifiziert hat, wird ein nationaler Nachweisabruf ausgelöst.	• Ein erneuter "explicit Request" scheint nicht notwendig, die Zustimmung zur Preview reicht aus.
[KPUC-09]	• Wird die Intermediäre Plattform notwendige Routingparameter ausschließlich über den Abruf der Registerdatennavigation erhalten oder wird ein Mapping zwischen Nachweistyp und Routingparameter in der Intermediäre Plattform hinterlegt sein?	• Bei Nachweisabrufen aus der EU findet keine Übermittlung von Routingparametern statt. • Die Intermediäre Plattform muss Kenntnis darüber besitzen, welche Routingparameter vom Antragssteller eingeholt werden müssen.	• Um einen nationalen Nachweisabruf auslösen zu können, werden spezifische Routingparameter benötigt, um die zuständige Behörde und den technischen Endpunkt zu ermitteln. • Bei einem nationalen Nachweisabruf werden diese durch den Data Consumer geliefert, der diesen im Vorfeld vom	• Die IP benötigt kein eigenes Mapping von Nachweistyp und Routingparameter, sondern greift dafür auf die RDN zurück.

ID	Offener Punkt	Erläuterung	Kontext	Arbeitsthese
			Antragssteller eingeholt hat. • Bei Abrufen aus dem EU-Ausland müssen die Routingparameter durch die Intermediäre Plattform vom Antragssteller abgefragt werden. Dazu muss die Intermediäre Plattform wissen, welche Routingparameter benötigt werden.	
[KPUC-10]	• Welche Informationen werden einer Intermediäre Plattform zur Aufbereitung der Previews durch die Data Provider zur Verfügung gestellt?	• Wird ein Nachweis in einem höheren Nachweisreifegrad (C / D) übermittelt, muss die Intermediäre Plattform syntaktisches und semantisches Wissen über die Nachweisdaten besitzen.	• Bevor ein Nachweis durch einen Evidence Requester verwendet werden darf, muss eine Preview der Nachweisdaten erfolgen. • Bei Nachweisabrufen im EU-Kontext wird die Aufbereitung der Previews durch die Intermediäre Plattform verantwortet. • Die Komplexität der Aufbereitung der Previews hängt davon ab, in	•

ID	Offener Punkt	Erläuterung	Kontext	Arbeitsthese
			welchem Format (PDF, strukturierte Daten) ein Nachweis übermittelt wird.	
[KPUC-11]	• Gibt es einen Grund (z.B. erneuter Abgleich aus Sicherheitsgründen), weshalb die initial übermittelten Query-Parameter bei einem EU-EDM-Request erneut übermittelt werden?	• Grundsätzlich wäre es denkbar, dass der Versuch des Abrufs des eigentlichen Nachweises (unabhängig von der Entscheidung der Preview) ausschließlich mit der Preview-ID durchgeführt wird.	• Wurde der Nachweisabruf durchgeführt und die Preview von den Nutzenden eingeholt, wird eine Preview-ID an den Evidence Requester übergeben. • Der Evidence Requester kann den Nachweis dann abrufen, in dem dieser einen EDM-Request gemäß den TDD-Vorgaben erzeugt, der die Query Parameter der initialen Abrufauslösung und die Preview-ID enthalten muss.	• Dieses Thema wird in der zweiten Iteration der nationalen TDDs adressiert.
[KPUC-12]	• Wird die Intermediäre Plattform Nachweise	• Die Übergänge der Kontrolle in die Intermediäre Plattform kann, analog zum EU-	• Es kann der Fall auftreten, dass mehr als ein Nachweis	• Nachweise werden sequenziell abgearbeitet. Aus Nutzersicht sinnvoll, da Nutzende sich ggf. direkt

ID	Offener Punkt	Erläuterung	Kontext	Arbeitsthese
	sequenziell oder gebündelt abrufen?	Nachweisabruf, jeweils Nachweis für Nachweis erfolgen. • Alternativ könnte der Abruf mehrerer Nachweise gebündelt werden.	aus dem EU-Ausland benötigt wird.	für den erst möglichen Nachweistyp von einem bestimmten Provider entscheiden kann und dadurch keine weiteren Nachweise abgerufen werden müssen.
[KPUC-13]	• Wer verwendet die Protokollierungsdaten der Vermittlungsstellen und zu welchem Zweck?	• Nach bisherigem Kenntnisstand wird das Datenschutzcockpit lediglich auf Protokolldaten aus den Registern zugreifen.	• Im §7 des Identifikationsnummerngesetz wird beschrieben, dass Vermittlungsstellen die Übermittlungs-berechtigung abstrakt prüfen und protokollieren müssen. • In §2 des Identifikationsnummerngesetz wird beschrieben, dass öffentliche Stellen und Bund und Länder dazu verpflichtet sind, natürlichen Personen die Übermittlung ihrer Daten unter Verwendung der Identifikationsnummer	• Dieses Thema wird in der zweiten Iteration der nationalen TDDs adressiert.

ID	Offener Punkt	Erläuterung	Kontext	Arbeitsthese
			digital über eine zentrale Stelle transparent zu machen (Datencockpit).	
[KPUC-14]	• In welchem Corner werden die Funktionen der Vermittlungsstellen gemäß IDNrG umgesetzt?	• Es ist nicht definiert, welches Corner im Zielbild der Registermodernisierung die Vermittlungsstelle im Sinne des IDNrG. darstellt. Es erscheint wenig sinnvoll, die Funktionalität in beiden Cornern (2 und 3) redundant auszuführen. Da es sich um eine Schutzfunktion der Daten aus Corner 4 handelt, wäre es naheliegend, diese in Corner 3 abzubilden.	• Im §7 des Identifikationsnummernge setz wird beschrieben, dass Vermittlungsstellen die Übermittlungs-berechtigung abstrakt prüfen und protokollieren müssen. • Für den Nachweisabruf ist die Kommunikation nach dem 4-Corner-Modell vorgesehen.	• Dieses Thema wird in der zweiten Iteration der nationalen TDDs adressiert.

1.4.3.2 Annahmen aus der Use-Case-Modellierung

Tabelle 11: Annahmen aus der Use-Case Modellierung

ID	Annahmen	Begründung
[AUC-01]	• Will ein Nationaler Data Consumer einen Nachweis von einem Nationalen Data Provider abrufen, ist der Nachweistyp bekannt	• Der Data Consumer benötigt den Nachweis für ein Verwaltungsverfahren. Welche Nachweistypen dafür erforderlich sind, ist in Verwaltungsvorschriften geregelt und dem Data Consumer daher bekannt. • Dies ist eine explizite Abweichung vom grenzüberschreitenden Nachweisabruf: Ausländische Nachweise sind in den nationalen Verwaltungsvorschriften in der Regel nicht benannt. Daher ist beim grenzüberschreitenden Nachweisabruf zunächst eine Ermittlung des benötigten Nachweistyps erforderlich. Dies kann im nationalen Fall entfallen
[AUC-02]	• Will ein Nationaler Data Consumer einen Nachweis von einem Nationalen Data Provider abrufen, sind die Routingparameter für die Ermittlung der Behörde und dem technischen Endpunkt bekannt.	• Der Data Consumer muss eine nachweisausstellende Behörde und den technischen Endpunkt ermitteln, um einen Nachweisabruf durchführen zu können. Dazu muss eine nachweisspezifische Menge an Routingparametern übergeben werden, die dem Nationalen Data Consumer bekannt ist.
[AUC-03]	• Der Data Consumer benötigt für Nachweisabrufe aus europäischen Mitgliedsstaaten keinen Lookup der Intermediäre Plattform, da diese bekannt ist.	• Derzeit gibt es keine Anforderung, dass der Abruf von Nachweisen aus dem EU-Ausland über mehr als eine Intermediäre Plattform erfolgen.

ID	Annahmen	Begründung
		• Eine Eingruppierung ausländischer Nachweise in Verwaltungsbereiche ist nicht vorgesehen.
[AUC-04]	• Um einen freigegebenen europäischen Nachweis von einer Intermediäre Plattform abzurufen, wird lediglich die Abruf-ID benötigt. Es ist nicht notwendig, dass ein nationaler EDM-Request erzeugt wird, der bereits bei der initialen Abrufauslösung übermittelte Query Parameter enthält.	• Im europäischen EDM ist vorgesehen, dass ein Nachweis nach der erfolgten Preview durch erneuten EDM-Request abgerufen wird. Dazu werden erneut alle Query Parameter und die Abruf-ID übermittelt. Um einen Nachweis bei einer Intermediäre Plattform abzuholen, ist die Übermittlung der Abruf-ID ausreichend, da die Query Parameter nicht mehr benötigt werden.
[AUC-05]	• Für Nachweisabrufe aus dem EU-Ausland genügt es nicht, dass der Data Consumer lediglich den nationalen Nachweistyp an die Intermediäre Plattform übermittelt, da die Übersetzung in einen EU-Sachverhalt nicht möglich ist.	• Für einen Nachweisabruf aus einem EU-Mitgliedsstaat ist es erforderlich, dass der EU-Sachverhalt (Requirement) bekannt ist. Über den Evidence Broker kann, der zu diesem Requirement passende europäische Nachweistyp ermittelt werden. • Ein Nachweistyp kann mehreren Sachverhalten zugewiesen sein. Die Intermediäre Plattform kann nicht wissen, welchen EU-Sachverhalt der Data Consumer belegen muss.

1.4.3.3 Anforderungen aus der Use-Case-Modellierung

Tabelle 12: Anforderungen aus der Use-Case Modellierung

ID	Annahmen	Begründung
[REQUC-´01]	• Der Vermittlungsdienst in der Vermittlungsstelle **muss** Kenntnis über den Nachweistyp und den Zweck des Nachweisabrufs haben.	• Die Vermittlungsstelle hat keine Kenntnis über die Inhaltsdaten der Nachricht, die sie transportieren soll. Um die abstrakte Berechtigungsprüfung durchführen zu können, muss sie jedoch mindestens den abgerufenen Nachweistyp und den Zweck des Nachweisabrufs kennen. • Daher kann kein generischer Transportdienst genutzt werden. Es muss zumindest eine Vereinbarung über die zu übermittelnden Metadaten geben und der Transportdienst muss diese Daten auswerten.
[REQUC-02]	• Die Intermediäre Plattform für **soll** über einen Single-Sign-On (SSO) Mechanismus verfügen.	• Wenn aus dem EU-Ausland mehrere Nachweise aus Deutschland abgerufen werden, werden die Nutzenden immer wieder auf die Intermediäre Plattform geleitet, um dort Routingparameter abzufragen und die Preview-Funktion anzubieten. Mindestens bei der ersten Weiterleitung zur IP ist eine Reauthentifizierung der Nutzenden erforderlich, da es im EU-OOTS kein SSO gibt. • Der SSO Mechanismus verhindert, dass immer wieder eine Anmeldung erforderlich ist, falls mehrere Nachweise abgerufen werden.

ID	Annahmen	Begründung
[REQUC-03]	• Die Intermediäre Plattform **soll** in den Single-Sign-On des Portalverbunds eingebunden werden.	• Wenn Nachweise aus dem EU-Ausland erfolgen, werden die Nutzenden aus dem Antragsverfahren in die IP weitergeleitet. Werden mehrere Nachweise aus dem EU-Ausland benötigt, kann das auch mehrmals erforderlich sein. • Die Einbindung in den SSO des Portalverbunds verhindert, dass die Nutzenden sich dabei ggfs. mehrfach erneut anmelden müssen.
[REQUC-04]	• Der DE-EDM-Standard muss beschreiben, wie mit dem Transport von Fachnachrichten (z.B. XÖV-Nachrichten) verfahren wird.	• Der DE-EDM-Standard ermöglicht einen generischen Nachweisabruf zwischen Data Consumer und Data Provider. Eine Standardisierung der Fachnachricht (Payload) ist kein Bestandteil des DE-EDM-Standards. Der Prozess eines DE-EDM-Abrufs muss beschrieben werden.
[REQUC-05]	• Der DE-EDM Standard muss beschreiben, welcher Mechanismus von Registern angeboten wird, um Intermediärer Plattformen die Ermittlung von fehlenden Identifikationsparametern zu ermöglichen.	• Wenn eine Intermediäre Plattform eine Anfrage aus der EU verarbeitet, besitzt diese keine Kenntnis darüber, welche Identifikationsparameter von einem Register erwartet werden. Es muss einen Mechanismus geben, diese Information auszutauschen. im EU-OOTS kommt dafür ein Exception-Mechanismus zum Einsatz.

1.5 Ausblick & Weiterführende Aspekte

1.5.1 Sequenzdiagramm zu Use-Case 3

Abruf von nationalen Nachweisen über das EU-OOTS:

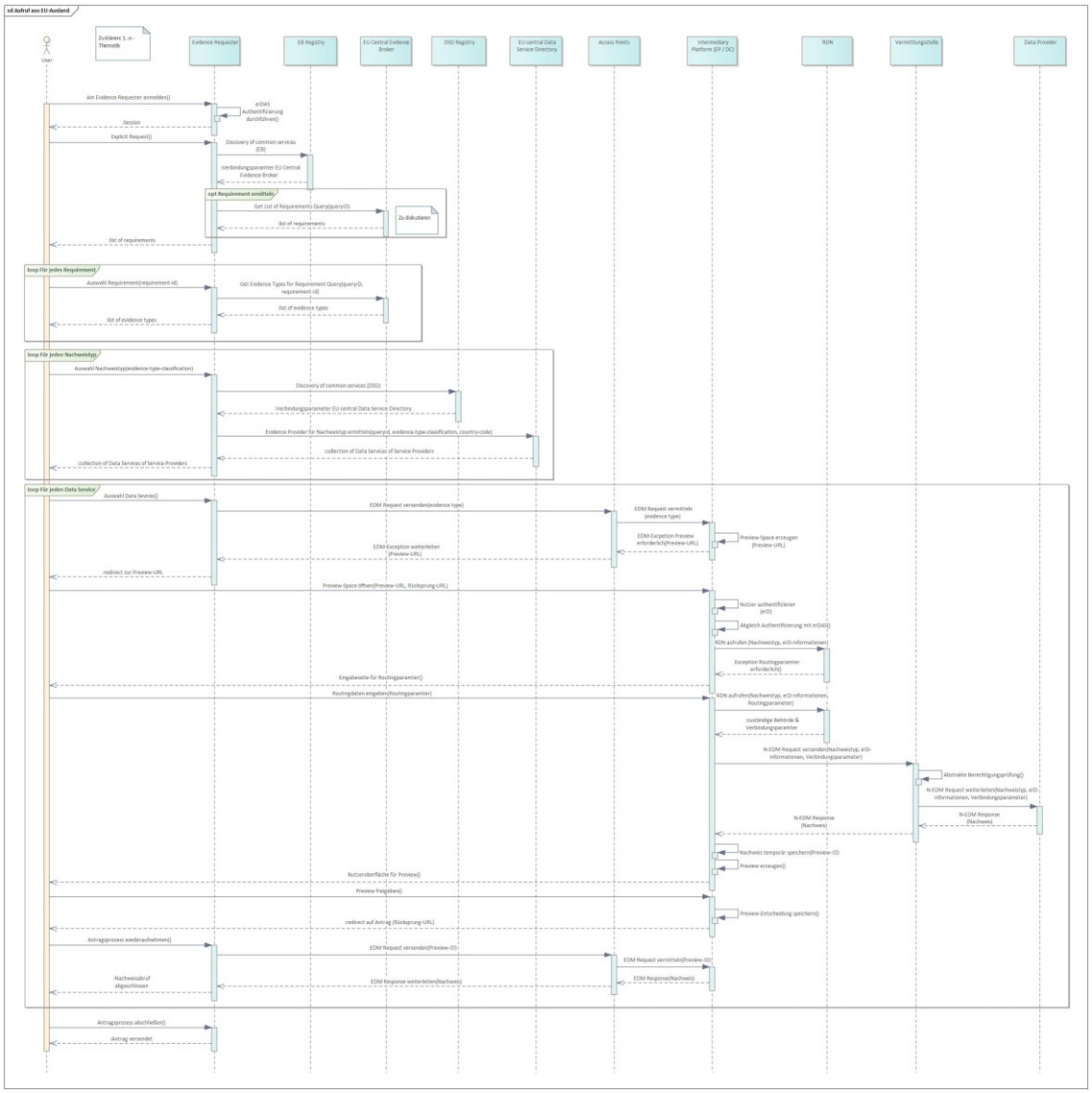


Abbildung 9: Sequenzdiagramm Use-Case 3

1.5.2 Sequenzdiagramm zu Use-Case 4

Abruf von europäischen Nachweisen über das EU-OOTS:

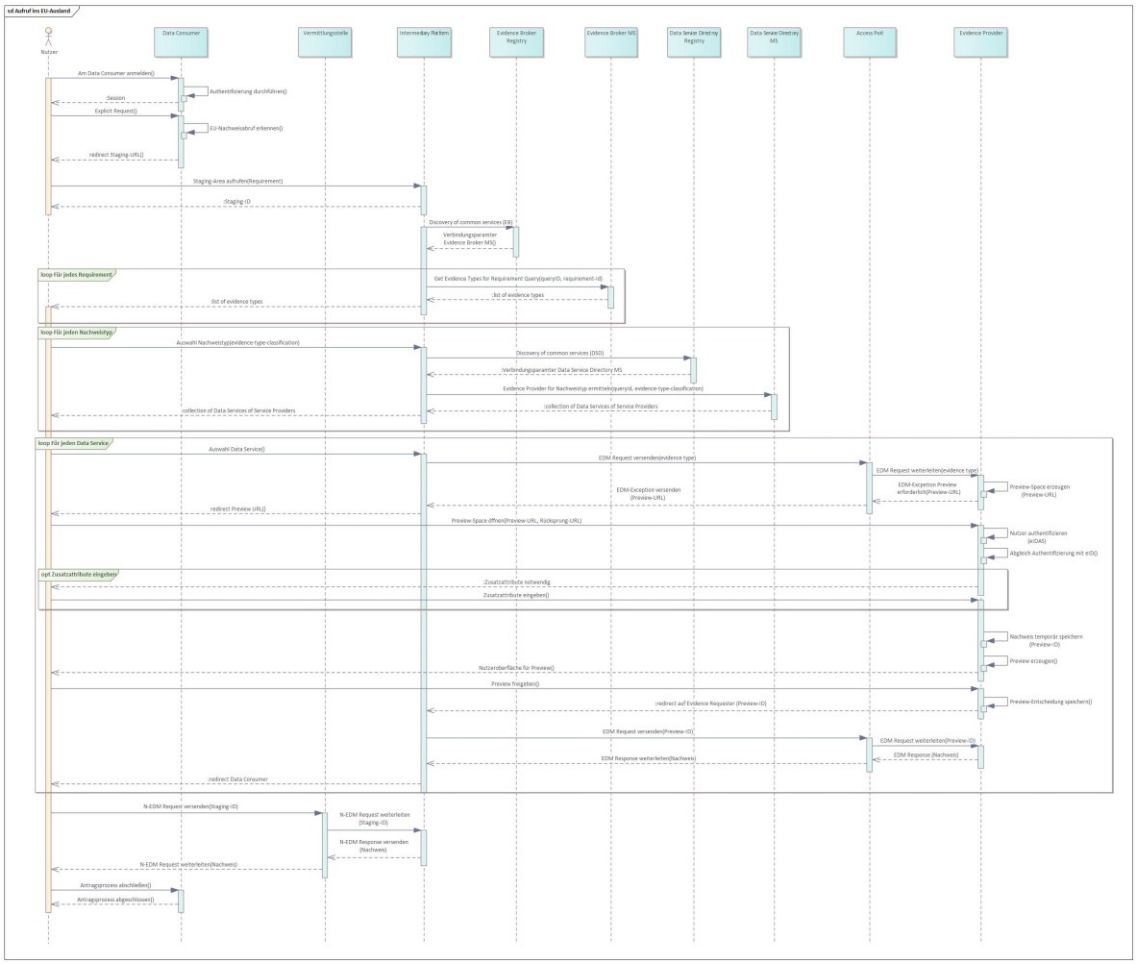


Abbildung 10: Sequenzdiagramm Use-Case 4

2 <Platzhalter Kapitel 2>

Wird aktuell noch nicht verwendet.

3 NOOTS Komponenten Beschreibung

3.1 Registerdatennavigation

3.1.1 Management Summary

Die Registerdatennavigation (RDN) ist eine zentrale Komponente des NOOTS. Sie liefert einem Data Consumer die Information, von welchem technischen Dienst dieser einen gewünschten Nachweis abrufen kann, welche Behörde diesen Dienst betreibt und welche Verbindungsparameter für einen Abruf erforderlich sind. Damit nimmt sie eine zentrale Rolle im Prozess des Nachweisabrufs ein. Die RDN wird sowohl für nationale Abrufe als auch für Abrufe aus dem EU-Ausland verwendet.

Dieses Kapitel dient als Grobkonzept für die Umsetzung der RDN. Es beschreibt mögliche konkrete Lösungsansätze für das Vorhaben der Registermodernisierung. Im weiteren Verlauf des Vorhabens müssen einerseits noch einige offene Punkte aufgelöst, andererseits in diesem Konzept skizzierte Lösungsansätze verifiziert und ausgearbeitet werden. Auf Basis erläuterter Annahmen beschreibt das vorliegende Dokument die Lösungsidee mit der Dokumentation von fachlichen Anforderungen, Schnittstellen, der sicheren Anbindung externer Systeme mittels Authentifizierung, Protokoll-Mechanismen sowie IT-betrieblichen Aspekten. Die identifizierten Punkte werden im weiteren Verlauf des Umsetzungsprojekts näher beleuchtet, sodass eine Spezifikation der Annahmen um die Ergänzung weiterer Faktoren und Erkenntnisse erfolgen wird. Die Entwicklung der Anwendung soll durch die Föderale IT-Kooperation (FITKO) übernommen werden. Durch die Erfahrungen mit FIT-Connect und DVDV, auf denen die präferierte Lösungsvariante der Registerdatennavigation aufbaut, wird eine Reduzierung von Umsetzungszeit und -kosten sowie eine Minimierung der Projektrisiken angestrebt.

3.1.2 Einleitung

3.1.2.1 Ziel des Kapitels

Dieses Dokument formuliert Anforderungen und architektonische Vorgaben für die Komponente Registerdatennavigation (RDN). Diese bilden die Grundlage zur Beauftragung der Umsetzung der Komponente Registerdatennavigation durch die FITKO gemäß dem IT-Planungsrat-Beschluss 2022/22 vom 26.06.2022.

3.1.2.2 Zielgruppe

Dieses Konzept richtet sich an die Umsetzer der Komponente Registerdatennavigation sowie an Interessierte an den Architekturkomponenten der Registermodernisierung.

3.1.2.3 Aufbau

In Kapitel 3.1.3 wird zunächst der Kontext dargestellt, in der die RDN genutzt werden soll. Kapitel 3.1.4 sammelt die Annahmen und Rahmenbedingungen, die für die Konzeption der RDN von Bedeutung sind. Kapitel 3.1.5 formuliert die Anforderungen an die RDN. Eine mögliche fachliche Umsetzung der Anforderungen wird in Kapitel 3.1.6 skizziert und insbesondere die Schnittstellen der RDN vertiefend dargestellt. Darüber hinaus benennt Kapitel 3.1.7 die technischen Anforderungen, soweit diese bisher bekannt sind.

3.1.3 Kontext

3.1.3.1 Ausgangslage

Im Zielbild der Registermodernisierung des IT-Planungsrats ist beschrieben, dass es bei Once-Only-Datenabfragen notwendig sei, die zuständige Behörde für ein Datum anhand eines zentralen Verzeichnisses für Nachweistypen zu ermitteln und eine entsprechende Navigation einzuleiten. Dazu sei es notwendig, ein Verzeichnis von Nachweisen zu führen.

Es sei zu prüfen, ob ein solches Verzeichnis sowie eine mögliche Registerdatennavigation über die Erweiterung des deutschen Verwaltungsdienste Verzeichnis (DVDV), die Verwaltungsdaten-Informationsplattform (VIP), die nach dem IDNrG zu erstellende Registerlandkarte oder eine gänzlich neue Komponente umgesetzt werden könne (IT-Planungsrat, Januar 2021, S. 9).

Nach entsprechender Analyse hat der IT-PLR-Beschluss 2022/22 vom 22.06.2022 die FITKO mit der Umsetzung der Komponente Registerdatennavigation als zentralen Routing-Dienst auf Grundlage des Deutschen Verwaltungsdienste Verzeichnis unter Wiederverwendung von Lösungsansätzen aus FIT-Connect beauftragt. Im Beschluss heißt es, das Kompetenzteam Architektur der Gesamtsteuerung Registermodernisierung soll den dafür notwendigen Projektauftrag konkretisieren. Dieser Auftrag liegt der Erstellung des vorliegenden Konzepts zugrunde.

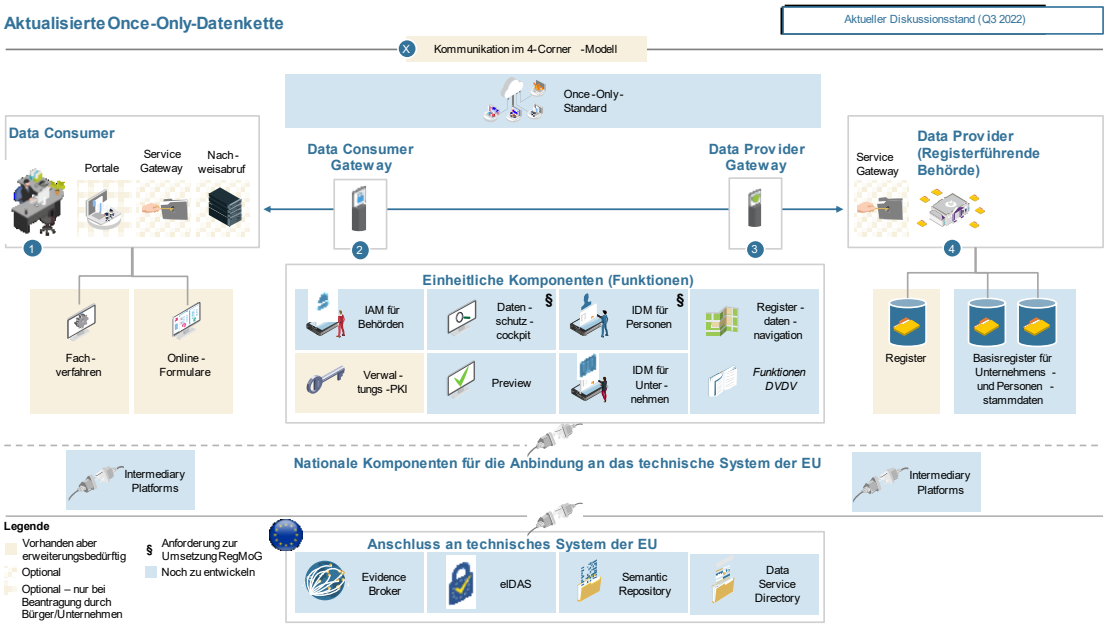


Abbildung 11: Vereinfachte Darstellung des Architekturmodells als Datenkette zur Umsetzung von "Once Only"

3.1.3.2 Ziel der Registerdatennavigation

Um einen Nachweisabruf gemäß der im Zielbild dargestellten Once-Only-Datenkette durchführen zu können, benötigt der Data Consumer Informationen zur zuständigen Behörde sowie die Dienst-Verbindungsparameter. Dementsprechend lautet das Ziel der Komponente Registerdatennavigation die Erfüllung dieser zwei Aufgaben: Auf Grundlage des gewünschten Nachweises und weiterer Informationen (Routingparameter) erstens die zuständige Behörde sowie zweitens, den für den Nachweisabruf benötigten Dienst und dessen Verbindungsparameter zu ermitteln.

Die Erwartung an die Registerdatennavigation ist dabei, dass sie alle von der deutschen Verwaltung vorgehaltenen Nachweistypen kennt und Auskunft über die Adressdaten der entsprechenden Dienste aller zentral wie dezentral organisierten Data Provider geben kann.

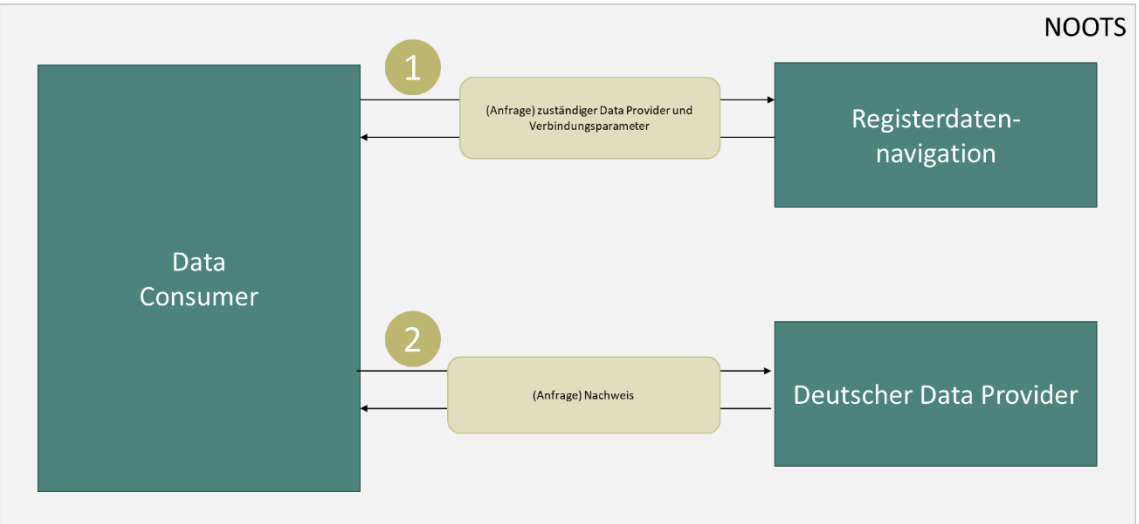


Abbildung 12: Zwei Schritte beim Nachweisabruf im NOOTS (Ausschnitt der Once-Only Datenkette)

3.1.3.3 Anschluss an das EU-OOTS

Das NOOTS muss laut der SDG-VO sicherstellen, dass ein Nachweisabruf auch grenzübergreifend mit Data Consumer und Data Provider aus dem EU-Ausland funktioniert. Auf europäischer Ebene ergibt sich also ebenfalls der Bedarf nach einer Komponente, die europäischen Data Consumer das passende deutsche Register mit dem benötigten Dienst und entsprechenden Verbindungsparametern nennt. Die SDG Technical Design Documents lassen den Mitgliedstaaten die Wahl, die Zuständigkeit ihrer Behörden entweder in einem zentralen europäischen Verzeichnis namens Data Service Directory (DSD) oder alternativ in einem eigenen national betriebenen DSD zu pflegen.

Der IT-PLR hat beschlossen, dass Deutschland auf die zweite Option setzen soll. Wesentliche Argumente dafür sind, dass zum einen die teilweise dezentrale Zuständigkeitslogik des föderalen Systems den Europäischen Data Consumer verborgen bleiben soll und diese zum anderen nicht doppelt in der RDN und einem europäischen DSD gepflegt werden müssen. Dieser Beschluss würde bedeuten, dass die RDN gleichzeitig als nationales DSD fungieren soll.

Das vorliegende Konzept empfiehlt jedoch, aufgrund neuer Erkenntnisse zu den Intermediären Plattformen, eine komplementäre Nutzung von europäischem DSD und RDN. Das SDG-OOTS und der Beschluss 2022/34 vom IT-Planungsrat [IT-PLR-B-09] sieht Intermediäre Plattformen vor, die als Vermittlerinnen zwischen europäischen und deutschen Akteuren dienen, indem sie Anfragen aus dem SDG-OOTS für eine weitere Bearbeitung im NOOTS umwandeln und weiterleiten, und umgekehrt. Der Einsatz Intermediärer Plattformen hat zur Folge, dass sich europäische Data Consumer mit ihrem

Nachweisabruf nicht direkt an ein deutsches Register wenden, sondern an eine Intermediäre Plattform, die den Nachweisabruf ins NOOTS weiterleiten.

Entsprechend müssen europäische Data Consumer nur die Zuständigkeit und Verbindungsparameter der Intermediäre Plattform erfahren. Dies spricht dafür, europäisches DSD und RDN im Zusammenspiel zu nutzen: Über das DSD ermittelt der europäische Data Consumer die zuständige Intermediäre Plattform. Diese routet den Nachweisabruf mithilfe der RDN an die zuständige Stelle in Deutschland weiter (siehe Abbildung 13).

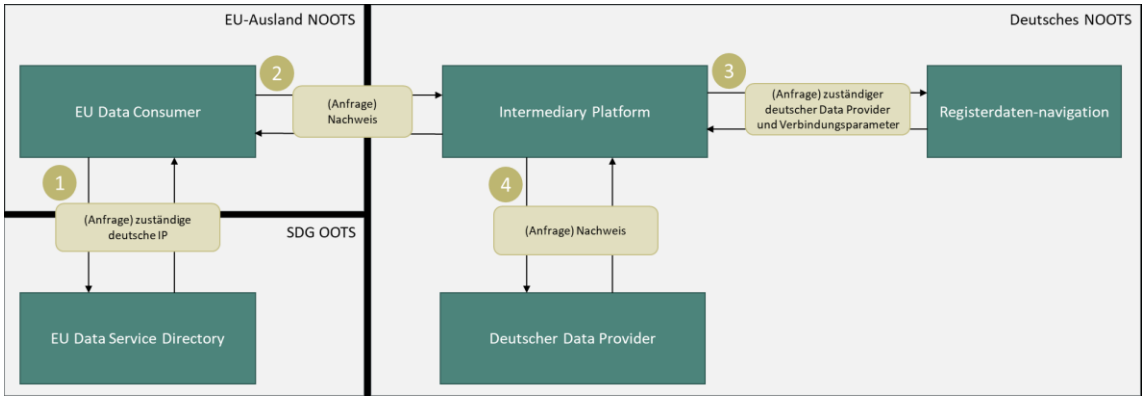


Abbildung 13: Zusammenspiel der Komponenten bei Nachweisabruf aus EU-Ausland mit IP

Hinweis: Ausgangspunkt dieser Darstellung ist, dass der europäische Data Consumer beim „EU Evidence Broker“ bereits den passenden deutschen Nachweistyp ermittelt, sowie beim „DSD Registry“ das für Deutschland zuständige Data Service Directory abgefragt hat.

Mit diesem Vorgehen werden die Präferenzen des IT-Planungsrat erfüllt, die föderale Struktur vor den europäischen Data Consumer zu verbergen und doppelte Pflege von Zuständigkeiten zu vermeiden, da das DSD und die RDN jeweils unterschiedliche Datenbestände umfassen. Gleichzeitig muss die RDN keine Schnittstelle zum EU-OOTS bereithalten, sondern überlässt diese Aufgabe den eigens dafür konzipierten Intermediären Plattformen.

Dieses Konzept geht von dem geplanten flächendeckenden Einsatz Intermediärer Plattformen aus, was in Annahme [ANN-002] festgehalten ist. Es besteht jedoch das Risiko, dass Intermediäre Plattformen nicht fristgemäß eingeführt werden können. In diesem Fall müsste die RDN, ggf. temporär, die Rolle des deutschen DSD übernehmen. Um dieser Möglichkeit – Nicht-Eintreten der Annahme [ANN-002] – Sorge zu tragen, enthält Anhang 3.1.9.7 die dann nötigen Funktionen der RDN mit einem Use-Case und zwei fachliche Anforderungen.

Bei Nachweisabrufen aus Deutschland ins EU-Ausland wenden sich deutsche Data Consumer direkt an die für sie zuständige nationale Intermediäre Plattform [ANN-005]. Die RDN wird in diesem Fall nicht verwendet; somit ist für diesen Fall kein Use-Case in diesem Konzept berücksichtigt.

3.1.3.4 Grobe Zeitplanung

Die folgende Zeitplanung stellt die initialen Überlegungen dar und muss im Rahmen der Umsetzung der Registerdatennavigation geprüft und fortgeschrieben werden.

Tabelle 13: Grobe Zeitplanung

Meilenstein	Datum	Verantwortlichkeit
Einreichung der Entscheidungsvorlage RDN	31.03.2022	Gesamtsteuerung Registermodernisierung - Kompetenzteam Architektur
Beschluss der Entscheidungsvorlage RDN	22.06.2022	IT-Planungsrat (Beschluss 2022/22)
Erstentwurf des Grobkonzepts	31.07.2022	Gesamtsteuerung Registermodernisierung - Kompetenzteam Architektur
Fertigstellung des Grobkonzepts	31.10.2022	Gesamtsteuerung Registermodernisierung - Kompetenzteam Architektur
Beauftragung der Umsetzung	Unbekannt	Unbekannt
Bestätigung des Architekturzielbilds	31.12.2022	IT-Planungsrat (erwarteter Beschluss 2022/n.a.)

3.1.4 Annahmen und Rahmenbedingungen

Das Zielbild der Lösungsarchitektur wird von verschiedenen übergreifenden organisatorischen, technischen, zeitlichen und fachlichen Faktoren eingegrenzt, die sich aus dem Gesetz und den infrastrukturellen Gegebenheiten ergeben. Diese werden im Folgenden aufgeführt.

Tabelle 14: Annahmen und Rahmenbedingungen für die Konzeption der Registerdatennavigation

ID	Annahme / Rahmenbedingung
[ANN-01]	Die Festlegung, welche Nachweistypen es gibt und welche Routingparameter für die dezentrale Zuständigkeit benötigt werden, ist nicht Aufgabe der RDN. Die RDN benötigt diese Informationen, ist jedoch nicht zwingend das führende System dafür.
[ANN-02]	Die Anbindung an das EU-OOTS erfolgt flächendeckend über Intermediäre Plattformen, die Anfragen aus dem EU-OOTS für eine weitere Bearbeitung im NOOTS umwandeln [IT-PLR-B-09]. Für das Routing der Anfragen bedeutet dies: Europäische Evidence Requester werden über das DSD zunächst an die Intermediären Plattformen in Deutschland geleitet. Von dort aus werden sie mithilfe der RDN weitervermittelt.
[ANN-03]	Das NOOTS wird über eine zentrale Komponente „IAM für Behörden“ verfügen (vgl. Kapitel 3.3). Darin erfolgt mittelfristig die Verwaltung von technischen Benutzerkonten und deren Rollen. Inwieweit deren Funktionen die Bedarfe der RDN-Zugriffsverwaltung abdeckt, ist im Rahmen der Feinkonzeption zu klären. Sollte diese Komponente kurzfristig nicht zur Verfügung stehen oder ungeeignet sein, wird die RDN mit einer eigenen IAM-Komponente ausgestattet sein müssen.
[ANN-04]	Die RDN wird in allen Use-Cases der High-Level-Architecture (siehe Kapitel 1.4.2) der Registermodernisierung genutzt werden.
[ANN-05]	Bei Nachweisabrufen aus Deutschland ins EU-Ausland wenden sich deutsche Data Consumer direkt an die für sie zuständige nationale Intermediäre Plattform (ggf. gibt es nur eine). Gegenwärtig wird davon ausgegangen, dass die RDN in diesem Fall nicht verwendet wird.
[ANN-06]	Die Zuständigkeit für einen Nachweis lässt sich eindeutig bestimmen, d.h. Routingparameter können so zugeschnitten werden, dass ein technischer Dienst eindeutig ermittelt werden kann und es zu keiner Trefferliste mit verschiedenen möglichen technischen Diensten kommt.
[RMBED-01]	Die für den Abruf eines Nachweises erforderlichen Parameter werden in Syntax und Semantik auf Basis der TDDs des EU-OOTS durch den Once-Only Standard des NOOTS definiert. Nach gegenwärtiger Planung liegt dieser ab 2023 vor.

ID	Annahme / Rahmenbedingung
[RMBED-02]	Ungeachtet der Nutzung des DVDV als einer der zentralen Datenspeicher der RDN bleibt das DVDV außerhalb der Registermodernisierung weiterhin als einzeln nutzbarer Dienst mit seinen bisherigen APIs verfügbar. Bestehende Nutzende des DVDV müssen nicht angepasst werden.
[RMBED-03]	Eine Nachweistypen-Liste wird gegenwärtig im Rahmen des Gesamtvorhabens Registermodernisierung erarbeitet und wird langfristig von einer zentralen Stelle verantwortet und gepflegt werden.

3.1.5 Fachliche Anforderungen

In diesem Abschnitt wird das fachliche Konzept der Registerdatennavigation (RDN) beschrieben.

3.1.5.1 Systemkontext

Die Registerdatennavigation wird als zentrale Komponente im Zielbild der Registermodernisierung konzipiert und liefert auf Anfrage die für einen Nachweis zuständige Behörde sowie den technischen Dienst mit seinen Adressdaten, über den ein Nachweis abgerufen werden kann. Neben den Abfrageschnittstellen bietet es auch Möglichkeiten zur Pflege und zum Import und Export von Zuständigkeitsdaten. In der Umsetzung können auch Pflegeclients oder Weboberflächen der RDN selbst zum Einsatz kommen.

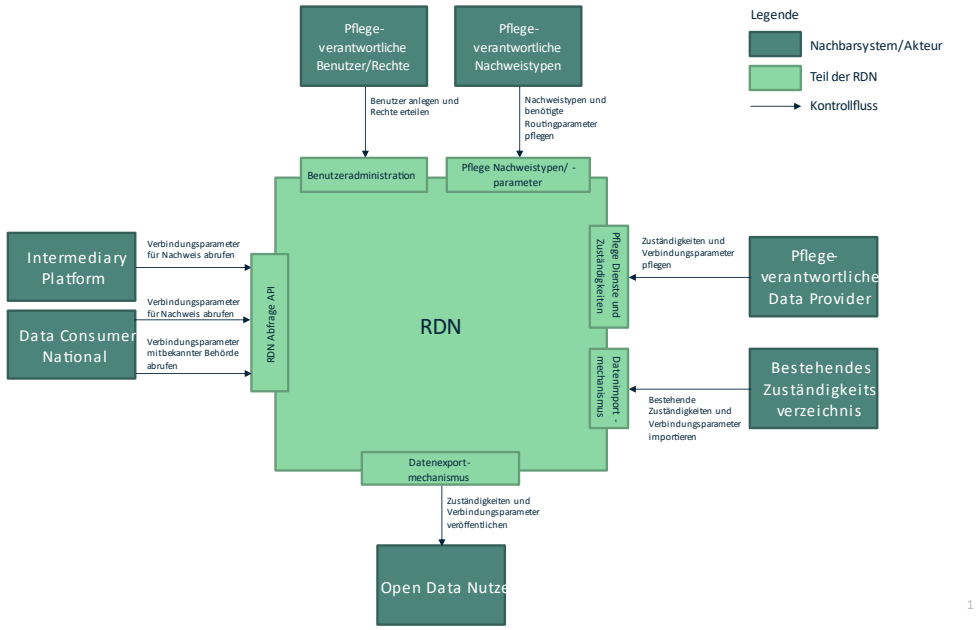


Abbildung 14: Kontextdiagramm Registerdatennavigation

3.1.5.2 Zentrale Begriffe

Im Rahmen der konzeptionellen Vorarbeiten zur Registerdatennavigation wurden zentrale Begriffe und Abhängigkeiten definiert und innerhalb des Kompetenzteams Architektur abgestimmt.

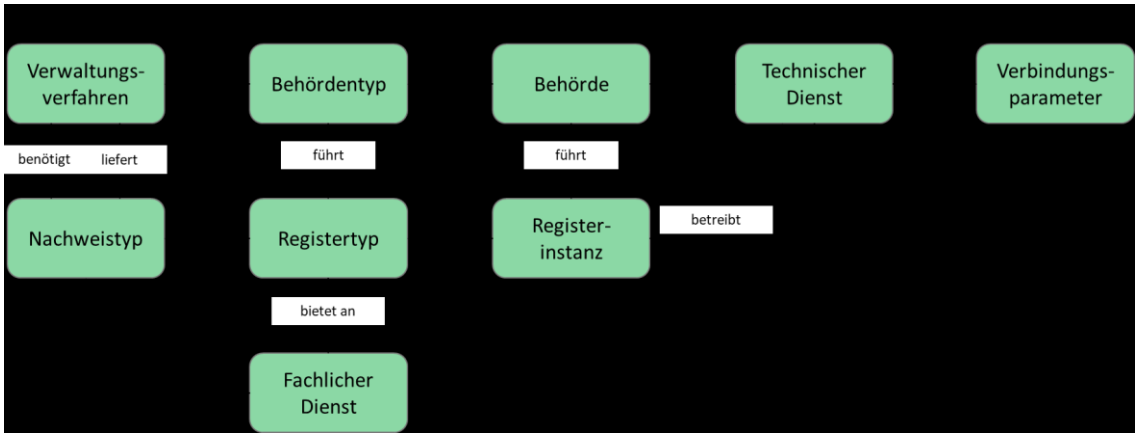


Abbildung 15: Modell Registerdatennavigation

Die in Abbildung 15 dargestellten Begriffe werden im Folgenden erläutert und mit einem Beispiel versehen.

Tabelle 15: Zentrale Begriffe und deren Zusammenhänge

Begriff	Bedeutung	Beispiel
Verwaltungsverfahren	Es liefert oder benötigt Nachweise. Es kann, muss sich aber dabei nicht um eine Leistung handeln.	„Meldedatensatz zum Abruf Bereitstellung“ (elektronische Meldebescheinigung)
Behördentyp	Kategorie von Behörden, die die gleichen Leistungen erbringen und die gleichen Prozesse ausführen. Je nach Fachdomäne gibt es eine oder mehrere Behörden vom selben Behördentyp. Behörden desselben Behördentyps führen Register desselben Registertyps. Behördentypen können auch mehrere Registertypen führen.	Meldebehörden
Behörde	Konkrete Behörde eines Behördentyps. Sie führt eine konkrete Registerinstanz und bietet einen technischen Endpunkt, über den auf diese zugegriffen werden kann.	Einwohnermeldeamt Köln
Technischer Dienst	Unter dem technischen Dienst wird die konkrete Implementierung eines fachlichen Dienstes zur Ausstellung eines Nachweises bei einer konkreten Registerinstanz verstanden. Andere technische Dienste, die Softwarekomponenten anbieten, sind im Kontext	Dienstinstanz von NOOTS_Meldebescheinigung für die Stadt Köln

Begriff	Bedeutung	Beispiel
	dieses Konzepts nicht gemeint. Für den Abruf von Nachweisen von einem technischen Dienst sind Verbindungsparameter erforderlich.	
Verbindungsparameter	Die Gesamtheit aller Informationen, die benötigt werden, um einen Technischen Dienst zu nutzen. Dazu gehört mindestens die URL des Dienstes, Zertifikate, etc.	Dienstinstanz von NOOTS_Meldebescheinigung für die Stadt Köln Zertifikat des Einwohnermeldeamts Köln
Nachweistyp	Ein fachliches Objekt, um einen Sachverhalt nachzuweisen. Dabei kann es sich um ein (elektronisches) Dokument oder eine Datenstruktur handeln. Ein Nachweistyp wird von Registern desselben Registertyps ausgestellt. Ein Nachweistyp wird von einem fachlichen Dienst geliefert.	Meldebescheinigung
Registertyp	Eine Kategorie von IT-Systemen, die Daten der Verwaltung speichern und elektronische Nachweise ausstellen können. Registerinstanzen desselben Registertyps werden von Behörden desselben Behördentyps geführt. Register desselben Registertyps bieten denselben fachlichen Dienst zur Ausstellung	Melderegister

Begriff	Bedeutung	Beispiel
	desselben elektronischen Nachweistyps an.	
Registerinstanz	Ein IT-System, welches von einer Behörde geführt wird. Registerinstanzen betreiben technische Endpunkte, über die von ihnen erstellte Nachweise abgerufen werden können.	Melderegister der Stadt Köln
Fachlicher Dienst	Logische Gruppierung technischer Dienste, die denselben Nachweistyp liefern.	NOOTS_Meldebescheinigung
Routingparameter	Je Nachweistyp festgelegte Informationen zur Ermittlung des für die Ausstellung des Nachweises zuständige Stelle.	Postleitzahl

3.1.5.3 Anwender und Systeme

Beschreibung der Nutzenden und Systeme, die auf die Registerdatennavigation oder das DSD zugreifen oder für die Aufgabenerfüllung notwendig sind.

Tabelle 16: Anwender und Systeme

Akteur	Typ	Beschreibung
Data Consumer National	Fremd-system	Nationale öffentliche Stellen, die auf die Registerdatennavigation zugreifen, um die Zuständigkeit für einen Nachweis und die technischen Verbindungsdaten zu ermitteln. Darunter fallen eine Vielzahl unterschiedlicher öffentlicher Stellen und deren Anwendungssysteme, beispielsweise Onlineanträge, Antragsportale oder Fachverfahren.

Akteur	Typ	Beschreibung
Data Consumer EU-Ausland	Fremd-system	Öffentliche Stellen der EU-Mitgliedsstaaten, die auf die RDN zugreifen, um die Zuständigkeit für einen Nachweis und die technischen Verbindungsdaten zu ermitteln. Hinweis: Im europäischen OOTS wird der Data Consumer als Evidence Requester bezeichnet.
Intermediäre Plattform	Fremd-system	Föderal betriebene Infrastrukturkomponente, die den Nachweisabruf von Data Providern aus dem EU-Ausland entgegennimmt und an Data Provider National weitervermittelt. Aus Sicht des NOOTS nimmt die Intermediäre Plattform die Rolle eines Data Consumers ein und nutzt daher dieselbe Schnittstelle wie der nationale Data Consumer.
Pflegeverant-wortliche für Nutzende/ Rechte	Nutzende/ Pflegeclient	Für die Verwaltung von Nutzenden und Rechten zuständige Stelle. Hinweis: Mit der geplanten Einführung eines zentralen IAM (siehe [ANN-003]) werden Teile dieser Pflegeverantwortung in IAM verschoben.
Pflegeverant-wortliche Nachweistypen	Öffentliche Stelle, ggfs. unterstützt durch ein Anwendungs system	Öffentliche Stelle, die verwaltet, welche Nachweistypen es gibt und welche Routingparameter je Nachweistyp erforderlich sind.
Pflegeverant-wortliche Data Provider	Öffentliche Stelle, ggfs. unterstützt durch ein Anwendungs system	Öffentliche Stelle, die verwaltet, welche Data Provider für welche Nachweise zuständig sind und mit welchen Verbindungsparametern diese abgerufen werden können.
Bestehendes Zuständigkeitsv erzeichnis	Ein oder mehrere Fremdsyste me	Bestehendes Zuständigkeitsverzeichnis, aus dem Zuständigkeits-informationen ganz oder zum Teil in die RDN übernommen werden können.
Open Data Nutzer	Zu klären	Noch zu bestimmende, öffentlich zugängliche Plattform, in der die Zuständigkeitsdaten der RDN

Akteur	Typ	Beschreibung
		publiziert werden, sofern diese keiner Sichtbarkeitseinschränkung unterliegen.

3.1.5.4 Use-Cases der Registerdatennavigation

Beschreibung von Anwendungsfällen (Use-Cases), für deren Erfüllung die Registerdatennavigation benötigt wird.

Verbindungsparameter für Nachweis abrufen

Dieser Anwendungsfall beschreibt die Nutzung der Registerdatennavigation für den Abruf der zuständigen nationalen Behörde für einen Nachweistyp mit dem entsprechenden technischen Dienst sowie dessen technische Verbindungsparameter, über die der gesuchte Nachweis abgerufen werden kann.

Tabelle 17: Use-Case 1: Verbindungsparameter für Nachweis abrufen

Use-Case ID	**Use-Case 1 [UC_1]**
Anmerkung	Dieser Use-Case ist im nationalen Kontext relevant.
Verbindlichkeit	Muss
Akteure	Data Consumer National
Vorbedingung/ auslösendes Ereignis	Ein Data Consumer benötigt einen Nachweis. Der gesuchte Nachweistyp sowie die zur Ermittlung der Zuständigkeit notwendigen Routingparameter sind bereits bekannt.
Nachbedingung/ Ergebnisse	Der Data Consumer erhält die Beschreibung der zuständigen Behörde sowie die Verbindungsparameter des technischen Dienstes. Die Verbindungsparameter umfassen alle Informationen, die für den Abruf eines Nachweises über den nationalen Once-Only Standard erforderlich sind. Das sind bspw. die URL des Endpunkts, Informationen für eine Ende-zu-Ende-Verschlüsselung zwischen Data Consumer und Data Provider sowie Informationen zum Datenformat, dem Schema und der Version des angebotenen Nachweises.

Use-Case ID	**Use-Case 1 [UC_1]**
Standardablauf	1. Der Data Consumer sendet eine Anfrage an die Registerdatennavigation und übermittelt den gesuchten Nachweistyp und notwendige Routingparameter. 2. Die RDN prüft, ob der Aufrufer für den Zugriff autorisiert ist. 3. Die Registerdatennavigation ermittelt die zuständige Behörde und deren Beschreibung. 4. Die Registerdatennavigation ermittelt die technischen Verbindungsparameter für den Nachweistyp und die zuständige Behörde.
Alternativer Ablauf	In Schritt 2 des Standardablaufs wurden nicht alle Informationen übermittelt, die für die Ermittlung der zuständigen Behörde benötigt werden. 2a. Die RDN wirft eine Exception. Darin übermittelt sie, welche Zuständigkeitsparameter für die Ermittlung der zuständigen Behörde erforderlich sind. 3a. Der Data Consumer erhebt die fehlenden Zuständigkeitsparameter. Handelt es sich um ein Onlineverfahren, fragt er die Information in der Regel beim angemeldeten Nutzenden ab. 4a.Der Data Consumer sendet erneut die Anfrage aus Schritt 1, ergänzt um die zusätzlich erhobenen Zuständigkeitsparameter aus Schritt 3a. 5a. Weiter mit dem Standardablauf Schritt 2.
Nutzungshäufigkeit	Für jeden Nachweisabruf aus der Leistungsverwaltung im nationalen Kontext und perspektivisch auch für Nachweisabrufe aus der Eingriffsverwaltung notwendig.

Verbindungsparameter für Nachweis abrufen mit bekannter Behörde

Dieser Anwendungsfall beschreibt die Nutzung der Registerdatennavigation für den Abruf eines technischen Dienstes sowie dessen technische Verbindungsparameter, über die der gesuchte Nachweis abgerufen werden kann. Die zuständige Behörde wird in diesem Fall über einen anderen Mechanismus als die RDN abgerufen.

Tabelle 18: Use-Case 2: Verbindungsparameter für bekannte Behörde abrufen

Use-Case ID	**Use-Case 2 [UC_2]**
Anmerkung	Dieser Use-Case ist im nationalen Kontext relevant. Er dient dazu, die Umstellung von Verfahren der Eingriffsverwaltung auf das NOOTS zu unterstützen, die bisher direkt das DVDV nutzen.
Verbindlichkeit	Soll
Akteure	Data Consumer National (Eingriffsverwaltung)
Vorbedingung/ auslösendes Ereignis	Ein Data Consumer benötigt einen Nachweis. Die für diesen Nachweis zuständige Behörde ist bereits bekannt und soll oder kann nicht erneut ermittelt werden. Der gesuchte Nachweistyp ist bekannt.
Nachbedingung/ Ergebnisse	Der Data Consumer erhält die Verbindungsparameter des technischen Dienstes. Die Verbindungsparameter umfassen alle Informationen, die für den Abruf eines Nachweises über den nationalen Once-Only Standard erforderlich sind. Das sind bspw. die URL des Endpunkts, Informationen für eine Ende-zu-Ende-Verschlüsselung zwischen Data Consumer und Data Provider sowie Informationen zum Datenformat, dem Schema und der Version des angebotenen Nachweises.
Standardablauf	1. Der Data Consumer sendet eine Anfrage an die Registerdatennavigation und übermittelt den gesuchten Nachweistyp und DVDV-Kennung der zuständigen Behörde. 2. Die RDN prüft, ob der Aufrufer für den Zugriff autorisiert ist. 3. Die RDN übermittelt die Beschreibung der zuständigen Behörde sowie die Verbindungsparameter des technischen Dienstes an den Data Consumer.
Alternativer Ablauf	Keiner
Nutzungshäufigkeit	Mittelfristig für Nachweiseabrufe aus der Eingriffsverwaltung notwendig.

Nutzende anlegen und Rechte erteilen

Dieser Anwendungsfall beschreibt die Einrichtung von Benutzerkonten und Berechtigungen für Data Consumer oder Pflegeverantwortliche zur Nutzung der Registerdatennavigation.

Tabelle 19: Use-Case 3: Nutzende anlegen und Rechte verteilen

Use-Case ID	**Use-Case 3 [UC_3]**
Anmerkung	Für alle von der RDN angebotenen Dienste muss das aufrufende System authentifiziert und autorisiert werden. Dieser Use-Case dient dazu, die dafür erforderlichen Benutzerkonten und Berechtigungen einzurichten.
Verbindlichkeit	Muss
Akteure	Pflegeverantwortliche für Nutzende/Rechte
Vorbedingung/ auslösendes Ereignis	Zugriffsrechte für ein System, das die RDN nutzen möchte, müssen eingerichtet oder geändert werden.
Nachbedingung/ Ergebnisse	Zugriffsrechte wurden eingerichtet oder geändert.
Standardablauf	1. Die Pflegeverantwortlichen für Nutzende/Rechte übermitteln eine Neuanlage oder Änderung an einem Benutzerkonto. 2. Die Pflegeverantwortlichen für Nutzende/Rechte übermitteln Änderungen an den Rechten, die einem Benutzerkonto zugeordnet sind. 3. Die RDN prüft, ob die Pflegeverantwortlichen für die Änderung autorisiert sind. 4. Die RDN speichert die übermittelten Daten.
Alternativer Ablauf	Keiner
Nutzungshäufigkeit	Selten

Nachweistypen und benötigte Routingparameter pflegen

Dieser Anwendungsfall beschreibt die Pflege von Nachweistypen und Routingparametern für die Registerdatennavigation.

Tabelle 20: Use-Case 4: Nachweistypen und benötigte Routingparameter pflegen

Use-Case ID	**Use-Case 4 [UC_4]**
Anmerkung	Für die Ermittlung der Zuständigkeit innerhalb eines Nachweistyps wird ein fester Satz an Routingparametern benötigt. Über diesen Use-Case wird gepflegt, welche Nachweistypen in der RDN bekannt sind und welche Routingparameter je Nachweistyp benötigt werden.
Verbindlichkeit	Muss
Akteure	Pflegeverantwortliche für Nachweistypen
Vorbedingung/ auslösendes Ereignis	Die von der RDN unterstützten Nachweistypen sollen ergänzt oder geändert werden und/oder die für die Auflösung der Zuständigkeit erforderlichen Routingparameter eines Nachweistyps sollen ergänzt oder geändert werden.
Nachbedingung/ Ergebnisse	Die Nachweistypen und Routingparameter werden aktualisiert. Alle Zuständigkeiten im Datenbestand der RDN sind konsistent mit den Nachweistypen und Routingparametern.
Standardablauf	1. Die Pflegeverantwortlichen übermitteln Änderungen an den Nachweistypen und/oder an den Routingparametern, die für einen Nachweistyp benötigt werden. 2. Die RDN prüft, ob die Änderungen in Konflikt mit dem bestehenden Datenbestand stehen und löst ggfs. eine Bereinigung der Konflikte aus. Die Umsetzung der Konfliktbereinigung ist noch zu klären. 3. Nach Auflösung der Konflikte werden die Änderungen in den Datenbestand übernommen.
Alternativer Ablauf	Keiner
Nutzungshäufigkeit	Selten

Zuständigkeiten und Verbindungsparameter pflegen

Dieser Anwendungsfall beschreibt die Pflege von Zuständigkeiten und Verbindungsparametern für die Registerdatennavigation.

Tabelle 21: Use-Case 5: Bestehende Zuständigkeiten und Verbindungsparameter pflegen

Use-Case ID	**Use-Case 5 [UC_5]**
Anmerkung	Dieser Use-Case soll die Pflege von Zuständigkeiten und Verbindungsparametern ermöglichen. Im Rahmen der Ausarbeitung der Pflegeprozesse ist zu klären, wer die Pflege verantwortet und welche IT-Unterstützung (Pflegeclient, Self-Service-Portal, etc.) dabei zum Einsatz kommt.
Verbindlichkeit	Muss
Akteure	Pflegebeauftragter des Data Provider
Vorbedingung/ auslösendes Ereignis	Ein Data Provider National ist bereit, einen elektronischen Nachweistyp im Rahmen seiner Zuständigkeit zu liefern und möchte, dass diese über das OOTS abgerufen werden können. Nachweistyp und Routingparameter sind in der RDN bereits bekannt.
Nachbedingung/ Ergebnisse	Die Daten der RDN sind aktualisiert. Aufrufe des UC_1 liefern von nun an den übermittelten Data Provider und die Verbindungsparameter, wenn der richtige Nachweistyp und die richtigen Routingparameter übergeben werden.
Standardablauf	1. Die Pflegeverantwortlichen des Data Provider übermitteln an die RDN, für welchen Nachweistyp und welche Ausprägungen der Routingparameter ein Data Provider zuständig ist und über welche Verbindungsparameter ein Nachweis abgerufen werden kann. 2. Die RDN prüft, ob die Pflegeverantwortlichen für die Pflege der Zuständigkeit berechtigt sind. 3. Die RDN prüft, ob die übermittelten Zuständigkeitsinformationen konform zu den für den Nachweistyp festgelegten Routingparametern sind. Ist dies nicht der Fall, wird die Änderung abgelehnt. 4. Die RDN speichert die Zuständigkeit und Verbindungsparameter.
Alternativer Ablauf	Keiner
Nutzungshäufigkeit	Selten

Bestehende Zuständigkeiten und Verbindungsparameter importieren

Dieser Anwendungsfall beschreibt die Möglichkeit eines Imports von Zuständigkeiten und Verbindungsparametern aus bereits existierenden Datenquellen.

Tabelle 22: Use-Case 6: Bestehende Zuständigkeiten und Verbindungsparameter importieren

Use-Case ID	**Use-Case 6 [UC_6]**
Anmerkung	Es ist fachlich zu klären, für welche Fachdomänen geeignete Quellen für einen Import von Zuständigkeiten und/oder Verbindungsparametern existieren. Bekannte Kandidaten sind: • PVOG • DVDV-Schlüsselkonzepte Ziel ist es, eine Mehrfachpflege von Zuständigkeiten und Verbindungsparametern zu vermeiden.
Verbindlichkeit	Kann
Akteure	Je nach Auslegung des Importmechanismus • Bestehendes Zuständigkeitsverzeichnis • RDN
Vorbedingung/ auslösendes Ereignis	Ein Import wird manuell oder zeitgesteuert ausgelöst.
Nachbedingung/ Ergebnisse	Die RDN kann zuständige Behörden anhand der importieren Zuständigkeiten ermitteln und Verbindungsparameter für den Nachweisabruf liefern.
Standardablauf	1. Das bestehende Zuständigkeitsverzeichnis übermittelt Zuständigkeiten und/oder Verbindungsparameter. 2. Die RDN prüft, ob die übermittelten Zuständigkeitsinformationen konform zu den für den Nachweistyp festgelegten Routingparametern sind. Datensätzen, bei denen diese nicht konform sind, werden ausgesteuert und einer manuellen Prüfung zugeführt. 3. Die RDN integriert die übermittelten Informationen in den eigenen Datenbestand. Gegebenenfalls müssen dabei weitere Informationen, wie Fachdomäne oder Nachweistyp

Use-Case ID	Use-Case 6 [UC_6]
	angegeben werden, damit die Informationen korrekt zugeordnet werden können.
Alternativer Ablauf	Keiner
Nutzungshäufigkeit	Offen

3.1.5.5 Liste der fachlichen Anforderungen

Auflistung der fachlichen Anforderungen an die Registerdatennavigation. Die Anforderungen sind wie folgt priorisiert:

- **Hoch:** Anforderung wird für die initiale Inbetriebnahme des NOOTS benötigt
- **Mittel:** Anforderung wird zu einem späteren Zeitpunkt benötigt

Tabelle 23: Registerdatennavigation - Funktionale Anforderungen

ID	Anforderung	Erläuterung	Priorität
[AFO-API-NAT-01]	Die RDN muss einen Dienst anbieten, der anhand des übergebenen Nachweistyps und weiterer Routingparameter die Verbindungsparameter des technischen Dienstes, über die der Nachweis abgerufen werden kann, sowie die den Dienst betreibende Behörde ermittelt.	Im Rahmen der Feinkonzeption ist ein geeigneter Identifikator für Nachweistypen festzulegen und zu klären, wie dessen Pflege erfolgt. Als mögliche Quelle kann die Registerlandkarte des BVA in Betracht gezogen werden. Welche Routingparameter für welchen Nachweistyp erforderlich sind, ist im Rahmen der Feinkonzeption zu klären.	hoch
[AFO-API-NAT-01a]	Die in [AFO-API-NAT-01] angewendete Zuständigkeitslogik muss eine regionale Zuständigkeit auf Grundlage des Amtlichen Gemeindeschlüssel (AGS) oder eines vergleichbaren nationalen	Ein vergleichbarer nationaler Zuständigkeitsschlüssel ist der Allgemeine Regionalschlüssel (ARS).	hoch

ID	Anforderung	Erläuterung	Priorität
	Zuständigkeitsschlüssels unterstützen.		
[AFO-API-NAT-01b]	Die in [AFO-API-NAT-01] angewendete Zuständigkeitslogik soll die Ermittlung der regionalen Zuständigkeit anhand der postalischen Adresse unterstützen.		mittel
[AFO-API-NAT-01c]	Die in [AFO-API-NAT-01] ermittelte Behörde soll eine Beschreibung der Behörde umfassen.	Welche Informationen in der Behördenbeschreibung konkret darzustellen sind, ist im Rahmen der Feinkonzeption zu klären.	hoch
[AFO-API-NAT-02]	Die RDN soll einen Dienst anbieten, der anhand des übergebenen Nachweistyps und der für den Nachweis zuständige Behörde alle Verbindungsparameter ermittelt, die für den Abruf eines Nachweises erforderlich sind.	Dieser Dienst erwartet, dass die zuständige Behörde bereits bekannt ist. Er dient dazu, Verfahren den Umstieg auf das NOOTS zu erleichtern, die bisher direkt das DVDV verwenden und die Zuständigkeit nicht über die RDN neu ermitteln können. Das ist dann der Fall, wenn die Zuständigkeit selbst im Datenbestand des Data Consumers vorliegt (Beispiel: Meldewesen), die für [AFO-API-NAT-01] erforderlichen Routingparameter jedoch nicht vorliegen und auch nicht einfach neu von den Nutzenden erfragt werden können (behördeninitiierte Use-Cases). Welche ID für die Behörde übergeben werden muss, ist im Rahmen der Feinkonzeption zu klären. Um eine einfache Umstellung vom DVDV zu ermöglichen, bietet es sich	mittel

ID	Anforderung	Erläuterung	Priorität
		an, dafür die DVDV-Kennung zu verwenden.	
[AFO-API-NAT-03]	Die RDN muss die erforderlichen Verbindungsparameter liefern, um eine Ende-zu-Ende-Verschlüsselung des Nachweisabrufs zwischen Data Consumer und Data Provider zu ermöglichen.	Die erforderlichen Verbindungsparameter werden durch den Nachweisabrufstandard definiert.	hoch
[AFO-API-NAT-04]	Falls die RDN die zuständige Behörde nicht zweifelsfrei ermitteln kann, muss sie fehlende Routingparameter in Form einer Exception melden.	Dazu muss der gleiche Mechanismus wie in [AFO-EU-API-01] verwendet werden.	mittel
[AFO-API-NAT-05]	Die RDN muss die Informationen liefern, die für den Abruf eines Nachweises im gewünschten Datenformat und dem gewünschten Schema und Version erforderlich sind.	Wo und in welcher Form die verfügbaren Nachweistypen und ggfs. deren Versionen verwaltet und publiziert werden, ist im Rahmen der Feinkonzeption zu klären.	hoch
[AFO-API-NAT-06]	Die RDN muss das für den Abruf eines Nachweises erforderliche Vertrauensniveau liefern.	Vergleiche dazu die Technische Richtlinie TR-03107-1 "Elektronische Identitäten und Vertrauensdienste im E-Government - Teil 1: Vertrauensniveaus und Mechanismen".	hoch
[AFO-API-NAT-07]	Die RDN soll alle Daten, die nicht schützenswert sind, als Open-Data bereitstellen.	Die RDN muss die Daten nicht selbst über eine Schnittstelle im Internet bereitstellen. Es genügt, wenn sie diese auf einer Open-Data Platform bereitstellt. Im Rahmen der Feinkonzeption ist zu prüfen, ob die Registerlandkarte dazu dienen kann.	mittel

ID	Anforderung	Erläuterung	Priorität
		Die Daten sollen mit Mitteln des Semantic Web auswertbar sein.	
[AFO-IMPL-01]	Die RDN muss auf dem bestehenden DVDV aufsetzen und dieses um eine weitere Komponente zur Abbildung der Zuständigkeit für Nachweistypen ergänzen.	Die Routinglogik soll nicht in das bestehende Datenschema des DVDV übernommen werden. Eine zum bestehenden DVDV redundante Pflege der Behörden soll vermieden werden. Es soll geprüft werden, ob diese Komponente über die Nachnutzung bestehender Zuständigkeitsfinder realisiert kann.	hoch
[AFO-IMPL-01a]	Die Komponente zur Abbildung der Zuständigkeit gemäß [AFO-IMPL-01] soll so gestaltet werden, dass sie perspektivisch nicht nur Zuständigkeiten für Nachweise, sondern auch andere Arten von Zuständigkeiten verwalten kann.		mittel
[AFO-IMPL-02]	Die RDN muss in der Lage sein, um beliebige Zuständigkeitslogiken erweitert zu werden.	Eine Erweiterbarkeit kann durch Konfigurierbarkeit oder durch Softwareentwicklung erfolgen, sollte aber keine destruktiven Änderungen an den Schnittstellen der RDN erfordern.	mittel
[AFO-PFL-01]	Die RDN muss die für eine konsistente Pflege von Zuständigkeitsinformationen für Nachweise benötigten Funktionen implementieren.	Ob dabei ein zentral überwachter Pflegeprozess, wie bisher im DVDV, zum Einsatz kommt oder ein eher dezentraler Self-Service Ansatz nach dem Vorbild von FIT Connect, ist im Rahmen der Umsetzung mit dem Kompetenzteam Recht &	hoch

ID	Anforderung	Erläuterung	Priorität
		Datenschutz und dem für die Governance zuständigen Federführer zu klären.	
[AFO-PFL-01a]	Falls es geeignete Quellen für Zuständigkeiten gibt und diese automatisiert bestehenden Zuständigkeitsdaten zugeordnet werden können, muss die RDN eine Schnittstelle anbieten, über die Daten importiert werden können.	Aus welcher Quelle die Zuständigkeitsinformationen übernommen werden, ist im Rahmen der Ausarbeitung der Pflegeprozesse zu klären. Eine redundante manuelle Pflege soll vermieden werden.	mittel
[AFO-PFL-1b]	Die RDN muss alle Änderungen im Rahmen der Pflege revisionssicher protokollieren.		hoch

3.1.6 Facharchitektur

Dieses Kapitel stellt einen empfohlenen Lösungsansatz zur Umsetzung der RDN vor. Es ist nicht als zwingende Vorgabe zu verstehen, sondern als Umsetzungsoption. Darüber hinaus dient es dem vertieften Verständnis der RDN.

3.1.6.1 Lösungsansatz Registerdatennavigation

Abbildung 16 stellt skizziert die Lösung aus Sicht der Registermodernisierung dar. Die Verortung des DVDV und DVZV innerhalb der RDN soll deutlich machen, dass diese von den Nutzenden der RDN nicht direkt verwendet werden sollen. Dies impliziert jedoch nicht, dass das DVDV in der RDN aufgeht. Gemäß [RMBED-02] bleibt das als DVDV als eigenständiges Dienste Verzeichnis erhalten.

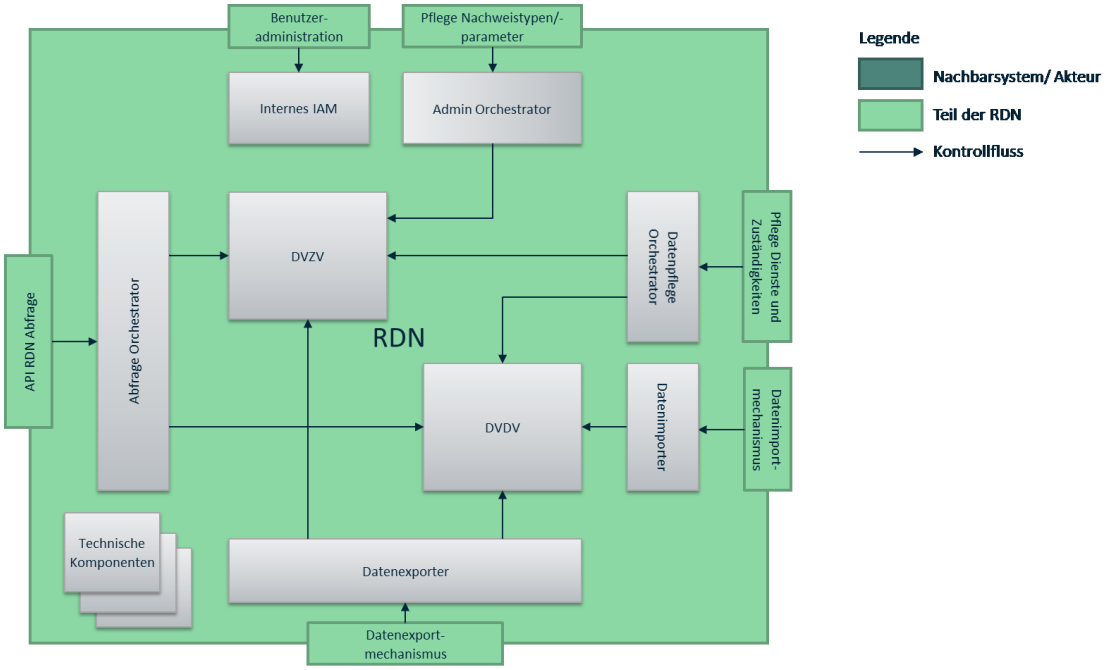


Abbildung 16: Skizze der RDN-Lösungsarchitektur

Tabelle 24: Registerdatennavigation - Bausteine der Lösungsarchitektur

Komponente	Aufgabe	Anmerkung
Deutsches Verwaltungsdienste Verzeichnis (DVDV)	Verwaltet die technischen Dienste mit ihren Verbindungsparametern.	Das bestehende DVDV soll so weit wie möglich wiederverwendet werden.
Deutsches Verwaltungszuständigkeitsverzeichnis (DVZV)	Verwaltet Behörden und ihre Zuständigkeiten für Nachweise.	Die Bezeichnung DVZV ist ein Arbeitstitel. Er weist darauf hin, dass mit zunehmender Anzahl an Zuständigkeitsverzeichnissen (bspw. PVOG, Zufi) über ein zentrales Verzeichnis nach dem Vorbild des DVDV nachgedacht werden sollte. Das DVZV könnte diese Rolle mittelfristig übernehmen.
Technische Komponenten	Für den Betrieb des Systems wichtige technische Bausteine wie Logging Systeme, betriebliche Überwachungssysteme, Lastverteiler, etc. Da die Systeme unabhängig von der konkreten Fachlichkeit der RDN sind, werden sie hier nicht weiter betrachtet.	Das bestehende DVDV verfügt bereits über viele entsprechende Lösungen, die für eine Wiederverwendung der RDN infrage kommen. Aufrufe zu technischen Komponenten werden der Übersicht halber nicht dargestellt.
Internes Identity and Access Management (IAM)	Interne Benutzer- und Rollendatenverwaltung sowie Authentifizierungs- und Autorisierungsmechanismus für alle Nutzenden der RDN.	Wird als Interimslösung benötigt, bis das zentrale IAM für Behörden zur Verfügung besteht. Eine Wiederverwendung des bestehenden IAM des DVDV sollte geprüft werden.

Komponente	Aufgabe	Anmerkung
		Aufrufe des internen IAM werden der Übersicht halber nicht dargestellt.
Abfrage Orchestrator	Führt Abfragen der Zuständigkeit und der Verbindungsparameter aus, indem es Daten des DVZV und des DVDV abfragt und miteinander verknüpft.	Diese Komponente stellt die Implementierung der Routing-API dar.
Datenpflege Orchestrator	Die Pflege von Zuständigkeitsdaten und Verbindungsparametern muss konsistent zum DVDV und DVZV erfolgen. Diese Komponente ist für die Verteilung von Pflegezugriffen auf beide Verzeichnisdienste und die Wiederherstellung der Konsistenz in Fehlerfällen zuständig.	
Admin Orchestrator	Übernimmt die Pflege von Nachweistypen und die je Nachweistyp erforderlichen Routingparameter	Die Komponente muss insbesondere dafür sorgen, dass durch Pflege an den Nachweistypen keine Inkonsistenzen im Gesamtdatenbestand entstehen.
Datenimporter	Modul zum Import von Datenbeständen aus bestehenden Datenquellen. Kümmert sich um Abbildung der übermittelten Daten auf interne Datenstrukturen und	Für unterschiedliche Datenquellen werden voraussichtlich unterschiedliche Importer benötigt.

Komponente	Aufgabe	Anmerkung
	Verknüpfung diese mit dem bestehenden Datenbestand.	Da Datenquellen vermutlich nur Teile des Datenbestands liefern werden (bspw. kennt PVOG den Begriff des Nachweistyps nicht), muss eine Möglichkeit zur Anreicherung der importierten Daten geschaffen werden.
Datenexporter	Modul zum Export der Datenbestände in eine noch festzulegende Open Data Platform.	

3.1.6.2 Entwurfsentscheidungen

Im Zuge der Konzeption einer Lösung wurden verschiedene Lösungsansätze geprüft. Um eine zuverlässige Bewertung durchführen zu können, wurden die lösungsspezifischen Vor- und Nachteile gegenübergestellt sowie Chancen und Risiken abgewogen. Im Folgenden wird der als am meisten tragfähig bewertete Lösungsansatz zur Umsetzung der Registerdatennavigation hergeleitet, der sich bereits in den oben ausgeführten fachlichen Anforderungen widerspiegelt. Zum Zwecke der Transparenz und der Vermeidung von Doppelarbeit sind im Anhang 3.1.9.5 Lösungsvarianten festgehalten, die sich nach eingehender Prüfung als nicht ausreichend tragfähig herausgestellt haben.

Der Lösungsansatz, der als vielversprechend für die Umsetzung der Registerdatennavigation bewertet wurde, setzt auf das DVDV für die Ermittlung von Verbindungsparameter, sieht jedoch den Aufbau einer neuen Komponente für die Zuständigkeitsermittlung vor. Inwieweit diese neue Komponente auf bestehende Systeme aufbaut, wird in der Feinkonzeption ausgearbeitet. Die einzelnen Entwurfsentscheidungen der Empfehlung lassen sich wie folgt begründen:

A. Die RDN wird als zentraler Routing-Dienst (Routing As a Service) entwickelt.

Die heterogenen Zuständigkeitslogiken unterschiedlicher Registertypen führen zu einer hohen Komplexität der Zuständigkeitsdaten, wenn alle Zuständigkeitslogiken im selben Datenbestand abgebildet werden müssen. Zudem ist diese auf Dauer schwer wartbar und schwerer weiterzuentwickeln, wenn Data Consumer die Zuständigkeitsinformationen direkt abrufen und interpretieren.

Daher wird eine einfach erweiterbare API vorgesehen, die die jeweilige Zuständigkeitslogik je Registertyp verbirgt und immer nur die für diesen Registertyp relevanten Routingparameter erwartet.

Dadurch wird die Komplexität der Zuständigkeitslogik vor dem Data Consumer verborgen. Zudem kann das interne Datenmodell der RDN nach Bedarf weiterentwickelt werden, ohne dass sich dies auf bestehenden Nutzenden der API auswirkt.

B. Das DVDV wird genutzt und wird Teil der RDN.

Das DVDV ist als zentrales Dienste Verzeichnis des IT-Planungsrats etabliert. Die Speicherung der Nachweisabrufdienste in einem anderen Dienste Verzeichnis würde dem Anspruch des DVDV als zentrales Dienste Verzeichnis widersprechen. Daher sollte das

DVDV als integraler Bestandteil der RDN betrachtet werden. Inwiefern diese Integration technisch vollzogen wird, bleibt der Feinkonzeption überlassen."

C. Zur Abbildung von Zuständigkeiten wird ein neues Verzeichnis aufgebaut, das DVZV.

Bestehende Zuständigkeitsverzeichnisse oder mithilfe von Schlüssellogiken abgebildete Zuständigkeiten im DVDV bieten nicht den Funktionsumfang, der von der RDN gefordert wird. Die Abbildung von Zuständigkeiten ist entweder auf einzelne Fachdomänen beschränkt (Beispiel: Schlüsselkonzept im Meldewesen) und nicht ausreichend flexibel für die Registermodernisierung oder auf andere Arten von Zuständigkeiten spezialisiert (Beispiel: PVOG für Antragsbearbeitung).

Für die RDN wird daher die Schaffung einer neuen Komponente ZVDV unterstellt, die explizit nicht nur für Nachweise ausgelegt werden soll, sondern künftig unterschiedliche Zuständigkeiten abbilden können soll. Hierdurch wird ausdrücklich nicht ausgeschlossen, dass das DVZV durch Weiterentwicklung einer bestehenden Komponente (bspw. PVOG) geschaffen werden kann. Dies ist Gegenstand der Feinkonzeption der RDN.

D. Die RDN bietet dem Data Consumer zwei Funktionen an.

Bei der Ermittlung von Verbindungsparametern für einen Nachweisabruf bearbeitet die Registerdatennavigation zwei Prozessschritte:

1. Die RDN ermittelt auf Grundlage des gewünschten Nachweistyps sowie verschiedener Routingparameter die (gemäß [ANN-006] eindeutige) zuständige Behörde, die den Dienst für die Nachweisausstellung betreibt.
2. Die RDN identifiziert den benötigten technischen Dienst und ermittelt auf Grundlage der zuständigen Behörde dessen Verbindungsparameter.

Es wird vorgeschlagen, die beiden oben genannten Prozessschritte zu trennen, sodass letzterer Prozessschritt auch einzeln abgefragt werden kann. Die RDN soll demnach zwei Funktionen anbieten:

- Eine Funktion API-NAT-1, bei der beide Prozessschritte auf einmal aufgerufen werden. Diese entspricht der Anforderung [AFO-API-NAT-01].
- Eine Funktion API-NAT-2, bei der der zweite Prozessschritt einzeln aufgerufen werden kann. Diese entspricht der Anforderung [AFO-API-NAT-02].

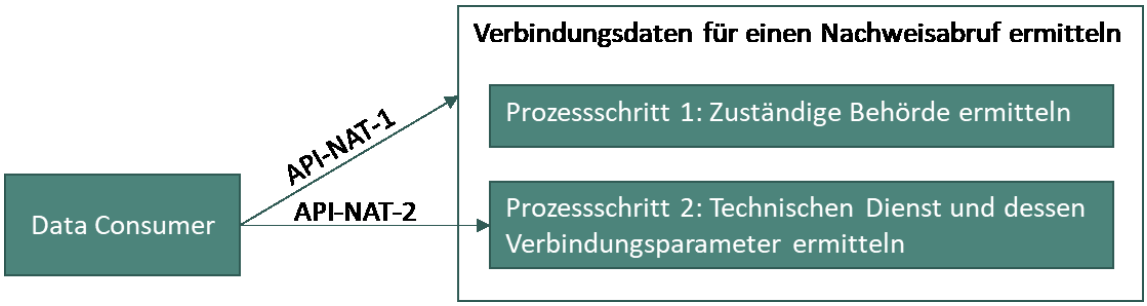


Abbildung 17: Funktionsbündelung der Registerdatennavigation

Vorteile und Begründung: Dieses Vorgehen ermöglicht eine flexible Nutzung der RDN für verschiedene Nutzergruppen. Die Entscheidung, über Funktion API-NAT-2 die Verbindungsparameter auch gesondert abrufen zu lassen, sorgt für Bestandsschutz, denn so können Data Consumer bei Bedarf über die RDN indirekt wie gewohnt die Funktion des DVDV aufrufen. Das vereinfacht ihnen den Übergang zur Nutzung der RDN. Zweitens wird die RDN so den Bedürfnissen der Eingriffsverwaltung gerecht [ANN-004], die in keiner aktiven Kommunikation mit Nutzenden steht und somit ggf. nicht über die für Prozessschritt 1 geforderten Routingparameter verfügt. Darüber hinaus kann die gesonderte Funktion API-NAT-02 vom Data Consumer in Anspruch genommen werden, die darüber Kenntnis besitzen, welche Behörde den für den gewünschten Nachweistyp nötigen Dienst betreibt, beispielsweise weil sie regelmäßig mit ihr kommunizieren oder es sich um ein leicht zu identifizierendes Zentralregister handelt. Aufwand wird insofern eingespart, als dass der Data Consumer nur eine sehr simple Anfrage an die RDN richtet, wie auch bei der RDN selbst, die in diesen Fällen einen verkürzten Prozess zur Beantwortung der Anfrage durchlaufen muss.

Ein **Risiko** bei Nutzung von Funktion API-NAT-2 liegt darin, dass Data Consumer nicht über Änderungen bei Zuständigkeiten informiert werden und mit veralteten Informationen arbeiten könnten. Die RDN würde in diesem Fall eine Fehlermeldung oder ein veraltetes Resultat zurückliefern, was ggf. erst beim Nachweisabruf auffallen würde. Letztendlich müsste der Data Consumer einen weiteren Abruf, diesmal der Funktion API-NAT-1, bei der RDN durchführen, wodurch sich das Vorgehen verlängern würde.

E. Die RDN setzt bei der Pflege von Zuständigkeiten und Nachweisen auf bestehende Quellen.

Vorteile und Begründung: Um das benötigte Zuständigkeitsverzeichnis DVZV aufzubauen, wird die Registerdatennavigation Daten aus bestehenden Quellen importieren oder darauf aufbauen. Dies spart Aufwand bei der Pflege von Zuständigkeitsinformationen und trägt

dazu bei, dass bestehende Zuständigkeits- und Nachweisverzeichnisse harmonisiert und aktuell sind.

3.1.6.3 Fachliches Datenmodell

Für die beschriebenen Funktionen der RDN muss diese in ihrem Datenbestand mindestens über die im folgenden Klassendiagramm dargestellten Informationen verfügen. Dies wird im Rahmen der Feinkonzeption weiter detailliert.

Hinweis: Die Zuständigkeitsstrategie meint die Logik, die die Zuständigkeit für einen Nachweistyp definiert, z.B. regionale Strukturierung der Zuständigkeit auf Grundlage des Allgemeinen Gemeindeschlüssels (AGS).

Abbildung 18: Klassendiagramm für Registerdatennavigation

3.1.6.4 Schnittstellen der Registerdatennavigation

Gemäß Lösungsarchitektur in Abbildung 18 benötigt die RDN die in der Tabelle aufgeführten Schnittstellen und Export- bzw. Importmechanismen in Verbindung mit anderen Akteuren. Eine direkte Benutzerschnittstelle ist zunächst nicht vorgesehen, könnte aber bei der Feinkonzeption des Pflegesystems als relevant erachtet werden.

Tabelle 25: Übersicht Schnittstellen der Registerdatennavigation

Name der Schnittstelle	Kommunikationspartner der RDN	Zweck
API RDN Abfrage	Data Consumer	Abruf RDN-Funktionen
Pflege Nachweistypen/-parameter	Pflegeverantwortliche für Nachweistypen	Pflege
Pflege Dienste und Zuständigkeiten	Pflegeverantwortliche für Data Provider	Pflege
Benutzeradministration	Pflegeverantwortliche für Nutzende/ Rechte	Administration der Pflege-Nutzenden
Datenimport-mechanismus	Bestehende(s) Zuständigkeitsverzeichnis(se)	Import von Zuständigkeiten und Verbindungsparameter
Datenexport-mechanismus	Open Data Platform	Veröffentlichung der Zuständigkeiten und weiterer Informationen

API RDN Abfrage

Wie in Entwurfsentscheidung D beschrieben, wird die RDN API zwei Funktionen vorhalten, die vom Data Consumer alternativ angefragt werden können, je nachdem, ob diesem die für den Nachweis zuständige Behörde unbekannt ist (Funktion API-NAT-1) oder bekannt (Funktion API-NAT-2).

Tabelle 26: Ein- und Ausgabedaten der zwei Funktionen der RDN API

Funktion	Eingabedaten (von Data Consumer)	Ausgabedaten (von RDN)
Funktion API-NAT-1 *findEvidenceService*	1. Routingparameter: Angaben zur regionalen Zuständigkeit, z.B. AGS,	1. Behördenbeschreibung

Funktion	**Eingabedaten (von Data Consumer)**	**Ausgabedaten (von RDN)**
	ARS, und weitere Parameter nach Bedarf 2. Nachweistyp 3. Dienst-Metadaten: Datenformat, gewünschtes Schema und Version	2. Verbindungsparameter des technischen Diensts
Funktion API-NAT-2 *findEvidenceServiceAddress*	1. DVDV-Schlüssel 2. Organisationskategorie 3. Nachweistyp 4. Dienst-Metadaten: Datenformat, gewünschtes Schema und Version	1. Behördenbeschreibung 2. Verbindungsparameter des technischen Diensts

Der Datenfluss für Funktion API-NAT-1 gestaltet sich wie folgt (siehe auch Abbildung 19): Der Data Consumer sendet eine Anfrage an die RDN, in der er den gewünschten Nachweistyp sowie erforderliche Routingparameter übergibt. Sind die Routingparameter nicht ausreichend, stellt der Abfrage Orchestrator der RDN eine entsprechende Rückfrage. Dieses Vorgehen entspricht dem des Data Service Directory („Exceptions“). Sind alle notwendigen Parameter erfasst, identifiziert der Abfrage Orchestrator im DVZV die den Dienst anbietende Behörde, deren DVDV-Schlüssel und Organisationskategorie. Parallel dazu setzt er aus den vorliegenden Informationen zu Nachweistyp und Dienst-Metadaten den „Uniform Resource Identifier“ (URI) des benötigten technischen Diensts zusammen.

Mit diesen Angaben stellt der Abfrage Orchestrator zwei separate Anfragen an das DVDV, eine zur Ermittlung der technischen Verbindungsparameter (*findServiceDescription*) und eine weitere zur Ermittlung der Behördenbeschreibung (*findOrganizationDescription*). Die Ergebnisse dieser beiden Anfragen fasst der Abfrage Orchestrator in eine Antwortnachricht an den Data Consumer zusammen.

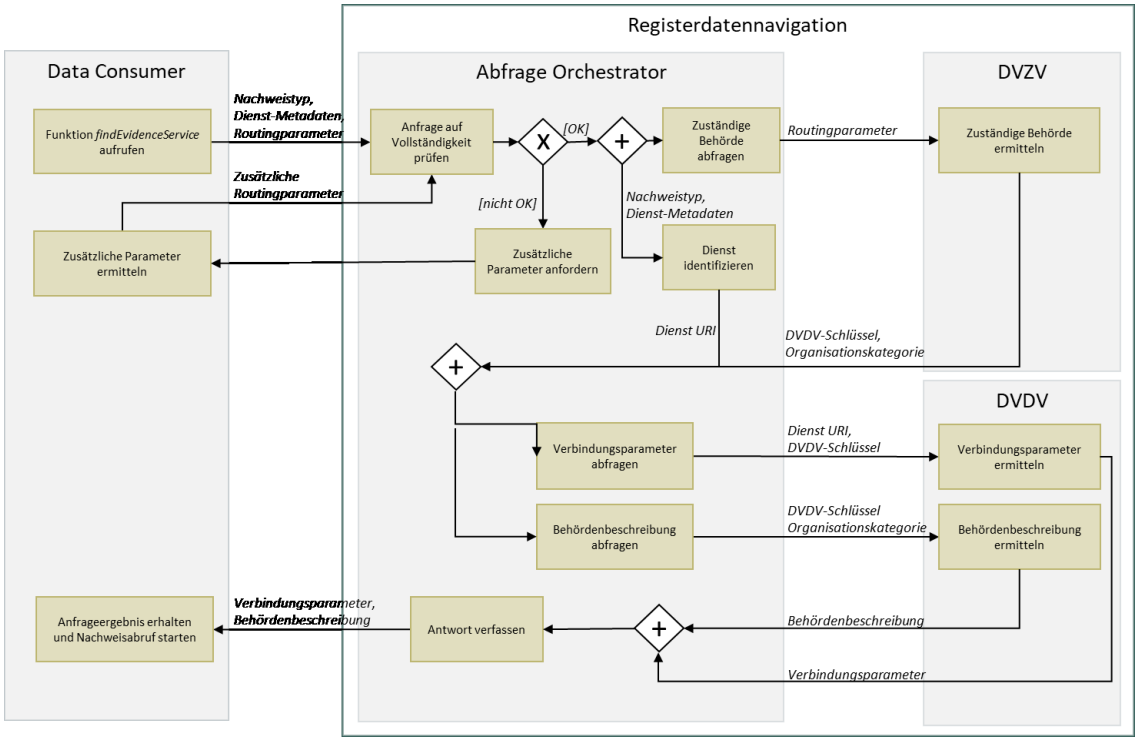


Abbildung 19: Datenfluss von Funktion API-NAT-1 der API RDN Abfrage

Der Datenfluss der Funktion API-NAT-2 ist entsprechend verkürzt (siehe Abbildung Abbildung 20): Hier besitzt der Data Consumer bereits Kenntnis über die den Dienst anbietende Behörde und sendet den entsprechenden DVDV-Schlüssel und die entsprechende Organisationskategorie zusammen mit den Dienst-Metadaten und Nachweistyp an den Abfrage Orchestrator. Dieser ermittelt im DVDV die technischen Verbindungsparameter und die Behördenbeschreibung und schickt diese zusammengefasst in einer Antwortnachricht an den Data Consumer zurück.

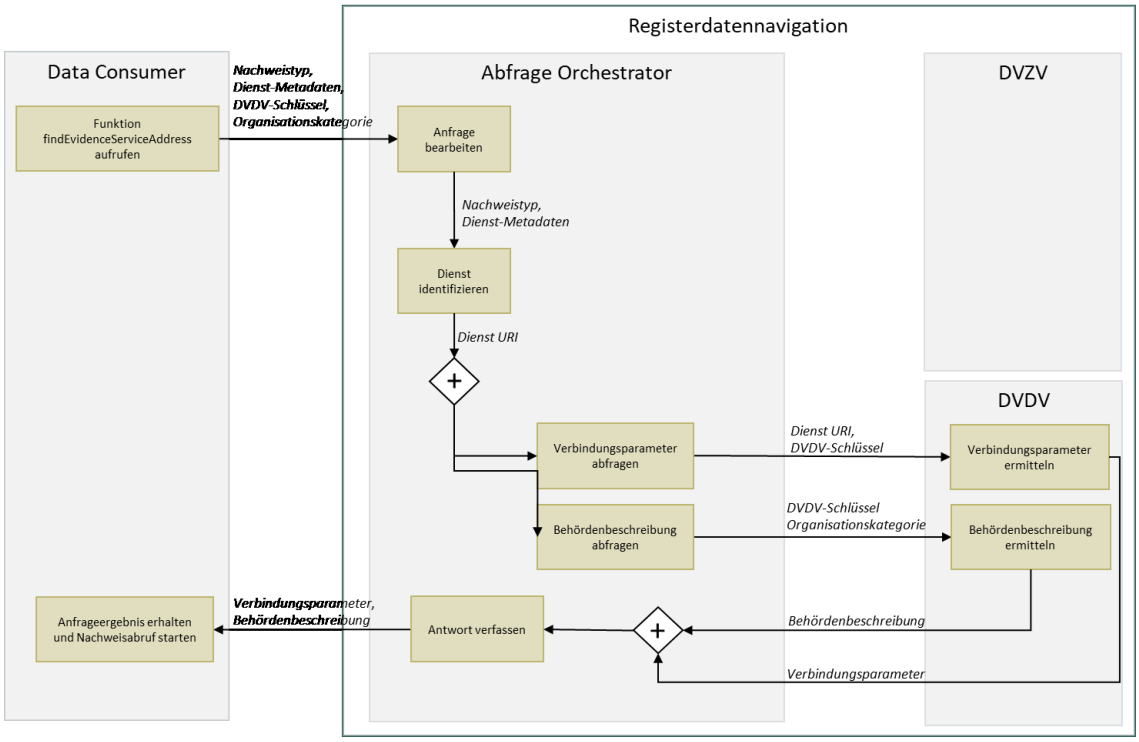


Abbildung 20: Datenfluss von Funktion API-NAT-2 der API RDN Abfrage

Pflege Nachweistypen/-parameter

Über diese Funktion erhält der Datenpflege Orchestrator vom Pflegesystem für Nachweistypen mindestens Informationen über:

- Verfügbare Nachweistypen aus der Verwaltung
  - für deutsche wie EU Data Consumer
  - für Nutzende-initiierte wie Behörden-initiierte Nachweisabrufe
- Benötigte Routingparameter pro Nachweistyp

Pflege Dienste und Zuständigkeiten

Über diese Funktion erhält der Datenpflege Orchestrator vom Pflegesystem für registerführenden Stellen (Data Provider) mindestens Informationen über:

- Bereitgestellte Nachweistypen
- Zuständiger Dienst pro Nachweistyp

- Passende Ausprägungen der Routingparameter pro Dienst, z.B. für welche Region ein Dienst genutzt werden kann.
- Verbindungsparameter für den Nachweisabruf pro Dienst

Benutzeradministration

Mit dieser Funktion werden die zuvor im Pflegesystem angelegten Nutzerprofile in das Identitäts- und Zugriffsmanagement (*Identity and Access Management - IAM)* der RDN importiert. Die Nutzerprofile bestehen mindestens aus

- der Bezeichnung der pflegenden Stelle (Behörde oder von ihnen beauftragte Stellen)
- eindeutige Kennnummer
- Passwörter oder Zertifikate für den Zugriff
- gewährte Schreibrechte für die Pflege von Nachweistypen und Data Provider-Daten.

Weiteres ist in der Feinkonzeption in Anlehnung an die Registermodernisierungskomponente „IAM für Behörden“ (Kapitel 3.3) zu klären.

Datenimportmechanismus

Die für die Zuständigkeitsermittlung notwendigen Informationen liegen zum Teil bereits in anderen Systemen (z.B. Zuständigkeitsfindern) vor. Damit keine redundante Erfassung von Zuständigkeitsinformationen erfolgt, werden im Rahmen der Feinkonzeption geeignete Quellen identifiziert, aus denen die Registerdatennavigation Zuständigkeitsinformationen importieren kann.

Hierfür kann sich eine XZuFi-Schnittstelle eignen, die standardisiert den unabhängigen Austausch von Informationen zu Verwaltungsdienstleistungen, Online-Diensten, Gebieten, Formularen und den hierfür zuständigen Organisationseinheiten im Kontext von Zuständigkeitsfindern, Bürger- und Unternehmensinformationssystemen und Leistungskatalogen ermöglicht.

Datenexportmechanismus

Über diesen Mechanismus werden Informationen zu Zuständigkeiten, Diensten und Verbindungsparametern, sofern sie als nicht schützenswert eingestuft werden, auf einer

noch zu definierenden Open Data Platform im Open-Data Format veröffentlicht. Dies kann in regelmäßigen Intervallen oder bei Änderungen wiederholt werden.

3.1.7 Technische Aspekte

3.1.7.1 Datenschutz

Die RDN ermittelt und beauskunftet Zuständigkeitsinformationen sowie technische Verbindungsparameter von Diensten. Für diese Aufgaben muss sie prinzipiell keine Kenntnis der Person haben, für die ein Nachweisabruf getätigt werden soll. Es gibt dennoch drei Bereiche, die potenziell datenschutzrelevant sind:

Szenario 1: Zuständigkeitsermittlung lässt Rückschlüsse auf Person zu

Bei Anfragen an die RDN zur behördlichen Zuständigkeit könnten die Angaben zum Nachweistyp, Adresse und ggf. weiterer Parameter der antragstellenden Person in ihrer Kombination so selten sein, dass daraus die Identität der antragstellenden Person abgeleitet werden kann. Dies könnte bei der Beantragung einer seltenen Leistung, für die nur eine eng gefasste Personengruppe anspruchsberechtigt sind, vorkommen.

Szenario 2: Personenbezogene Daten im Pflegesystem

Die Pflege von behördlichen Zuständigkeiten oder Nachweisen könnte von verantwortlichen Personen vorgenommen werden, die für diese Aufgabe eindeutig identifizierbar im Pflegesystem angemeldet sind. Deren personenbezogenen Daten sind schützenswert gemäß DSGVO.

Szenario 3: Personenbezogene Daten als Teil von Zuständigkeitsinformationen

Verzeichnisse zu behördlichen Zuständigkeiten, wie das PVOG, enthalten die FIM-Leistungsbeschreibung. Obwohl diese es formell nicht vorsieht, kann es vorkommen, dass in dieser Beschreibung Personen namentlich und ggf. mit Kontaktdaten genannt werden. Bei Integration oder Import von Daten aus diesen Verzeichnissen kann es entsprechend zur Übernahme von personenbezogenen Daten in die RDN kommen.

Diese Szenarien sollten im Rahmen der Feinkonzeption bewertet und bei Bedarf durch die Anwendung der DSGVO adressiert werden. Dies schließt auch die personenbezogenen Daten ein, die in Protokollen erfasst werden.

3.1.7.2 IT-Sicherheit

Während der Konzeption wurde eine vorläufige Einschätzung zum Schutzbedarf vorgenommen. Ausführungen zu der Begründung sind im Anhang 3.1.9.8 zu finden.

Tabelle 27: Vorläufige Einschätzung zum Schutzbedarf der RDN

Kategorie	Vorläufige Einschätzung zu Schutzbedarf	Begründung	Resultierende nicht funktionale Anforderung
Vertraulichkeit	Normal	Daten zu behördlichen Zuständigkeiten und Verbindungsdaten zu Diensten bieten wenig Grundlage für Missbrauch und können im Nutzerkreis von Behörden geteilt werden. Hinweis: Die bestehenden Schutzmechanismen des DVDV bleiben hiervon unberührt.	[NFA_S004] [NFA_S005]
Integrität	Hoch	Eine Manipulation der Daten der RDN könnte die Fehlleitung von Nachweisabrufen und damit potenziell Falschausstellung von Nachweisen zur Folge haben und ist aufgrund der Betrugsmöglichkeiten zu vermeiden.	[NFA_S001]
Verfügbarkeit	Hoch	Die RDN muss verlässlich erreichbar sein, da sonst kein Nachweisabruf möglich ist, was zum einen die Leistung der Nutzenden und zum anderen das korrekte Arbeiten der Verwaltung beeinträchtigt. Dies ist vor allem im Zusammenhang mit Sicherheitsbehörden kritisch.	[NFA_Z001]

Die Konkretisierung der IT-Sicherheitsanforderungen, entsprechend den Anforderungen des IT-Grundschutzes, wird in der Projektplanung umgesetzt. Insbesondere ist hier eine Risikoanalyse frühzeitig einzuplanen und ein Sicherheitskonzept in Einvernehmen mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI) zu erstellen. Dabei müssen Betriebsumgebung sowie das Rechte- und Rollensystem für die Zugriffe auf die RDN den formulierten Schutzzielen entsprechen.

3.1.7.3 Antwortzeit und Last

Zum aktuellen Zeitpunkt sind weder die Antwortzeiten noch das Lastprofil vorhersehbar. In jedem Fall sollen sie einen synchronen Prozess des Nachweisabrufs ermöglichen. Die dafür nötigen Antwortzeiten des gesamten Nachweisabrufs werden zu einem späteren Zeitpunkt für das NOOTS festgelegt. Zur Anzahl zugreifender Verfahren, deren Nutzungshäufigkeit und zeitliche Verteilung gibt es keine ausreichenden Erkenntnisse.

Daraus lassen sich folgende Konsequenzen ableiten:

- Eine abschließende Anforderung an Lastfähigkeit und Antwortzeiten ist nicht möglich.
- Die Lastanforderungen sind mit jeder Zuschaltung weiterer Data Consumer zu überprüfen und die Skalierung der Registerdatennavigation ist entsprechend anzupassen. Initiale Lastanforderungen sind im Folgenden aufgeführt und im Rahmen der Feinkonzeption zu überprüfen.
- Langfristig ist eine hochgradig automatisiert skalierbare Betriebsumgebung anzustreben, welche auch die erforderliche Elastizität bietet, um Lastspitzen aus Onlineverfahren abzufedern.

3.1.7.4 Liste der nichtfunktionalen Anforderungen

Tabelle 28: Registerdatennavigation - Nichtfunktionale Anforderungen

ID	Kriterium	Anforderung	Prüfkriterium
Leistungseffizienz			
NFA_L001	Zeitverhalten	Im Gesamtverfahren eines Nachweisabrufes muss die Antwort der RDN so schnell durchgeführt werden, dass die Nutzerfreundlichkeit des	Architekturreview

ID	Kriterium	Anforderung	Prüfkriterium
		Gesamtablaufs aufrechterhalten wird. Das genaue Zeitverhalten ist bei Tests in Pilotverfahren und unter Berücksichtigung des Zusammenspiels aller eingesetzten Komponenten zu definieren.	
NFA_L002	Kapazität	**Im regulären Wirkbetrieb muss eine hohe Anzahl an Anfragen pro Sekunde verarbeitet werden.** Eine Abschätzung ist zum aktuellen Zeitpunkt nicht möglich. Daher muss die RDN einen sukzessiven Ausbau der Kapazität ermöglichen.	Erfolgreiche Durchführung entsprechender Ende-zu-Ende Tests auf einer produktionsnahen Umgebung an allen externen Schnittstellen.
NFA_L003	Skalierbarkeit	Das System muss so ausgelegt werden, dass perspektivisch bei Lastspitzen eine automatische Skalierung erfolgen kann. **Diese Anforderung ist bei jeder Ausbaustufe, in der weitere Verfahren angebunden werden, zu berücksichtigen.**	Architekturreview
Zuverlässigkeit			
NFA_Z001	Verfügbarkeit	Vorläufige Einschätzung: Die Registerdatennavigation muss eine **hohe** Verfügbarkeit erreichen und perspektivisch zu 99,9% verfügbar sein.	Bewertung durch ein Architekturreview Messungen im Produktivbetrieb
NFA_Z002	Nutzungszeiten	Die RDN muss 24/7 nutzbar sein.	

ID	Kriterium	Anforderung	Prüfkriterium
NFA_Z003	Reifegrad	Die Lösung verwendet ausgereifte Authentifizierungsverfahren wieder, die im NOOTS und EU-OOTS verwendet werden.	Bewertung durch ein Architekturreview
NFA_Z003	Fehlertoleranz	Die Registerdatennavigation muss Mechanismen zur Wiederherstellung nach vorübergehenden Übertragungsausfällen sicherstellen.	
Sicherheit			
NFA_S001	Integrität	Vorläufige Einschätzung: Es muss eine **hohe** Integrität (gemäß Schutzbedarf) gewährleistet werden.	Bewertung durch ein Sicherheitsaudit
NFA_S002	Nachweisbarkeit	Die RDN muss alle Änderungen im Rahmen der Pflege revisionssicher protokollieren.	Bewertung durch ein Architekturreview Erfolgreiche Durchführung eines funktionalen Tests.
NFA_S003	Authentizität	Die Authentizität der Nutzenden muss in allen Fällen sichergestellt werden.	Bewertung durch ein Architekturreview Bewertung durch ein Sicherheitsaudit
NFA_S004	Vertraulichkeit	Vorläufige Einschätzung: Die Vertraulichkeit wird als **normal** eingeordnet. Alle Nutzenden dürfen nur die Daten sehen, für die sie ermächtigt wurden (eine	Bewertung durch ein Architekturreview Bewertung durch ein Sicherheitsaudit

ID	Kriterium	Anforderung	Prüfkriterium
		rechtliche Grundlage zur Einsicht der Daten besteht). Allen Nutzenden werden nur die Funktionen angeboten, die sie auch tatsächlich nutzen dürfen.	
NFA_S005	Rollen und Berechtigungen	Die RDN muss über ein Rollen- und Rechtesystem verfügen, über das ihre Dienste gemäß der dafür noch zu identifizierenden Schutzziele vor unberechtigtem Zugriff geschützt werden.	Bewertung durch ein Architekturreview Bewertung durch ein Sicherheitsaudit
Kompatibilität			
NFA_K001	Interoperabilität	Die Abfragedienste der RDN müssen aus dem NdB, dem NdB-VN und dem Internet erreichbar sein.	Bewertung durch ein Architekturreview
NFA_K002	Interoperabilität	Die Dienste der RDN sollen auf einfache Nutzbarkeit ausgelegt werden und auf gängigen Marktstandards aufsetzen.	Bewertung durch ein Architekturreview

3.1.8 Ausblick & Weiterführende Aspekte

3.1.8.1 Offene Punkte

Tabelle 29: Offene Punkte relevant für die Konzeption der Registerdatennavigation

ID	Offene Punkte
OP-01	Bei mehrstufigen Zuständigkeitslogiken ist zu prüfen, ob der RDN-Mechanismus tragfähig ist.

ID	Offene Punkte
OP-02	Die nichtfunktionalen Anforderungen sind anzupassen, sobald nichtfunktionalen Anforderungen auf Ebene der Gesamtarchitektur spezifiziert werden.

3.1.8.2 IT-PLR Entscheidungsvorlage Registerdatennavigation 2022-22 Juni 2022

Beschlussvorschlag des Einreichenden (Kompetenzteam / Tandem):

1. Der Lenkungskreis Registermodernisierung schlägt dem IT-Planungsrat vor, die Förderale IT-Kooperation (FITKO) mit der Umsetzung der Komponente Registerdatennavigation als zentralen Routing-Dienst (Routing As a Service) auf Grundlage des Deutschen Verwaltungsdienste Verzeichnis (DVDV) unter Wiederverwendung von Lösungsansätzen aus FIT-Connect zu beauftragen.
2. Der Lenkungskreis Registermodernisierung beauftragt das Kompetenzteam Architektur mit der Formulierung eines Projektauftrags, aus dem Zielsetzung und Rahmenbedingungen zur Umsetzung der Komponente Registerdatennavigation hervorgehen.

Sachverhalt: (kurze Darstellung des Problems)

Ziel dieser Beschlussvorlage ist es, eine Entscheidung zum Funktionsumfang und der technischen Realisierung der zentralen Komponente „Registerdatennavigation“ aus dem Zielbild des IT-Planungsrats zu unterstützen.

Mit Hilfe der Registerdatennavigation ermitteln abrufenden Stellen, von welcher konkreten Behörde sie einen Nachweis abrufen können und welche technischen Verbindungsparameter sie dazu benötigen. Diese Aufgabe zerfällt in zwei Schritte:

1. Ermittlung der originär für den Nachweis zuständigen Behördeninstanz anhand fachlicher, regionaler und weiterer **Zuständigkeiten**
2. Ermittlung von dieser Behördeninstanz bereitgestellten **technischen Dienstes**, über den der Nachweis abgerufen werden kann, sowie der zu dessen Nutzung erforderlichen technischen Parameter.

Das KT Architektur hat in der Verwaltung etablierte Lösungen für diese Aufgabenstellung untersucht und auf ihre Eignung für die Registermodernisierung geprüft:

Das DVDV ist durch den IT-PLR bereits als zentrales Dienste Verzeichnis der Verwaltung positioniert und in Teilen der Verwaltung etabliert. Für die Aufgabe als Dienste Verzeichnis wird es als geeignet erachtet. Derzeit sind bereits über 40.000 Stellen dort erfasst. Eine explizite Abbildung von Zuständigkeiten ist im DVDV nicht vorgesehen. Die in Teilen der Innenverwaltung eingesetzte Abbildung von Zuständigkeiten über Schlüssellogiken wird als nicht ausreichend flexibel für die Registermodernisierung angesehen.

In FIT-Connect wird ein Routing-Dienst bereitgestellt, der ähnliche Aufgabe wie die Registerdatennavigation hat. Der Routing-Dienst verwendet das DVDV als Verzeichnis der technischen Dienste, nutzt jedoch bestehenden Datenbestände von Verwaltungszuständigkeiten, die bereits im PVOG. Diese werden dabei zunächst über die Redaktionssysteme des föderalen Informationsmanagements (FIM) gepflegt und über XZuFi in PVOG eingespielt. Der Ansatz ist tragfähig, jedoch in mehrerlei Hinsicht auf den Kontext des OZG zugeschnitten. Eine Verwendung in der Registermodernisierung würde umfangreiche Neuausrichtungen mit sich bringen, bspw.:

- eine Erweiterung der Zuständigkeitslogik um eine mehrstufige Ableitung
- Aufnahme von potenziell sehr vielen Registerabrufleistungen in den Leistungskatalog (LeiKa), die dort bisher noch nicht existieren
- Erweiterung der bestehenden Systematik des Leistungskatalog (LeiKa) zur Abbildung feingranularer Nachweisabrufe
- Erweiterung der Prozessmodelle des föderalen Informationsmanagement um große Teile der Eingriffsverwaltung
- einer eingeschränkten Nutzung des Deutschen Verwaltungsdienste Verzeichnis (DVDV), da Metadaten zu Diensten und Behörden nicht mehr im DVDV gespeichert werden würden

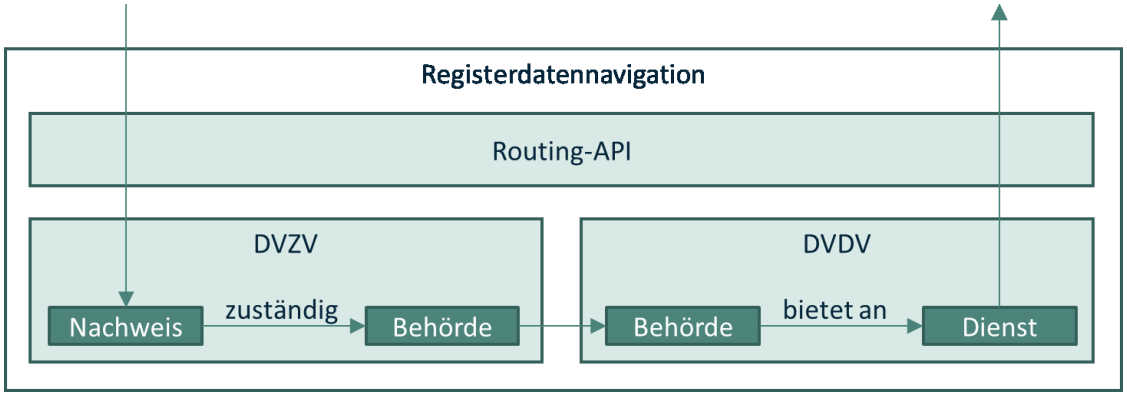


Abbildung 21: Entscheidungsvorlage Registerdatennavigation

Das KT Architektur empfiehlt daher, die Komponente Registerdatennavigation als neue Komponente nach dem Vorbild des FIT-Connect Routingdienstes aufzubauen. Die technischen Dienste werden, wie bisher im DVDV, zentral verwaltet. Für die Zuständigkeiten wird ein neues Zuständigkeitsverzeichnis aufgebaut, das jedoch Zuständigkeiten in einer verallgemeinerten Form speichert, so dass es gleichermaßen für Leistungen aus dem Leika, für Nachweise aus der Registermodernisierung und für Zuständigkeiten für beliebige Rechtegrundlagen geeignet ist. Die Pflege der Daten soll analog zum PVOG über XZuFi erfolgen. Darüber sind bspw. automatisierte Abgleiche mit dem PVOG möglich. Perspektivisch kann dieses Zuständigkeitsverzeichnis zu einem zentralen Zuständigkeitsverzeichnis der Deutschen Verwaltung (DVZV) entwickelt werden.

Der Zugriff auf die Registerdatennavigation soll über einen Routingdienst erfolgen, der die Kapselung der Datenhaltung übernimmt und eine einfach zu nutzende Schnittstelle nach außen bereitstellt. Als Vorlage des Routingdienstes wird der FIT-Connect-Ansatz mit dessen Routing-API empfohlen, eine Wiederverwendung bestehender Bausteine sollte durch die FITKO geprüft werden.

Mit der Umsetzung der neuen Komponente sollte die FITKO beauftragt werden. Als Produktverantwortliche des DVDV, des PVOG und FIM sowie dem Projekt FIT-Connect kann weitreichendes Know-How zu beiden Lösungen eingebracht werden und dafür Sorge tragen, dass beide Verzeichnisse DVDV und DVZV konform zu den strategischen Zielsetzungen des IT-Planungsrats in geeigneter Weise gekoppelt und die zugehörigen Pflegeprozesse entsprechend aufeinander abgestimmt werden. Zudem können Lösungsansätze und bestehende Softwarekomponenten aus FIT-Connect wiederverwendet und auf die neue Komponente übertragen werden.

Die folgenden, bisher nicht abschließend geklärten Aspekte, müssen durch die Formulierung des Projektauftrags durch das KT Architektur und nachfolgend im Rahmen der Umsetzung durch die FITKO weiterführend ausgearbeitet werden.

- Verantwortung der Erstellung, Pflege, Speicherung und Bereitstellung der Nachweistypen mit eindeutigen IDs.
- Denkbar ist die Nutzung von FIM-Datenfelder zur Abbildung der Nachweistypen, indem Dokumentensteckbriefe vom Typ "Registerantwort" angelegt werden. Dies würde auch eine Definition der Datenstruktur und Datenaustauschformate der Nachweistypen in FIM ermöglichen.
- Darstellung von Pflege- und Austauschprozessen zwischen Dienste- und Zuständigkeitsverzeichnis
- Realisierung des Anschlusses der Registerdatennavigation an die Systeme des EU-OOTS und notwendiger Pflegeprozesse.
- Prüfung, ob bestehende Zuständigkeitsinformationen in DVDV und PVOG, die bereits heute redundant vorliegen und mehrfach gepflegt werden müssen, perspektivisch im Zuständigkeitsverzeichnis konsolidiert werden sollten. Damit könnte eines zentrales Zuständigkeitsverzeichnis (DVZV) nach dem Vorbild des DVDV geschaffen werden.
- Prüfung von automatisierten Datenübernahmen / Datensynchronisationen ins DVDV, die bisher noch nicht technisch und konzeptionell umgesetzt sind, aber notwendig werden könnten.
- Zur Anbindung an das europäische EU-OOTS wird die Registerdatennavigation um zusätzliche Funktionalitäten erweitert werden müssen. Da die Entwicklung der europäischen Komponenten Data Service Directory (DSD) und Evidence Broker, die in engem Zusammenhang mit der Registerdatennavigation stehen, weiter andauert, kann eine Detaillierung dieser Funktionen erst zu einem späteren Zeitpunkt erfolgen.

Vorteile:

- Wiederverwendung der bestehenden technischen Lösung und bereits etablierter Pflegeprozesse des Deutschen Verwaltungsdiensteverzeichnis (DVDV).
- Schaffung einer wiederverwendbaren und skalierbare Lösung zur Abbildung und Ermittlung von Zuständigkeiten innerhalb der öffentlichen Verwaltung (DVZV).

- Wiederverwendung existierender Lösungsansätze aus dem Portalverbund Online Gateway (PVOG) und dem Zuständigkeitsfinder (XZuFi).

Nachteile:

- Aufbau einer weiteren Zuständigkeitsdatenbank, teilweise redundant zu PVOG & DVDV. Die Zuständigkeitsinformationen sollten perspektivisch im DVZV konsolidiert werden.

Alternativen:

- Umbau der XZuFi basierten Redaktionssysteme um einen nachweisorientierten Ansatz. Die oben genannten Anpassungserfordernisse sind detailliert zu untersuchen.
- Umsetzung der Registernavigation auf Basis eines leistungsorientierten Ansatzes mit Registerabrufleistungen, der eine 1:1 des bisherigen XZuFi Standards ermöglicht, aber eine zusätzliche Abstraktionsschicht schafft.

3.1.8.3 IT-PLR Entscheidungsvorlage Evidence Broker und Data Service Directory

Beschlussvorschlag des Einreichenden (Kompetenzteam / Tandem):

1 Der Lenkungskreis Registermodernisierung schlägt dem IT-Planungsrat vor, bei der Bereitstellung des Data Service Directory (DSD) für das technische System der EU zum Nachweisabruf nach Art. 14 SDG-VO zur Bereitstellung der Routing-Informationen zu deutschen Evidence Providern (registerführenden Stellen) auf eine nationale Implementierung des DSD zu setzen.

2 Der Lenkungskreis bittet das Kompetenzteam Architektur, bei der weiteren Konzeption der Registerdatennavigation vorzusehen, dass die Registerdatennavigation zugleich als nationale Implementierung des DSD nach den Vorgaben des technischen Systems der EU zum Nachweisabruf nach Art. 14 SDG-VO übernimmt.

3 Der Lenkungskreis Registermodernisierung schlägt dem IT-Planungsrat vor, bei der Bereitstellung des Evidence Brokers (EB) für das technische System der EU zum Nachweisabruf nach Art. 14 SDG-VO die von der Europäischen Kommission zentral bereitgestellte Lösung zu nutzen und auf eine separate nationale Implementierung zu verzichten.

Sachverhalt: (kurze Darstellung des Problems)

Für die Umsetzung von Once-Only in der EU bedarf es eines von allen Mitgliedstaaten genutzten technischen Systems (Once Only Technical System – OOTS), das von der Europäischen Kommission in Zusammenarbeit mit den Mitgliedstaaten entwickelt wird. Für dieses System sind zentrale Verzeichnisse der Nachweistypen (Evidence Broker) und der an das System angeschlossenen Register (Data Service Directory) notwendig.

Für beide Systeme ist ein hybrides Bereitstellungsmodell vorgesehen. Die Mitgliedstaaten können jeweils ihre Daten zu einem zentralen Verzeichnis der Europäischen Kommission zuliefern oder ein eigenes nationales Verzeichnis für diese Aufgaben bereitstellen.

Aufgabe des Evidence Broker ist es, zu einer abstrakten, nachzuweisenden Tatsache den richtigen Nachweistyp in einem bestimmten EU-Mitgliedstaat zu ermitteln. Damit wird das Problem adressiert, dass die meisten Nachweistypen in der EU nicht harmonisiert sind und daher verschiedene Mitgliedstaaten unterschiedliche Nachweise vorsehen können, um den gleichen Sachverhalt zu belegen.

Das Data Service Directory stellt ein Verzeichnis aller Register zur Verfügung, die an das OOTS angebunden sind, und ermöglicht es, für einen konkreten Nachweisabruf das richtige Register zu identifizieren. Es muss dafür die Zuständigkeitslogiken der jeweiligen Domäne abbilden können.

Nach Einschätzung der Kompetenzteams EU-Interoperabilität und Architektur kann im nationalen Kontext in aller Regel davon ausgegangen werden, dass ein Data Consumer beurteilen kann, welche deutschen Nachweise sie für ihren Fachprozess benötigt/akzeptieren kann. Zudem sind diese häufig einheitlich durch Bundesrecht vorgegeben. Die Funktionalität des Evidence Broker wird daher im nationalen Rahmen nicht dringend benötigt. Zudem ändert sich die Menge der über das OOTS verfügbaren Nachweistypen und deren Geltungsbereich nur selten, was eine Pflege in einem zentralen Verzeichnis der EU möglich macht. Perspektivisch könnte ein Evidence Broker auch in Deutschland interessant sein, um z.B. Änderungen an den rechtlichen Nachweisanforderungen für einzelne Verfahren dynamisch ohne Anpassung an den jeweiligen Online-Services oder Fachverfahren ausspielen zu können. Im Sinne einer Priorisierung der Umsetzungsaufwände soll dennoch zunächst die zentrale europäische Lösung genutzt werden. Dies schließt einen späteren Übergang zu einer nationalen Implementierung nicht aus.

Im Gegensatz dazu wird die Ermittlung des konkreten Registers, aus dem im Einzelfall der gesuchte Nachweis abgerufen werden kann, auch im nationalen Kontext benötigt und ist

dort als Komponente „Registerdatennavigation“ im Zielbild des IT-Planungsrats vorgesehen. Für viele existierende Informationsverbünde – insbesondere in der Eingriffsverwaltung – gibt es hierfür bereits Lösungen, in der Regel durch die Abbildung der Zuständigkeitslogik auf ein DVDV-Schlüsselkonzept. Die Registerdatennavigation soll hierfür zukünftig jedoch eine allgemeinere und dadurch zugleich für die Anbindung neuer Kommunikationspartner niedrigschwelliger Lösung bereitstellen. Die Ermittlung der zuständigen Stelle benötigt – aus der Perspektive der Registerdatennavigation wie aus der des DSD – fachspezifische Routinglogiken, die sich für jeden Nachweistyp unterscheiden und im Zeitablauf verändern können. Daher ist es vorteilhaft, wenn diese Logiken direkt national implementiert und nicht erst an die Europäische Kommission vermittelt werden müssen. Zudem benötigen das DSD und die Registerdatennavigation sehr stark überschneidende Datenbestände zu Registern und deren Zuständigkeiten. Es ist sinnvoller, diese Informationen zentral an einer Stelle vorzuhalten, statt sie redundant in einem deutschen und einem europäischen System zu pflegen.

Vorteile

- Reduktion der Umsetzungsaufwände durch Fokussierung der nationalen Implementierung ausschließlich auf die für Deutschland spezifische und auch im nationalen Kontext benötigte Funktionalität
- Schnelle und weniger fehleranfällige Umsetzung von nationalen Zuständigkeitslogiken
- Reduktion der Pflegeaufwände durch Vermeidung einer Doppelpflege von Registerinformationen in einem deutschen und einem europäischen Verzeichnis
- Arbeiten zur Umsetzung des DSD können mit denen zur Registerdatennavigation gebündelt werden und dadurch in wichtigen Bereichen bereits voranschreiten, bevor die europäischen Vorgaben final beschlossen sind.

Risiken

- Alle Planungen bauen auf dem aktuellen Verhandlungsstand des Durchführungsrechtsakts zu Art. 14 SDG-VO und der begleitenden technischen Dokumente auf, die bisher nicht in einer finalen Fassung vorliegen. Die für diese Entscheidung relevanten Aspekte sind aktuell zwischen Kommission und Mitgliedstaaten nicht mehr kontrovers und daher voraussichtlich stabil. Dennoch kann nicht ausgeschlossen werden, dass sich noch Änderungen in diesen Rahmenbedingungen ergeben. Mit Blick auf die enge Umsetzungsfrist Ende 2023 kann

die Planung der deutschen Anbindung des OOTS aber nicht erst auf einen finalen europäischen Beschluss warten.

- Die genauen Pflegeprozesse und -mechanismen für den zentralen europäischen Evidence Broker sind noch nicht abschließend definiert.
- Die zentrale europäische Instanz der Evidence Broker könnte durch die Kommission ggf. verspätet bereitgestellt werden.

Alternativen

- Nationale Umsetzung des Evidence Brokers: schafft eine zum europäischen Evidence Broker redundante Infrastruktur, für die derzeit kein Bedarf erkennbar ist
- Nutzung des zentralen europäischen Data Service Directory statt einer nationalen Implementierung: spart den Umsetzungsaufwand für eine nationale Lösung zum DSD (aber nicht für die nationale Registerdatennavigation), führt aber zu einem dauerhaften doppelten Pflegeprozess von Registerinformationen auf nationaler und europäischer Ebene
- Getrennte Umsetzung von nationalem Data Service Directory und nationaler Registerdatennavigation: führt zu zwei getrennten Systemen, die einen stark überschneidenden Datenbestand zu Registern und Zuständigkeiten benötigen, und damit voraussichtlich zu dauerhaft redundanter Datenpflege

3.1.8.4 Datenquellen für das Konzept der Registerdatennavigation

Aufbereitung von Datenquellen, die im Rahmen der Lösungskonzeption der Registerdatennavigation bewertet wurden.

Verwaltungsdaten-Informationsplattform (VIP): Die vom Statistischen Bundesamt geführte Verwaltungsdaten-Informationsplattform (VIP) bietet einen umfassenden Überblick über die in der Verwaltung gehaltenen Datenbestände. Die VIP erfasst hierbei ausschließlich Metadaten. Neben allgemeinen Informationen, etwa zur Registerführung oder technischen und rechtlichen Aspekten, liefert die Plattform detaillierte Beschreibungen zu den in den Datenbeständen erfassten Merkmalen: so z.B. "Familienname" oder "E-Mail-Adresse“.

Quelle: Destatis

Evidence Survey: Erhebung der Europäischen Kommission. Umfasst die für SDG-2 relevanten Leika-Leistungen sowie die abstrakten verfahrensbezogenen Nachweisanforderungen für 20 SDG Verfahren (Batch 1) (ausgenommen Verfahren Nr. 16 Business Procedure und Nr. 21-24 EU-Richtlinien, die erst in Batch 2 bearbeitet werden). Auch Nachweistypen, die jeweils für die einzelnen LeiKa-Leistungen relevant sind, wurden in einem ersten Schritt national bei den Bundesressorts erhoben und liegen ohne verbindliche Abstimmung vor. Für die finale Erhebung der Nachweistypen bedarf es weiterer Abstimmung mit den Vollzugsbehörden / Ländern. Zudem stehen neue Anforderungen seitens der Europäischen Kommission im Raum, die noch in der Klärung mit der Kommission sind. Seitens der Europäischen Kommission wurde noch kein Zeitplan für die Meldung konkreter Nachweistypen aus den Mitgliedstaaten formuliert.

Quelle: Auszug aus dem BMI Evidence Survey Zwischenbericht

Leistungskatalog (LeiKa): Die Abkürzung LeiKa bezeichnet den "Leistungskatalog der öffentlichen Verwaltung“. Der Leistungskatalog stellt ein einheitliches, vollständiges und umfassendes Verzeichnis der Verwaltungsleistungen über alle Verwaltungsebenen in Deutschland hinweg dar und wird ständig fortgeschrieben. Der LeiKa umfasst derzeit einen Bestand von mehr als 8.000 Einträgen im Katalog des Bausteins Leistungen (Stand: 30.06.2021). Dies beinhaltet alle drei Arten: Leistungsobjekte, Leistungsobjekte mit Verrichtungskennung sowie Leistungsobjekte mit Verrichtungskennung und Detail.

Quelle: Onlinezugangsgesetz

Deutsches Verwaltungsdienste Verzeichnis (DVDV): Das Deutsche Verwaltungsdienste Verzeichnis (DVDV) ermöglicht es E-Government-Anwendungen, deutschlandweit sicher und rechtskonform Daten auszutauschen. Das Dienste Verzeichnis ist eine föderale Anwendung des IT-Planungsrats und wurde 2007 zunächst für das elektronische Melderegister entwickelt und im Oktober 2019 von der neuen, flexibleren Version DVDV 2.0 abgelöst. Über 30.000 Fachverfahren bundesweit sind derzeit in dem Verzeichnis registriert. Für Beratung und Weiterentwicklung ist die Koordinierende Stelle DVDV im ITZBund zuständig. Das DVDV wird von Bund, Ländern und Kommunen gemeinsam bereitgestellt. Das föderale Prinzip spiegelt sich in der dezentralen Serverstruktur wider, die die Sicherheit und Verfügbarkeit des Datenaustauschs erhöht. In ihrem Kern steht der Bundesmaster, den das ITZBund betreibt. Er ist der einzige Server, an dem die für die Kommunikation relevanten Daten der angeschlossenen Behörden ergänzt und verändert werden können.

Jedes Bundesland beauftragt eigens dazu eine Pflegende Stelle. Nur berechtigte Personen können über einen modernen Web-Client auf die zentrale Datenbank zugreifen.

Quelle: ITZBund

XRepository: Mit dem XRepository steht allen E-Government-Vorhaben eine verlässliche Drehscheibe zur Bereitstellung und zum Bezug XÖV-konformer Standards und Codelisten zur Verfügung. Die Plattform wird im Auftrag des IT-Planungsrats durch die Koordinierungsstelle für IT-Standards (KoSIT) betrieben.

Quelle: XRepository

Föderales Informationsmanagement (FIM): Das Föderale Informationsmanagement (FIM) dient dazu, leicht verständliche Bürgerinformationen, einheitliche Datenfelder für Formularsysteme und standardisierte Prozessvorgaben für den Verwaltungsvollzug bereitzustellen. Ziel ist es, den Übersetzungs- und Implementierungsaufwand rechtlicher Vorgaben zu senken. Länder und Kommunen sollen - bezogen auf die redaktionelle und organisatorische Umsetzung eines Verwaltungsverfahrens - nicht mehr für sich alleine agieren müssen. Stattdessen können sie auf qualitätsgesicherte Vorarbeiten der nächsthöheren Verwaltungsebene zurückgreifen.

Quelle: FIM-Portal

Registerlandkarte: Mit der Bereitstellung der Registerübersicht für die Federführenden der Registermodernisierung wurde ein wichtiges Etappenziel in der Entwicklung der Registerlandkarte erreicht. Die Registerübersicht ist eine Access-Datenbank, die zentral fachliche, technische und rechtliche Informationen für die 51 Register nach IDNrG und den damit verbundenen Verwaltungsleistungen übersichtlich darstellt. Damit liefert sie nicht nur nachhaltig wichtige Erfahrungen für das Endprodukt Registerlandkarte; sie ist auch ein wichtiges Planungstool für die Registermodernisierung, welche nicht zuletzt die OZG-Umsetzung forciert. Die Verknüpfung von Leistungen und Registern ermöglicht eine Planung von Digitalisierungs- und Modernisierungsvorhaben.

Quelle: BVA

3.1.8.5 Alternative Lösungsansätze Registerdatennavigation

Die folgenden Lösungsansätze wurden durch das KT Architektur geprüft und für nicht ausreichend tragfähig befunden.

Eigene Routing-Datenbank: Der erste Ansatz sieht vor, alle für die Zuständigkeitsermittlung notwendigen Daten in einer einzigen Routing-Datenbank abzulegen. Innerhalb der Routing-Datenbank würden sich demnach Informationen zu Nachweistypen, den dafür zuständigen Behörden, durch dieses angebotene Diensten und deren technische Verbindungsparameter abgelegt werden. Diese Lösung hätte den Vorteil, dass auf eine verteilte Datenhaltung verzichtet werden kann, was Synchronisations- und Pflegeaufwände reduziert. Zudem könnten Zuständigkeiten einfach modelliert und Zuständigkeitslogiken ohne großen Aufwand erweitert werden. Da dieser Ansatz jedoch auf die Wiederverwendung bestehender Komponenten wie DVDV und PVOG verzichtet und einen redundanten Datenbestand aufbauen würde, wäre dieser Ansatz nicht konform zur Strategie des IT-Planungsrats.

DVDV erweitert um Routingdaten: Der zweite Ansatz sieht vor, die im DVDV geführten Einträge zu Behörden, die durch Behörden angebotenen Dienste und deren technischen Verbindungsparameter wiederzuverwenden und um Routingdaten zu erweitern, die zur Ermittlung der Zuständigkeit notwendig sind. Neben den Informationen des DVDV könnten zudem vorhandene Replikationsmechanismen und das DVDV-Pflegekonzept nachgenutzt werden. Ein weiterer Vorteil ist die einfache Modellierung von Zuständigkeiten und die aufwandsarme Erweiterbarkeit der Zuständigkeitslogik. Auch würde diese Lösung keine eigene Datenhaltung benötigen, da die Zuständigkeitsdaten im DVDV ergänzt werden würden. Dies jedoch hätte eine umfangreiche und aufwendige Erweiterung des DVDV zur Folge. Auch würde auf die Verwendung von bereits im PVOG geführten Zuständigkeitsdaten verzichtet werden, was zu einem doppelten Pflegeaufwand führt und deshalb als nicht erstrebenswert bewertet wird.

DVDV mit erweiterter Schlüssellogik: Dieser dritte Ansatz sieht vor, die im DVDV geführten Einträge zu Behörden, die durch Behörden angebotene Dienste und deren technischen Verbindungsparameter wiederzuverwenden und Zuständigkeiten über eine Erweiterung der Schlüssellogik abzubilden. Auch hier wäre der Vorteil, dass eine zentrale Datenhaltung im DVDV zum Tragen kommen würde und dass bereits etablierte Replikationsmechanismen und das DVDV-Pflegekonzept nachgenutzt werden könnten. Im Rahmen der Bewertung wurde jedoch festgestellt, dass die Erweiterung der Schlüssellogik an sich sehr aufwändig und zum Teil unzureichend ist, wenn es um die Abbildung komplexer Zuständigkeiten geht.

3.1.8.6 Alternativer Lösungsansatz API RDN Abfrage

Betrachtet, jedoch verworfen, wurde folgende Alternative der vollständigen Bündelung der beiden Prozessschritte in einer einzigen Schnittstellen-Funktion, die von allen Data Consumern zu nutzen wäre:

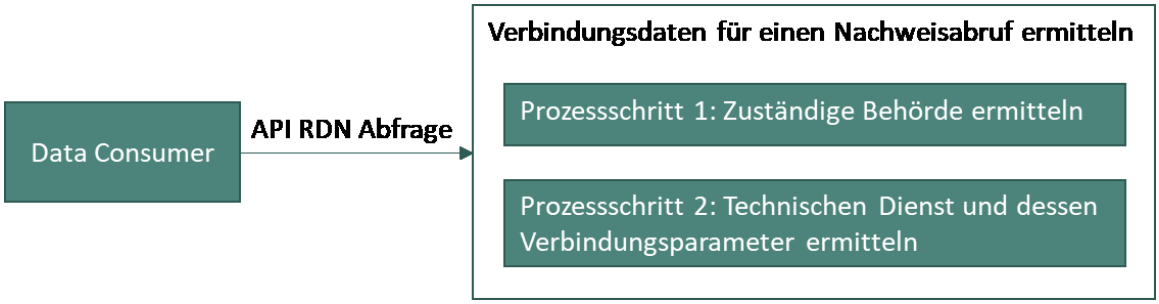


Abbildung 22: Registerdatennavigation API mit gebündelter Funktion

Der Vorteil dieser vollständigen Bündelung liegt darin, dass für das Nutzen der Registerdatennavigation ein einheitlicher Aufruf implementiert werden muss, was Aufwand auf Seiten der Data Consumer und der RDN spart. Als entscheidend nachteilig bewertet wurde aber, dass in Fällen, in denen Prozessschritt 1 aufgrund fehlender Routingparameter vom Data Consumer nicht durchlaufen werden kann, die gebündelte Funktion für diese Nutzergruppe nicht genutzt werden kann.

3.1.8.7 Optionale Konzeption der RDN als nationales Data Service Directory

Dieser Anwendungsfall beschreibt die Nutzung der Registerdatennavigation aus dem EU-Ausland über die DSD-API des EU-OOTS. Aufgrund der Annahme [ANN-002] ist dieser Use-Case für die gegenwärtige Konzeption der RDN entfallen.

Tabelle 30: Use-Case 8: Verbindungsparameter für Nachweis abrufen

Use-Case ID	**Use-Case 8 [UC_8]**
Anmerkung	Dieser Use-Case ist im SDG-Kontext relevant.
Akteure	EU Data Consumer RDN - hier: nationale Implementierung des Data Service Directory, nationales DSD
Vorbedingung/ auslösendes Ereignis	Der gesuchte Nachweistyp sowie die zur Ermittlung der Zuständigkeit notwendigen Routingparameter sind dem

Use-Case ID	**Use-Case 8 [UC_8]**
	Data Consumer vor dem Aufruf des Data Service Directory bereits bekannt.
Nachbedingung/ Ergebnisse	Der Data Consumer erhält die Beschreibung der zuständigen Behörde sowie die Verbindungsparameter des technischen Dienstes. Der Umfang der Verbindungsparameter ist der DSD-API Spezifikation zu entnehmen.
Standardablauf	1. Der Data Consumer sendet eine Anfrage an das nationale DSD und übermittelt den gesuchten Nachweistyp und notwendige Routingparameter. 2. Das nationale DSD ermittelt den technischen Dienst in der zuständigen Behörde. 3. Das nationale DSD übermittelt die Beschreibung der zuständigen Behörde sowie die Verbindungsparameter des technischen Dienstes an den Data Consumer.
Alternativer Ablauf	In Schritt 2 des Standardablaufs wurden nicht alle Informationen übermittelt, die für die Ermittlung der zuständigen Behörde benötigt werden. 2a. Das nationale DSD wirft eine Exception. Darin übermittelt es, welche Zuständigkeitsparameter für die Ermittlung der zuständigen Behörde erforderlich sind. 3a. Der Data Consumer erhebt die fehlenden Zuständigkeitsparameter. Handelt es sich um ein Onlineverfahren, fragt er die Information in der Regel bei den angemeldeten Nutzenden ab. 4a. Der Data Consumer sendet erneut die Anfrage aus Schritt 1, ergänzt um die zusätzlich erhobenen Zuständigkeitsparameter aus Schritt 3a. Weiter mit dem Standardablauf Schritt 2.
Nutzungshäufigkeit	Für jeden Nachweisabruf im SDG-Kontext notwendig.

Tabelle 31: Anforderungen an die RDN für den EU Use-Case 8

ID	Anforderung	Erläuterung	Priorität
[AFO-EU-01)	Die RDN muss eine Schnittstelle zum SDG-OOTS bereitstellen und darüber die Funktion eines Nationalen DSD im Hybridmodell gem. Kapitel 3 der TDDs bereitstellen.	Im Rahmen der Umsetzung der Registerdatennavigation muss untersucht werden, wie der Anschluss an die Systeme des EU-OOTS und notwendige Pflegeprozesse realisiert werden können.	Aktuell entfallen aufgrund von [ANN-002]
[AFO-EU-01a]	Die RDN soll für die Anbindung an das DSD gemäß AFO-EU-1 dieselbe Datenbasis nutzen, wie im nationalen Kontext gemäß AFO-API-NAT-1 und AFO-API-NAT-2, um eine doppelte Datenpflege zu vermeiden.		Aktuell entfallen aufgrund von [ANN-002]

3.1.8.8 Erläuterung zur vorläufigen Einschätzung zum Schutzbedarf

Vertraulichkeit

Wie in Kapitel 3.1.7.1 ausgeführt, ist die Erfassung und Verarbeitung von personenbezogenen Daten durch die RDN eine Ausnahme, weshalb hier ein geringes Risiko für die Verletzung der Vertraulichkeit für Personen entsteht.

Bei den Daten zur behördlichen Zuständigkeit ist davon auszugehen, dass es sich um öffentliche Datenbestände handelt, die auch in anderen Quellen nachzulesen und deshalb nicht als vertraulich einzustufen sind. Technische Verbindungsparameter sind ebenfalls unkritische Informationen innerhalb des Nutzerkreises von Behörden.

Um den Zugriff ausschließlich Behörden zu ermöglichen, muss die Authentizität der nachfragenden Stellen zweifelsfrei belegbar sein und auf ihre Zugangsberechtigung geprüft werden. Dabei kann, analog zum IAM für Behörden, eine Differenzierung der Behörden vorgenommen werden. Sicherheitsbehörden und ihre Daten haben ggf. höhere

Anforderungen an die Vertraulichkeit, die in der Feinkonzeption berücksichtigt werden müssen; in diesem Fall wäre die Einschätzung ggf. anzupassen.

Einschätzung zu Vertraulichkeit: Normal

Integrität

Angriffsszenario 1: Korruption der RDN-Datenbestände

Ein Angreifer verschafft sich Zugang zur RDN und manipuliert dort Datenbestände, beispielsweise die Verbindungsdaten zu technischen Diensten. Auf diese Weise können Nachweisabrufe entweder nicht erfolgreich abgeschlossen oder auf unbefugte Server geleitet werden, wodurch sich zwei Betrugsmöglichkeiten ergeben:

- Möglichkeit 1: Die personenbezogenen Daten des Nachweisabrufs geraten in unbefugte Hände und geben dem Angreifer Rückschlüsse auf die Antragstellenden.
- Möglichkeit 2: Die unbefugte Stelle stellt gefälschte Nachweise aus. Damit wäre es den Antragstellenden möglich, sich auf Grundlage falscher Nachweise Leistungen zu erschleichen, was wirtschaftliche Konsequenzen für die Verwaltung hat.

Angriffsszenario 2: Abfangen und Verändern von RDN-Auskünften

Ein Angreifer fängt die Antwort der RDN an einen Data Consumer ab und manipuliert die gesendeten Informationen, z.B. zu den technischen Verbindungsdaten eines Dienstes. In der Folge wird der Nachweisabruf des Data Consumers an eine unbefugte Stelle geschickt, woraus sich die zwei unter Angriffsszenario 1 geschilderten Möglichkeiten mit ihren datenschutzrelevanten, wirtschaftlichen und vertrauenseinbüßenden Folgen ergeben.

Einschätzung zu Integrität: Hoch

Verfügbarkeit

Die RDN wird für Nachweisabrufe im Kontext von Bürgeranträgen auf Verwaltungsleistungen oder behördeninternen Verfahren eingesetzt. Ein Ausfall der RDN hätte eine Verzögerung oder einen Abbruch der Nachweis-Bereitstellung und somit der damit im Zusammenhang stehenden Antragstellungen oder Behördenprozesse zur Folge.

Zwar könnten im Notfall bei längerem Ausfall alternative Papier-gebundene Wege der Nachweisübermittlung genutzt werden, dies würde aber bei den Nutzenden zu Vertrauensverlust und Frustration mit dem neuen System führen und ist daher soweit es geht zu vermeiden.

Sollten Sicherheitsbehörden die Infrastruktur der Registermodernisierung nutzen wollen und eigene, strengere Anforderungen an die Verfügbarkeit der RDN-Dienste stellen, wäre die hier gefasste Einschätzung neu zu bewerten.

Einschätzung zu Verfügbarkeit: Hoch

3.2 Preview

3.2.1 Überblick

Im Rahmen eines Online-Antrags (OZG) können die Antragstellenden ihre Nachweise direkt über das NOOTS aus den entsprechenden Registern abrufen und dem Antrag beifügen. Dabei muss sichergestellt werden, dass den Antragstellenden vollständige Transparenz über sämtliche Daten hergestellt wird, die sie für die weitere Bearbeitung in der zuständigen Behörde mit dem Antrag übermitteln.

Definition
„Preview“ (Vorschaufunktion) umfasst die Darstellung der abgerufenen Nachweisdaten gegenüber den Antragstellenden und die Absicherung (Anfrage) des Wunsches der Antragstellenden, diese Nachweisdaten der zuständigen Sachbearbeitung bereitzustellen.

3.2.2 Annahmen & Rahmenbedingungen

Eine Zustimmung des Antragsstellers bzgl. der Verwendung der Nachweisdaten ist erforderlich: Es muss sichergestellt werden, dass die Nachweisdaten der Antragstellenden erst durch die zuständige Fachbehörde verwendet werden können, nachdem die Antragstellenden der Verwendung zugestimmt haben.

Preview der Nachweisdaten ist notwendig: Stand heute gibt es keine gesetzlichen Anforderungen, die erfordern, dass den Antragstellenden die abgerufenen Nachweisdaten angezeigt werden. Allerdings sind derzeit viele Beteiligte im Kontext der Registermodernisierung der Auffassung, dass eine Preview durchgeführt werden sollte. Das vorliegende Preview-Konzept greift diese Auffassung auf. Bei Bedarf sind daher u. U. Gesetzesänderungen oder Rechtsprechung notwendig. Weiterhin können Änderungen der gesetzlichen Anforderungen dazu führen, dass das hier vorliegende Konzept angepasst werden muss. Bei Gesetzesänderungen muss dafür gesorgt werden, dass Gesetze ausschließlich umsetzungsneutrale „Anforderungen“ enthalten.

Preview nur bei Online-Antragsverfahren: Entsprechend der Konzeption der High-Level-Architecture wird eine Preview-Funktion nur bei Online-Antragsverfahren für Bürgerinnen und Bürger und für Unternehmen angeboten, siehe Kapitel 1.4.2.1 und 1.4.2.2.

Keine Preview bei behördeninitiierten Nachweisabrufen: Für einen behördeninitiierten Abruf von Nachweisen, d. h. der nicht durch Bürgerinnen und Bürger oder Unternehmen initiiert wird, ist keine Preview durch Antragstellende notwendig bzw. möglich, siehe auch

High-Level-Architecture Kapitel 1.4.2.3. Der „Sonderfall“, dass eine zuständige Behörde selbst in ihrer Web-Software (Portal / Online-Dienst) die Daten von einer Behörde (Data Provider) abruft, ist eine Ausnahme und für das NOOTS-Konzept nicht relevant und muss ggf. gesondert betrachtet werden.

Eine Protokollierung der Zustimmung der Nutzenden ist erforderlich: Es gibt Stand heute keine eindeutigen Anforderungen bzgl. der Protokollierung der Zustimmung der Nutzenden. Protokollierung / Nachweisbarkeit muss prinzipiell gegenüber dem Datenschutz abgewogen werden. Es wird also davon ausgegangen, dass eine Protokollierung (wie etwa in einem Laufzettel) stattfinden muss. In der derzeitigen Arbeitsfassung werden die Kriterien wie „Notwendigkeit“ und „Datensparsamkeit“ berücksichtigt.

Für Nachweisabrufe im EU-Rahmen (siehe Artikel 14 der SDG Verordnung 2018/1724) basiert dieses Kapitel (Preview) auf der Konzeption der Intermediären Plattform, siehe Kapitel 3.9. Bei Änderungen der Konzeption der Intermediären Plattform können sich auch Änderungsbedarfe für die nationale Umsetzung der Preview ergeben.

3.2.3 Fachliches Konzept

Das fachliche Konzept umfasst Anwendungsfälle und Anforderungen an die Preview.

3.2.3.1 Anwendungsfälle

Die Anwendungsfälle (Use-Cases) für die Preview im nationalen Kontext ist in den Tabellen unten aufgeführt.

Tabelle 32: Anwendungsfall (Use-Case) UC-PREVIEW-01

Use-Case ID	Use-Case Preview 1 (UC-PREVIEW-01)
Anmerkung	Dieser Use-Case ist im nationalen Kontext relevant.
Akteure	Antragstellende
Vorbedingung / auslösendes Ereignis	Betrachtet wird der Fall eines Online-Antragsverfahrens, der z. B. als zentral betriebener „Einer für Alle“ (EfA)-Online-Dienst für verschiedene Behörden Anträge entgegennimmt. Für den Antrag sind Nachweise aus Registern notwendig.

Use-Case ID	Use-Case Preview 1 (UC-PREVIEW-01)
Nachbedingung / Ergebnisse	Die Antragstellenden haben die bemi OOTS abgerufenen Nachweise gesehen und entschieden, welche davon übermittelt werden dürfen.
Standardablauf	1. Die Antragstellenden öffnen den Antrag im (EfA)-Online-Antragsverfahren. 2. Sie müssen sich für den Antrag authentifizieren. Das notwendige Vertrauensniveau hängt vom Antrag ab. 3. Die Antragstellenden müssen ggf. weitere Informationen eingeben, so dass das Online-Antragsverfahren ermitteln kann, welche Nachweise für diesen Antrag notwendig sind bzw. aus welchen Registern die Nachweise abgerufen werden müssen. 4. Den Antragstellenden wird dargestellt, welche Nachweise für diesen Antrag notwendig sind. 5. Die Antragstellenden können im Online-Antragsverfahren entscheiden, ob die Nachweise entsprechen dem Once-Only-Prinzip direkt aus den Registern abgefragt werden sollen („User Choice“). Wenn die Antragsstellenden sich nicht für einen Once-Only-Nachweisabruf entscheiden, sollen sie stattdessen die Möglichkeit bekommen, Nachweise hochzuladen. 6. Wenn die Antragsstellenden sich für einen Once-Only-Nachweisabruf entscheiden, fragt der Online-Dienst über das NOOTS den / die Nachweise von der zuständigen Behörde ab. 7. Das Online-Antragsverfahren agiert als „nachweisabrufende Stelle“ und fügt die Nachweisdaten dem Antrag hinzu. 8. Bevor die Antragstellenden den Antrag an die "für die Entscheidung zuständige Behörde" übermitteln, haben sie die Möglichkeit, sämtliche Daten aus den Nachweisen zu prüfen und sich für die Übermittlung zu entscheiden. Dabei wird nicht genau vorgegeben, an welcher Stelle im Antragsprozess sir die Nachweisdaten einsehen können. So ist z. B. eine Preview bereits während des Schrittes 7 möglich. Die Antragsstellenden können, sofern sie es wünschen, auf eine Preview der Nachweisdaten verzichten und dennoch einer Datenübermittlung zustimmen.

Tabelle 33: Anwendungsfall (Use-Case) UC2-PREVIEW-02

Use-Case ID	Use-Case Preview 2 (UC2-PREVIEW-02)
Anmerkung	Dieser Use-Case ist im EU / SDG Kontext relevant.
Akteure	Antragstellende
Vorbedingung / auslösendes Ereignis	Betrachtet wird der Fall eines Online-Antragsverfahrens eines EU-Mitgliedstaats. Für den Antrag sind Nachweise aus deutschen Registern notwendig.
Nachbedingung / Ergebnisse	Die Antragstellenden haben die bei OOTS abgerufenen Nachweise gesehen und sich für eine Verwendung im Antrag entschieden.
Standardablauf	1. Die Antragstellenden öffnen den Antrag in einem Online-Antragsverfahren eines anderen EU-Mitgliedsstaats. 2. Sie müssen sich ggf. für den Antrag authentifizieren. 3. Dem Antragstellenden wird dargestellt, welche Nachweise („Evidences“) für diesen Antrag notwendig sind. (EU-Begriff: das Online-Antragsverfahren der EU agiert als „Evidence Requester“ gegenüber den deutschen Registern) 4. Die Antragstellenden können im Online-Antragsverfahren entscheiden, ob die Nachweise entsprechend dem Once-Only-Prinzip direkt aus den deutschen Registern abgefragt werden sollen („Explicit Request“). 5. Wenn die Antragstellenden sich für einen Once-Only-Nachweisabruf entscheiden, ermittelt der Evidence Requester über das Data Service Directory (DSD) die entsprechende deutsche Intermediäre-Plattform-Instanz und initiiert den Datenabruf über diese Intermediäre Plattform. (Der Prozess hierzu wird im Kapitel „Intermediäre Plattformen“ im Detail dargestellt, siehe Kapitel 3.9). 6. Die Intermediäre-Plattform agiert im EU-Kontext als Evidence Provider und im NOOTS-Kontext als „nachweisabrufende Stelle“ und fragt die Nachweise aus dem entsprechenden Register ab. 7. Bevor die Daten an den Online-Dienst des anderen EU-Landes übergeben werden, werden die Antragstellenden auf die Deutsche Instanz der Intermediären Plattform

Use-Case ID	Use-Case Preview 2 (UC2-PREVIEW-02)
	weitergeleitet. Dort werden ihnen die Daten aus dem Nachweis dargestellt. 8. Sie haben die Möglichkeit sämtliche Daten aus den Nachweisen zu prüfen und sich für die Übermittlung zu entscheiden.

3.2.3.2 Anforderungen

Die Anforderungen an die Preview sind in der Tabelle unten aufgeführt.

Tabelle 34: Übersicht der Anforderungen

ID	Anforderung	Use-Case
PREV-UI-01	Die Antragstellenden MÜSSEN entscheiden, ob sie die Daten direkt aus einem Register über das NOOTS abrufen möchten, bevor der Nachweis abgerufen wird.	UC-PREVIEW-01
PREV-UI-02	Den Antragstellenden MÜSSEN sämtliche Daten aus dem abgerufenen Nachweis angezeigt werden, die dem Antrag als Anlage beigefügt werden sollen.	UC-PREVIEW-01, UC-PREVIEW-02
PREV-UI-03	Den Antragstellenden SOLLEN NICHT sämtliche Daten aus dem abgerufenen Nachweis angezeigt werden, die nicht mit dem Antrag weitergeleitet werden. (Dies betrifft Informationen aus dem Nachweis, die ggf. nicht für den Antrag relevant sind. Entscheidend ist hier, ob diese Daten an die zuständige Behörde übermittelt werden - siehe PREV-UI-02)	UC-PREVIEW-01, UC-PREVIEW-02
PREV-UI-04	Die Anzeige der Nachweisdaten KANN direkt nach dem Nachweisabruf oder KANN auf der finalen Bestätigungsseite erfolgen. (Ziel ist hierbei, die Darstellung sinnhaft für den Antragsprozess zu gestalten und hier keine Vorgabe zu machen. Es kann unterschiedliche Anforderungen bzgl. Usability geben. Dies ist abhängig davon, wie die Nachweisdaten im Formular oder wie viele Nachweise im Antrag verwendet werden bzw. ob die notwendigen Nachweise sich entsprechend den Eingaben verändern.)	UC-PREVIEW-01

ID	Anforderung	Use-Case
PREV-UI-05	Die Antragstellenden MÜSSEN entscheiden („User-Choice“), ob sie die Nachweisdaten dem Antrag beifügen möchte, bevor sie an die über den Antrag entscheidende Stelle weitergeleitet werden.	UC-PREVIEW-01, UC-PREVIEW-02
PREV-PROT-01	Die Entscheidung der Antragstellenden („User-Choice“, siehe (Anforderung PREV-UI-05) KANN vom Online-Dienst (bzw. der Intermediären Plattform) protokolliert werden – z. B. in einem „Laufzettel“.	UC-PREVIEW-01, UC-PREVIEW-02
PREV-PROT-02	Das Online-Antragsverfahren MUSS den Antragsstellenden die Möglichkeit anbieten, auf eine Preview zu verzichten und dennoch zustimmen, dass die Nachweisdaten den Antragsdaten beigefügt werden.	UC-PREVIEW-01, UC-PREVIEW-02
PREV-USAB-01	Den Antragsstellenden MÜSSEN Nachweise in einer für Menschen verständlich aufbereiteten Darstellung präsentiert werden.	UC-Preview-01, UC-Preview-02
PREV-USAB-02	Das Online-Antragsverfahren MUSS so gestaltet werden, sodass die Antragsstellenden die Preview im Antragsablauf zu einem sinnvollen und nachvollziehbaren Zeitpunkt angezeigt bekommen können.	UC-Preview-01

3.2.4 Facharchitektur

Die Beschreibung der Facharchitektur erfolgt getrennt für nationale Online-Antragsverfahren (entsprechend dem Anwendungsfall „UC-PREVIEW-01“) und für den Nachweisabruf aus einem anderen Land (entsprechend dem Anwendungsfall „UC-PREVIEW-02“).

3.2.4.1 Facharchitektur "nationales Online-Antragsverfahren"

Für den Fall eines nationalen Online-Antragsverfahrens wird die Preview der Nachweise durch das Online-Antragsverfahren (Data Consumer) durchgeführt, siehe Abbildung 23 unten.

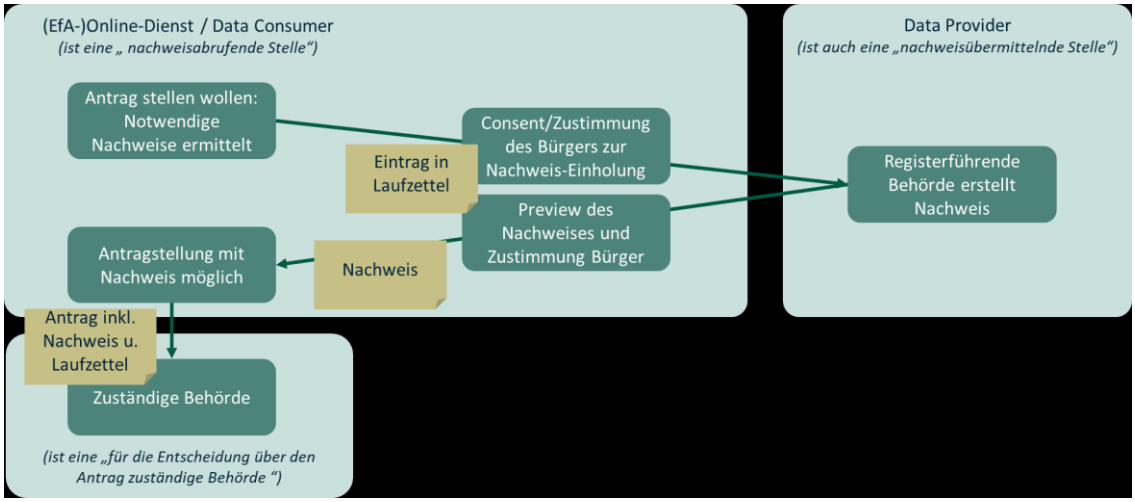


Abbildung 23: Überblick über den fachlichen Ablauf bei nationalen Online-Antragsverfahren

Vorteile:

- Der Online-Dienst (Online-Antragsverfahren) kennt die Syntax und Semantik der Nachweisdaten und kann daher auch die Darstellung entsprechend dem Antragsprozess einfach durchführen.
- Der Online-Dienst kann flexibel die Anzeige der Nachweise nach Abruf oder am Ende vor dem Versenden des Antrags (inkl. Nachweise) anzeigen und hierbei den Prozess auf Usability optimieren.
- Bürgerinnen und Bürger werden nicht zwischen verschiedenen Web-Anwendungen (Online-Dienst und einer ggf. separaten Preview-Komponente) weitergeleitet, wodurch die Fehleranfälligkeit reduziert und die Usability verbessert wird.
- Der Aufwand wird damit für die Umsetzung der Registermodernisierung in den Registern reduziert.

Verworfene Ideen bzw. Lösungsansätze:

- Die Umsetzung der Preview durch den Data Provider würde bedeuten, dass sämtliche Register in Deutschland eine Schnittstelle für die Preview implementieren müssten, die als Benutzerinterface aus dem Internet erreichbar sein müsste. Dies ist aus praktischen, organisatorischen und sicherheitstechnischen Gründen nicht umsetzbar bzw. wäre deutlich aufwändiger. Des Weiteren würde die Nutzerfreundlichkeit unter einer solchen Lösung leiden, da die Antragstellenden vom Online-Dienst auf eine weitere Seite vom Register für die Preview weitergeleitet werden müssten.

- Eine Umsetzung der Preview durch einen zentralen „Software-As-A-Service“ ist durch die datenschutzrechtlichen Regelungen nicht möglich, da diese die Trennung zwischen den Verwaltungsbereichen[1] aufbrechen würde und den Datenschutz der Antragstellenden gefährden.

3.2.4.2 Facharchitektur "Nachweisabruf aus einem anderem EU-Land"

Auf EU-OOTS findet die Preview auf Seiten des Evidence-Providers statt (siehe Abbildung 24). Hier wird die Preview durch die Intermediäre Plattform realisiert. Aus Sicht des Registers ist es damit "transparent", ob ein Nachweisabruf aus Deutschland oder der EU erfolgt, d. h. der Ablauf ist identisch.

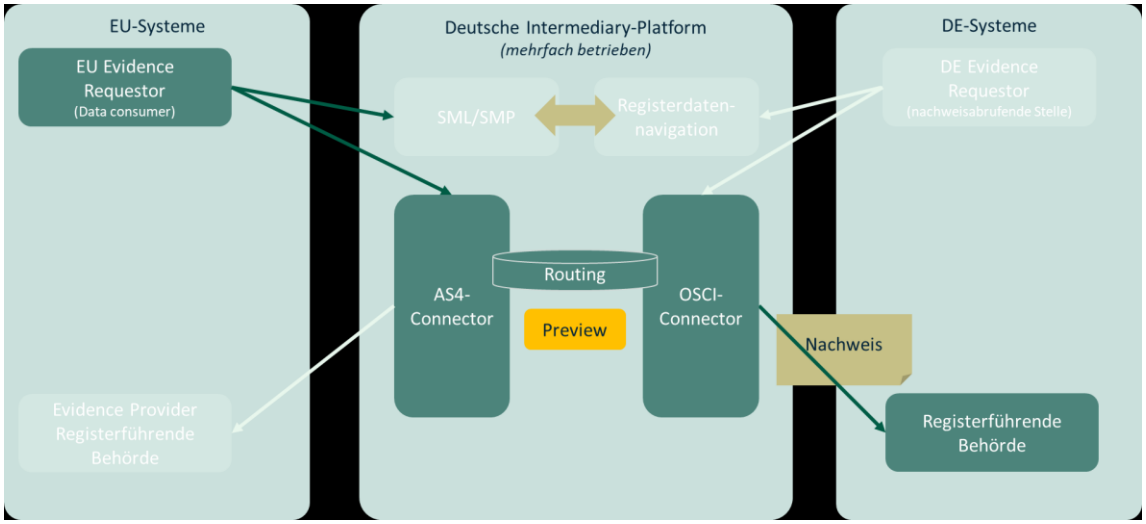


Abbildung 24: Überblick über den Nachweisabruf aus einem anderem EU-Land

Da die Intermediäre Plattform generisch eine Preview der Daten umsetzt, ergeben sich verschiedene Varianten der Realisierung. Dies muss im Weiteren noch analysiert und gegenübergestellt werden.

Variante 1: Preview-PDF vom Register mitgeliefert

- Die Registerführende Behörde liefert immer eine PDF-Datei mit menschenlesbaren Daten. Diese PDF-Datei kann zur Preview verwendet werden.

[1] Für Anfragen an personenbezogene Registern werden mit aller Voraussicht auch für Anfragen aus EU-Staaten die Identifikationsnummer als Identifikator eingesetzt. Gemäß §7 Absatz 2 IDNrG muss eine fachliche Trennung in mindestens sechs Verwaltungsbereiche erfolgen.

- Da im EU-Kontext immer PDF-Dateien übermittelt werden, ist diese Lösung für den EU-Kontext kein Mehraufwand.

Variante 2: Strukturierte Daten und Darstellungsregeln vom Register geliefert

- Das Register liefert strukturierte Daten für den Nachweis.
- Des Weiteren liefert das Register Regeln für die Darstellung der Preview - z. B. durch eine XSLT-Datei:
    - Diese Datei könnte direkt mit dem Nachweis geliefert werden oder vorab in der Intermediären Plattform hinterlegt werden
    - Für andere technische Formate (z. B. JSON) müssten andere Lösungen gefunden werden, da XSLT-Format nur für XML-Daten einsetzbar ist.

Variante 3: Strukturierte Daten und Darstellungs-Hinweise im xDSC Format

- Register, die unter das IDNrG fallen, müssen die Schnittstelle für das Datenschutzcockpit implementieren.
- Über diese Schnittstelle / Datenformat können Daten mit Label und Inhalt beschrieben und auch Gruppierungen und damit Bäume / Wiederholungen realisiert werden.
- Daher ist zu prüfen, ob das Register neben den strukturierten Daten auch einen xDSC-Datensatz für die Anzeige der Daten in der Intermediären Plattform mitliefern könnte.

3.2.5 Technisches Konzept

Für den nationalen Teil der Preview verantwortet der Data Consumer (d. h. das Online-Antragsverfahren). Im EU-Kontext erfolgt die Preview durch die Intermediäre Plattformen.

3.2.6 Ausblick & Weiterführende Aspekte

Das vorliegende Konzept wurde bereits mit Vertretern aus dem Kompetenzteam Recht und Datenschutz abgestimmt. Weitere Abstimmungen sind notwendig, um die Vorgaben für die Preview abzustimmen.

Im EU-Kontext sind weitere Abstimmungen notwendig, um eine Variante zur Realisierung einer Preview zu bewerten und auszuwählen, siehe Kapitel 3.2.4.2.

Weiterhin sind die Anforderungen an Protokollierung der Zustimmung eines Nachweisabrufes zu konkretisieren und mit Vertretern aus dem Kompetenzteam-Recht und Datenschutz abzustimmen.

3.3 IAM für Behörden

3.3.1 Überblick

Ein Identity und Access Management (IAM) stellt sicher, dass nur berechtigte Personen oder Systeme Zugriff auf andere Systeme erhalten können. Im Kontext der Registermodernisierung wird der Zugriff auf die Register und auf die Komponenten des NOOTS betrachtet.

Begriffsdefinition – Das IAM für Behörden:

- ermöglicht die sichere Authentifizierung von berechtigten öffentlichen Stellen der deutschen öffentlichen Verwaltung beim Zugriff auf Register und Komponenten der NOOTS.
- stellt die Governance für eine gesetzeskonforme Erteilung von Identitäten sowie berechtigungsrelevanten Informationen (Rollen der Identitäten) sicher.
- protokolliert und überwacht IAM-relevante Zugriffsanfragen auf Register und Komponenten der NOOTS.
- umfasst alle hierfür notwendigen technischen Lösungen und Standards sowie Rechtsgrundlagen, Organisationen und Prozesse
- besteht aus technischer Sichtweise sowohl aus zentralen IAM-Komponenten (innerhalb der NOOTS), als auch aus vorgabenkonformen dezentralen IAM-Funktionen/Komponenten/Schnittstellen der beteiligten Systeme.

3.3.1.1 Funktionsumfang und Abgrenzungen

Der Funktionsumfang kann wie folgt festgelegt und abgegrenzt werden:

Abgrenzung zu IAM für Personen (Antragsstellende und Sachbearbeitende): Im IAM für Behörden ist ausschließlich der Zugriff von Behörden (bzw. IT-Lösungen der Behörden) enthalten. Zugriffsanfragen können sowohl von der Leistungsverwaltung als auch von der Eingriffsverwaltung kommen. Bei der Leistungsverwaltung handelt es sich um Behörden, die Portale bzw. Online-Dienste innerhalb der Portale betreiben und bei der Eingriffsverwaltung um Behörden die Fachverfahren betreiben. Das IAM für Behörden umfasst nicht das IAM für die Antragsstellenden (Leistungsverwaltung) oder die

Sachbearbeitenden (Eingriffsverwaltung). In der Leistungsverwaltung sind stattdessen im Kontext des OZG Nutzerkonten (d. h. Bürgerinnen und Bürger und Organisationskonten) eingerichtet worden. In der Eingriffsverwaltung sorgen separate IAM-Lösungen in den jeweiligen Behörden dafür, dass Identität und Zugriffsrechte der Sachbearbeitenden für den Zugriff auf Fachverfahren geprüft werden.

Abgrenzung zu IDM für Personen und IDM für Unternehmen: IDM für Personen und IDM für Unternehmen haben als Aufgabe, eindeutige Identifikatoren für natürliche Personen und Unternehmen festzulegen. Das IAM für Behörden behandelt diese Komponenten wie andere NOOTS-Komponenten und sorgt dafür, dass nur berechtigte Behörden, d. h. Betreiber von Portalen und Fachverfahren, Zugriff erhalten können.

Abgrenzung zu Registerzugriffen im EU-Kontext: Die Grenze zwischen IAM für Behörden und der EU wird durch die geplante Intermediäre Plattform definiert. Es gibt folgende Varianten:

- Anfragen aus EU-Mitgliedstaaten an deutsche Register: Die Intermediäre Plattform ist aus Sicht des EU-OOTS ein Nachweislieferant. Diese prüft Anfragen aus EU-Staaten entsprechend eventuelle IAM-Vorgaben aus der EU. Diese Prüfung liegt außerhalb von IAM für Behörden. In der Binnensicht des NOOTS agiert die Intermediäre Plattform anschließend als Nachweis anfordernde Behörde (Data Consumer). Die Registeranfrage ab Intermediäre Plattform bis hin zu den Registern in Deutschland muss mit den Vorgaben aus IAM für Behörden übereinstimmen.
- Deutsche Anfragen an Register in EU-Mitgliedstaaten: Die Grenze wird ebenfalls durch die Intermediäre Plattform definiert. Der Zugriff auf die Intermediäre Plattform muss mit den Vorgaben aus IAM für Behörden konform sein. Ab Intermediäre Plattform bis hin zu den Registern der EU-Mitgliedstaaten gelten die EU-Vorgaben für das Identity und Access Management.

Umfang von Protokollierungen: Es werden ausschließlich Protokollierungen von IAM-relevanten Zugriffsanfragen vorgenommen. Weitere Protokollierungsanforderungen, die über das IAM hinaus gehen, sind nicht im Umfang von IAM für Behörden. Die Protokollierungsanforderungen sind noch zu spezifizieren. In diesem Zusammenhang muss auch festgelegt werden, wer für wen protokolliert. Haben z. B. Aufsichtsbehörden Zugriff auf die protokollierten Zugriffsanfragen?

Abstrakte Berechtigungsprüfung nicht im Umfang von IAM für Behörden: Gemäß §7 (2) IDNrG kontrollieren und protokollieren Vermittlungsstellen "abstrakt" die Berechtigungsprüfung. Diese abstrakte Berechtigungsprüfung wird im Rahmen des Konzepts für die Vermittlungsstellen festgelegt. Es wird angenommen, dass die IAM für Behörden die Berechtigungsprüfung bis hin zu den Vermittlungsstellen verantwortet. Die Vermittlungsstellen übernimmt die Berechtigungsprüfung für den Zugriff auf die Register.

3.3.2 Annahmen & Rahmenbedingungen

Für die Gestaltung der IAM für Behörden gelten folgende Annahmen und Rahmenbedingungen:

Keine Einführung von eindeutigen Identifikatoren für Behörden: Das geplante IAM für Behörden benötigt keine eindeutigen Identifikatoren, wie etwa eine Identitätsnummer für Behörden. Der Grund dafür ist, dass es nicht möglich ist, auf der Grundlage einer Behördenzugehörigkeit die zulässigen Zugriffe abzuleiten. Stattdessen sind für die Rollen innerhalb der Behörde eindeutige Identifikatoren notwendig. Anhand dieser können Berechtigungen/Berechtigungsmerkmale zugeordnet werden. Zudem kann das IAM-System im Rahmen einer Protokollierung die Protokolleinträge zu den beteiligten Rollen zuordnen.

Umgang mit kompromittierten Data Consumer ist nicht im Umfang von IAM für Behörden: Es besteht grundsätzlich das Risiko, dass ein kompromittierter Data Consumer, z. B. ein Online-Dienst innerhalb eines Portals, unberechtigte Registeranfragen stellen kann. Ein Online-Dienst, das an die Registermodernisierung angebunden ist, verfügt durch das IAM für Behörden über Zugriffsrechte an NOOTS-Komponenten und Register. Folglich können unberechtigte Anfragen nur mit weiteren zusätzlichen Maßnahmen verhindert werden. Angesichts des stetig zunehmenden Risikos von Cyberangriffen muss die öffentliche Verwaltung in der Lage sein, solche Angriffsszenarien abzuwehren. Allerdings kann diese Aufgabe nicht isoliert im Rahmen der Registermodernisierung gelöst werden, sondern muss ganzheitlich für Online-Dienste und ggf. weitere IT-Lösungen der föderalen IT-Landschaft betrachtet werden. Im Rahmen des OZG können ggf. technische Richtlinien durch das BSI entwickelt werden.

Vermittlungsstellen werden auf der Grundlage von OSCI

-**Intermediären und XTA-Servern realisiert**: Aktuell wird geprüft, ob Vermittlungsstellen auf der Grundlage der Standards OSCI und XTA umgesetzt werden können. In diesem Konzept wird davon ausgegangen, dass diese Entscheidung positiv ausfallen wird.

Bestehende und in Entwicklung befindliche Komponenten bringen bereits eigene IAM-Lösungen mit: IDM für Personen, Datenschutzcockpit, Vermittlungsstellen auf der Grundlage von OSCI/XTA planen eigene IAM-Lösungen und Funktionen zu verwenden. Bei der Planung der Umsetzung von IAM für Behörden muss diese Tatsache berücksichtigt werden.

TR-03107-1 ist für IAM für Behörden einschlägig: Die Technische Richtlinie TR-03107-1 "Vertrauensniveaus und Mechanismen" des BSI beschreibt Vertrauensniveaus für den Zugriff auf so genannte Vertrauensdienste. Vertrauensdienste bieten Funktionen an, die auf elektronischen Identitäten basieren. Diese Funktionen können die Abgabe von Willenserklärungen, Übermittlung von Dokumenten oder föderierte Identitätsverfahren umfassen. Eine Identität bezieht sich gemäß TR-03107-1 unter anderem auf natürliche und juristische Personen sowie auf Dinge, Ressourcen, Dienste und andere Objekte. Im Kontext des vorliegenden Konzepts ist die Identität eine anfragende IT-Lösung, die Zugriffe auf Register und NOOTS-Komponenten benötigt.

IAM für Behörden ist auf das Vertrauensniveau hoch ausgerichtet: Das TR-03107-1 des BSI unterscheidet zwischen dem niedrigen, mittleren und hohen Vertrauensniveau. Bei einem hohen Vertrauensniveau sind die "Schadensauswirkungen bei einer Kompromittierung beträchtlich". Dieses Vertrauensniveau entspricht in etwa dem hohen Sicherheitsniveau gemäß IT-Grundschutz [BSI100-2]. Es ist davon auszugehen, dass die Infrastruktur, Organisation, Prozesse und verwendete Identifizierungsmittel im Kontext von IAM für Behörden entsprechend dem hohen Vertrauensniveau ausgelegt werden müssen. Die entsprechenden Anforderungen sind in der technischen Richtlinie definiert.

3.3.3 Fachliches Konzept (inkl. Facharchitektur)

Das Klassendiagram in der Abbildung unten beschreibt die Beziehungen zwischen Informationsobjekten, die für das IAM relevant sind.

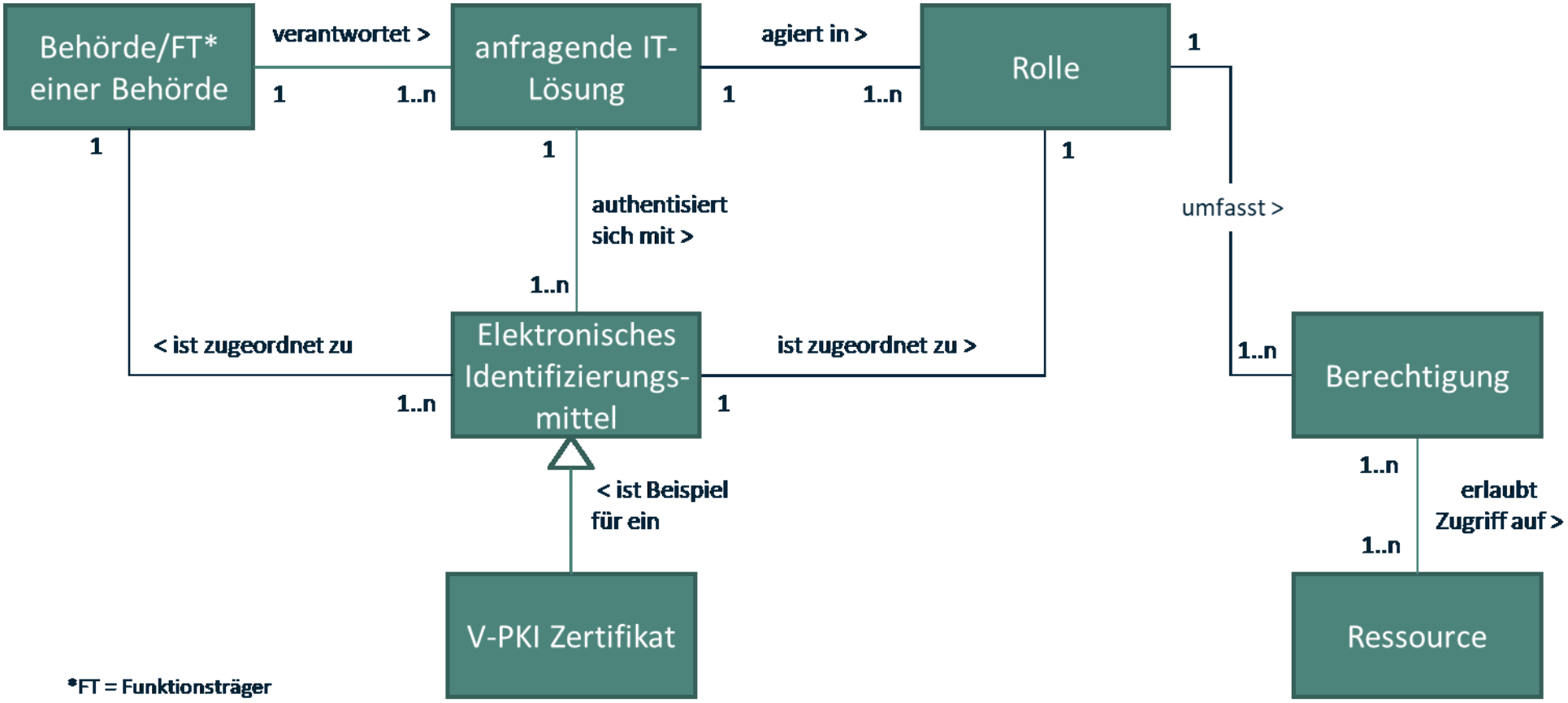


Abbildung 25: Klassendiagramm - IAM für Behörden

Die Klassen/Entitäten sind:

Behörde/Funktionsträger (FT) innerhalb einer Behörde: Eine Behörde ist eine öffentliche Stelle, die Aufgaben der öffentlichen Verwaltung wahrnimmt. Betrachtet werden sowohl Behörden der Leistungsverwaltung als auch Behörden der Eingriffsverwaltung. In einigen Fällen haben Behörden mehrere „Funktionsträger", die jeweils Aufgaben aus separaten Rechtsgrundlagen durchführen. Rechte, die sich aus den Rechtsgrundlagen ergeben, dürfen nur von den Teilen der Behörde wahrgenommen werden, die mit den entsprechenden Aufgaben vertraut sind. Ein IAM-System muss deshalb Rollen und Rechte von unterschiedlichen Funktionsträgern einer Behörde strikt voneinander trennen können.

Anfragende IT-Lösung: Unter anfragenden IT-Lösungen werden Data Consumer, Data Provider, NOOTS-Komponenten und Intermediärer Plattformen verstanden, die Zugriffe auf Funktionen und Daten bei Ressourcen (Data Provider, NOOTS-Komponenten und Intermediärer Plattform) benötigen.

Rolle: IT-Lösungen können je nach fachlichem Kontext unterschiedliche Rollen einnehmen. So können z. B. Portale der Leistungsverwaltung mehrere Rollen in Form von Kategorien von Online-Diensten enthalten, die jeweils unterschiedliche Registernachweise benötigen.

Elektronisches Identifizierungsmittel: Die elektronischen Identifizierungsmittel werden genutzt, um Behörden bzw. Funktionsträger einer Behörde zu identifizieren. Anfragende IT-Lösungen, die Teil einer Behörde bzw. eines Funktionsträgers der Behörde sind, nutzen diese Identifizierungsmittel, um sich zu authentifizieren. Es kann für eine IT-Lösung mehrere Identifizierungsmittel ausgestellt werden, wenn die anfragende IT-Lösung mehrere Rollen mit jeweils unterschiedlichen Berechtigungen wahrnimmt.

V-PKI-Zertifikat: Die V-PKI-Zertifikate sind Beispiele für die Identifizierungsmittel.

Berechtigung: Eine Rolle kann über mehrere Berechtigungen verfügen. Unter Berechtigungen werden Berechtigungsmerkmale verstanden, die die angefragten Ressourcen erhalten. Auf Grundlage der Berechtigungen bzw. Berechtigungsmerkmale einer Rolle kann die Ressource ableiten, ob die Anfrage zugelassen oder abgelehnt werden muss.

Ressource: Die Ressource enthält die Daten und Funktionen, die angefragt werden. Eine Ressource stellt somit z. B. Nachweise oder bestimmte Funktionen zur Verfügung. Zu den Ressourcen zählen die NOOTS-Komponenten und die Intermediäre Plattform. Im Rahmen des IAM für Behörden wird anhand einer Berechtigungsprüfung abgeleitet, ob die anfragenden IT-Lösungen Zugriffe auf diese Ressourcen erhalten dürfen. Die Vermittlungsstellen übernehmen gemäß §7 (2) IDNrG. die Berechtigungsprüfung für die Register, siehe auch Kapitel 3.3.2.

Das IAM für Behörden muss Anwendungsfälle im Umfeld (1) Administration/Registrierung, (2) Zugriffe auf Register und NOOTS-Komponenten und (3) Protokollierung und Monitoring unterstützen.

3.3.3.1 Anwendungsfälle im Kontext der Administration/Registrierung:

I-AR1: Identität der Behörde bzw. Funktionsträgerinnen und -träger einer Behörde festlegen: Eine Instanz prüft die Identität einer Behörde. Diese Identitätsprüfung erfolgt auf Antrag einer Behörde, die Zugriffe auf Ressourcen benötigt. Es handelt sich um eine Instanz, die von der Betriebseinheit der zentralen IAM-Lösung für Behörden getrennt ist, wie etwa eine Registrierungsstelle der V-PKI.

I-AR2: Elektronisches Identifizierungsmittel ausstellen: Nach erfolgter Prüfung der Identität werden ein oder mehrere elektronische Identifizierungsmittel für die Behörde bzw. einem Funktionsträger innerhalb der Behörde ausgestellt. Die Identifizierungsmittel sind eineindeutig einer Rolle innerhalb der Behörde bzw. einem Funktionsträger der Behörde zugeordnet.

I-AR3: Berechtigungen zu Rollen zuweisen: Zu einer Rolle werden Berechtigungen bzw. berechtigungsrelevante Merkmale zugewiesen. Diese berechtigungsrelevanten Merkmale sind einem Identifizierungsmittel zugeordnet.

I-AR4: Identifizierungsmittel sperren: Identifizierungsmittel werden gesperrt, wenn eine Behörde bzw. ein Funktionsträger innerhalb einer Behörde keinen Zugang auf Register und NOOTS-Komponenten mehr benötigt. Gleiches gilt, wenn ein Identifizierungsmittel kompromittiert wird.

3.3.3.2 Anwendungsfall beim Zugriff auf Register und NOOTS-Komponenten:

I-Z1: Zugriffsanfrage auf Register und NOOTS-Komponenten: Ein anfragendes System (Data Consumer, Data Provider, NOOTS-Komponente oder Intermediäre Plattform) benötigt Zugriff auf eine Ressource (NOOTS-Komponente, Register via Vermittlungsstellen, oder eine Intermediäre Plattform). Die Zugriffsanfrage wird auf der Grundlage von Berechtigungen bzw. Berechtigungsmerkmalen abgeleitet. Der genaue Ablauf ist abhängig von der gewählten IAM-Architektur und umfasst ein Zusammenspiel zwischen der anfragenden IT-Lösung, der zentralen IAM-Lösung der NOOTS und der angefragten Ressource. Als Ergebnis wird der Zugriff gewährt oder verweigert. Eine Prüfung der Zugriffsrechte ist in zwei Schritten geplant. Im ersten Schritt wird die IAM-Lösung der NOOTS den grundsätzlichen Zugriff gewähren oder ablehnen. Im zweiten Schritt kann die angefragte Ressource auf Grundlage der Informationen über Berechtigungen/Berechtigungsmerkmale differenzierter ermitteln, ob in dem Fall einen Zugriff gewährt werden kann oder nicht. Im Rahmen der Feinkonzeption ist festzuhalten, welche Prüfungen im ersten und im zweiten Schritt notwendig sind, um eine ausreichend sichere IAM-Lösung zu etablieren.

3.3.3.3 Anwendungsfälle im Kontext der Protokollierung und des Monitorings:

I-PM1: IAM-Aktivitäten protokollieren: Hier werden sowohl Ereignisse im Rahmen der Administration/Registrierung als auch Ereignisse beim Zugriff auf Ressourcen protokolliert. Es werden ausschließlich IAM-relevante Ereignisse protokolliert. Darüber hinaus gehende Protokollierungen, die ggf. wegen fachspezifischen gesetzlichen Grundlagen notwendig sind, liegen nicht im Umfang der Protokollierung. Bei der Protokollierung muss die anfragende IT-Lösung und verwendete Rolle eineindeutig identifiziert werden. So kann das Protokoll beispielsweise einen Verweis auf eine ID-Nummer des verwendeten Identifizierungsmittels enthalten. Als Ergebnis der Protokollierung entstehen Protokolldateien. Bestimmte Ereignisse werden zentral durch die IAM-Lösung der NOOTS protokolliert. Andere Ereignisse werden lokal durch die anfragenden IT-Lösungen und Ressourcen (Register über Vermittlungsstellen, NOOTS-Komponenten, Intermediärer Plattform) entsprechend den Vorgaben aus dem IAM für Behörden protokolliert.

I-PM2: Protokollierte IAM-Aktivitäten einsehen: Berechtigte Personen können protokollierte IAM-relevante Ereignisse einsehen und dadurch z. B. ableiten, ob bestimmte Zugriffsanfragen zugestimmt oder abgelehnt wurden.

I-PM3: IAM-Aktivitäten überwachen und analysieren: Die Log-Einträge werden überwacht und analysiert. Das Ziel ist es, die Angriffsversuche und die Sicherheitsrisiken zu erkennen.

3.3.3.4 Anforderungen (Qualitätskriterium - Funktionale Software):

Im Folgenden werden lediglich architekturrelevante Anforderungen aufgeführt. Diese Anforderungen sind zu erweitern und zu detaillieren, nachdem die grundlegende IT-Architektur für die Umsetzung von IAM für Behörden feststeht. Anforderungen werden nach dem Standard ISO 25010 (Norm für die Qualitätskriterien von Software, IT-Systemen und Software-Engineering) kategorisiert. Betrachtet wird das gesamte funktionale IAM-System, d. h. sowohl Organisation, Prozesse und Technik. Aus technischer Sicht werden sowohl IAM-Lösungen innerhalb des NOOTS als auch angebundene Komponenten betrachtet, vgl. Definition IAM für Behörden oben. Sofern nur die IAM-Lösung der NOOTS betrachtet wird, wird dies explizit in den Anforderungen erwähnt.

Die funktionalen Anforderungen an IAM für Behörden sind in der Tabelle unten aufgeführt.

Tabelle 35: Funktionale Anforderungen an IAM für Behörden

ID	Anforderung	Anwendungsfall
FIAR1	Das IAM-System MUSS fähig sein, die Identität einer Behörde/Funktionsträger innerhalb einer Behörde zu prüfen und festzustellen. (Ziel Identifizierungsmittel ausstellen).	I-AR1
FIAR2	Das IAM-System MUSS fähig sein, Identifizierungsmittel nach erfolgter Identitätsprüfung auszustellen.	I-AR2
FIAR3	Falls rechtlich erforderlich MUSS das Identifizierungsmittel auf einen Funktionsträger innerhalb der Behörde (mit separater Rechtsgrundlage) ausgestellt werden.	I-AR2
FIAR4	Das Identifizierungsmittel MUSS den Namen der Behörde und in Abhängigkeit von der Anforderung FIAR3 den Funktionsträger innerhalb der Behörde enthalten.	I-AR2

ID	Anforderung	Anwendungsfall
FIAR5	Das Identifizierungsmittel MUSS für eine spezifische Rolle innerhalb einer Behörde/Funktionsträger innerhalb einer Behörde ausgestellt sein.	I-AR2
FIAR6	Das IAM-System MUSS einem Administrator die Möglichkeit bieten, ein elektronisches Identifizierungsmittel zu einer Rolle zuzuordnen.	I-AR3
FIAR7	Das IAM-System MUSS einem Administrator die Möglichkeit bieten, eine oder mehrere Berechtigungen/Berechtigungsmerkmale einer Rolle zuzuordnen.	I-AR3
FIAR8	Das IAM-System MUSS ausgestellte Identifizierungsmittel sperren, wenn diese nicht mehr benötigt, oder kompromittiert wurden.	I-AR4
FIZ1	Das IAM-System der NOOTS MUSS fähig sein, auf der Grundlage des verwendeten Identifizierungsmittels den Zugriff auf Ressourcen zu gewähren oder abzulehnen.	I-Z1
FIZ2	Falls das Identifizierungsmittel einen Zugriff auf die Ressourcen der Registermodernisierung erlaubt, MUSS das IAM-System der NOOTS fähig sein, auf der Grundlage des verwendeten Identifizierungsmittels Information über die Rollen und die Berechtigungen/ Berechtigungsmerkmale zu ermitteln und an die angefragte Ressource zur Verfügung zu stellen.	I-Z1
FIZ3	Die Ressource MUSS fähig sein, die Information über Rollen und Berechtigen/Berechtigungsmerkmale der anfragenden IT-Lösung zu interpretieren, um daraus abzuleiten, ob der Anfrage zugestimmt oder abgelehnt werden muss.	I-Z1
FIPM1	Bei IAM-relevanten Ereignissen MUSS das IAM-System fähig sein, diese zu protokollieren und eine Protokoll-Datei zu erzeugen und fortzuschreiben.	I-PM1
FIPM2	Das IAM-System muss fähig sein, Protokolleintragungen zu Rollen innerhalb einer Behörde eindeutig zuzuordnen. (Umsetzungshinweis: Diese eindeutige Zuordnung kann	I-PM1

ID	Anforderung	Anwendungsfall
	mit Hilfe einer eindeutigen Nummer des verwendeten Identifizierungsmittels erfolgen.)	
FIPM3	Das IAM-System MUSS Administratorinnen und Administratoren sowie berechtigten Personen und Systemen lesenden Zugriff auf Eintragungen in der IAM-Protokolldatei gewähren.	I-PM2
FIPM4	Das IAM-System MUSS Administratorinnen und Administratoren sowie berechtigten Personen und Systemen Zugang zu Analysen von IAM-Ereignissen gewähren.	I-PM3

Hinweis zu FIAR4: Diese Information wird für Protokollierungszwecke benötigt.

3.3.3.5 Nichtfunktionale Anforderungen (Sonstige Qualitätskriterien entsprechend ISO 25010):

Die nichtfunktionalen Anforderungen an IAM für Behörden sind in der Tabelle unten aufgeführt.

Tabelle 36: Nichtfunktionale Anforderungen an IAM für Behörden

ID	Anforderung	Qualitätskriterium (ISO 25010)	Anwendungsfall
NIP1	Das IAM-System MUSS eine noch zu ermittelnde Zahl von Identitätsprüfungsanträge pro Zeiteinheit verarbeiten.	Performanz - Kapazitäten	V-AR1
NIP2	Das IAM-System MUSS Identitätsprüfungen innerhalb eines noch zu definierenden Zeitfensters abschließend bearbeiten.	Performanz - Zeitverhalten	V-AR1
NIP3	Das IAM-System MUSS eine noch zu ermittelnde Zahl von	Performanz - Kapazitäten	V-AR2

ID	Anforderung	Qualitätskriterium (ISO 25010)	Anwendungsfall
	Identifizierungsmitteln pro Zeiteinheit ausstellen.		
NIP4	Nach erfolgter Identitätsprüfung MUSS das IAM-System Identifizierungsmittel innerhalb eines noch zu definierenden Zeitfensters ausstellen.	Performanz - Zeitverhalten	V-AR2
NIP5	Das IAM-System der NOOTS MUSS fähig sein, eine noch zu ermittelnde Anzahl von Zugriffsanfragen von IT-Lösungen pro Zeiteinheit beantworten können.	Performanz - Kapazitäten	V-Z1
NIP6	Das IAM-System der NOOTS MUSS fähig sein Zugriffsanfragen von IT-Lösungen innerhalb einer noch zu definierenden Zeiteinheit beantworten zu können.	Performanz - Zeitverhalten	V-Z1
NIP7	Das IAM-System MUSS fähig sein eine noch zu ermittelnde Anzahl von IAM relevanten Protokollierungen pro Zeiteinheit vorzunehmen.	Performanz - Kapazitäten	V-PM1
NIP8	Das IAM-System MUSS fähig sein IAM-relevante Protokollierungen innerhalb eines noch zu definierenden Zeitfensters vorzunehmen.	Performanz - Zeitverhalten	V-PM1
NISi1	Falls das IAM-System personenbezogene Daten transportiert, MUSS das IAM-	Sicherheit - Datenschutz	Alle

ID	Anforderung	Qualitätskriterium (ISO 25010)	Anwendungsfall
	System die Daten vor dem Transport verschlüsseln.		
NISi2	Das IAM-System MUSS Informationen über Rollen und Berechtigungen/ Berechtigungsmerkmale einer anfragenden IT-Lösung so zur Verfügung stellen, damit die angefragte Ressource erkennen kann, dass diese Informationen aus dem IAM-System der NOOTS stammen. (Umsetzungshinweis: Dies könnte z. B. im Rahmen einer Versiegelung einer Nachricht erfolgen).	Sicherheit - Authentizität	V-Z1
NISi3	Ressourcen MÜSSEN gegenüber anfragenden IT-Lösungen ihre Identität nachweisen.	Sicherheit - Authentizität	V-Z1
NISi4	Das IAM-System MUSS Informationen über Rollen und Berechtigungen/ Berechtigungsmerkmale einer anfragenden IT-Lösung manipulationssicher transportieren.	Sicherheit - Manipulationssicherheit	V-Z1
NISi5	Das IAM-System des NOOTS MUSS so gestaltet sein, dass es 24x7 verfügbar ist.	Sicherheit - Verfügbarkeit	Alle
NISi6	Das IAM-System des NOOTS MUSS so gestaltet sein, dass es zu einem noch zu definierenden Prozentwert verfügbar ist.	Sicherheit - Verfügbarkeit	Alle

ID	Anforderung	Qualitätskriterium (ISO 25010)	Anwendungsfall
NISi7	Das IAM-System des NOOTS MUSS georedundant betrieben sein.	Sicherheit - Wiederherstellbarkeit	Alle
NISi8	Das IAM-System des NOOTS MUSS bei einem Ausfall innerhalb von einer noch zu definierenden Zeit wiederhergestellt werden.	Sicherheit - Wiederherstellbarkeit	Alle
NIK1	Das IAM-System des NOOTS MUSS für die Berechtigungsanfragen über Internet verfügbar sein.	Kompatibilität	Alle
NIK2	Das IAM-System des NOOTS MUSS über NDB-VN verfügbar sein.	Kompatibilität	Alle
NIK3	Das IAM-System MUSS entsprechend der TR-03107-1 des BSI "Vertrauensniveaus und Mechanismen" die Anforderungen des hohen Vertrauensniveaus erfüllen.	Kompatibilität	Alle

Hinweis zu NIK4: Admin-Oberflächen müssen nicht zwangsläufig über das Internet verfügbar sein.

3.3.4 Technisches Konzept

Das technische Konzept enthält Feststellungen zu den folgenden Themenbereichen:

- Stufen zur Umsetzung von IAM
- Technische Realisierung von IAM für Behörden
- Auswahl eines elektronischen Identifizierungsmittels

3.3.4.1 Stufen zur Umsetzung von IAM für Behörden

Es ist davon auszugehen, dass die Umsetzung einer Zielarchitektur für IAM für Behörden bis hin zur vollumfänglichen Nutzung durch alle Behörden mehr als ein Jahr dauern wird. Neben der Auswahl der Architektur sind mit Vorlaufzeiten bei der Auswahl eines geeigneten IT-Dienstleisters zu rechnen. Darüber hinaus muss sich die IAM-Lösung im Rahmen einer produktiven Pilotierung bewähren, bevor diese flächendeckend eingesetzt werden kann.

Es wird daher empfohlen, IAM für Behörden stufenweise einzuführen, siehe Abbildung unten.

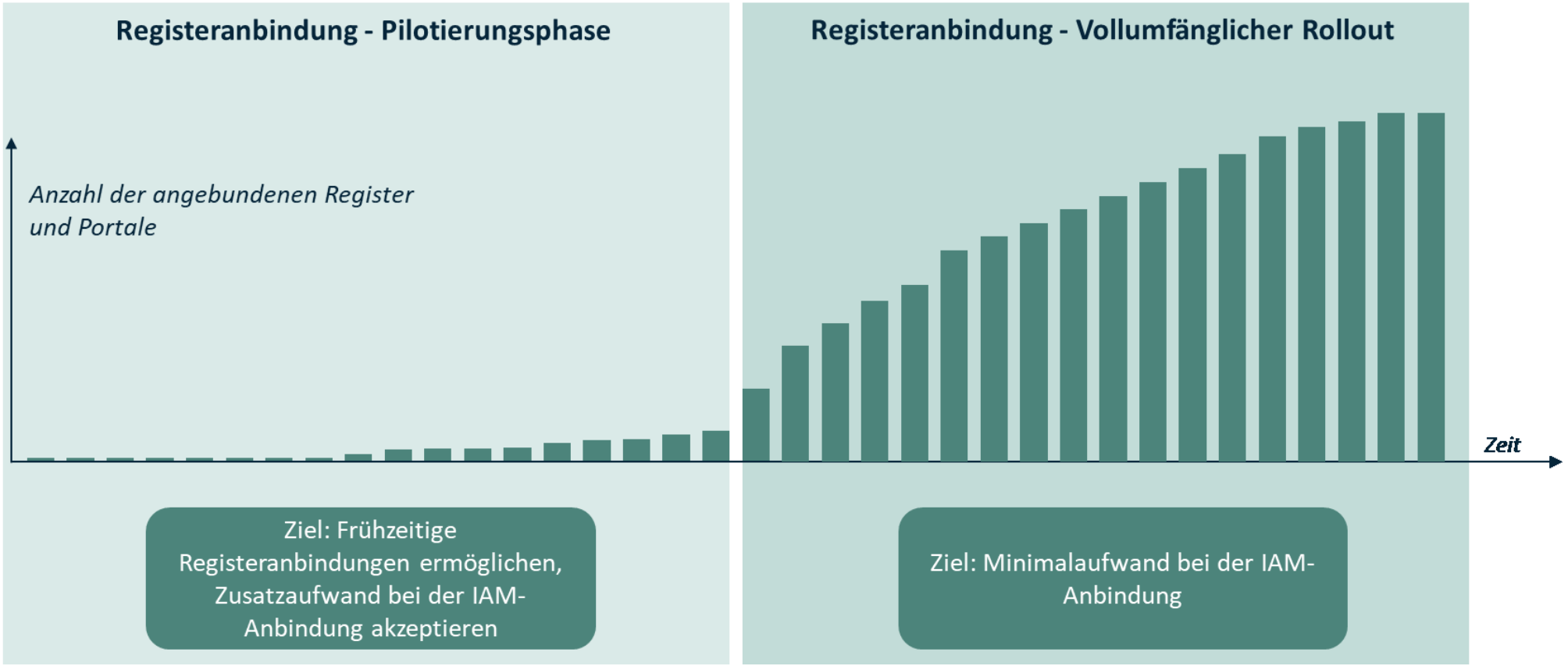


Abbildung 26: Phasen für die Umsetzung von IAM für Behörde

Während der Pilotierungsphase (d. h. der Phase mit den ersten Registeranbindungen) wird dafür gesorgt, dass aus dem IAM-Kontext keine Hürden für eine frühzeitige Pilotierung einer Registeranbindung entstehen. Somit können frühzeitig wertvolle Praxiserfahrungen bei der Registermodernisierung gewonnen werden. Die Pilotierungsbehörden müssen im Gegenzug akzeptieren, dass der Aufwand für eine IAM-Anbindung während dieser Phase höher sein wird.

Während des vollumfänglichen Rollouts der Registeranbindungen steht eine IAM-Lösung zur Verfügung, die den Aufwand für eine Registeranbindung auf ein Minimum reduziert. Das Ziel ist es, eine sichere und gleichzeitig eine möglichst einfache anbindbare IAM-Lösung anzubieten.

Die folgende Tabelle konkretisiert die Pilotierungsphasen der Registeranbindungen:

Tabelle 37: Beschreibung der Phasen für die Umsetzung von IAM für Behörden

Phase	Ziel	Lösungsansatz	Beschreibung
Pilotierung	Frühzeitige Pilotierungen von Registeranbindungen ermöglichen, Zusatzaufwand bei der IAM-Anbindung akzeptieren	Anbindung an bereits etablierten IAM-Lösungen, keine einheitliche IAM-Lösung	• Registerzugriff über Vermittlungsstellen (voraussichtlich OSCI/XTA): (1) Zertifikatsbasierter Zugriff (V-PKI) entsprechend etablierten Mechanismen, (2) Nutzung der Funktion „VerifyCategory“ in DVDV, d. h. zertifikatsbasierte und rollenbasierte Autorisierungsprüfung. • Zugriff auf IDA, Basisregister (Unternehmen), Registerdatennavigation und Intermediäre Plattform entsprechend den jeweiligen Vorgaben der einzelnen Komponenten.

Phase	Ziel	Lösungsansatz	Beschreibung
Vollumfänglicher Rollout	Minimalaufwand bei der IAM-Anbindung	• Anbindung an einheitliche und standardisierte IAM-Lösung	• Zugriff auf Data Provider, NOOTS-Komponenten und Intermediäre Plattform über eine einheitliche IAM-Lösung der Registermodernisierung.

Parallel zur Pilotierungsphase der Registeranbindungen wird somit eine einheitliche IAM-Lösung umgesetzt. Sobald diese einheitliche IT-Lösung über die erforderliche Reife verfügt, wird bei allen neuen Registeranbindungen an diese einheitliche IAM-Lösung angebunden. Alle bereits während der Pilotierungsphase etablierte IAM-Anbindungen an bestehende IAM-Lösungen werden anschließend in einer noch zu definierenden Übergangszeit auf diese einheitliche IAM-Lösung umgestellt.

3.3.4.2 Technische Realisierung von IAM für Behörden

Für die **Pilotierungsphase der Registeranbindung** erfolgt eine Anbindung an mehrere nicht einheitliche IAM-Komponenten:

- Falls die Vermittlungsstellen durch die OSCI-Intermediäre realisiert werden sollten, erfolgt ein Zugriff mit Hilfe von den V-PKI-Zertifikaten. Die Autorisierungsprüfungen werden durch, die vom DVDV bereitgestellte und vorhandene Funktion VerifyCategory unterstützt.
- Die Registeranfragen vom Datenschutzcockpit erfolgen ebenfalls über OSCI und somit ebenfalls mit Hilfe von den V-PKI-Zertifikaten und der DVDV-Funktion VerifyCategory.
- Der Zugriff auf IDA erfolgt durch die Vorgaben durch das BVA. Hier kommt eine Token basierte Authentifizierung nach OAuth Version 2 unter der Verwendung von spezieller V-PKI Zertifikaten zum Einsatz. Das BVA fungiert als eine Registrierungsstelle, d. h. es prüft die Identität der Behörden, die auf IDA zugreifen möchten, und vergibt die Zertifikate. Darüber hinaus administriert das BVA die technischen Benutzerkonten in den IAM-Systemen IDA.

- Der Zugriff auf das Basisregister Unternehmen erfolgt auf der Grundlage der dort geplanten IAM-Infrastruktur (Das Statistische Bundesamt verantwortet die Einführung des Basisregisters für Unternehmen).
- Der Zugriff auf die Intermediäre Plattform erfolgt auf der Grundlage der dort geplanten IAM-Infrastruktur.

Falls für die einzelnen Projekte, wie z. B. die Einführung des Basisregisters für Unternehmen oder die Einführung einer Intermediäre Plattform, noch keine IAM-Infrastruktur vorliegen, sollten diese Projekte prüfen, wie eine wirtschaftliche IAM-Lösung für eine Übergangszeit umgesetzt wird. In diesem Zusammenhang sollte auch geprüft werden, inwieweit die bereits in Produktion befindlichen IAM-Lösungen eingesetzt werden können.

Für den **vollumfänglichen Rollout** der Registeranbindung wird eine einheitliche IAM-Lösung eingesetzt. Die Autorisierungsprüfung erfolgt auf der Grundlage von Tokens (vgl. OAuth 2.0). Dies entspricht der "State of the Art-Umsetzung" von IAM-Lösungen heute. Eine Token basierte Autorisierung ermöglicht es, eine Autorisierung von einer Anwendung auf eine andere zu übertragen. Die angefragte Ressource kann anhand der Token Informationen entscheiden, ob ein Zugriff gewährt wird oder nicht.

Das Kernelement dieser Variante ist ein zentral betriebener Autorisierungsserver, der berechtigungsrelevante Merkmale in Form eines signierten Tokens bereitstellt. Der Ablauf ist in der Abbildung unten dargestellt.

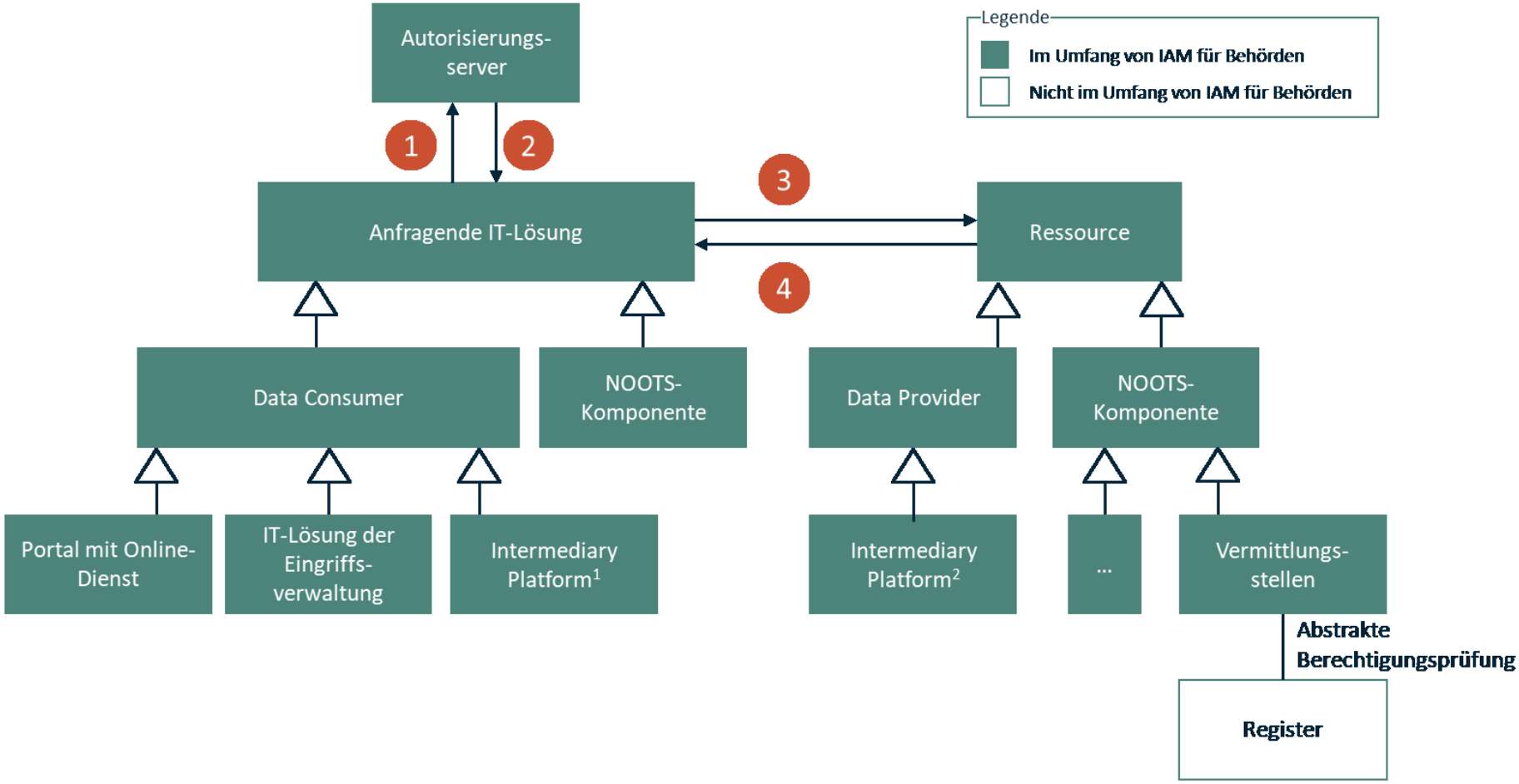


Abbildung 27: Darstellung der einheitlichen IAM-Lösung auf Token-Basis (UML-Notation)

Der Ablauf ist wie folgt:

1 Eine "anfragende IT-Lösung", wie z. B. ein Portal mit einem Online-Dienst, benötigt Zugriff auf eine Ressource, wie z. B. ein Register (über Vermittlungsstellen) oder eine NOOTS-Komponente. Diese IT-Lösung authentifiziert sich mit einem elektronischen Identifizierungsmittel (Zertifikat) gegenüber einem Authentifizierungsserver. Der Autorisierungsserver prüft das für die Authentifizierung verwendete Zertifikat und prüft, ob ein Zugriff auf eine Ressource grundsätzlich gewährt werden kann. Falls ein Zugriff auf den Data Provider und die NOOTS-Komponenten gewährt werden kann, ermittelt der Autorisierungsserver detaillierte Berechtigungen bzw. Berechtigungsmerkmale der anfragenden IT-Lösung. Für einen Online-Dienst „Gewerbeanmeldung“ könnte z. B. folgende Berechtigungsmerkmale enthalten sein: „Online-Dienst“, „Unternehmen“, „Handelsregister“ und „NOOTS-Nutzende“. Die im Rahmen der Registermodernisierung zu verwendenden Berechtigungsmerkmale müssen noch im Rahmen eines Rollen- und Rechtekonzepts festgelegt werden.

2 Der Autorisierungsserver sendet als Antwort einen vom Autorisierungsserver signierten bzw. versiegelten[2] Token. Der Token enthält alle Berechtigungsmerkmale der anfragenden IT-Lösung. Der Token kann als ein OAuth 2.0-Token realisiert werden. Grundsätzlich sind auch weitere Token-Technologien denkbar, wie z. B. SAML.

3 Die anfragende IT-Lösung fragt die Ressource (z. B. eine Vermittlungsstelle für einen Registerzugriff) an und verwendet dabei den Token vom Autorisierungsserver. Die Ressource erhält die Anfrage. So benötigt z. B. ein Online-Dienst einen Registerauszug aus einem Handelsregister. Die Ressource prüft, dass der Token vom Autorisierungsserver der Registermodernisierung gesiegelt worden ist und dass das für die Siegelung verwendete Zertifikat valide und nicht gesperrt ist. Anschließend prüft sie die Berechtigungsmerkmale innerhalb des Tokens.

4 Die Ressource gibt die Antwort an die anfragenden IT-Lösung zurück. Entweder wird die angefragte Funktion ausgeführt oder die angefragten Daten geliefert. Alternativ erhält die anfragende IT-Lösung eine Ablehnungsmitteilung von der angefragten Ressource.

IAM für Behörden umfasst nicht vollständig die Prüfung der Zugriffberechtigung für ein Register. Das IAM für Behörden endet bei der Vermittlungsstelle. Die Vermittlungsstelle

[2] Gemäß eIDAS-VO 910/2024 können nur natürliche Personen Signaturen anbringen. Für juristische Personen wird der Begriff Siegel verwendet. Ziel von Siegeln ist es, den Ursprung und Unversehrtheit des gesiegelten Dokuments bzw. Objekts nachzuweisen.

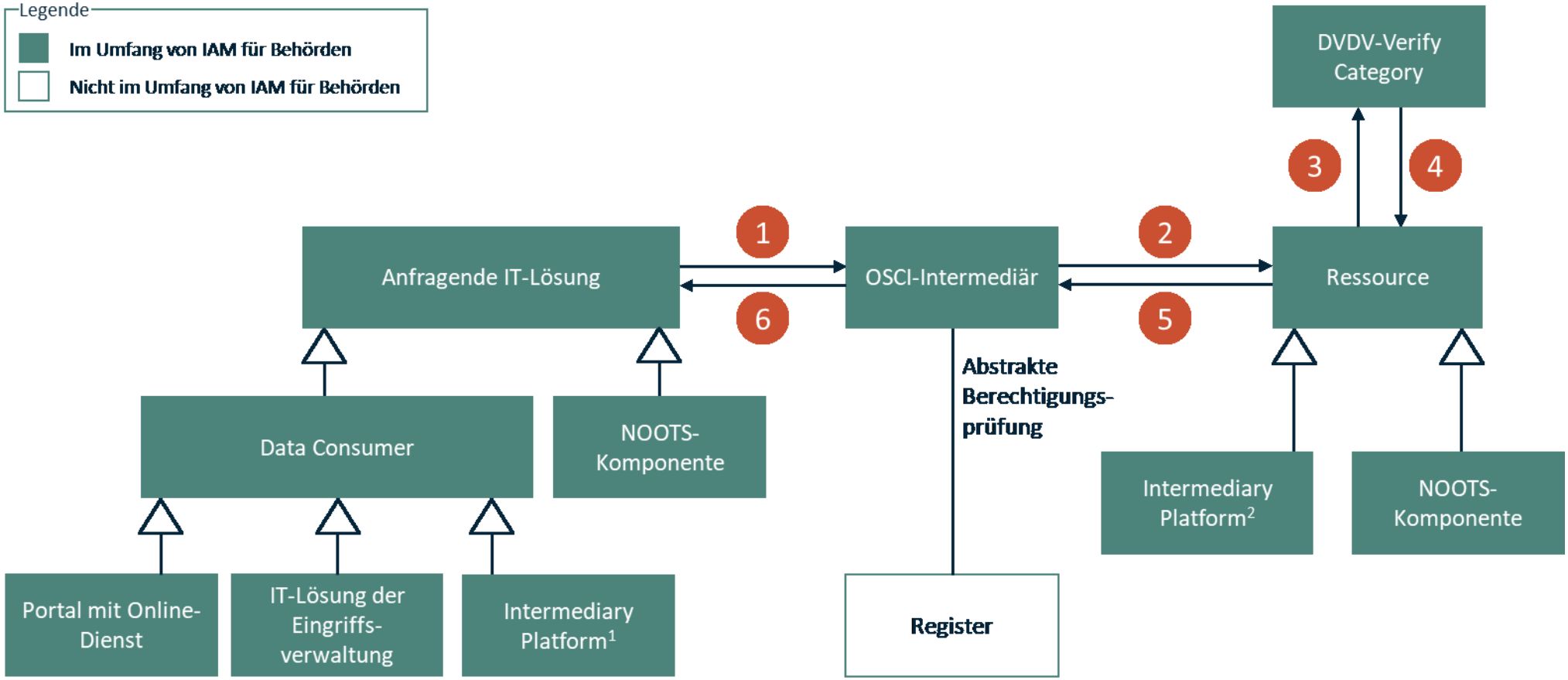
erhält den Token vom Autorisierungsserver. Die abschließende Prüfung, ob ein Zugriff gewährt werden kann oder nicht, wird durch die gemäß §7 (2) aufgeführte abstrakte Berechtigungsprüfung als Teil der Vermittlungsstellen realisiert. Es ist wichtig, dass der Token alle Informationen enthält, damit die Vermittlungsstelle anschließend die abstrakte Berechtigungsprüfung vornehmen kann.

Damit der oben beschriebene Ablauf funktioniert, muss der Autorisierungsserver im Rahmen eines laufenden Aktualisierungsprozess mit allen notwendigen Informationen versehen werden, damit (1) das verwendete elektronische Identifizierungsmittel und (2) die dort aufgeführten Berechtigungsmerkmale bekannt sind. Es ist geplant V-PKI-Zertifikate als elektronische Identifizierungsmittel einzusetzen, siehe weiter unten. Dabei kann die bereits vorhandene Funktionalität und der Datenpflegeprozess beim DVDV eingesetzt werden. Das DVDV ermöglicht mit der Methode VerifyCategory, die Berechtigungsmerkmale zu einzelnen Zertifikaten zuzuordnen. In diesem Zusammenhang kann eine Schnittstelle zwischen dem DVDV und dem Autorisierungsserver realisiert werden, damit der Autorisierungsserver die Daten vom DVDV importieren kann.

3.3.4.3 Geprüfte und verworfene Varianten

Variante: IAM auf der Grundlage von OSCI-Intermediären

Bei dieser Variante wird eine einheitliche IAM-Lösung auf der Grundlage der IAM-Funktionen, die typischerweise ein OSCI-Intermediär anbietet realisiert. Die hier beschriebene Variante ist somit nur dann eine Option, wenn Vermittlungsstellen als OSCI-Intermediäre realisiert werden. Da es sich bei den Anfragen um synchrone Abrufe handelt, erfolgt die OSCI-Abfrage entsprechend dem Request-Response-Szenario (siehe Kapitel 3.5.3 der OSCI-Spezifikation Version 1.2). Der Ablauf ist in der Abbildung unten dargestellt. Um die Komplexität aus der Darstellung herausnehmen, wird lediglich die OSCI-Kommunikation (ohne XTA-Server) realisiert. Grundsätzlich ist der Ablauf auch mit XTA-Servern möglich.



[1]Intermediary Platform holt deutsche Nachweise auf Anfragen der EU-Staaten
[2]Intermediary Platform holt Nachweise aus EU-Staaten auf Anfragen aus Deutschland

Abbildung 28: Verworfene Variante IAM auf der Grundlage von OSCI-Intermediären (UML-Notation)

Der folgende Ablauf ist vereinfacht beschrieben. Für weitere Informationen siehe OSCI-Spezifikation Version 1.2:

1 Die anfragende IT-Lösung stellt die Anfrage über einen OSCI-Intermediär. Die Anfrage (der "Abwicklungsauftrag") wird zunächst mit einem V-PKI-Zertifikat versiegelt. Das verwendete Siegelungszertifikat wird dabei mitgeliefert. Der OSCI-Intermediär kann auf Grundlage des Siegelungszertifikat die Zugangsberechtigung an den Intermediär prüfen. Diese Prüfung der Zugriffsrechte an den OSCI-Intermediär liegt außerhalb des OSCI-Standards. Sie wird dennoch z. B. durch den OSCI-Intermediär Governikus COM-Tauri unterstützt. Diese Authentifizierungsprüfung folgt dem Challenge-Response-Authentifizierungsmuster. Dabei stellt der Intermediär eine Aufgabe (Challenge), die die anfragende IT-Lösung mittels des korrespondierenden privaten Schlüssels des Siegelzertifikats lösen muss. Der OSCI-Intermediär kann anschließend mit Hilfe des Siegelzertifikats prüfen, ob die anfragende IT-Lösung die Aufgabe gelöst hat und somit über den privaten Schlüssel verfügt. Dabei muss der private Schlüssel nicht geteilt werden.

2 Der OSCI-Intermediär entschlüsselt entsprechend der OSCI-Spezifikation den so genannten äußeren Umschlag des Abwicklungsauftrags. Dieser protokolliert den Empfang in einem Laufzettel und verschlüsselt den äußeren Umschlag mit Hilfe des Verschlüsselungszertifikats der angefragten Ressource. Die Inhaltsdaten mit der Anfrage verbleiben verschlüsselt. Anschließend stellt der OSCI-Intermediär entsprechend dem Request-Response-Szenario der OSCI-Spezifikation einen "Bearbeitungsauftrag" an die Ressource. Die Ressource nutzt dabei das verwendete Verschlüsselungszertifikat bzw. den korrespondierenden privaten Schlüssel, um Zugriff auf dem OSCI-Intermediär zu erhalten und die Daten zu empfangen. Dabei wird außerhalb des OSCI-Standards beim OSCI-Intermediär Governikus COM-Tauri ebenfalls das Challenge-Response-Authentifizierungsmuster eingesetzt. Die Ressource führt anschließend eine Entschlüsselung der Nachricht durch. Für diesen Zweck wird der private Schlüssel des Verschlüsselungszertifikats verwendet. Dabei werden sowohl der äußere als auch der innere Umschlag entschlüsselt, damit die Nachricht, d. h. die Anfrage, gelesen werden kann.

3 Die Ressource prüft mit Hilfe der DVDV-VerifyCategory Funktion, inwieweit die anfragende IT-Lösung berechtigt ist, die angefragten Daten zu erhalten. Für diesen Zweck wird das Siegelzertifikat bzw. die Seriennummer des Siegelzertifikats der anfragenden IT-Lösung als ein eindeutiger Identifikator verwendet. Das DVDV enthält

pro Zertifikat Informationen über die Berechtigungsmerkmale (aktuell "Behördenkategorien") des Zertifikatsinhabers. Die Ressource fragt bei dem DVDV an, inwieweit der Zertifikatsinhaber über das erforderliche Berechtigungsmerkmal (bzw. Zugehörigkeit zur Behördenkategorie) verfügt. Anschließend bestätigt oder verneint das DVDV die Behördenzugehörigkeit.

4 Sofern die anfragende IT-Lösung über die erforderlichen Berechtigungsmerkmale verfügt, gibt die Ressource eine Antwort mit den geforderten Daten an die anfragende IT-Lösung zurück. Ansonsten erhält die anfragende ID-Lösung eine Ablehnungsmitteilung.

Der oben beschriebene Ablauf beschreibt die Anfragen an die NOOTS-Komponenten und an die Intermediäre Plattform und nicht die Anfragen an die Register. Hier sind gemäß §7 (2) IDNrG die Vermittlungsstellen (d. h. der OSCI-Intermediär) und nicht die Register für die Berechtigungsprüfung zuständig. Diese Prüfung liegt außerhalb des Umfangs für IAM für Behörden. Diese kann grundsätzlich ebenfalls auf der Grundlage der Informationen über die Zertifikate und die Berechtigungsmerkmale im DVDV erfolgen.

Diese Variante wurde aus den folgenden Gründen verworfen:

- Der Zweck von OSCI/XTA und die dazugehörigen IT-Lösungen liegen im Bereich des sicheren Datentransports und nicht im Bereich des IAM.
- Diese Variante steht in Widerspruch zur Architekturrichtlinie der Registermodernisierung hinsichtlich einer losen Kopplung und eines modularen Aufbaus der Architektur (SR10): Die hier beschriebene IAM-Funktion wäre ein Teil von OSCI-Intermediären und kein separates Modul. Folglich ist eine, von OSCI-Intermediären und XTA-Servern, getrennte Weiterentwicklung von IAM für Behörden nicht möglich.
- Mit der Architektur werden die OSCI-Intermediären nicht nur für die Registeranbindungen, sondern auch für die Kommunikation mit sämtlichen NOOTS-Komponenten erforderlich sein. Dies führt zu längeren Antwortzeiten und verglichen mit einer REST-Kommunikation zu einem erhöhten Umsetzungsaufwand.
- Mit dieser Variante wird auf ausgereifte und im Markt etablierten Standards und Open Source-Lösungen verzichtet.
- Aus technischer Sicht ist die Variante ein Rückschritt. So stellt DVDV aktuell auf eine Token basierte IAM-Lösung (OAuth 2.0) um.

Variante IAM-Lösung der EU

Bei dieser Variante wird eine IAM-Lösung aus der EU eingesetzt. Die grundsätzliche Idee ist, dass die Registermodernisierung in Deutschland von den europäischen Entwicklungen profitieren kann. Diese Synergiegewinne umfassen sowohl die Dauer der Einführung der Registermodernisierung als auch die Betriebsphase nach der Einführung. Darüber hinaus sorgt eine Nutzung von EU-Komponenten dafür, dass Herausforderungen bei der Schaffung einer EU-weiten Interoperabilität einfacher gemeistert werden können. Folgende Quellen für eine potenzielle EU-weite IAM-Lösung wurden geprüft:

- Digital Building Blocks der EU-Kommission (siehe https://ec.europa.eu/digital-building-blocks/wikis/display/DIGITAL/Digital+Homepage). Diese sind:
  - Once Only Technical System: Das Ziel ist die Schaffung eines EU-weiten automatisierten Austauschs von Nachweisen entsprechend Artikel 14 der SDG-Verordnung 2018/1724.
  - eDelivery: eDelivery umfasst technische Spezifikationen, Standards und Hilfsmittel zum sicheren Datenaustausch zwischen den Mitgliedstaaten
  - eID: Das Ziel ist es, die elektronische Identifizierungsmittel der EU-Staaten interoperabel zu gestalten. Somit sollen EU-Bürgerinnen und Bürger die Möglichkeit haben, die nationale Identifizierungsmittel bei anderen EU-Staaten einzusetzen.
  - eSignature: Das Ziel ist es, dass elektronische Signaturen EU-weit erzeugt und validiert werden können.
  - eInvoicing: Mit eInvoicing kann der öffentliche Sektor elektronische Rechnungen von Vertragspartnern (z. B. Unternehmen) empfangen und verarbeiten. Für diesen Zweck wurden EU-weite Standards und Werkzeuge etabliert.
- Peppol (https://peppol.eu/): Peppol ermöglicht eine länderübergreifende elektronische Beschaffung. Es enthält Spezifikationen und Standards für einen elektronischen Datenaustausch von z. B. elektronischen Bestellungen, Lieferscheinen, Rechnungen und Katalogen. Der Peppol Datenaustausch basiert auf eDelivery, siehe oben. Für diesen Zweck ist ein dediziertes Netzwerk (Peppol eDelivery Network) etabliert worden.
- X-Road/X-tee: Die X-Road/X-tee-Plattform ist das digitale Rückgrat in Estland und ermöglicht einen sicheren Austausch über automatische e-Services mit der öffentlichen

Verwaltung. Seit 2017 wird X-Road für einen länderübergreifenden Datenaustausch zwischen Estland und Finnland eingesetzt. Island setzt die X-Road Plattform für einen nationalen Datenaustausch innerhalb der öffentlichen Verwaltung und zwischen der öffentlichen Verwaltung und dem privaten Sektor ein. Inzwischen wird die Plattform X-tee benannt. Lediglich die technische Variante, die in Zusammenarbeit zwischen Estland, Finnland und Norwegen erarbeitet wurde, heißt noch X-Road.

Diese Variante wurde aus den folgenden Gründen verworfen:

Das Once Only Technical System, eID, eSignature und eInvoicing bieten keine relevanten Funktionen für IAM für Behörden an. eID und eSignature befassen sich mit einem zu engen fachlichen Rahmen. Da der Datenaustausch bei eInvoicing und Peppol auf eDelivery basieren, sind somit lediglich eDelivery und X-Road/X-tee übrig:

- eDelivery: eDelivery bietet eine eDelivery Public Key Infrastruktur (PKI) an, damit transportierte Daten signiert und verschlüsselt werden können. Es gibt keine weiteren (veröffentlichten) IAM-Funktionen, die über den Einsatz von Zertifikaten hinaus gehen.
- X-Road/X-tee: X-tee bietet ebenfalls eine PKI für die Zwecke der Signatur an. Es gibt keine weiteren (veröffentlichten) IAM-Funktionen, die über den Einsatz von Zertifikaten hinausgehen.

Zusammengefasst ist der Einsatz einer IAM-Lösung der EU keine valide Option, da die EU-Komponenten („Building Blocks“) die in diesem Dokument aufgeführten Anforderungen nur vereinzelt erfüllen kann. Darüber hinaus bietet Deutschland bereits mit der Verwaltungs-PKI (V-PKI) eine PKI-Infrastruktur an.

3.3.4.4 Einsatz eines elektronischen Identifizierungsmittels

Im Rahmen der Registermodernisierung werden als elektronische Identifizierungsmittel Zertifikate aus der Verwaltungs-PKI eingesetzt. Das Bundesamt für Sicherheit in der Informationsverarbeitung (BSI) betriebt für die deutschen Verwaltungen die Verwaltung-PKI (V-PKI). Die V-PKI ist eine Ablauf- und Aufbauorganisation für die Erstellung und Verwaltung von Zertifikaten. Die V-PKI-Zertifikate dienen der Sicherstellung von Vertrauen und Authentizität in der digitalen Kommunikation zwischen Bund, Ländern und Kommunen. Das BSI selbst gibt keine nutzbaren Zertifikate heraus; dies erfolgt über operative Zwischenzertifizierungsstellen. Darüber hinaus werden V-PKI-Zertifikate für die Zwecke der Siegelung und Verschlüsselung eingesetzt. Weitere Informationen zu der V-PKI im Kontext der Registermodernisierung sind in dem Kapitel 3.4 zu finden.

3.3.4.5 Geprüfte und verworfene Variante

Ergänzend zu den V-PKI-Zertifikaten wurde auch der Einsatz von Zertifikaten aus dem ELSTER-Unternehmenskonto geprüft. Das ELSTER-Unternehmenskonto ist nicht nur auf Unternehmen reduziert, sondern bietet Funktionalitäten eines Organisationskontos an. Gemäß §2 OZG ist ein Organisationskonto "ein Nutzerkonto, das juristischen Personen, Vereinigungen, denen ein Recht zustehen kann, natürlichen Personen, die gewerblich oder beruflich tätig sind, oder Behörden zur Verfügung steht.“ Für eine Organisation können bis zu 500 Zertifikate ausgestellt werden. Das aktuell (Stand Oktober 2022) in Bremen entwickelte Autorisierungsmodul ermöglicht es, auf Ebene der einzelnen Zertifikate (d. h. Rollen) Zugriffsrechte festzulegen. Dies würde somit der Funktion DVDV-VerifyCategory entsprechen, siehe oben.

Diese Variante wurde aus den folgenden Gründen verworfen:

- Die Variante erfüllt nicht die Anforderung FIAR3: "Falls rechtlich erforderlich MUSS das Identifizierungsmittel auf einen Funktionsträger innerhalb der Behörde (mit separater Rechtsgrundlage) ausgestellt werden." Die Organisationszertifikate des Unternehmenskontos sind immer einer Steuernummer zugeordnet, die von den Finanzämtern für steuerpflichtige Funktionsträger vergeben werden. Funktionsträger innerhalb einer Behörde ohne eigene Steuernummer können daher kein dediziertes auf den Funktionsträger ausgestelltes Zertifikat erhalten.
- Die notwendigen Anpassungen im Umfeld des Unternehmenskontos, wie etwa im Bereich des Autorisierungsmoduls, stehen ggf. im Konflikt zu den OZG bezogenen Anpassungsbedarfen. Es besteht daher das Risiko, dass die Anpassungen, die aus Sicht der Registermodernisierung dringend und zwingend notwendig sind, erst nach höherpriorisierten OZG-Anpassungen erfolgen können.

3.3.4.6 Infrastruktur und Betrieb

Für die Pilotierungsphase der Registeranbindung wird die bestehende Infrastruktur und die Betriebsorganisation der einzelnen NOOTS-Komponenten mit IAM-Funktionalität verwendet.

Für die nach der Pilotierungsphase geplante einheitliche Lösung gilt Folgendes:

- Der Autorisierungsserver wird deutschlandweit bei einem IT-Dienstleister betrieben. Zur Sicherstellung eines ausfallsicheren Betriebs muss der IT-Dienstleister den

Autorisierungsserver georedundant betreiben. Der Betrieb muss 24x7 gewährleistet sein (siehe auch Anforderungen in Kapitel 3.3.4.2).

- Die Organisation zur Pflege der Daten im Autorisierungsserver muss ausgewählt werden. Es bietet sich an, dass bereits etablierte Organisationen dafür sorgen, dass zu den Zertifikaten entsprechende Rechte zugeordnet werden. So kann z. B. die DVDV-Betriebsorganisation diese Aufgabe übernehmen und bei Bedarf entsprechende technische Schnittstellen zwischen dem DVDV-Bundesmaster und dem Autorisierungsserver einrichten.

Insgesamt muss für diese kritische und sicherheitsrelevante Infrastruktur dafür gesorgt werden, dass Kompetenzen, z. B. im Rahmen eines Kompetenz-Zentrums etabliert werden.

Für den Betrieb der V-PKI-Infrastruktur, siehe Kapitel zu V-PKI.

3.3.5 Ausblick & Weiterführende Aspekte

Für die Pilotierungsphase der Registeranbindung müssen die Anschlussbedingungen in Form eines Leitfadens beschrieben werden. Dabei werden bereits etablierte oder kurzfristig geplante IAM-Lösungen der einzelnen NOOTS-Komponenten beschrieben.

Für die nach der Pilotierungsphase geplante einheitliche und Token basierte IT-Lösung müssen die Anforderungen finalisiert werden. Insbesondere folgende Konkretisierungen sind notwendig:

- Die Festlegung von funktionalen Anforderungen im Bereich der Protokollierung.
- Die Festlegung der Schnittstelle zwischen IAM für Behörden und der abstrakten Berechtigungsprüfung der Vermittlungsstellen.
- Die Prüfung von technischen Möglichkeiten die Anforderungen aus der TR-03107 des BSI zu erfüllen und bei Bedarf im Dialog mit BSI vergleichbare und sichere Alternativen zu diskutieren und festzulegen.
- Die Festlegung von Abläufen und der Architektur zur Pflege der Daten, die der Autorisierungsserver benötigt, um Tokens ausstellen zu können.
- Eine grobe quantitative Schätzung der nichtfunktionalen Anforderungen.

Parallel dazu muss ein geeigneter IT-Dienstleister für den Betrieb des Autorisierungsservers gefunden werden. Dabei soll soweit möglich auf bereits etablierte Organisationen, Prozesse

und ggf. bereits etablierte Technologien (wie etwa ein bereits vorhandener Autorisierungsserver) aufgesetzt werden.

Es bietet sich an, in einem ersten Schritt die IAM-Lösung zunächst für ausgewählte Registerabrufe und NOOTS-Komponenten zu pilotieren.

Ergänzend zur technischen Umsetzung muss ein Rollen- und Rechtekonzept mit standardisierten Berechtigungsmerkmalen etabliert werden.

3.4 V-PKI Infrastruktur

3.4.1 Überblick

Die Kernforderung für den elektronischen Rechts- und Geschäftsverkehr zwischen öffentlichen Stellen ist die Sicherheit (Schutz vor unbefugter Kenntnisnahme und vor Manipulation) und Rechtsverbindlichkeit aussagekräftige Authentizität (Schutz vor gefälschter Identität und Unabstreitbarkeit) in der Kommunikation. Diese können auf der Grundlage einer Public Key Infrastruktur (PKI) erreicht werden

Eine PKI ist eine organisierte Aufbau- und Ablauforganisation, welche die dazu notwendigen organisatorischen und technischen Funktionen bietet. Die Anwendung einer PKI ist einfach und wirkungsvoll; jedem Kommunikationspartner wird ein individuelles Schlüsselpaar zugewiesen. Dieses Schlüsselpaar besteht aus einem geheimen und einem öffentlichen Schlüssel (private key / public key). Mit Hilfe dieses Schlüsselpaares können die Teilnehmer einer Kommunikation sich gegenseitig authentifizieren und vertraulich kommunizieren. Jede PKI ist auf verlässliche Instanzen angewiesen, die die Schlüssel erzeugen und diese authentisch in Form eines digitalen Zertifikates an Ihre Besitzer ausgeben.

Der typische Funktionsumfang einer PKI ist in der folgenden Abbildung zu sehen:

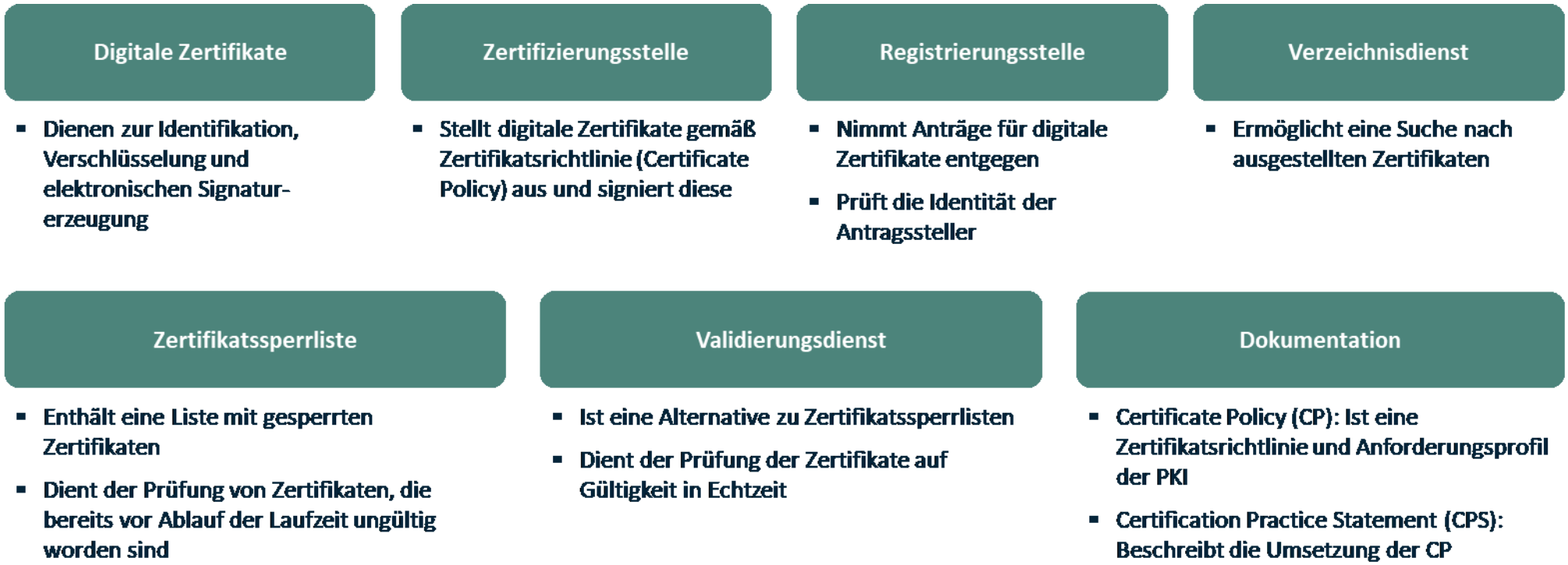


Abbildung 29: Funktionsumfang einer PKI-Infrastruktur

Durch Beschluss der Bundesregierung vom 16.01.2002 "Sicherheit im elektronischen Rechts- und Geschäftsverkehr mit der Bundesverwaltung" (siehe https://www.bsi.bund.de/dok/6616262),wurde die Public Key Infrastruktur der Verwaltung (im Folgenden als Verwaltungs-PKI bezeichnet oder als V-PKI abgekürzt) etabliert. Diese bildet die einheitliche Basis der organisatorischen, rechtlichen und technischen Standards für zertifikatsbasierte Sicherheitsdienstleistung der Bundes- und Landesbehörden, Kommunen sowie öffentliche Institutionen an. Die V-PKI ist föderal gegliedert, sodass die Länder, wie z. B. die Hessen-PKI, eigene Instanzen als Teil der bundesweiten Verwaltungs-PKI bilden können.

Die Organisation der V-PKI wird von Zertifizierungsstellen der öffentlichen Verwaltung gebildet, die in ihrem Verwaltungsbereich für Antragstellende digitale Zertifikate ausstellen. Ein digitales Zertifikat ist ein standarisierter digitaler Datensatz, der bestimmte Eigenschaften von Personen oder Objekten bestätigt und dessen Authentizität und Integrität durch kryptografische Verfahren geprüft werden kann. Das digitale Zertifikat enthält insbesondere die zu seiner Prüfung erforderlichen Daten und öffentlichen Schlüssel.

Mit Hilfe von digitalen Zertifikaten und dem zugehörigen geheimen Schlüssel können Objekte (z. B. Dokumente, Daten und Nachrichten) signiert, versiegelt und verschlüsselt werden. Darüber hinaus können Zertifikate im Rahmen eines Identity und Access Managements als Identifikationsmittel verwendet werden.

Die Zertifizierungsstellen stellen, als verlässliche Instanzen der V-PKI, die digitalen Zertifikate aus, nachdem die Registrierungsstellen die Identität von Organisation und Antragstellenden geprüft und bestätigt haben. Die Regeln und Vorgaben für die Ausstellung von Zertifikaten durch die Zertifizierungsstelle und die Nutzung der Zertifikate durch die Antragstellenden werden durch Zertifizierungsrichtlinien (Certificate Policy) und Certification Practice Statements festgelegt. Mit Hilfe von Verzeichnisdiensten können Zertifikate gesucht und gefunden werden. Bei Bedarf können ausgestellte Zertifikate vor Ablauf der Gültigkeit gesperrt werden, z. B., weil der geheime Schlüssel kompromittiert worden ist. Mit Hilfe von Zertifikatssperrlisten und Validierungsdiensten können die Validität von Zertifikaten und eventuelle Sperrungen geprüft werden.

Als oberste Instanz in der föderalen Organisation der V-PKI betreibt das BSI mit der "PCA-1-Verwaltung" die Wurzelzertifizierungsstelle (englisch: Policy Certificate Authority, kurz: PCA) der Verwaltungs-PKI für die öffentliche Verwaltung. Sie führt die Zertifizierung von nachgeordneten Zertifizierungsstellen (Certificate Authority, kurz: CA) durch und stellt ihr

Wurzelzertifikat zur Verifikation der Vertrauenskette zur Verfügung. Für die Verwaltungs-PKI wird dieser Sicherungsanker seit dem 20. Februar 2001 im BSI betrieben. Die Wurzelzertifizierungsstelle des BSI bearbeitet die Anträge von öffentlichen Stellen zur Aufnahme in die bundesweite Verwaltungs-PKI. Sie prüft die Konformität der Zertifizierungsrichtlinie (Certificate Policy) der Wurzelzertifizierungsstelle sowie deren Umsetzung in den Zertifizierungsstellen und sichert damit die Einheitlichkeit des Sicherheitsniveaus der ausgegebenen digitalen Zertifikate.

3.4.1.1 Funktionsumfang und Abgrenzungen

Der Funktionsumfang im Kontext der Registermodernisierung kann wie folgt festgelegt und abgegrenzt werden:

V-PKI Zertifikate für Behörden, aber nicht für Bürgerinnen und Bürger, Unternehmen und Mitarbeiter: Die im Rahmen der Registermodernisierung notwendigen Zertifikate werden für Behörden ausgestellt. Diese können für automatisierte IT-Prozesse sogenannte V-PKI-Funktionszertifikate erhalten. In Kontext der Registermodernisierung würden Data Consumer (z. B. Portale) und Data Provider (z. B. Register), NOOTS-Komponenten sowie die Intermediäre Plattform automatisierte IT-Prozesse unterstützen und somit V-PKI-Funktionszertifikate erhalten. Es werden keine Zertifikate für Verwaltungskunden (d. h. für Bürgerinnen und Bürger oder Unternehmen) notwendig sein. Die V-PKI sieht aktuell nicht vor, dass Zertifikate für diese Nutzergruppe ausgestellt werden.

Die V-PKI basierte Verschlüsselung bei Nachweisaustauschen zwischen Deutschland und EU-Staaten endet bei der Intermediäre Plattform: Verschlüsselte deutsche Nachweise, die für EU-Staaten vorgesehen sind, werden bei der geplanten Intermediäre Plattform entschlüsselt. Sollte ein verschlüsselter Datentransport ab der Intermediäre Plattform bis hin zum Evidence Requester der EU notwendig sein, erfolgt diese Verschlüsselung mit Zertifikaten von Certificate Authorities (CAs) der EU und nicht mit Hilfe von CAs der V-PKI. Gleiches gilt für das umgekehrte Szenario, d. h., wenn verschlüsselte Nachweise aus EU-Staaten nach Deutschland transportiert werden. Die Intermediäre Plattform entschlüsselt die Nachricht mit Zertifikaten der EU. Ab der Intermediäre Plattform bis hin zum Data Consumer in Deutschland werden hingegen Verschlüsselungszertifikate der V-PKI verwendet. Als Konsequenz wird für den EU-weiten Datenaustausch keine Ende-zu-Ende-Verschlüsselung möglich sein.

Die V-PKI basierte Signatur bei Nachweisaustauschen zwischen Deutschland und EU-Staaten endet bei der Intermediäre Plattform: Nachweise an EU-Staaten, die mit V-PKI-Zertifikaten versiegelt wurden, werden bei der Intermediäre Plattform abschließend geprüft. Für den weiteren Datentransport in EU-Staaten siegelt die Intermediäre Plattform, die Nachricht mit Hilfe von Zertifikaten der EU, sofern die EU dies fordert. Für das umgekehrte Szenario, d. h., wenn versiegelte Nachweise aus EU-Staaten nach Deutschland transportiert werden, endet die Siegelprüfung ebenfalls bei der Intermediäre Plattform. Bei Bedarf wird für den weiteren Datentransport zum Data Consumer in Deutschland, die Intermediäre Plattform die Nachricht mit Hilfe von Zertifikaten der V-PKI siegeln.

Die TLS-Zertifikate zwischen dem Browser und dem Webserver liegen nicht im Umfang der Betrachtung: Für die Kommunikation zwischen dem Browser und dem Webserver dürfen, anstelle von V-PKI-Zertifikaten, kommerzielle Zertifizierungsstellen beauftragt werden, die entsprechende TLS/SSL-Zertifikate auszustellen. Unabhängig davon müssen V-PKI-Zertifikate für die interne TLS-Kommunikation eingesetzt werden, siehe Anforderung FVV1 unten. Dies trifft für die interne Kommunikation ohne Einbindung eines Browsers zu, wie etwa im Rahmen einer REST-basierten Kommunikation zwischen Online-Diensten und NOOTS-Komponenten.

Qualifizierte elektronische Siegel (entsprechend eIDAS VO Nr. 910/2014) nicht im Umfang der V-PKI: Im Folgenden liegt der Schwerpunkt darauf, dass der Nachrichtenaustausch zwischen beteiligten Komponenten manipulationssicher ist, Nachrichten bei Bedarf verschlüsselt werden und beteiligte Komponente sich gegenseitig authentisieren können. Durch V-PKI-Zertifikate versiegelte Nachweise entsprechen gemäß Einschätzung BSI das eIDAS-Niveau „fortgeschrittene Siegel“. Fortgeschrittene Siegel auf der Grundlage von V-PKI-Zertifikaten werden u. a. auch für den Austausch von hoheitlichen Dokumenten verwendet und dürfte somit auch für die Registermodernisierung als ausreichend sicher eingestuft werden. Gemäß Artikel 35 (1) der eIDAS-VO Nr. 910/2014 „darf die Rechtswirkung und die Zulässigkeit als Beweismittel in Gerichtsverfahren nicht allein deshalb abgesprochen werden, weil es [= das elektronische Siegel] in einer elektronischen Form vorliegt oder nicht die Anforderungen an qualifizierte elektronische Siegel erfüllt.“ Um das Niveau qualifizierte elektronische Siegel erreichen zu können, muss gemäß eIDAS-VO Nr. 910/2014 der elektronischen Siegel durch eines qualifizierten Vertrauensdienstanbieters ausgestellt werden. Im Rahmen der Novellierung der eIDAS-VO ist eine Ergänzung um Fernsiegeleinheiten vorgesehen. Ein eventueller Bedarf an qualifizierten elektronischen Siegeln ist nicht nur auf die Registermodernisierung

einzuschränken. Stattdessen muss die Umsetzung von qualifizierten elektronischen Siegeln übergreifend über Initiativen wie die Registermodernisierung und die Umsetzung des OZG geprüft und behandelt werden.

3.4.2 Annahmen und Rahmenbedingungen

Für den Einsatz der V-PKI im Kontext der Registermodernisierung gelten folgende Annahmen und Rahmenbedingungen:

Der Einsatz von V-PKI-Zertifikaten wird Teil der NOOTS-Anschlussbedingungen sein: Für den nationalen Nachrichtenaustausch siegeln und verschlüsseln Data Consumer, Data Provider, NOOTS-Komponenten und die Intermediäre Plattform Nachrichten mit Hilfe von V-PKI-Zertifikaten und dazugehörigen geheimen Schlüsseln. Zusätzlich werden V-PKI Zertifikate als Identifikationsmittel im Rahmen der Authentifizierung eingesetzt (siehe Konzept zu IAM für Behörden).

Die Inhaber der V-PKI-Zertifikate sind automatisierte IT-Prozesse: Die V-PKI bietet vier Varianten an. Die Inhaber sind entweder (1) eine natürliche Person, (2) eine juristische Person, (3) eine Personengruppe oder Funktionen, die durch Mitarbeiter ausgeführt werden oder (4) automatisierte IT-Prozesse. Die vierte Variante ist für die Registermodernisierung relevant. Es handelt sich hier um Prozesse, die vollautomatisch durch die Unterstützung der IT realisiert werden.

Im Rahmen der Registermodernisierung werden Objekte versiegelt und nicht signiert: Gemäß der Definition in der eIDAS-Verordnung (910/2014) können nur natürliche Personen Objekte (Dokumente, Daten und Nachrichten) signieren. Da diese für die Registermodernisierung relevanten Zertifikate nicht auf natürliche Personen ausgestellt sind (siehe oben), sind gemäß dieser Definition keine Signaturen möglich. Stattdessen verwendet die eIDAS-Verordnung für juristische Personen den Begriff "Siegel". Dabei werden elektronische Siegel als "Daten in elektronischer Form, die anderen Daten in elektronischer Form beigefügt oder logisch mit ihnen verbunden werden, um deren Ursprung und Unversehrtheit sicherzustellen" bezeichnet. Juristische und nicht natürliche Personen stellen Siegel aus.

V-PKI Zertifikate für Authentifizierung folgen der Konzeption IAM für Behörden: Der Einsatz von V-PKI-Zertifikaten für den Zweck der Authentisierung und Authentifizierung ist von der Konzeption IAM für Behörden abhängig, siehe Kapitel "IAM für Behörden".

Gemäß aktueller Zertifizierungsrichtlinie (Certification Policy) der V-PKI können Zertifikate neben Siegel und Verschlüsselung auch für Authentisierung eingesetzt werden.

Nutzung bestehender V-PKI-Strukturen und Policies: Die V-PKI ist eine Organisation, die eine standardisierte Dienstleistung erbringt. Die Certificate Policy der V-PKI gilt für die Ausstellung aller V-PKI Zertifikate unabhängig vom fachlichen Kontext. Der Vorteil dieser standardisierten und fachunabhängigen Dienstleistung liegt darin, dass keine redundanten PKI-Strukturen für die öffentliche Verwaltung entstehen. Für die Registermodernisierung bedeutet dies, dass registermodernisierungsspezifische PKI-Policies konform zu der Zertifizierungsrichtlinie der Wurzelzertifizierungsstelle sein müssen.

Umsetzungsneutrale Anforderungen für die Ertüchtigung der V-PKI Infrastruktur: Aus der Registermodernisierung werden Anforderungen an die V-PKI-Organisation festgehalten. Diese Anforderungen werden umsetzungsneutral formuliert, damit die V-PKI-Organisation die freie Wahl bei der Umsetzung einer passenden Lösung haben kann.

Die Ertüchtigung der V-PKI ist nicht Gegenstand der Registermodernisierung: Das BSI als Aufsichtsbehörde für die V-PKI bewertet die Anforderungen der Registermodernisierung und ertüchtigt die V-PKI, um diese Anforderungen zu erfüllen. Die Registermodernisierung wird über den Fortschritt der Ertüchtigung informiert, sofern es für die Erfüllung der Anforderungen relevant ist.

Die NOOTS-Komponente Registerdatennavigation enthält V-PKI Verschlüsselungszertifikate und Siegelungszertifikate: Damit Sender Nachrichten verschlüsseln können, wird es erforderlich sein, V-PKI Verschlüsselungszertifikate des Empfängers zentral abzulegen und suchbar zu machen. Gleiches gilt für die Antwort auf einer Anfrage eines Senders. Ggf. müssen auch Siegelungszertifikate zentral hinterlegt werden, wenn diese nicht Teil der Nachricht sind. Es wird angenommen, dass die NOOTS-Komponente Registerdatennavigation die Ablage und Suche nach Verschlüsselungszertifikaten und Siegelungszertifikaten realisieren wird.

3.4.3 Fachliches Konzept (inkl. Facharchitektur)

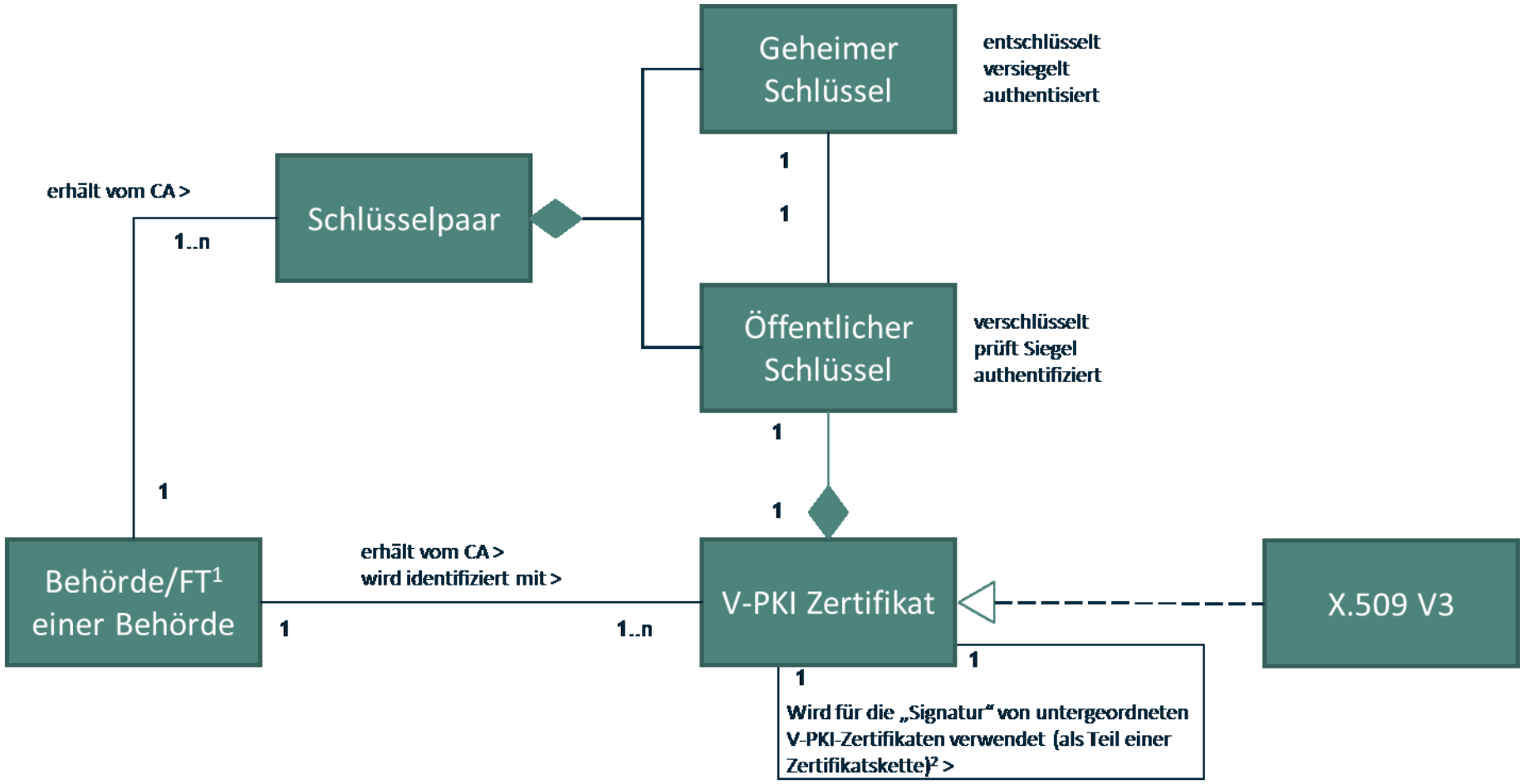
Die V-PKI kann mit Hilfe von den folgenden Klassendiagrammen beschrieben werden:

- Klassendiagramm V-PKI (Zertifikate und Schlüssel): Betrachtet werden Zertifikate und Schlüssel sowie deren unmittelbaren Verwendung. Für diesen Teil gibt es keine Besonderheiten im Kontext der Registermodernisierung.

- Klassendiagramm V-PKI (Übergreifend im Kontext der Registermodernisierung): Betrachtet wird die gesamte V-PKI-Infrastruktur inkl. Registrierung. Für diesen Teil gibt es registermodernisierungsspezifische Klassen/Entitäten.

3.4.3.1 Klassendiagramm V-PKI (Zertifikate und Schlüssel)

Das Klassendiagramm für Zertifikate und Schlüssel ist in der Abbildung unten dargestellt (UML-Notation):



[1]FT = Funktionsträger
[2]Die Zertifikatskette beginnt mit dem V-PKI-Wurzelzertifikat und endet mit dem V-PKI-Zertifikat für die Behörde

Abbildung 30: Klassendiagramm für Zertifikate und Schlüssel

Es wird zwischen Authentisierung und Authentifizierung unterschieden:

- Bei der Authentisierung legt der Nutzenden ein Identifikationsmittel vor, welches seine Identität gegenüber der angefragten Ressource nachweisen soll.
- Bei der Authentifizierung prüft eine Verification Authority, ob die Behauptung der Identität bestätigt werden kann. Die Verification Authority kann entweder als Funktion einer IT-Lösung (der angefragten Ressource) oder separat realisiert werden. So ist z. B. geplant, dass gemäß §7 (2) IDNrG die Vermittlungsstellen und nicht die Register eine abstrakte Berechtigungsprüfung vornehmen.

Die Klassen/Entitäten sind:

- **Behörde/Funktionsträger (FT) einer Behörde:** Eine Behörde ist eine öffentliche Stelle, die Aufgaben der öffentlichen Verwaltung wahrnimmt. Betrachtet werden sowohl Behörden der Leistungsverwaltung als auch Behörden der Eingriffsverwaltung. In einigen Fällen haben Behörden mehrere "Funktionsträger", die jeweils Aufgaben aus separaten Rechtsgrundlagen durchführen. Rechte, die sich aus den Rechtsgrundlagen ergeben, dürfen nur von den Teilen der Behörde wahrgenommen werden, die mit den entsprechenden Aufgaben vertraut sind. Ein Zertifikat muss sich daher bei Bedarf auf diesen Funktionsträger mit separater Rechtgrundlage innerhalb der Behörde beziehen können. Die Behörde bzw. Funktionsträger der Behörde wird durch ein V-PKI-Zertifikat identifiziert. Sie beantragt oder besitzt ein oder mehrere V-PKI-Zertifikate sowie entsprechende Schlüsselpaare.
- **Schlüsselpaar**: Das Schlüsselpaar wird durch die CA erzeugt. Es besteht aus einem geheimen und einem öffentlichen Schlüssel.
- **V-PKI-Zertifikat**: Das V-PKI-Zertifikat wird von der CA für die Behörde ausgestellt. Es enthält den öffentlichen Schlüssel aus dem Schlüsselpaar und weitere Attribute zur Beschreibung der Behörde sowie der vorgesehenen Nutzung des Zertifikats. Das V-PKI-Zertifikat kann geteilt und muss nicht geschützt werden. Das V-PKI-Zertifikat wird vom Aussteller (Zertifizierungsstelle) signiert bzw. versiegelt.
- **Öffentlicher Schlüssel:** Der öffentliche Schlüssel ist ein Attribut des V-PKI-Zertifikats. Er wird bei Verschlüsselungen, Signaturprüfungen und Authentifizierungen verwendet.

  - Verschlüsselung: Nach der Verschlüsselung kann nur der Eigentümer des korrespondierenden geheimen Schlüssels das verschlüsselte Objekt (z. B. Dokument, strukturierte Daten (XML, JSON...)) entschlüsseln.
  - Siegelprüfungen: Der öffentliche Schlüssel wird verwendet, um das Siegel auf ein Objekt zu prüfen.
  - Authentifizierungen: Bei einer Authentifizierung erfolgt die Prüfung, ob die Authentisierung der Nutzenden valide ist. Dies kann z. B. mit Hilfe eines sogenannten Challenge-Response-Verfahrens überprüft werden. Die Nutzenden (IT-Lösung einer Behörde) haben bereits eine sogenannte Challenge mit Hilfe seines geheimen Schlüssels gelöst, siehe unten. Nun wird der öffentliche Schlüssel verwendet, um zu prüfen, ob die Nutzenden die Challenge korrekt gelöst haben und somit über den geheimen Schlüssel verfügen.
  -

- **Geheimer Schlüssel:** Der geheime Schlüssel muss geschützt und darf nicht geteilt werden. Er wird bei Entschlüsselungen, Signaturerzeugungen und Authentisierungen verwendet.
  - Entschlüsselung: Mit Hilfe des geheimen Schlüssels können Objekte (z. B. Dokumente, strukturierte Daten (XML, JSON...)) entschlüsselt werden.
  - Siegelerzeugung: Der geheime Schlüssel wird genutzt, um Objekte zu versiegeln.
  - Authentisierung: Eine Authentisierung kann z. B. im Rahmen eines Challenge-Response-Verfahrens erfolgen. Dabei löst die Nutzenden (IT-Lösung einer Behörde) eine Challenge mit Hilfe des geheimen Schlüssels. Sie können z. B. eine Zufallszahl erhalten und diese mit Hilfe eines geheimen Schlüssels verschlüsseln.
- Ein Sonderfall sind elektronische Zeitstempel. Gemäß der eIDAS-Verordnung der EU Nr. 910/2014 sind elektronische Zeitstempel "Daten in elektronischer Form, die andere Daten in elektronischer Form mit einem bestimmten Zeitpunkt verknüpfen und dadurch den Nachweis erbringen, dass diese anderen Daten zu diesem Zeitpunkt vorhanden waren". Qualifizierte Zeitstempel müssen gemäß Art 42 (1) c der eIDAS VO mit einem fortgeschrittenen elektronischen Siegel des Vertrauensdienstanbieters

versiegelt werden. Dabei können für diese Siegelungen Zertifikate der V-PKI eingesetzt werden.

3.4.3.2 Klassendiagramm V-PKI (Übergreifend im Kontext der Registermodernisierung)

Das Klassendiagramm für den übergreifenden Kontext ist in der Abbildung unten dargestellt (UML-Notation):

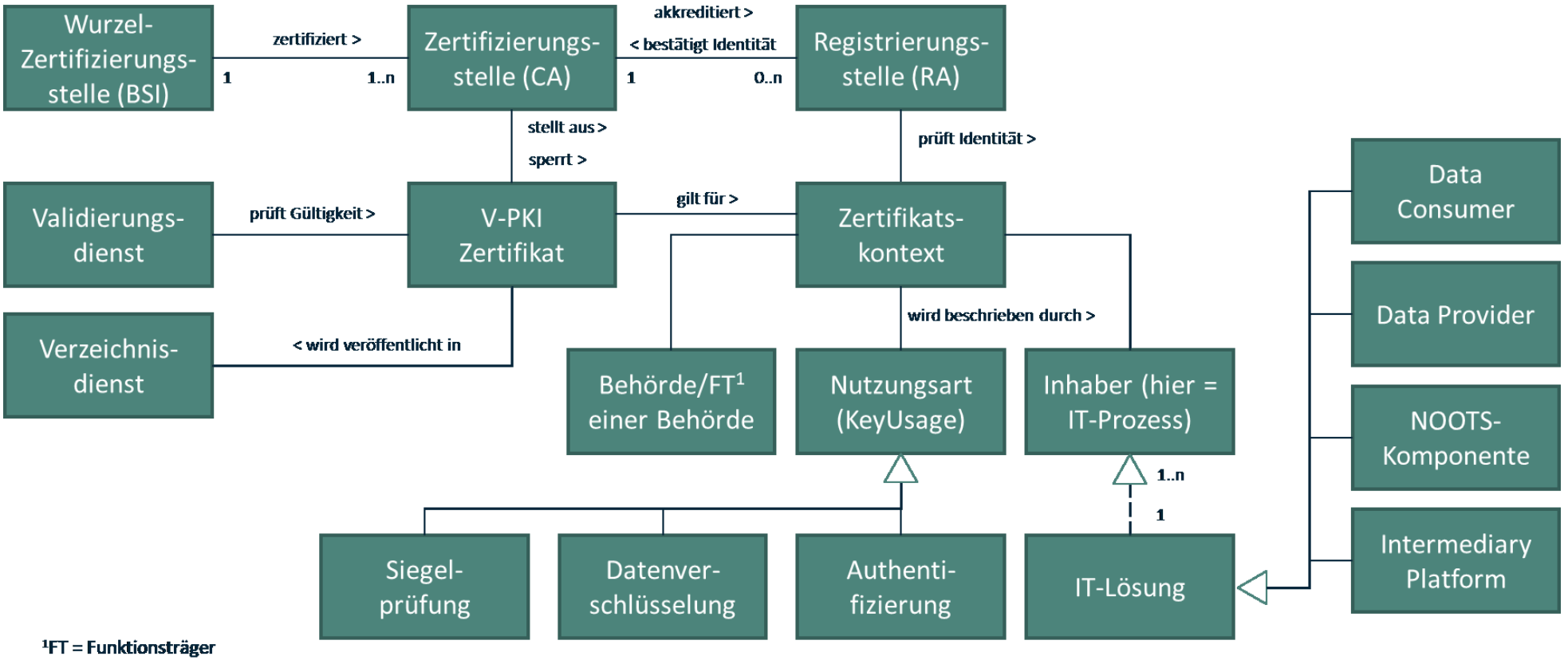


Abbildung 31: Klassendiagramm V-PKI - Übergreifend im Kontext der Registermodernisierung

Die Klassen/Entitäten sind:

- **Wurzelzertifizierungsstelle (BSI):** Die Wurzelzertifizierungsstelle ist für die Zertifizierung von nachgeordneten CAs verantwortlich. Alle durch die Wurzelzertifizierungsstelle ausgestellten Zertifikate werden mit dem Wurzelzertifikat der V-PKI signiert.
- **Zertifizierungsstellen (CA):** Die Zertifizierungsstellen sind für das Ausstellen und das Sperren von Zertifikaten zuständig. Sie können die Funktion einer Registrierungsstelle wahrnehmen oder separate Registrierungsstellen beauftragen.
- **Registrierungsstellen (RA):** Die Registrierungsstelle erhält Zertifikatsanfragen und prüft die Identität der Behörde/OE der Behörde, die ein Zertifikat ausstellen möchte. Sie bestätigt die Identität an die Zertifizierungsstelle.
- **V-PKI Zertifikat:** Das V-PKI Zertifikat gilt für einen konkreten Zertifikatskontext, siehe auch Klassendiagramm V-PKI (Zertifikate und Schlüssel) oben.
- **Zertifizierungskontext:** Der Begriff ist kein etablierter Begriff der V-PKI. Er beschreibt hier den Kontext der Verwendung eines Zertifikats nach Ausstellung. Der Kontext umfasst (1) Zugehörigkeit zu einer Behörde/Funktionsträger einer Behörde, (2) Nutzungskontext des Zertifikats und (3) Inhaber des Zertifikats. Im Kontext der Registermodernisierung ist der Inhaber ein automatischer IT-Prozess.
- **Behörde/Funktionsträger (FT) innerhalb einer Behörde:** Siehe Beschreibung in "Klassendiagramm V-PKI (Zertifikate und Schlüssel)".
- **Nutzungsart:** Die Nutzungsart eines Zertifikats kann mit Hilfe der Zertifikatserweiterung KeyUsage - eingeschränkt werden. Für das V-PKI-Zertifikat der Endnutzenden (End-Entity-Zertifikat) können Zertifikate für Datenverschlüsselung (DataEncipherment), Siegelprüfung (nonRepudiation) und Authentisierung (digitalSignature) zugelassen werden. Ergänzend dazu können weitere Nutzungsarten mit Hilfe der Zertifikatserweiterung - KeyUsage Extension festgelegt werden. So kann z. B. angegeben werden, ob das Zertifikat für Siegelungen von Zeitstempeln verwendet werden soll. Für weitere Informationen siehe Dokument BSI: BSI Technische Richtlinie TR-02103: X.509 Zertifikate und Zertifizierungspfadvalidierung.
- **Inhaber (hier: IT-Prozess):** Der Inhaber der Zertifikate ist für die Registermodernisierung ein (automatisierter) IT-Prozess. Das Zertifikat enthält

zusätzlich Informationen darüber, welche Behörde/Funktionsträger einer Behörde die IT-Lösung verantwortet.

- **IT-Lösung:** Eine IT-Lösung realisiert eine oder mehrere IT-Prozesse. Im Kontext der Registermodernisierung sind die IT-Lösungen (1) Data Consumer (z. B. Portal oder Online-Dienst), (2) Data-Provider (z. B. Register, Spiegelregister oder Abfrageportale), (3) NOOTS-Komponenten, wie z. B. die Registerdatennavigation, und die (4) Intermediäre Plattform.
- **Validierungsdienst:** Ein Validierungsdienst ermöglicht die Prüfung der Zertifikate auf Echtheit in Echtzeit[3]. Ergänzend dazu veröffentlichen Zertifizierungsstellen Sperrlisten, die genutzt werden können, um die Validität von Zertifikaten zu prüfen. Validierungsdienste werden von Validation Authorities, als vertrauenswürdige Instanzen, die für die Bereitstellung von Prüfmitteln zuständig sind. Oft führen Zertifizierungsstellen Aufgabe eines Validation Authority durch
- **Verzeichnisdienst**: Es handelt sich um ein durchsuchbares Verzeichnis, das ausgestellte Zertifikate enthält. Der Verzeichnisdienst der Wurzelzertifizierungsstelle enthält Zertifikate der Zertifizierungsstellen der V-PKI. Die einzelnen Zertifizierungsstellen haben jeweils eigene Verzeichnisdienste. Darüber hinaus sind im Kontext der Registermodernisierung Verzeichnisdienste erforderlich, damit unabhängig vom eingesetzten CA passende Zertifikate für Verschlüsselungen und Siegelprüfungen einfach gefunden werden können.

Die V-PKI muss Anwendungsfälle im Umfeld (1) Administration/Registrierung, (2) Siegelerzeugung und Prüfung, (3) Verschlüsselung, (4) Authentisierung/Authentifizierung und (5) Prüfung der Zertifikate unterstützen. Betrachtet werden ausschließlich Anwendungsfälle für V-PKI-Zertifikate der Behörden (End-Entry-Zertifikate) und nicht die Zertifikate der Zertifizierungsstellen. Betrachtet werden hier die möglichen Anwendungsfälle. Je nach fachlichem Kontext kann es sein, dass bestimmte Anwendungsfälle, wie z. B. Versiegelung, nicht notwendig sein werden. Die jeweiligen fachspezifischen Festlegungen sind separat zu dokumentierten, wie z. B. als Transportprofil einer XÖV-Spezifikation.

[3] Unter „Echtzeit“ wird verstanden, dass der technische Kommunikationsweg keine Verzögerungen mit sich führt. Sobald ein Zertifikat als gesperrt gekennzeichnet wurde, haben alle Beteiligten unmittelbar danach Zugriff auf diese Information.

3.4.3.3 Anwendungsfälle im Kontext der Administration/Registrierung:

V-AR1: V-PKI-Schlüsselpaar und Zertifikat beantragen (erstmalige Ausstellung): Eine Behörde beantragt ein Schlüsselpaar mit dazugehörigem V-PKI-Zertifikat, das im Rahmen der Registermodernisierung eingesetzt werden soll. Das Zertifikat kann für Siegelprüfungen, Datenverschlüsselungen oder gemäß Konzeption IAM für Behörden für Authentisierungen eingesetzt werden. Die Behörde bereitet alle notwendigen Informationen für den Antrag vor und sendet diesen Antrag an die Registrierungsstelle.

V-AR2: V-PKI-Antrag prüfen (erstmalige Ausstellung): Die Registrierungsstelle prüft den Antrag. Im Falle, dass die Identitätsprüfung erfolgreich war, erhält die Zertifizierungsstelle die bestätigte Identität und alle notwendigen Informationen.

V-AR3: V-PKI-Schlüsselpaar und Zertifikat (erstmalig) ausstellen: Die Zertifizierungsstelle erzeugt das V-PKI-Schlüsselpaar und das V-PKI-Zertifikat. Sie signiert bzw. siegelt das V-PKI-Zertifikat der Behörde mit dem V-PKI-Zertifikat der Zertifizierungsstelle. Die Behörde erhält das Zertifikat und das Schlüsselpaar.

V-AR4: V-PKI Zertifikat erneuern: Bei einer Erneuerung eines V-PKI-Zertifikats kann wie bei einer erstmaligen Ausstellung vorgegangen werden. Alternativ kann ein Antrag online und teilautomatisiert mit dem existierenden (noch gültigen) V-PKI-Zertifikat signiert bzw. versiegelt werden.

V-AR5: V-PKI Zertifikat sperren: Sollte ein V-PKI Zertifikat kompromittiert werden und z. B. der geheime Schlüssel nicht mehr geheim sein, muss das V-PKI Zertifikat gesperrt werden. (Bei einer Entsperrung wird ein erneuter Antrag gestellt, siehe Anwendungsfälle V-AR1 - V-AR3).

V-AR6: V-PKI Zertifikat veröffentlichen: Das V-PKI-Zertifikat wird veröffentlicht und suchbar gemacht. Dies ist insbesondere für Anwendungsfälle im Kontext der Verschlüsselung wichtig, siehe Anwendungsfall V-V1.

3.4.3.4 Anwendungsfälle im Kontext der Siegelerzeugung und -prüfung:

V-SI1: Objekt elektronisch versiegeln: Mit Hilfe des geheimen Schlüssels wird ein Objekt (z. B. Dokument, strukturierte Daten, Zeitstempel) elektronisch versiegelt. Mit der Versiegelung werden der Ursprung und die Unversehrtheit des Objekts sichergestellt.

V-SI2: Elektronisch versiegeltes Objekt prüfen: Bei der Prüfung wird sichergestellt, dass das elektronisch versiegelte Objekt nicht nachträglich manipuliert worden ist. Darüber hinaus

wird geprüft, ob der Siegelersteller bei der Versiegelung ein einschlägiges und valides Zertifikat eingesetzt hat, siehe auch Anwendungsfall V-P1 und V-P2.

V-SI3: Zertifikat für Siegelung suchen/holen: Im Kontext der Registermodernisierung müssen Empfänger von Nachrichten prüfen, ob das für die Siegelung verwendete Zertifikat valide ist. Für diesen Zweck benötigt der Empfänger das V-PKI-Zertifikat, das für die Siegelung eingesetzt wurde.

3.4.3.5 Anwendungsfälle im Kontext der Verschlüsselung:

V-V1: Zertifikat für Verschlüsselung suchen/holen: Im Kontext der Registermodernisierung müssen Sender Nachrichten verschlüsseln, bevor diese transportiert werden. Dies trifft sowohl für die verschlüsselte Anfrage als auch für die verschlüsselte Antwort zu. Dabei sollen die Nachrichten nur durch den Empfänger mit deren geheimen Schlüssel entschlüsselt werden können. Für diesen Zweck benötigt der Sender der Nachricht das V-PKI-Zertifikat mit dem korrespondierenden öffentlichen Schlüssel des Empfängers.

V-V2: Objekt verschlüsseln: Der Autor oder Sender einer Nachricht verschlüsselt diese mit Hilfe des öffentlichen Schlüssels. Der öffentliche Schlüssel ist Teil des V-PKI-Zertifikats.

V-V3: Objekt entschlüsseln: Der Empfänger oder Leser der Nachricht entschlüsselt diese mit Hilfe des zum V-PKI-Zertifikat korrespondierenden geheimen Schlüssels.

3.4.3.6 Anwendungsfälle im Kontext der Authentisierung/Authentifizierung:

V-A1: Authentisierung und Authentifizierung: Eine anfragende IT-Lösung, die einen Zugriff auf eine NOOTS-Komponente, ein Register oder ein Intermediäre Plattform benötigt, authentisiert sich mit Hilfe eines V-PKI-Zertifikats. Eine Verification Authority prüft im Rahmen einer Authentifizierung, aufgrund des verwendeten Zertifikats, inwieweit ein Zugriff gewährt werden kann.

Für eine detaillierte Beschreibung der Anwendungsfälle im Kontext der Authentisierung/Authentifizierung siehe das Kapitel IAM für Behörden.

3.4.3.7 Anwendungsfälle im Kontext der Prüfung von Zertifikaten:

V-P1: V-PKI-Zertifikat auf Validität prüfen: Die Zertifizierungsstelle bietet einen Validierungsdienst an. Dieser Validierungsdienst kann genutzt werden, um Zertifikate in

Echtzeit auf Validität zu prüfen (z. B. auf Grundlage des OCSP-Standards). Alternativ dazu veröffentlicht die Zertifizierungsstelle für ihre ausgestellte Zertifikate eine Sperrliste. Sofern diese Sperrlisten statt Echtzeitprüfungen eingesetzt werden, müssen die Beteiligten der Registermodernisierung die Sperrliste in regelmäßigen Abständen in der PKI-Infrastruktur importieren.

V-P2: V-PKI-Zertifikatsketten prüfen: In diesem Anwendungsfall werden alle Zertifikate in einer Zertifikatskette bis hin zum Wurzelzertifikat geprüft.

Im Folgenden werden lediglich architekturrelevante Anforderungen aufgeführt. Diese Anforderungen sind im Rahmen der Feinkonzeption weiter auszuarbeiten. Anforderungen werden nach dem Standard ISO 25010 (Norm für Qualitätskriterien von Software, IT-Systemen und Software-Engineering) kategorisiert. Unter dem V-PKI-System werden sowohl alle notwendigen technischen als auch organisatorische Funktionen betrachtet.

3.4.3.8 Anforderungen (Qualitätskriterium - Funktionale Software):

Tabelle 38: Anforderungen an V-PKI (Qualitätskriterium – Funktionale Software)

ID	Anforderung	Anwendungsfall
FVAR1	Die V-PKI Registrierungsstelle MUSS einen Zertifikatsantragssteller die Möglichkeit bieten, V-PKI-Zertifikate zu beantragen.	V-AR1
FVAR2	Die V-PKI Registrierungsstelle MUSS fähig sein, die Identität von Zertifikatsantragsstellern zu prüfen.	V-AR2
FVAR3	Die V-PKI Zertifizierungsstelle MUSS fähig sein, Zertifikate inkl. Schlüsselpaare zu erzeugen.	V-AR3
FVAR4	Sobald die V-PKI Registrierungsstelle die Identität bestätigt hat, MUSS die V-PKI Zertifizierungsstelle das Zertifikat und den geheimen Schlüssel an den Zertifikatsantragssteller sicher übermitteln.	V-AR3
FVAR5	Zertifikatsinhaber MÜSSEN geheime Schlüssel sicher aufbewahren.	V-AR3

ID	Anforderung	Anwendungsfall
FVAR7	Die V-PKI Registrierungsstelle MUSS Zertifikatsantragsstellern die Möglichkeit bieten, Verlängerungsanträge vollständig elektronisch einzureichen. Umsetzungshinweis: Der Verlängerungsantrag kann mit dem geheimen Schlüssel des noch gültigen und zu ersetzenden V-PKI-Zertifikats versiegelt werden.	V-AR4
FVAR8	Zertifizierungsstellen MÜSSEN fähig sein, auf Antrag der Beteiligten im Registermodernisierungskontext V-PKI-Zertifikate zu sperren.	V-AR5
FVAR9	Die NOOTS-Komponente Registerdatennavigation MUSS Zertifikatsinhabern die Möglichkeit anbieten, Zertifikate zu veröffentlichen und suchbar zu machen.	V-AR6, V-SI3
FVSI1	Data Provider, Data Consumer, NOOTS-Komponenten und die Intermediäre Plattform MÜSSEN bei Versiegelungen V-PKI-Zertifikate einsetzen.	V-SI1
FVSI2	Data Provider, Data Consumer, NOOTS-Komponenten und die Intermediäre Plattform MÜSSEN fähig sein, versiegelte Objekte mit Hilfe des V-PKI-Zertifikats auf Validität zu prüfen, siehe auch Anforderung NVSi1.	V-SI2
FVV1	Data Provider, Data Consumer, NOOTS-Komponenten und die Intermediäre Plattform MÜSSEN bei Verschlüsselungen V-PKI-Zertifikate einsetzen. (Ausgenommen sind TLS-Kommunikationen zwischen Browser und Web-Server, siehe auch Kapitel 3.4.3)	V-V2
FVV2	Die NOOTS-Komponente Registerdatennavigation MUSS Sendern von Nachrichten die Möglichkeit anbieten, Verschlüsselungszertifikate von Empfängern zu suchen und zu holen.	V-V1
FVV3	Die NOOTS-Komponente Registerdatennavigation MUSS Empfängern von Nachrichten die Möglichkeit anbieten, Signaturzertifikate von Sendern zu suchen und zu holen.	V-SI3

ID	Anforderung	Anwendungsfall
FVV4	Data Provider, Data Consumer, NOOTS-Komponenten und die Intermediäre Plattform MÜSSEN fähig sein, verschlüsselte Objekte mit Hilfe des zum V-PKI-Zertifikat korrespondierenden geheimen Schlüssel zu entschlüsseln.	V-V3
FVA1	Bei Zugriffen auf NOOTS-Komponenten, Register und Intermediäre Plattformen MÜSSEN anfragende IT-Lösungen V-PKI-Zertifikate für die Authentisierung einsetzen. (Für detaillierte Anforderungen, siehe Konzept IAM für Behörden)	V-A1
FVP1	Die Zertifizierungsstelle MUSS Zertifikatsnutzenden die Möglichkeit bieten, die Validität der Zertifikate online zu prüfen.	F-P1
FVP2	Die Zertifizierungsstelle MUSS Zertifikatsnutzenden die Möglichkeit bieten, aktuelle Zertifikatssperrlisten in die eigene PKI-Infrastruktur zu importieren.	F-P1
FVP3	Die Zertifizierungsstelle MUSS Zertifikatsnutzenden die Möglichkeit bieten, Zertifikatsketten bis hin zum V-PKI-Wurzelzertifikat auf Validität zu prüfen.	F-P2
FVAR1	Die V-PKI Registrierungsstelle MUSS einen Zertifikatsantragssteller die Möglichkeit bieten, V-PKI-Zertifikate zu beantragen.	V-AR1

3.4.3.9 Anforderungen (Sonstige Qualitätskriterien entsprechend ISO 25010):

Tabelle 39: Anforderungen an V-PKI – Sonstige Qualitätskriterien entsprechend ISO 25010

ID	Anforderung	Anwendungsfall
NVP1	Die Summe aller V-PKI-Registrierungsstellen MÜSSEN eine noch zu ermittelnde Zahl von V-PKI-Zertifikatsanträgen (Neuanträge + Verlängerungsanträge) pro Zeiteinheit verarbeiten. (**Umsetzungshinweis**: Dafür müssen die V-PKI-	V-AR1

ID	Anforderung	Anwendungsfall
	Registrierungsstellen hinsichtlich der Personalstärke ausreichend dimensioniert sein. Darüber hinaus sollten die Verlängerungsanträge von einem automatisierten Verfahren unterstützt werden.	
NVP2	Die Summe aller V-PKI-Registrierungsstellen MÜSSEN V-PKI-Zertifikatsanträge (Neuanträge + Verlängerungsanträge) innerhalb eines noch zu definierenden Zeitfensters verarbeiten. (**Umsetzungshinweis**: Dafür müssen die V-PKI-Registrierungsstellen hinsichtlich der Personalstärke ausreichend dimensioniert sein. Darüber hinaus sollten die Verlängerungsanträge von einem automatisierten Verfahren unterstützt werden.	V-AR1
NVP3	Die Summe aller V-PKI-Zertifizierungsstellen MÜSSEN eine noch zu ermittelnde Zahl von V-PKI-Zertifikaten (Neu- und Verlängerungsanträgen) pro Zeiteinheit ausstellen. (**Umsetzungshinweis**: Dafür müssen die V-PKI-Zertifizierungsstellen hinsichtlich der Personalstärke ausreichend dimensioniert sein. Darüber hinaus sollten die Verlängerungsanträge von einem automatisierten Verfahren unterstützt werden.	V-AR2
NVP4	Nach erfolgreicher Identitätsprüfung MÜSSEN die V-PKI-Zertifizierungsstellen (Neuanträge + Verlängerungsanträge) V-PKI-Zertifikate innerhalb eines noch zu definierenden Zeitfensters ausstellen. (**Umsetzungshinweis**: Dafür müssen die V-PKI-Registrierungsstellen hinsichtlich der Personalstärke ausreichend dimensioniert sein. Darüber hinaus sollten die Verlängerungsanträge von einem automatisierten Verfahren unterstützt werden.	V-AR2
NVP5	Nachdem ein Zertifikat als kompromittiert angemeldet wurde, MUSS die Zertifizierungsstelle das Zertifikat als gesperrt anzeigen (Sperrliste, Antwort auf Online-Anfragen).	V-AR5
NVSi1	Data Provider, Data Consumer, NOOTS-Komponenten und die Intermediäre Plattform MÜSSEN Zertifikate und Zertifikatsketten bis hin zum Vertrauensanker der BSI auf Validität prüfen. Als verbindliche Grundlage für die Prüfung der Zertifikate und Zertifikatsketten dient die	Alle

ID	Anforderung	Anwendungsfall
	Technische Richtlinie TR-02103: X.509 Zertifikate und Zertifizierungspfadvalidierung (BSI).	
NVSi2	Die Ablage des geheimen Schlüssels MUSS so gestaltet sein, dass nur berechtigte IT-Lösungen Zugriff auf den geheimen Schlüssel erhalten dürfen.	Alle
NK1	Durch End-Nutzer-Zertifikate erzeugte Siegel MÜSSEN die Anforderungen an fortgeschrittene elektronische Siegel aus Artikel 36 der eIDAS-Verordnung (Nr. 910/2014) erfüllen.	V-SI1 - V-SI2
NK2	Die End-Nutzer-Zertifikate MÜSSEN die Vorgaben aus BSI Technische Richtlinie "TR-02103: X.509 Zertifikate und Zertifizierungspfadvalidierung" erfüllen.	V-AR1 - V-AR5
NVP1	Die Summe aller V-PKI-Registrierungsstellen MÜSSEN eine noch zu ermittelnde Zahl von V-PKI-Zertifikatsanträgen (Neuanträge + Verlängerungsanträge) pro Zeiteinheit verarbeiten. (**Umsetzungshinweis**: Dafür müssen die V-PKI-Registrierungsstellen hinsichtlich der Personalstärke ausreichend dimensioniert sein. Darüber hinaus sollten die Verlängerungsanträge von einem automatisierten Verfahren unterstützt werden.	V-AR1
NVP2	Die Summe aller V-PKI-Registrierungsstellen MÜSSEN V-PKI-Zertifikatsanträge (Neuanträge + Verlängerungsanträge) innerhalb eines noch zu definierenden Zeitfensters verarbeiten. (**Umsetzungshinweis**: Dafür müssen die V-PKI-Registrierungsstellen hinsichtlich der Personalstärke ausreichend dimensioniert sein. Darüber hinaus sollten die Verlängerungsanträge von einem automatisierten Verfahren unterstützt werden.	V-AR1
NVP3	Die Summe aller V-PKI-Zertifizierungsstellen MÜSSEN eine noch zu ermittelnde Zahl von V-PKI-Zertifikaten (Neu- und Verlängerungsanträgen) pro Zeiteinheit ausstellen. (**Umsetzungshinweis**: Dafür müssen die V-PKI-Zertifizierungsstellen hinsichtlich der Personalstärke ausreichend dimensioniert sein. Darüber hinaus sollten die Verlängerungsanträge von einem automatisierten Verfahren unterstützt werden.	V-AR2

3.4.4 Umsetzung

Folgende Aktivitäten zur Umsetzung sind notwendig. Diese liegen vorrangig außerhalb der Registermodernisierung, siehe auch Kapitel 3.4.3:

- Rechtlich/Normativ:
    - Beschluss IT-Planungsrat, dass die V-PKI ein Standard des IT-Planungsrates und vom Bund zu betreiben ist. (Die fachliche Zuständigkeit ist beim BMI und die technische Zuständigkeit beim BSI zu verorten).
    - Beschluss IT-Planungsrat, dass die V-PKI im Kontext der Registermodernisierung verpflichtend einzusetzen ist.
- Organisatorisch:
    - Erstellung einer Zertifikatsrichtlinie (CA Policy) dediziert für die Registermodernisierung. Eine Zertifikatsrichtlinie (englisch „certificate policy“) definiert die Regeln, nach denen ein Zertifikat ausgestellt, verwaltet und benutzt wird. Auf Grundlage der Informationen in der Zertifikatsrichtlinie, kann geprüft werden, ob das Zertifikat für einen bestimmten Anwendungsfall zulässig ist. Ergänzend zur Zertifikatsrichtlinie enthält ein „Certificate Practice Statement“ zusätzlich die vom Aussteller getroffenen Maßnahmen zu deren Umsetzung. Ausgestellte V-PKI Zertifikate verlinken mit Hilfe des Zertifikatsfeld bzw. Zertifikatserweiterung „Certificate Policy“ auf einschlägige Zertifikatsrichtlinien und Certificate Practice Statements.
    - Festlegung Struktur und Zuständigkeiten für die Organisation der V-PKI für die Registermodernisierung.
    - Dimensionierung der V-PKI Infrastruktur hinsichtlich der Personalstärke. Dabei muss die Summe der betroffenen Zertifizierungsstellen und Registrierungsstellen die nichtfunktionalen Anforderungen aus der Registermodernisierung erfüllen können. Dies betrifft insbesondere Anforderungen an Durchsatz und Reaktionszeiten bei Zertifikatsanträgen.
- Semantisch:

  - Festlegung inhaltlicher registerspezifischer Vorgaben für Inhalt der End-Nutzer-Zertifikate, z. B. hinsichtlich Eintragungen in "KeyUsage", "extendedKeyUsage" und "SubjectAlternativeName".

- Technisch:
  - Schaffung eines Self-Serviceportals zur vereinfachten Antragsstellung bei Verlängerungsanträgen und zur vereinfachten Sperrung von Zertifikaten.
  - Schaffung von organisatorischen und technischen Schnittstellen zur NOOTS-Komponente Registerdatennavigation, damit direkt in Zusammenhang mit Registeranfragen nach Verschlüsselungszertifikaten und Siegelungszertifikaten gesucht werden können.

3.4.5 Ausblick & Weiterführende Aspekte

Der Einsatz von V-PKI-Zertifikaten reicht aus, um Anforderungen der eIDAS VO 910/2014 an fortgeschrittenen elektronischen Siegeln zu erfüllen. Um das höhere Niveau „qualifizierte elektronische Siegel“ erreichen zu können, müssen elektronische Siegel durch einen qualifizierten Vertrauensanbieter ausgestellt werden. Gemäß Art. 3 der eIDAS VO werden Vertrauensdienste, wie etwa ein Siegelungsdienst, „in der Regel gegen Entgelt erbracht“. Es ist daher zunächst zu klären, ob im Kontext der Registermodernisierung ein zwingender rechtlicher Bedarf an qualifizierten elektronischen Siegeln besteht. Sollte einen Bedarf bestehen, wird empfohlen übergreifend über die Programme Registermodernisierung und OZG hinweg zu prüfen, wie diese Anforderung umgesetzt werden kann. Somit können Synergien zwischen diesen beiden Programmen gewonnen werden. Bei der Prüfung ist auch die Initiative zur Novellierung der eIDAS VO zu beobachten, wie etwa im Kontext der Einführung von Vertrauensdiensten im Bereich der Fernsiegelung.

3.5 IDM Unternehmen (Basisregister für Unternehmen)

3.5.1 Überblick

Definition

Das Basisregister für Unternehmen dient dazu, ein Register über Unternehmensbasisdaten zu errichten und zu führen sowie die bundeseinheitliche Wirtschaftsnummer für Unternehmen einzuführen.

Gemäß §2 UBRegG dient als bundeseinheitliche Wirtschaftsnummer für Unternehmen die Wirtschafts-Identifikationsnummer nach § 139c der Abgabenordnung. Die bundeseinheitliche Wirtschaftsnummer für Unternehmen dient dem Zweck der registerübergreifenden eindeutigen Identifikation der im Basisregister geführten Unternehmen. Die bundeseinheitliche Wirtschaftsnummer wird durch das Bundeszentralamt für Steuern (BZSt) vergeben und von der Wirtschafts-Identifikationsnummern-Datenbank des BZSt bereitgestellt.

Rechtliche Grundlagen

Rechtlichen Grundlagen dafür sind im Unternehmensbasisdatenregistergesetz (UBRegG) geregelt. Als UBRegG wird Gesetz zur Errichtung und Führung eines Registers über Unternehmensbasisdaten und zur Einführung einer bundeseinheitlichen Wirtschaftsnummer für Unternehmen bezeichnet.

Gemäß §1 des UBRegG wird beim Statistischen Bundesamt ein Register über Unternehmensbasisdaten errichtet und betrieben (Basisregister für Unternehmen). Unter Unternehmensbasisdaten im Sinne dieses Gesetzes werden Stammdaten, Identifikationsnummern und Metadaten verstanden, die in §3 UBRegG aufgeführt sind. §5 UBRegG regelt die Übermittlung der Daten durch die Registerbehörde (das Statistische Bundesamt) an die angebundenen Register.

3.5.2 Fachliches Konzept

Zielsetzung

- Registerübergreifende eindeutige Identifikation (anhand der bundeseinheitlichen Wirtschaftsnummer) der im Basisregister geführten Unternehmen (gemäß §3 Abs. 1 UBRegG)
- Indirekt: Verbesserung der Qualität der gespeicherten Daten, Ergänzung der fehlenden Daten oder Einheiten; Bereitstellung von konsolidierten Daten für andere Register
- Indirekt: Verringerung der erneuten oder mehrfachen Beibringung von bei öffentlichen Stellen nach § 5 Absatz 1 UBRegG bereits vorhandenen Daten durch die betroffenen Unternehmen nach § 3 Absatz UBRegG

Zuständigkeiten

Gemäß §1 UBRegG übernahm das Statistische Bundesamt die Rolle der Registerbehörde. Das Funktionspostfach des Statistischen Bundesamtes für das Basisregister für Unternehmen: basisregister@destatis.de Die Zuständigkeiten innerhalb des Statistischen Bundesamtes ist in der folgenden Tabelle aufgeführt.

Tabelle 40: Zuständigkeiten für das Basisregister für Unternehmen innerhalb des Statistischen Bundesamtes

Abteilung I Gruppe I 1 Verwaltungsregister Nils Holzmann Stakeholdermanager Nils.Holzmann@destatis.de	Abteilung I Gruppe I 1 Verwaltungsregister Björn Witting Gesamtprojektleitung Bjoern.Witting@destatis.de	Abteilung I Gruppe I 1 Verwaltungsregister Referat I 13 Basisregister für Unternehmen: Annabell Heinrichs Fachliche Projektleitung Annabell.Heinrichs@destatis.de

Funktionale und Nichtfunktionale Anforderungen

- Zentrale funktionale Anforderungen sind im UBRegG definiert. Ergänzend dazu liegt ein XÖV-Standard „XUnternehmen.Basisregister“ als Entwurf vom 07.10.2022 auf Seiten von www.repository.de vor.
- Nichtfunktionale Anforderungen liegen noch nicht vor.

3.5.3 Technisches Konzept

Der Datenbestand des Basisregisters wird stufenweise aufgebaut. Die Erstbefüllung findet aus vier Quellregistern statt:

- Wirtschafts-Identifikationsnummern-Datenbank
- Zentrales Unternehmensverzeichnis
- Handels- Partnerschafts-, Genossenschafts- und Vereinsregister
- Legal Entity Identifier-Datenbanken

Der XÖV-Standard „XUnternehmen.Basisregister“ soll als die standardisierte Schnittstelle zur Meldung von Unternehmensbasisdaten und Unternehmensereignissen an angebundene öffentliche Stellen sowie für Abrufe aus dem Basisregister dienen. Der Standard „XUnternehmen.Basisregister“ baut auf dem semantischen Datenstandard „XUnternehmen.Kerndatenmodell“ und seiner Bereitstellung als XÖV-Standard „XUnternehmen.Basismodul“ auf. Er folgt dem Rollenmodell des XTA2-Standards. Der Datentransport erfolgt auf der Grundlage des OSCI-Standards. Das DVDV wird dabei als Verzeichnis für die technischen Adressen und Zertifikate der Kommunikationspartner eingesetzt.

Abhängigkeiten

Das Basisregister weist Abhängigkeiten zu den angebundenen Registern und Quellregistern z. B. durch die Betriebsumgebungen und Netzwerke der Register auf. Somit wird der Aspekt der Kompatibilität über Schnittstellenvereinbarungen berücksichtigt. Besonders wichtige Abhängigkeit besteht mit der Wirtschafts-Identifikationsnummern-Datenbank des Bundeszentralamtes für Steuern durch die Bereitstellung der Wirtschafts-Identifikationsnummer/ bundeseinheitlichen Wirtschaftsnummer. Da das Basisregister eine Vielzahl von Daten aus Quellregistern beziehen wird, sind umfassende Sicherheitsmaßnahmen sowie Schutz- und Sicherheitskonzepte zwingend erforderlich.

Außerdem müssen XÖV-Standards wie z. B. XBasisdatenverordnung sowie verschiedene Übertragungs- und Transportstandards berücksichtigt werden.

Abgrenzung

Basisregister für Unternehmen ersetzt nicht die Anfragen an Fachregister, die im Basisregister als Quellregister aufgeführt worden sind (vgl. § 1 und § 3 UBRegG). Nach der Einführung des Basisregisters müssen somit Portale bzw. Online-Dienste weiterhin direkte Abfragen an die Fachregister stellen, um den kompletten Auszug aus dem jeweiligen Register zu erhalten.

3.5.4 Ausblick & Weiterführende Aspekte

Die Projektplanung besteht aus den folgenden Meilensteinen (Stand: 30.11.2022):

- Q3 2023 – Q4 2024: Konsolidierung der bereits zugelieferten Daten aus Unternehmerverzeichnis, Justizregistern und Bundeszentralamt für Steuern
- Q3 2023: Das Kernsystem Basisregister steht zur internen Nutzung zur Verfügung und ist testbar
- Ende Q1 2024: Das System Basisregister wird mit den geplanten Funktionalitäten und Schnittstellen fertiggestellt
- Q2 2024 – Q4 2024: Umfangreiches Testen der Schnittstellen und weiteren Funktionalitäten des Systems Basisregister
- Q2 2024 – Q4 2024: Gegebenenfalls Implementierung erster Elemente der 2. Ausbaustufe, z. B. Anbindung weiterer öffentlichen Stellen
- Voraussichtlich Q4/2024: Erste bundeseinheitliche Wirtschaftsnummern werden bereitgestellt

3.6 IDM Personen (IDA)

3.6.1 Überblick

3.6.1.1 Ausgangslage

Für den automatisierten Abruf von Nachweisen aus Registern ist eine trennscharfe Zuordnung der Nachweise zu Personen erforderlich, welche zum Abruf berechtigt sind. Diese Zuordnung erfolgt in vielen Registern anhand persönlicher Identifikationsmerkmale, wie Name, Geburtsort und Geburtsdatum. Insbesondere bei ausländischen Namen und Namen nicht ungewöhnlichen Schreibweisen, bspw. diakritischen Zeichen, gestaltet sich die Zuordnung schwierig, bspw. weil die Namen bei der Erfassung der Daten falsch übernommen und in der Folge fehlerhaft in den Registern gespeichert werden. In manuell ausgeführten Verwaltungsvorgängen kommen daher häufig unscharfe Suchen, bspw. phonetische Suchen oder Suchen mit Toleranzen gegenüber abweichenden Schreibweisen, zum Einsatz, um trotzdem Datensätze zu finden und das Verfahren durchführen zu können. Auftretende Mehrdeutigkeiten werden durch die zuständigen Sachbearbeiter individuell gelöst, indem sie aus Trefferlisten die richtigen Einträge auswählen und dafür erforderliche Merkmale von den betroffenen Personen einholen.

In voll automatisierten Verfahren wie dem synchronen Nachweisabruf sind solche manuellen Identifizierungsschritte nicht mehr zulässig. Auf Grundlage des IDNrG wird daher die Steuer-ID als Ordnungsmerkmal für natürliche Personen in alle im RegMoG genannten Registertypen eingespeichert. Die Register müssen nicht nur die Identifikationsnummer (IDNr.) zusichern, sondern auch die zugeordneten Personendaten aktuell halten. Zu diesem Zweck wird ein Basisregister für Personendaten geschaffen, aus dem sowohl die IDNr. als auch ein Kranz aus persönlichen Merkmalen von den Registern abgerufen werden können.

Es gibt derzeit keine Rechtsgrundlage, die IDNr. im Data Consumer zu speichern. Damit Nachweisabrufe unter Verwendung der IDNr. ermöglicht werden können, muss die abrufende Stelle die IDNr. daher zunächst in Erfahrung bringen.

3.6.1.2 Ziel IDM für Personen

Das IDM für Personen liefert die IDNr. eines Bürgers anhand dessen persönlicher Identifikationsmerkmale, wie sie bspw. in der eID bzw. dem Bürgerkonto zu finden sind.

Damit schafft es die Voraussetzung, dass Data Consumer Nachweise unter Verwendung der IDNr. abrufen können, sofern die zuständigen Register dies unterstützen.

3.6.1.3 Abgrenzung

Sowohl die Bereitstellung der IDNr. als auch die Bereitstellung persönlicher Merkmale im Sinne eines Basisregisters natürlicher Personen übernimmt das Verfahren IDA (Identitätsdatenabruf), welches vom BVA entwickelt und betrieben wird. IDA speichert gem. IDNrG dabei selbst keine Personendaten, sondern bezieht diese aus der Steuer-ID-Datenbank des Bundeszentralamts für Steuern (BZSt). Darüber hinaus bietet IDA Funktionen zur Unterstützung von Neuanlagen oder Datenkorrekturen im Datenbestand des BZSt an. Diese Funktionen sind Teil des Basisregisters für Personendaten, nicht jedoch Teil der hier beschriebenen Komponente IDM für Personen.

3.6.2 Annahmen & Rahmenbedingungen

Tabelle 41: Übersicht Annahmen IDM Personen

ID	Annahme
[ANN_01]	Die Speicherung der IDNr. im Data Consumer ist unzulässig. Der Data Consumer muss daher die IDNr. für jeden Nachweisabrufprozess immer wieder neu ermitteln.
[ANN_02]	Die Funktionalität der Komponente IDM für Personen wird vollumfänglich durch das Verfahren IDA erbracht.
[ANN_03]	IDM für Personen ist ausschließlich für die Lieferung der IDNr. für natürliche Personen zuständig. Weitere Funktionen von IDA, insbesondere in der Rolle als Basisregister für Personenstammdaten, werden hier nicht betrachtet.
[ANN_04]	Die initiale Zuordnung von Personendaten zur IDNr. in den Registern muss erfolgt sein, bevor Nachrichtenabrufe aus den Registern unter Verwendung der IDNr. erfolgen können.
[ANN_05]	Die Abrufe der IDNr. über das IDM für Personen unterliegt der Protokollierungspflicht gem. §9 IDNrG.

ID	Annahme
[ANN_06]	Die Verantwortung für die Rechtmäßigkeit des Abrufs der IDNr. liegt bei der abrufenden Stelle. IDM für Personen prüft nicht, ob für den geplanten Nachweisabruf die Verwendung einer IDNr. zulässig ist.

Tabelle 42: Übersicht Rahmenbedingungen IDM Personen

ID	Rahmenbedingung
[RMBED_01]	IDM für Personen speichert keine Identifikationsnummern. Sämtliche Abrufe werden an die Steuer-ID-Datenbank des BZSt durchgereicht.
[RMBED_02]	Die Kommunikation mit IDA erfolgt ausschließlich über den XBasisdaten Standard.

3.6.3 Fachliches Konzept

3.6.3.1 Kontext

Das folgende Diagramm zeigt den Systemkontext der Komponente IDM für Personen. Zum besseren Verständnis wird dabei auch das Basisregister Personenstammdaten und damit die zweite Rolle des IDA Verfahrens dargestellt. Im Folgenden wird jedoch nur die Rolle als Lieferant der IDNr. näher betrachtet.

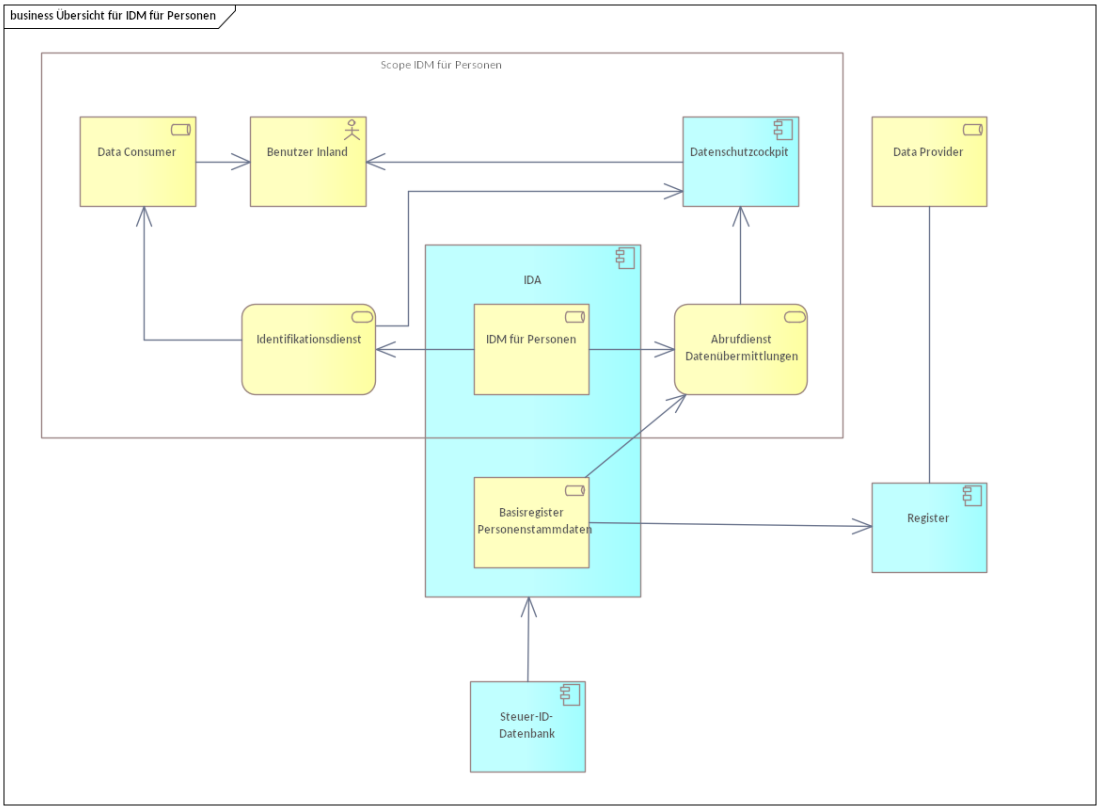


Abbildung 32: Business Übersicht für IDM für Personen

3.6.3.2 Anwender und Systeme

In diesem Kapitel werden die Anwender und Systeme im Kontext von IDM für Personen erläutert. Allgemeine Definitionen der hier genutzten Begriffe finden sich auch im Glossar.

Tabelle 43: Akteure

Akteur	Typ	Beschreibung
Data Consumer	Rolle	System, das nationale Nachweisabrufe unter Verwendung der IDNr. durchführen möchte.
Data Provider	Rolle	System, das nationale Nachweise liefert. Hier werden nur Data Provider betrachtet, die Nachweise unter Verwendung der IDNr. liefern.

Akteur	Typ	Beschreibung
Datenschutzcockpit	Komponente	Komponente, über die Bürgerinnen und Bürger (neben sonstigen Datenübermittlungen unter Verwendung der IDNr.) Abrufe der IDNr. aus dem IDM für Personen nachvollziehen können.
IDM für Personen	Rolle	Komponente des NOOTS. Wird durch IDA bereitgestellt.
Basisregister Personenstammdaten	Rolle	Liefert Personenstammdaten zu einer IDNr. Ermöglicht die initiale Zuordnung von IDNr. und Personendatensatz in den Registern.
Identifikationsdienst	Fachlicher Dienst	Dienst um die IDNr. für eine natürliche Person abzurufen. Wird vom IDM für Personen angeboten.
Abrufdienst Datenübermittlungen	Fachlicher Dienst	Dienst um protokollierte Datenabrufe unter Verwendung der IDNr. abzurufen. Wird sowohl vom IDM für Personen als auch vom Basisregister Personenstammdaten angeboten.
IDA	IT-System	Implementiert sowohl IDM für Personen als auch das Basisregister für Personendaten. Entwickelt und betrieben durch das BVA.
Steuer-ID-Datenbank	IT-System	Datenhaltung für Personenstammdaten und Identifikationsnummern beim BZSt.

3.6.3.3 Use-Cases

Im Folgenden werden die Use-Cases von IDM für Personen beschrieben. Die Nummerierung der Use-Cases wurde aus dem IDA Verfahren übernommen. Die nicht durchgängige Nummerierung ist darauf zurückzuführen, dass in IDA auch Use-Cases existieren, die nicht für IDM für Personen benötigt werden.

Tabelle 44: Use-Case 1: IDM für Personen

Use-Case ID	**UC_1**
Kurzbeschreibung	Bevor ein Data Consumer einen Nachweisabruf unter Verwendung der IDNr. durchführen kann, muss er diese in Erfahrung bringen. Dazu nutzt er diesen Use-Case.
Anmerkung	IDM für Personen hat keine Kenntnis darüber, in welchem Kontext welcher Nachweis abgerufen werden soll und ob die Verwendung der IDNr. dafür zulässig ist.
Akteure	Data Consumer
Vorbedingung/ auslösendes Ereignis	Ein Data Consumer möchte einen Nachweis unter Verwendung der IDNr. von einem nationalen Data Consumer abrufen und benötigt zu diesem Zweck die IDNr. der Person, für die der Nachweisabruf erfolgen soll.
Nachbedingung/ Ergebnisse	Der Data Consumer kennt die IDNr. der Person, für die der Nachweisabruf erfolgen soll.
Standardablauf	1. Der Data Consumer authentifiziert sich bei IDM für Personen 2. Der Data Consumer übermittelt einen Abruf der IDNr. mittels der XBasisdaten-Schnittstelle. Dazu übermittelt er mindestens den Familiennamen, den Wohnort, die Postleitzahl sowie das Geburtsdatum der betroffenen Person (§6 Abs. 3 Nr. 1 IDNrG). 3. IDM für Personen prüft mithilfe der Komponente IAM für Behörden, ob der Data Consumer für die Verwendung dieses Use-Case berechtigt ist. Ist die nicht der Fall, wird die Abfrage mit einer Fehlermeldung abgelehnt. 4. Das IDM für Personen ermittelt die IDNr. der betroffenen Person in der Steuer-ID-Datenbank des BZSt. 5. Kann die IDNr. eindeutig ermittelt werden, liefert IDM für Personen diese an den Data Consumer zurück.
Alternativer Ablauf	4. Kann die IDNr. nicht oder nicht eindeutig ermittelt werden, liefert IDM für Personen eine neutrale Antwort. Aus der neutralen Antwort geht nicht hervor, aus welchen Gründen kein eindeutiger Treffer geliefert werden konnte.

Tabelle 45: Use-Case 10 IDM für Personen

Use-Case ID	**UC_10**
Kurzbeschreibung	Über das Datenschutzcockpit kann eine Bürgerin oder Bürger alle Datenübermittlungen unter Verwendung seiner IDNr. nachvollziehen. Das Datenschutzcockpit ruft dann von allen potenziell betroffenen Registern alle betroffenen Datenübermittlungen ab.
Anmerkung	IDM für Personen muss Aufrufe von UC_1 protokollieren und für den Betrachtungszeitraum von zwei Jahren aufbewahren, damit das Datenschutzcockpit diese abrufen kann. Das Datenschutzcockpit darf die IDNr. der Nutzenden nicht speichern. Es muss sie zunächst über UC_1 in Erfahrung bringen, bevor UC_10 ausgeführt werden kann. Die Übermittlung der Protokolldaten ist hier vereinfacht dargestellt. Eine detailliertere Darstellung ist dem XDatenschutzcockpit Standard zu entnehmen.
Akteure	Datenschutzcockpit
Vorbedingung/ auslösendes Ereignis	Eine Bürgerin oder Bürger hat sich beim Datenschutzcockpit angemeldet. Darin lässt er sich die ihn betreffenden Datenübermittlungen unter Verwendung seiner IDNr. für einen Suchzeitraum von maximal zwei Jahren anzeigen. Das Datenschutzcockpit hat die IDNr. der angemeldeten Nutzenden über UC_1 abgerufen.
Nachbedingung/ Ergebnisse	Das Datenschutzcockpit zeigt alle Übermittlungen der betroffenen IDNr. mittels UC_1 im Laufe des Suchzeitraums an.
Standardablauf	1. Das Datenschutzcockpit authentifiziert sich gegenüber IDM für Personen 2. Das Datenschutzcockpoit übermittelt die Anfrage nach Protokolldaten unter Verwendung der IDNr. der dort angemeldeten Nutzenden und des von den Nutzenden gewählten Suchzeitraums mittels der XDatenschutzcockpit Schnittstelle. 3. IDM für Personen ermittelt alle Übermittlungen von UC_1 für die übergebene IDNr. und den übergebenen Suchzeitraum und liefert diese an das Datenschutzcockpit zurück.

Use-Case ID	UC_10
	4. Das Datenschutzcockpit zeigt die gefundenen Übermittlungen an.
Alternativer Ablauf	3. Wurden keine Übermittlungen gefunden, liefert IDM für Personen eine leere Treffermenge.

3.6.4 Technisches Konzept

3.6.4.1 Nicht-funktionale Anforderungen

Die folgenden nicht-funktionale Anforderungen stellen einen Auszug der Anforderungen aus IDA dar.

Tabelle 46: Nicht-funktionale Anforderung IDM Personen

ID	Kriterium	Anforderung
Leistungseffizienz		
NFA_L001	Zeitverhalten	Synchrone Anfragen werden • zu 80% unter 1 Sekunde, • zu 95% unter 2 Sekunden beantwortet. Asynchrone Anfragen werden möglichst schnell, aber spätestens in 24 Stunden beantwortet.
NFA_L003	Kapazität (Durchsatz)	Im regulären Wirkbetrieb müssen bis zu 300 Auskunftsanfragen pro Sekunde verarbeitet werden. Die Anbindung weiterer Verfahren ist hierbei nicht berücksichtigt. Diese Anforderung ist bei jeder Ausbaustufe zu überprüfen und zu aktualisieren.
NFA_L005	Skalierbarkeit	Das System muss so ausgelegt werden, dass perspektivisch bei Lastspitzen eine automatische Skalierung erfolgen kann.

ID	Kriterium	Anforderung
		Diese Anforderung ist bei jeder Ausbaustufe, in der weitere Verfahren angebunden werden, zu aktualisieren.
Zuverlässigkeit		
NFA_Z001	Verfügbarkeit	Das Gesamtverfahren muss vorbehaltlich ausreichender Verfügbarkeit der Steuer-ID-Datenbank perspektivisch zu 99,9%, 24x7, verfügbar sein.
Sicherheit		
NFA_S001	Vertraulichkeit	Es muss eine hohe Vertraulichkeit (gemäß Schutzbedarf) gewährleistet werden.
NFA_S002	Vertraulichkeit	Nach Abschluss eines Geschäftsvorfalls sind die verarbeitenden Basisdaten in keinem System/Datenbestand der Identitätsdatenabruf-Komponente (mit Ausnahme der Protokolldaten) gespeichert.
NFA_S003	Integrität	Es muss eine hohe Integrität (gemäß Schutzbedarf) gewährleistet werden.
NFA_S004	Nachweisbarkeit	Alle Geschäftsvorfälle müssen lückenlos und nachvollziehbar protokolliert werden.
NFA_S005	Authentizität	Die Authentizität der Nutzenden muss in allen Fällen sichergestellt werden.
Kompatibilität		
NFA_K001	Interoperabilität	Um die Nutzungsschwelle gering zu halten, sollen mehrere benutzergruppenspezifische Schnittstellen auf Basis deutscher und internationaler Standards angeboten werden.

3.6.5 Ausblick & Weiterführende Aspekte

3.6.5.1 Offene Punkte

Tabelle 47: Offene Punkte

ID	Beschreibung
[OP_01]	Wenn der Abruf der IDNr. eine neutrale Antwort liefert, kann der Data Consumer den Nachweis dann auch ohne IDNr abrufen, oder muss der gesamte Prozess abgebrochen werden?
[OP_02]	Die Aufteilung von IDA in IDM für Personen und Basisregister Personenstammdaten ist konsistent zum Zielbild des IT-PLR. Bei der Komponente IDM für Unternehmen sollte eine analoge Trennung vorgenommen werden.

3.7 Datenschutzcockpit

3.7.1 Überblick

Begriffsänderung

In der ursprünglichen Fassung des RegMoG wurde diese Komponente als Datencockpit bezeichnet. Mit dem BeamtEReg/DienstRÄndG (BGBl I 2021, 2250) wurde die offizielle Bezeichnung in Datenschutzcockpit geändert.

Definition

Das Datenschutzcockpit ist ein IT-Verfahren, welches Bürgerinnen und Bürger ermöglicht, sich digital über die Datenübermittlungen zwischen Behörden zur eigenen IDNr. informieren zu können.

Kernaufgabe des Datenschutzcockpits ist das Anzeigen von Datenübermittlungen zwischen öffentlichen Stellen, die unter Nutzung der neu einzuführenden Identifikationsnummer (IDNr.) stattgefunden haben. Diese Datenübermittlungen sind seitens der registerführenden Stellen und der Registermodernisierungsbehörde gem. RegMoG, Art. 1 §2, §9 zu protokollieren und können dann von Bürgerinnen und Bürger im Datenschutzcockpit einfach, transparent und zeitnah abgerufen und nachvollzogen werden.

Rechtliche Grundlagen

Das RegMoG sieht die Einführung und Verwendung einer Identifikationsnummer in der öffentlichen Verwaltung vor.

Artikel 21 des RegMoG in Verbindung mit Art. 2 §11 RegMoG enthält eine Übergangsregelung für die Pilotierung des Datenschutzcockpits. Die Identifikationsnummer darf regional begrenzt als zusätzliches Ordnungsmerkmal im Personenstandsregister, Melderegister und der Elterngeldstellen gespeichert werden und ist auf die Beantragung von Elterngeld sowie Anzeige von Geburt und Namensbestimmung beschränkt. Diese Regelung gilt bis zum Inkrafttreten der Einführung der Identifikationsnummer im RegMoG.

Gemäß Art. 2 §10 RegMoG wird unter einem „Datenschutzcockpit" eine IT-Komponente im Portalverbund[4] verstanden, mit der sich Bürgerinnen und Bürger Auskünfte zu Datenübermittlungen (gemäß §5 IDNrG) zwischen öffentlichen Stellen anzeigen lassen können.

3.7.2 Fachliches Konzept

Zielsetzung

Das Datenschutzcockpit sieht folgende Ziele vor:

- Herstellung von Transparenz über Datenübermittlungen unter Nutzung der IDNr. für betroffene natürliche Personen (siehe Schritt 3 „Statusabfrage“)
- Herstellung von Transparenz über die in Registern zur Person erfassten Daten für betroffene natürliche Personen (siehe Schritte 4-5 „Protokolldatenabfrage und Inhaltsdatenabfrage“)

Zuständigkeiten

- Die Freie Hansestadt Bremen entwickelt im Auftrag des Bundesministeriums des Innern und für Heimat (BMI) das bundesweite Datenschutzcockpit. Die Rolle des Auftraggebers wird voraussichtlich ab 2023 vom BMI auf das Bundesverwaltungsamt (BVA) übertragen.
- Das Datenschutzcockpit wird durch Dataport betrieben.
- Die Entwicklung des XÖV-Standards „XDatenschutzcockpit“ wird durch die Koordinierungsstelle für IT Standards beim Senator für Finanzen Bremen (KoSiT) erarbeitet.

Der funktionale Ablauf des Datenschutzcockpits

Die Ablaufbeschreibung im Datenschutzcockpit unterteilt sich dabei in die folgenden Schritte:

1 **Anmeldung**:

- Die Nutzenden melden sich mit dem elektronischen Personalausweis im Datenschutzcockpit unter dem Vertrauensniveau „hoch“ an.

[4] Gemäß §1 OZG sind Bund und Länder verpflichtet, ihre Verwaltungsleistungen auch elektronisch über Verwaltungsportale anzubieten sowie die Verwaltungsportale miteinander zu einem Portalverbund zu verknüpfen.

- Nach der Authentifizierung stehen dem Datenschutzcockpit neben dem dienst- und kartenspezifischen Merkmal auch Personendaten aus dem Personalausweis zur Verfügung. Es dient der eindeutigen elektronischen Wiedererkennung eines elektronischen Identitätsnachweises mit dem Personalausweis oder mit einem mobilen Endgerät. Gemäß §2 Abs 5 Satz 1 PAuswG wird unter einem dienste- und kartenspezifischen Merkmal eine Zeichenfolge verstanden, die im Speicher- und Verarbeitungsmedium des Personalausweises oder eines mobilen Endgeräts berechnet wird.
- Anhand des dienst- und kartenspezifischen Merkmals ermittelt das Datenschutzcockpit, ob die Nutzenden schon registriert sind. Für registrierte Nutzende kann das Datenschutzcockpit im Konto der Nutzenden die Identifikationsnummer abrufen und mit der Statusabfrage fortfahren, siehe unten.

2 Registrierung (sofern nicht bereits registriert):

- Die Identifikationsnummer wird in der regional begrenzten Pilotierung des Datenschutzcockpits aus dem Meldewesen ermittelt, in einer späteren Ausbaustufe (überregionale Erprobung) über den Identitätsdatenabruf (IDA) der Registermodernisierungsbehörde.
- Das Datenschutzcockpit stellt dazu die XMeld-konforme Anfrage an das regionale Melderegister zur Ermittlung der Identifikationsnummer. In der späteren Ausbaustufe stellt das Datenschutzcockpit die XBasisdaten-konforme Anfrage zur Ermittlung der Identifikationsnummer an IDA. Die Anfrage erfolgt mit den aus dem Personalausweis stammenden Personendaten der Nutzenden.
- Wenn die Identifikationsnummer vorliegt, legt das Datenschutzcockpit für die Nutzenden ein Konto bestehend aus dem dienst- und kartenspezifischen Merkmal und der Identifikationsnummer an. Die Nutzenden gelten danach als im Datenschutzcockpit registriert.

3 Statusabfrage: Die Nutzenden erhalten die Information, ob Daten zu ihrer IDNr. zwischen Behörden im Suchzeitraum (maximal 24 Monate zurück) ausgetauscht wurden (Ja/Nein-Antwort):

- Die Nutzenden lösen im Datenschutzcockpit eine Statusabfrage (siehe Tabelle 1) an die angebundenen Register aus, ob diese unter Verwendung der Identifikationsnummer der Nutzenden Daten übermittelt haben.

- Das Datenschutzcockpit reicht die XDatenschutzcockpit-konforme Statusabfrage mit der Nutzer-Identifikationsnummer an alle angebundenen Register weiter.
- Das Register nimmt die Statusabfrage über die XDatenschutzcockpit-konforme Schnittstelle entgegen.
- Das Register prüft, ob Datenübermittlungen für die übergebene Identifikationsnummer im Protokolldatenspeicher vorhanden sind.
- Das Register übermittelt eine XDatenschutzcockpit-konforme Antwort, ob Datenübermittlungen stattgefunden haben oder nicht.
- Das Datenschutzcockpit reicht die Statusantworten an den Browser der Nutzenden weiter und zeigt diese dort in nahezu Echtzeit an.

4 **Protokolldatenabfrage:** Die Nutzenden werden mit den folgenden Inhalten informiert (1) Anlass (d. h. bei welchem Antrag), (2) Kategorien an Daten, (3) Zeitpunkt der IDNr.-Nutzung und (4) von welcher Behörde & an welche Behörde:

- Die Nutzenden wählen eine angezeigte Statusmeldung nach Wunsch aus und lassen sich dazu über einen zweiten Datenabruf die Protokollinformationen zur ausgewählten Datenübermittlung von dem Register anzeigen.
- Das Datenschutzcockpit reicht die XDatenschutzcockpit-konforme Protokolldatenanfrage mit der Nutzer-Identifikationsnummer an das von den Nutzenden ausgewählte Register weiter.
- Das ausgewählte Register nimmt die Protokolldatenabfrage über die XDatenschutzcockpit-konforme Schnittstelle entgegen.
- Das Register sucht die ausgewählte Datenübermittlung für die übergebene Identifikationsnummer im Protokolldatenspeicher.
- Das Register übermittelt aus den ausgewählten Protokolldaten eine XDatenschutzcockpit-konforme Antwort.
- Das Datenschutzcockpit reicht die Protokolldatenantwort an den Browser der Nutzenden weiter und zeigt diese dort in nahezu Echtzeit an.

5 **Inhaltsdatenabfrage:** Die Nutzenden haben die Möglichkeit, ausführliche Informationen (d. h. den Inhalt der Übermittlung) zu einer spezifischen Datenübermittlung zu erhalten, die bei der Protokolldatenabfrage aufgelistet wurde:

- Die Nutzenden wählen eine angezeigte Protokolldatenantwort nach Wunsch aus und lassen sich dazu über einen dritten Datenabruf die Inhaltsinformationen zur ausgewählten Datenübermittlung von dem Register anzeigen.
- Das Datenschutzcockpit reicht die XDatenschutzcockpit-konforme Inhaltsdatenabfrage mit der Nutzer-Identifikationsnummer an das von den Nutzenden ausgewählte Register weiter.
- Das ausgewählte Register nimmt die Inhaltsdatenabfrage über die XDatenschutzcockpit-konforme Schnittstelle entgegen.
- Das Register sucht die ausgewählte Datenübermittlung für die übergebene Identifikationsnummer im Protokolldatenspeicher.
- Das Register übermittelt aus den ausgewählten Inhaltsdaten eine XDatenschutzcockpit-konforme Antwort.
- Das Datenschutzcockpit reicht die Inhaltsdatenantwort an den Browser der Nutzenden weiter und zeigt diese dort in nahezu Echtzeit an.
- Das Datenschutzcockpit löscht nach Beendigung der Sitzung bzw. nach Abmeldung der Nutzenden alle Auskunftsdaten im Browser und dem Datenschutzcockpit.
- Bei der Abmeldung werden die Nutzenden gefragt, ob das in Schritt 2 ("Registrierung") im Zuge der Registrierung angelegte Konto gelöscht werden soll. Wird dies verneint, bleiben die Nutzenden registriert und die Identifikationsnummer muss von IDA bei der nächsten Benutzung durch die Nutzenden nicht erneut vom Datenschutzcockpit abgefragt werden.

Ergänzend zur textuellen Beschreibung ist die Ablaufbeschreibung im Datenschutzcockpit in der folgenden Abbildung dargestellt:

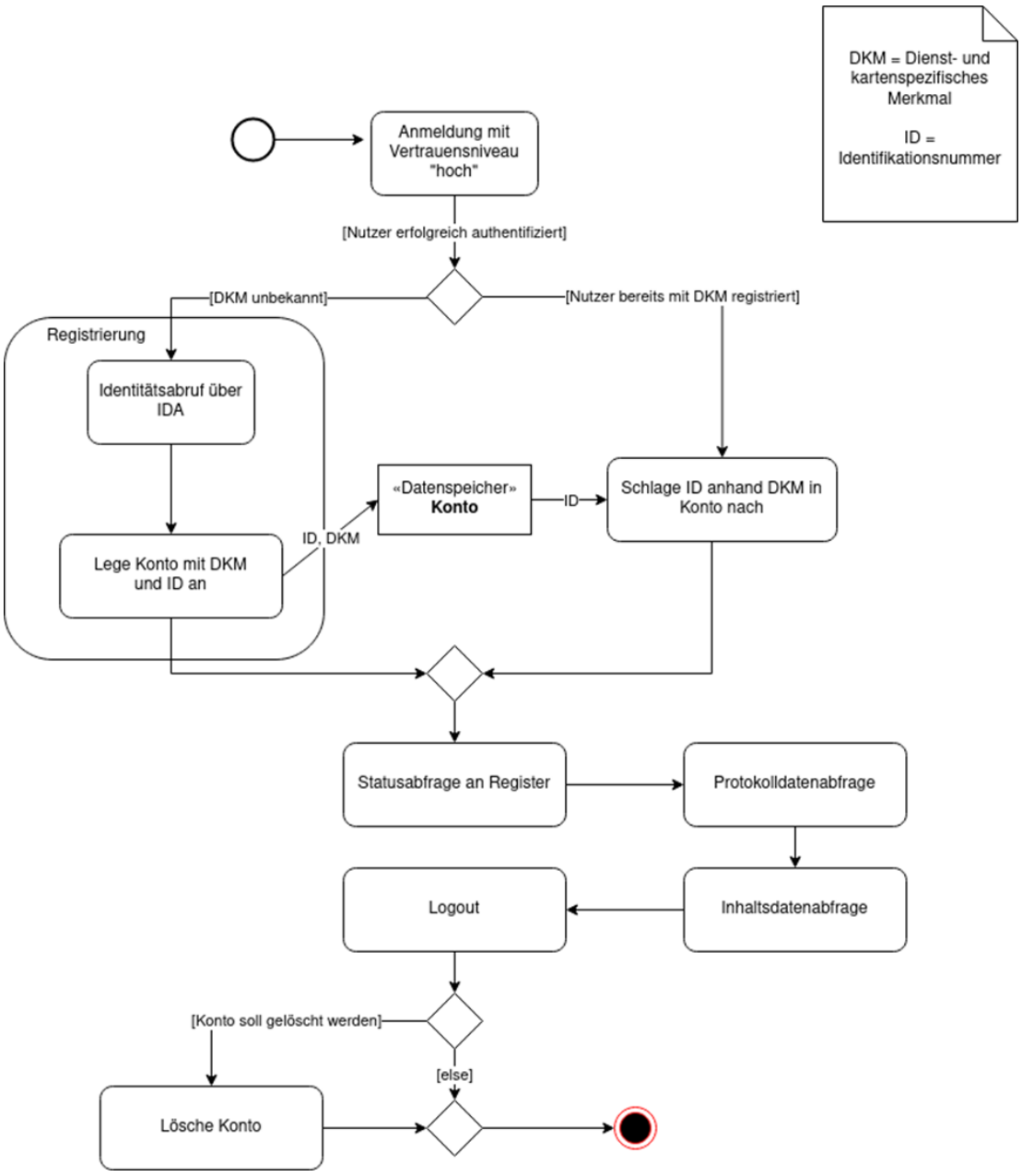


Abbildung 33: Grafische Ablaufbeschreibung im Datenschutzcockpit

Aufgaben der Register in Bezug auf das Datenschutzcockpit

Register müssen folgende Aufgaben wahrnehmen (sofern sie in der Anlage 1 zum IDNrG aufgeführt sind):

- Vorbedingungen erfüllen, d. h. (1) Einspielung der IDNr. in Fachregister und (2) gesetzkonforme Verarbeitung der IDNr.
- Anbindung an das Datenschutzcockpit

- Bereitstellung von bürgerlesbaren Daten zu einer IDNr. entsprechend dem mehrstufigen Registerdatenabruf. Der mehrstufige Registerdatenabruf ist im Standard XDatenschutzcockpit definiert.
- Protokollierung zur Datenübermittlung unter Nutzung einer IDNr.
- Verschlüsselte Datenübermittlung über Vermittlungsstellen, die dem aktuellen Stand von Sicherheit und Technik entsprechen muss (§7 Abs. 2 IDNrG)

3.7.3 Technisches Konzept

Das Datenschutzcockpit wird als zentrale bundesweite digitale IT-Lösung betrieben und verfügt über folgende Schnittstellen, siehe folgende Tabelle:

Tabelle 48: Schnittstellen zwischen dem Datenschutzcockpit und externen System sowie Zuordnung zum funktionalen Ablauf

Schnittstelle	**Funktionaler Ablauf**
Zur Bürgerin oder Bürger über eine Web-Oberfläche.	Alle Schritte
Zum Governikus Mercury-Service für eine Authentifizierung des Bürgers mit Hilfe eines elektronischen Personalausweises oder eines elektronischen Aufenthaltstitels.	Schritt 1 (Anmeldung)
Zur IT-Lösung Identitätsdatenabruf IDA, die durch das BVA verantwortet wird. Mit Hilfe der IDA kann das Datenschutzcockpit die IDNr. des Bürgers ermitteln. Die Kommunikation erfolgt auf Grundlage des Datenaustauschstandards XBasisdaten.	Schritt 2 (Registrierung)
Zu Fachregistern, die die Daten im Rahmen des mehrstufigen Registerdatenabrufs an das Datenschutzcockpit bereitstellen. Die Kommunikation mit den Fachregistern erfolgt über OSCI-Intermediäre. Die Kommunikation erfolgt auf Grundlage des Datenaustauschstandards XDatenschutzcockpit.	Schritte 3-5 (Abfragen)

Im Kontext der Kommunikation des Datenschutzcockpits mit anderen Stellen werden zwei Standards verwendet:

- Der Standard XDatenschutzcockpit beschreibt die Datenübermittlungen zwischen dem Datenschutzcockpit und den öffentlichen und registerführenden Stellen sowie entsprechende Datenstrukturen.
- Der Standard XBasisdaten ist ein Standard des Bundesverwaltungsamtes (BVA) für den elektronischen Datenaustausch mit registerführenden Stellen und weiteren öffentlichen Stellen im Rahmen des Identitätsdatenabrufs nach dem Identifikationsnummerngesetz (IDNrG).

3.7.4 Ausblick & Weiterführende Aspekte

- Aktuell findet eine lokal begrenzte Pilotierung durch Anbindung des Melderegisters der Freien Hansestadt Bremen an das Datenschutzcockpit bis Q4 2022 / Q1 2023 statt. Der Fokus liegt beim technischen Durchstich und anschließend bei der Testung in einem kleinen Rahmen. Eine fachliche Freigabe für die lokal begrenzte Pilotierung durch das Bürgeramt ist noch in Abstimmung. Bis dahin erfolgen eingeschränkte Nutzertests auf einer Testumgebung mit Fokus auf die Bedienbarkeit des DSC.
- Ab dem Jahr 2023 ist geplant, mit einer nationalen Erprobung zu beginnen. Bei dieser Erprobung soll das Datenschutzcockpit an ein nationales Fachregister mit großer Reichweite und dem Identitätsdatenabruf über XBasisdaten angebunden werden.
- Voraussichtlich wird Ende Dezember 2022 der Standard „XDatenschutzcockpit“ in der ersten Version unter www.xrepository.de veröffentlicht und kontinuierlich über den Gesamtzeitraum der Registermodernisierung bis 2025 weiterentwickelt.

3.8 Vermittlungsstellen

3.8.1 Überblick

3.8.1.1 Ausgangslage

Mit der Einführung der Identifikationsnummer (IDNr.) nach dem Identifikationsnummerngesetz (IDNrG) wird ein übergreifendes Ordnungsmerkmal für die öffentliche Verwaltung geschaffen, das die zuverlässige Identifikation von Bürgern in deutschen Registern ermöglichen soll. Dabei muss sichergestellt werden, dass die unzulässige Zusammenführung von Personendaten und die Bildung von Persönlichkeitsprofilen verhindert wird. Aus diesem Grund schreibt das § 7 Absatz 2 IDNrG vor, dass Datenübermittlungen unter Nutzung der Identifikationsnummer zwischen öffentlichen Stellen verschiedener Verwaltungsbereiche über Vermittlungsstellen erfolgen soll.

3.8.1.2 Ziel

Vermittlungsstellen sind dritte öffentliche Stellen und übermitteln berechtigte Nachweisabrufe zwischen Data Consumer und Data Provider. Vermittlungsstellen sind ein zentraler Baustein in der Überwachung und Protokollierung des Nachweisabrufs. Im Rahmen der Konzeption der Vermittlungsstellen ist vorgesehen, eine mögliche Ertüchtigung der bestehenden Transportinfrastruktur zur Bereitstellung der nach § 7 Absatz 2 IDNrG geforderten Funktionalitäten zu untersuchen.

Vermittlungsstellen müssen öffentliche Stellen im Sinne des § 2 BDSG sein und verantworten den sicheren, verlässlichen und nachvollziehbaren Transport elektronischer Nachrichten zwischen öffentlichen Stellen verschiedener Bereiche. Der Datenaustausch über Vermittlungsstellen muss verschlüsselt in gesicherten Verfahren erfolgen, die dem aktuellen Stand von Sicherheit und Technik entsprechen. Vermittlungsstellen müssen ihre Aufgaben ohne Kenntnis der Nachrichteninhalte erbringen können. Insbesondere kontrollieren und protokollieren Vermittlungsstellen abstrakt die Übermittlungsberechtigung. Die abstrakte Berechtigungsprüfung wird in Kapitel 3.8.3.2 beschrieben. Liegt die Übermittlungsberechtigung nicht vor, z.B. wenn für die Datenübermittlung keine Rechtsgrundlage besteht oder bei denen die Angaben zu Sender, Empfänger und Zweck nicht zueinander passen, müssen Vermittlungsstellen sicherstellen, dass keine personenbezogenen Daten übermittelt werden.

3.8.1.3 Zeitplanung

Die folgende Zeitplanung stellt die bisherige Bearbeitung der Vermittlungsstellen dar und muss im Rahmen der weiteren Konzeption geprüft und fortgeschrieben werden.

Tabelle 49: Zeitplan Vermittlungsstellen

Meilenstein	Datum	Verantwortlichkeit
Einführung von Vermittlungsstellen durch das Registermodernisierungsgesetz (RegMoG)	28.03.2021	Bundesministeriums des Innern und für Heimat, Bundesverwaltungsamt
Aufnahme der konzeptionellen Untersuchung von Vermittlungsstellen im NOOTS	01.10.2021	Gesamtsteuerung Registermodernisierung - Kompetenzteam Architektur
Entscheidung zur Durchführung einer Studie zur Bewertung der Leistungsfähigkeit und Skalierbarkeit von OSCI und XTA (OSCI-Studie)	01.07.2022	Bundesministeriums des Innern und für Heimat, Bundesverwaltungsamt
Entscheidung zur Unterbrechung der konzeptionellen Untersuchung von Vermittlungsstellen im NOOTS	01.07.2022	Gesamtsteuerung Registermodernisierung - Kompetenzteam Architektur
Vorstellung des Zwischenberichts zur OSCI-Studie im Kompetenzteam Architektur	16.11.2022	Gesamtsteuerung Registermodernisierung - Kompetenzteam Architektur
Entscheidung zur Wiederaufnahme der konzeptionellen Untersuchung von Vermittlungsstellen im NOOTS	16.11.2022	Gesamtsteuerung Registermodernisierung - Kompetenzteam Architektur
Dokumentation erster Erkenntnisse zu Vermittlungsstellen in den nationalen TDDs Version 1.0	31.12.2022	Gesamtsteuerung Registermodernisierung - Kompetenzteam Architektur
Fortsetzung der Konzeption von Vermittlungsstellen für die nationalen TDDs Version 2.0	ab 01.01.2023	Gesamtsteuerung Registermodernisierung - Kompetenzteam Architektur

3.8.1.4 Weiterführende Dokument

Tabelle 50: Weiterführende Dokumente zu den Vermittlungsstellen

Referenz	Dokument	Beschreibung
[SQ-2]	Kabinettsfassung Registermodernisierungsgesetz	Kabinettsfassung des Registermodernisierungsgesetzes
[KT-Arch-003]	Prüffrage KT-Arch-003	Rechtliche Prüffrage KT-Architektur zur "Durchführung einer abstrakten Berechtigungsprüfung".
[SQRV-1]	Bericht der Projektgruppe Meldewesen	Pflege und Weiterentwicklung OSCI-XMeld
[SQRV-2]	Spezifikation des XTA-Standards	Spezifikation des Interoperabilitätsstandards XTA2 in der Version 3
[SQRV-3]	Website KoSIT - OSCI & XTA	Website des Herausgebers des Interoperabilitätsstandards XTA2
[SQRV-4]	Entwurfsprinzipien des OSCI-Standards	Entwurfsprinzipien des OSCI-Standards in der Version 1.2

3.8.2 Annahmen & Rahmenbedingungen

Tabelle 51: Annahmen - Vermittlungsstellen

ID	Annahme
[ANN_01]	Es wird aktuell davon ausgegangen, dass eine niedrige (noch zu bestimmende) Anzahl von Vermittlungsstellen eingesetzt wird, vgl. dazu [OP_007].
[ANN_02]	Aus § 10 Abs. 2 Onlinezugangsgesetz i.V.m § 9 Abs. 2 Identifikationsnummerngesetz ergibt sich die Anforderung, dass Vermittlungsstellen die Protokolldaten an das Datenschutzcockpit liefern müssen.

Tabelle 52: Rahmenbedingungen - Vermittlungsstellen

ID	Rahmenbedingung
[RMBED_01]	Die im IDNrG beschriebenen Verwaltungsbereiche müssen definiert sein.

3.8.3 Fachliches Konzept

3.8.3.1 Kontext

Das folgende Diagramm zeigt den Systemkontext der Komponente Vermittlungsstellen.

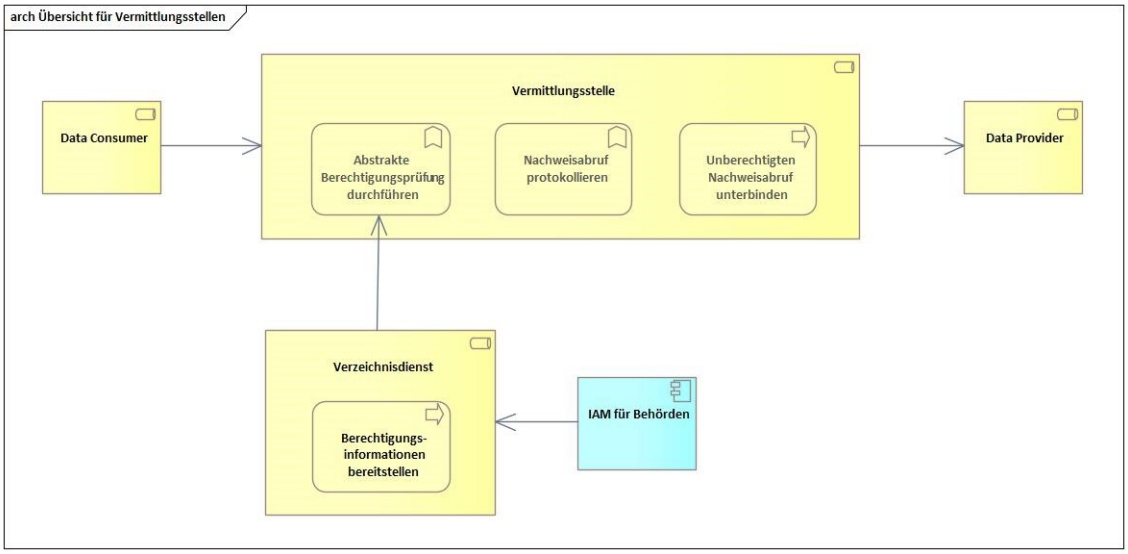


Abbildung 34: Systemkontext Vermittlungsstellen

3.8.3.2 Abstrakte Berechtigungsprüfung nach dem Identifikationsnummerngesetz

In § 7 Abs. 2 IDNrG ist definiert, dass bei der verwaltungsbereichsübergreifenden Datenübermittlung zwischen öffentlichen Stellen unter Verwendung der IDNr. eine abstrakte Berechtigungsüberprüfung der Datenübermittlung über eine dritte Stelle, die sogenannte Vermittlungsstelle, erfolgen muss.

Die abstrakte Berechtigungsprüfung sieht vor, dass ein Datenaustausch zwischen einem Data Consumer und einem Data Provider nur dann erfolgen darf, wenn eine Berechtigung zum Austausch eines spezifischen Nachweises zu einem gegebenen Zweck vorliegt.

Zur Prüfung der Berechtigung greift die Vermittlungsstelle auf einen Vermittlungs- bzw. Verzeichnisdienst zurück. Die Vermittlungsstelle muss, zur Vermeidung der Profilbildung, in der Lage sein, die Berechtigungsprüfung ohne Kenntnis der Nachrichteninhalte durchzuführen. Entsprechend ist es erforderlich, die am Nachrichtenaustausch beteiligten Data Consumer und Data Provider, den Nachweistyp sowie den Zweck des Nachweisabrufs anhand von Metadaten ermitteln zu können.

Liegt abstrakt eine Übermittlungsberechtigung zwischen Sender und Empfänger für den angegebenen Zweck nicht vor, so erfolgt keine Datenübermittlung. Die Vermittlungsstelle muss die Datenübermittlung inkl. der Berechtigungsprüfung zudem protokollieren.

3.8.3.3 Anforderungen an Vermittlungsstellen

Die aktuell bekannten Anforderungen an Vermittlungsstellen der Registermodernisierung leiten sich größtenteils aus dem IDNrG und seiner Begründung, insbes. § 7 IDNrG und §9 IDNrG, sowie aus dem § 10 OZG ab. Dementsprechend ergibt sich die Einschätzung der Priorität als hoch für die betreffenden Anforderungen. Die abstrakte Berechtigungsprüfung ist auch Untersuchungsgegenstand im KT Recht und Datenschutz ([KT-Arch-003]). Darin getroffene Bewertung wurden ebenfalls in der Anforderungstabelle aufgenommen.

Tabelle 53: Übersicht Anforderungen Vermittlungsstellen

ID	Anforderung	Erläuterung	Priorität
[AFO-VS-01]	Eine Vermittlungsstelle ist eine dritte öffentliche Stelle und muss eingesetzt werden, wenn eine verwaltungsbereichs-übergreifende Datenüber-mittlung zwischen öffentlichen Stellen unter Nutzung der Identifikationsnummer erfolgt.	Für andere Datenübermittlungen ist es ebenfalls möglich, Vermittlungsstellen einzusetzen.	hoch
[AFO-VS-02]	Eine Vermittlungsstelle fungiert bei bereichsübergreifender Datenübermittlung als	Data Consumer und Data Provider dürfen nicht direkt miteinander kommunizieren. In ihrer Funktion als Gateway	hoch

ID	Anforderung	Erläuterung	Priorität
	Gateway, sie ist in der Kommunikation zwischen Data Consumer und Data Provider zwischengeschaltet.	stellt eine Vermittlungsstelle Transportinfrastruktur zur Verfügung und kann ihre Aufgaben bzgl. Protokollierung und Berechtigungsprüfung wahrnehmen sowie ggf. die Kommunikation zwischen den beteiligten Parteien unterbinden.	
[AFO-VS-03]	Eine Vermittlungsstelle muss ihre Aufgaben ohne Kenntnis des Nachrichteninhaltes erbringen. Sie hat lediglich Zugriff auf Metadaten der Kommunikation, die sie zur Durchführung ihrer Aufgaben benötigt (bspw. nachweisabrufende Stelle, nachweisliefernde Stelle, Grund der Datenübermittlung, Zeitstempel).	Die Übertragung der personenbezogenen Daten zwischen Data Consumer und Data Provider erfolgt (aus Sicht der Vermittlungsstelle) Ende-zu-Ende-verschlüsselt.	hoch
[AFO-VS-04]	Eine Vermittlungsstelle muss eine abstrakte Berechtigungsprüfung durchführen. Dazu prüft sie, ob Sender und Empfänger zu einem anzugebenden Zweck kommunizieren dürfen. Liegt eine solche Berechtigung nicht vor, so muss die Vermittlungsstelle die Datenübermittlung unterbrechen ("Wächterfunktion").	Abstrakt bedeutet in diesem Kontext, dass die Vermittlungsstelle keine Einsicht in den konkreten Nachrichteninhalt hat, sondern ausschließlich anhand der Metadaten das Vorliegen einer Berechtigung zur Datenübermittlung zwischen Sender und Empfänger prüft.	hoch
[AFO-VS-05]	Für die abstrakte Berechtigungsprüfung muss eine Vermittlungsstelle Anschluss an einen Vermittlungs- bzw. Verzeichnisdienst haben, der die Zweckprüfung ermöglicht.	Die Vermittlungsstelle erhält von dem Vermittlungs- bzw. Verzeichnisdienst die Information, ob es für den angegebenen Zweck und die angegebenen Kommunikationspartner einen entsprechenden Eintrag gibt.	hoch

ID	Anforderung	Erläuterung	Priorität
[AFO-VS-06]	Eine Vermittlungsstelle muss den Transport elektronischer Nachrichten und die abstrakte Berechtigungs-prüfung protokollieren.		hoch
[AFO-VS-07]	Eine Vermittlungsstelle muss die datenschutzrechtliche Prüfung von Datenübermittlungen durch die Bürgerin und Bürger unterstützen. Dazu liefert sie die Protokolldaten an das Datenschutzcockpit.	Basiert auf Annahme [ANN_02], Verifikation durch KT Recht offen. Prinzipiell könnte eine Anbindung an das Datenschutzcockpit auch aus Sicht der Gesamt-Architektur sinnvoll erscheinen, vgl. [OP_05]	hoch
[AFO-VS-07a]	Für die datenschutzrechtliche Prüfung von Datenübermittlungen durch die Bürgerin und Bürger im Datenschutzcockpit muss die Vermittlungsstelle die Zuordnung der Protokolldaten zu den ihr unbekannten fachlichen Inhaltsdaten ermöglichen.	Basiert auf Annahme [ANN_02], Verifikation durch KT Recht offen. Prinzipiell könnte eine Anbindung an das Datenschutzcockpit auch aus Sicht der Gesamt-Architektur sinnvoll erscheinen, vgl. [OP_05]	hoch
[AFO-VS-08]	Die Vermittlungsstelle muss die Protokolldaten nach §9 IDNrG zwei Jahre aufbewahren und anschließend unverzüglich löschen.		hoch

3.8.3.4 Vermittlungsstellen in anderen Kontexten

Der Terminus "Vermittlungsstelle" wird bereits in anderen Kontexten verwendet und ist dort aber u.U. anders definiert.

Vermittlungsstellen im Meldewesen

In § 2 der Bundesmeldeübertragungsverordnung ([RGVS-03]) wird die Durchführung von regelmäßigen Datenübermittlungen zwischen den Meldebehörden geregelt.

Datenübermittlungen im Meldewesen erfolgen elektronisch unter Zugrundelegung des Datenaustauschformats OSCI-XMeld und Nutzung des Übermittlungsprotokolls OSCI-Transport. Werden Daten zwischen Meldebehörden ausgetauscht, kann dies unmittelbar, über zentrale Meldedatenbestände der Länder, durch sonstige durch das Landesrecht definierte Stellen oder über die über Vermittlungsstellen der Länder erfolgen. Vermittlungsstellen können durch mehrere Länder gemeinsam betrieben werden. In diesem Fall kann die Übermittlung auch in einem von OSCI abweichenden Übermittlungsprotokoll erfolgen, wenn eine gleichwertige Vertraulichkeit, Integrität und Authentizität der übertragenen Daten sichergestellt werden kann. In einem Land kann es mehrere Vermittlungsstellen geben.

In § 2 des Landesmeldegesetz des Landes Mecklenburg-Vorpommern werden die Aufgaben der Vermittlungsstellen weiterführend beschrieben. Für die überörtliche elektronische Datenübermittlung zwischen den Meldebehörden und in andere Bundesländer werden Vermittlungsstellen eingerichtet und mit den Aufgaben der Entgegennahme und Weiterleitung der Anmeldung betraut. Zudem wird beschrieben, dass Meldebehörden im Rahmen der Auftragsdatenverarbeitung (§ 4 des Landesdatenschutzgesetzes) weitere Aufgaben an die Vermittlungsstellen übertragen können.

In einem Bericht der Projektgruppe Meldewesen ([SQRV-1]), der sich mit der Pflege und Weiterentwicklung von OSCI-XMeld beschäftigt hat, werden die zentrale Aufgaben der Vermittlungsstellen des Meldewesens beschrieben. Vermittlungsstellen dienen der Bewältigung von Medienbrüchen, die dann entstehen, wenn Meldebehörden der Länder nicht in der Lage sind, OSCI-konforme Meldungen abzusenden oder entgegenzunehmen. Vermittlungsstellen müssen also die Formatumwandlung von Nachrichten aus Meldebehörden übernehmen, die nach § 5 Abs.2 Satz 1 1. BMeldDÜV nicht fähig sind, die geforderten Kommunikationsstandards einzuhalten.

Ersteinschätzung

Im Meldewesen werden Vermittlungsstellen für die Kommunikation innerhalb eines Bereichs eingesetzt wohingegen Vermittlungsstellen des IDNrG für die bereichsübergreifende Datenübertragung zuständig sind. Auch können Vermittlungsstellen nach IDNrG keine fachlich-inhaltlichen Aufgaben übernehmen, da sie keine Kenntnis des Nachrichteninhalts besitzen dürfen.

Vermittlungsstellen im Interoperabilitätsstandard XTA2

Im Spezifikationsdokument des Interoperabilitätsstandard XTA2 (Version 3) des IT-Planungsrats ([SQRV-02]) werden die am Nachrichtenaustausch beteiligten Rollen beschrieben.

XTA standardisiert den Austausch von Nachrichten zwischen Fach- und Transportverfahren und unterstützt zudem die automatisierte, fachunabhängige Weiterverarbeitung von Nachrichten. XTA bildet die „4-Corner" des Modells auf die Rollen Autor und Leser der Anwendungsebene sowie Sender und Empfänger auf der Transportebene ab. Die Spezifikation legt fest, welche Funktionen von diesen Ebenen grundsätzlich und von den darin enthaltenen einzelnen Rollen im Besonderen zur Verfügung gestellt werden müssen. ([SQRV-03])

- **Leser**: Behörden, an die Fachdaten adressiert wurden und die diese verarbeiten
- **Sender**: Vermittlungsstellen (auch Clearingstellen oder Nachrichtenbroker genannt), die Daten von Behörden entgegennehmen und sie entsprechend der rechtlichen und fachlichen Vorgaben aufbereiten und versenden
- **Empfänger**: Vermittlungsstellen auf der Gegenseite, die Nachrichten vom Sender entgegennehmen
- **Autoren**: Behörden, die in den IT-Fachverfahren die Fachdaten erstellen und sie für den Transport zur Verfügung stellen

Hierbei ist es in der konkreten Ausgestaltung grundsätzlich denkbar, dass einzelne Rollen zusammenfallen.

Ersteinschätzung

Sender und Empfänger gem. XTA2 werden dort auch als Vermittlungsstellen bezeichnet. Ihre Aufgaben bzw. Funktionalitäten weichen jedoch von den Vermittlungsstellen im Sinne der Registermodernisierung ab.

- Aus Sicht des IDNrG müssen Vermittlungsstellen ihre Aufgaben ohne Kenntnis des Nachrichteninhalts erfüllen sowie eine abstrakte Berechtigungsprüfung durchführen.
- Vermittlungsstellen entsprechend XTA2 dürfen Zugriff auf die Nachrichteninhalte erhalten, um Leser oder Autor Mehrwertdienste anzubieten, bspw. eine Transport-Verschlüsselung.

Vermittlungsstellen im OSCI-Standard

Auch im OSCI-Standard gibt es zentrale Instanzen, die (OSCI-) Intermediäre, die – vergleichbar den Vermittlungsstellen der Registermodernisierung – die Kommunikation zwischen zwei Partnern durchführen.

- OSCI-Intermediäre bieten eine Verschlüsselung der Inhaltsdaten an und sind somit in der Lage, Mehrwertdienste zu erbringen, ohne die Vertraulichkeit der ausgetauschten Daten zu gefährden.
- Sie werden vor allem zur (aber nicht ausschließlich) asynchronen Kommunikation eingesetzt, wenn nicht sichergestellt werden kann, dass Sender und Empfänger einer Nachricht zeitgleich erreichbar sind. In diesem Fall wird die Nachricht für eine spätere Abholung zwischengespeichert.
- OSCI-Intermediäre nehmen eine neutrale Rolle ein, können jedoch bei einem der Kommunikationspartner lokalisiert sein.

Ersteinschätzung

OSCI-Intermediäre bieten aktuell nicht alle Funktionalitäten an, die eine Vermittlungsstelle bereitstellen muss.

- Sie unterstützen einen verschlüsselten Nachrichtentransport.
- Eine abstrakte Berechtigungsprüfung sowie eine Protokollierung gem. IDNrG. ist aktuell nicht möglich.

3.8.3.5 Anwender und Systeme

Tabelle 54: Übersicht Anwender und Systeme - Vermittlungsstellen

Akteuer	Typ	Beschreibung
Data Consumer	Rolle	Nationales System, das Nachweisabrufe unter Verwendung der Identifikationsnummer durchführt. Vermittlungsstellen prüfen anhand von Metadaten, ob Data Consumer und Data Provider zum Austausch des abzurufenden Nachweises berechtigt sind.
Data Provider	Rolle	Nationales System, das nationale Nachweise liefert. Vermittlungsstellen prüfen anhand von Metadaten, ob Data Consumer und Data Provider

Akteuer	Typ	Beschreibung
		zum Austausch des abzurufenden Nachweises berechtigt sind.
IAM für Behörden	Komponente	Komponente des NOOTS, verantwortet die Authentifizierung und Autorisierung von öffentlichen Stellen. Liefert Informationen, die der abstrakten Berechtigungsprüfung dienen.
Verzeichnis-dienst	Service	Dienst, der anhand von Kommunikationspartnern und Kommunikationszweck Informationen für die abstrakte Berechtigungsprüfung liefert.
Datenschutz-cockpit	Komponente	Komponente des NOOTS, mit der sich die Bürgerin oder Bürger Auskünfte zu Datenübermittlungen zwischen öffentlichen Stellen anzeigen lassen kann.

3.8.3.6 Use-Cases der Vermittlungsstellen

Bereichsübergreifende Datenübermittlung

Tabelle 55: Use-Case 1: Bereichsübergreifende Datenübermittlung

Use-Case ID	UC-VS-1
Kurzbeschreibung	Datenübermittlung zwischen öffentlichen Stellen verschiedener Bereiche nach IDNrG
Anmerkung	Die Vermittlungsstelle hat keine Kenntnis über die Inhaltsdaten, ihr sind nur die Metadaten der Kommunikation bekannt.
Akteure	• Data Consumer • Data Provider • Verzeichnisdienst • Vermittlungsstelle
Vorbedingung/ auslösendes Ereignis	Ein Data Consumer möchte einen Nachweis unter Verwendung der IDNr. von einem nationalen Data Consumer abrufen.

Use-Case ID	UC-VS-1
Nachbedingung/ Ergebnisse	Die Berechtigung zum Nachweisabruf wird mit positivem Ergebnis geprüft, der Nachweisabruf wird prozessiert und protokolliert.
Standardablauf	1 Der Data Consumer erzeugt einen DE-EDM-Request. Dieser enthält die verschlüsselten Inhaltsdaten und einen definierten Satz an Metadaten, u.a. für die abstrakte Berechtigungsprüfung. 2 Der Data Consumer übermittelt den DE-EDM-Request über das NOOTS an eine Vermittlungsstelle. 3 Die Vermittlungsstelle prüft anhand der Metadaten aus dem DE-EDM-Request, ob der Data Consumer berechtigt ist, einen gesuchten Nachweis zu dem angegebenen Zweck von einem Data Provider abzurufen. Die Vermittlungsstelle prüft dazu, ob im Verzeichnisdienst ein Eintrag für die Kommunikation zwischen Data Consumer und Data Provider zum angegebenen Zweck existiert. 4 Die Vermittlungsstelle übermittelt den DE-EDM-Request an den Data Provider. 5 Die Vermittlungsstelle protokolliert den Übermittlungsvorgang und die abstrakte Berechtigungsprüfung.
Alternativer Ablauf	• In Schritt 3 des Standardablaufs ergibt die abstrakte Berechtigungsprüfung, dass die Berechtigung zum Nachweisabruf nicht vorliegt. 1 Die Vermittlungsstelle unterbricht die Datenübermittlung zwischen Data Consumer und Data Provider. 2 Die Vermittlungsstelle informiert den Data Consumer über das negative Ergebnis der abstrakten Berechtigungsprüfung. • Weiter mit Schritt 5 des Standardablaufs.

Protokolldaten bereitstellen

Tabelle 56: Use-Case 2: Protokolldaten bereitstellen

Use-Case ID	UC-VS-2
Kurzbeschreibung	Bereitstellung der Protokolldaten für die datenschutzrechtliche Prüfung durch die Bürgerinnen und Bürger.
Anmerkung	Die Bürgerin oder der Bürger haben über das Datenschutzcockpit die Möglichkeit, sich Auskünfte zu Datenübermittlungen zwischen öffentlichen Stellen unter Verwendung der IDNr. anzeigen zu lassen. Basiert auf [ANN_02].
Akteure	• Datenschutzcockpit • Vermittlungsstelle
Vorbedingung/ auslösendes Ereignis	Die Bürgerin oder der Bürger ruft über das Datenschutzcockpit die Protokolldaten nach IDNrG ab.
Nachbedingung/ Ergebnisse	Die zur Bürgerin oder Bürger vorliegenden Protokolldaten sind an das Datenschutzcockpit übermittelt und ermöglichen eine Zuordnung zu den der Vermittlungsstelle unbekannten Inhaltsdaten.
Standardablauf	1 Das Datenschutzcockpit fragt von der Vermittlungsstelle die Protokolldaten zu einer IDNr. an. 2 Die Vermittlungsstelle ermittelt die Protokolldaten zur IDNr. 3 Die Vermittlungsstelle übermittelt die Protokolldaten zur IDNr. an das Datenschutzcockpit, sodass eine Zuordnung zu den unbekannten Inhaltsdaten möglich ist.
Alternativer Ablauf	*keiner*

Protokolldaten nach Aufbewahrungsfrist löschen

Tabelle 57: Use-Case 3: Protokolldaten nach Aufbewahrungsfrist löschen

Use-Case ID	UC-VS-3
Kurzbeschreibung	Löschen der IDNr.-bezogenen Protokolldaten (gem. §9 IDNrG) nach der Aufbewahrungsfrist
Anmerkung	Die Vermittlungsstelle Protokolldaten zwei Jahre aufbewahren und dann unverzüglich löschen.
Akteure	Vermittlungsstelle
Vorbedingung/ auslösendes Ereignis	Es liegen Protokolldaten vor.
Nachbedingung/ Ergebnisse	Die Protokolldaten, deren Aufbewahrungsfrist abgelaufen ist, sind gelöscht.
Standardablauf	1 Die Vermittlungsstelle prüft, ob Protokolldaten vorliegen, deren Aufbewahrungsfrist abgelaufen ist. 2 Die Vermittlungsstelle prüft, ob Protokolldaten vorliegen, deren Aufbewahrungsfrist abgelaufen ist. 3 Die Vermittlungsstelle löscht die betreffenden Protokolldaten 4 Die Vermittlungsstelle löscht die betreffenden Protokolldaten.
Alternativer Ablauf	*keiner*

3.8.4 Ausblick & Weiterführende Aspekte

3.8.4.1 Offene Punkte

Die konzeptionelle Ausgestaltung der Vermittlungsstellen sowie der Durchführung der abstrakten Berechtigungsprüfung erfolgt ab dem ersten Quartal 2023 und wird in die zweite Iteration der nationalen TDDs einfließen.

Dabei werden die im folgenden beschriebenen Klärungspunkte adressiert werden.

Tabelle 58: Übersicht Offener Punkte Vermittlungsstellen

Offener Punkt	Bezeichnung	Beschreibung
[OP_01]	Zeitpunkt der abstrakte Berechtigungsprüfung im Nachweisabrufprozess	Das IDNrG trifft keine Aussage dazu, zu welchen Zeitpunkten im Nachweisabrufprozess die Prüfung der Übermittlungsberechtigung durchgeführt werden muss. Die abstrakte Berechtigungsprüfung könnte entweder beim initialen Aufruf des Data Provider (Request) erfolgen, vor der Übermittlung des Nachweises an den Data Consumer (Response) oder in beiden Fällen.
[OP_02]	Steuerung der Vermittlungsstellen	Vermittlungsstellen müssen laut IDNrG und Einschätzung des KT Recht & Datenschutz öffentliche dritte Stellen sein. Um den Nutzen der Vermittlungsstellen (Verhinderung unrechtmäßiger Nachweisabrufe) sicherzustellen, ist es mindestens erforderlich, dass eine Fachaufsicht über die Vermittlungsstellen eingerichtet ist Übersicht über alle Vermittlungsstellen geführt wird Weitere Anforderungen, zum Beispiel zu der Verantwortung für und den Betrieb von Vermittlungsstellen werden gemeinsam durch das KT Architektur und das KT Recht & Datenschutz erhoben.
[OP_03]	Protokolldaten der Vermittlungsstellen	Neben der abstrakten Berechtigungsprüfung definiert das IDNrG, dass Vermittlungsstellen den Datenaustausch protokollieren müssen. Das IDNrG trifft keine Aussage dazu, zu welchem nachgelagerten Zweck die Protokolldaten erhoben werden.
[OP_04]	Nutzung der Protokolldaten durch das Datenschutzcockpit	Die Konzeption des Datenschutzcockpit sieht derzeit keine Nutzung der Protokolldaten Vermittlungsstellen vor, sondern nutzt die Protokolldaten der Register. Der Aufwand, die Ermittlung der Nachweisabrufe über die (wenigen) zentralen

Offener Punkt	Bezeichnung	Beschreibung
		Vermittlungsstellen erfolgen zu lassen, scheint geringer als alle Register einzeln anzufragen. Mögliche Begründung: Durch das IDNrG ist lediglich die Protokollierung von Verwaltungsbereich-übergreifenden nachweisabrufen unter Verwendung der Identifikationsnummer gefordert. Die Vermittlungsstellen würden demnach keine Daten zu Verwaltungsbereich-internen Nachweisabrufen liefern können.
[OP_05]	Verwendbarkeit der OSCI/XTA-Infrastruktur	Zielsetzung gemäß Beschluss 2021/05 des IT-Planungsrats ist nach Möglichkeit die Weiterverwendung bewährter bestehender Infrastruktur, bei Bedarf andernfalls die Entwicklung und Integration neuer Komponenten. Es ist zu prüfen, ob die bestehende OSCI/XTA-Infrastruktur derart erweitert werden kann, dass sie die Anforderungen an die Vermittlungsstellen erfüllt. In diesem Kontext erscheint nach ersten Diskussionen auch eine Betrachtung von Alternativen als sinnvoll, insbes. sind AS4 als europäischer Standard sowie FIT-Connect interessant.
[OP_06]	Ertüchtigung bestehender Vermittlungsstellen	Es muss geprüft werden, ob bereits existierenden Vermittlungsstelle z.B. aus dem Meldewesen für die Verwendung in der Registermodernisierung geeignet sein könnten und ob eine Ertüchtigung dazu führt, dass die Anforderungen aus dem IDNrG abgedeckt werden können.
[OP_07]	Anzahl bzw. Organisation der Vermittlungsstellen	Es ist zu klären, wie viele Vermittlungsstellen eingesetzt werden sollen bzw. benötigt werden und wie diese organisiert sind, z.B. (eine) je Verwaltungsbereich entsprechend IDNrG, (eine) je Land oder eine möglichst geringe Anzahl unabhängiger Vermittlungsstellen.

Offener Punkt	Bezeichnung	Beschreibung
[OP_08]	Kommunikation innerhalb eines Verwaltungsbereichs	Im IDNrG wird gefordert, dass die Kommunikation immer dann über Vermittlungsstellen erfolgen muss, wenn verwaltungsbereichsübergreifende Nachweisabrufe unter Verwendung der Identifikationsnummer durchgeführt werden. Für Nachweisabrufe innerhalb eines Verwaltungsbereichs würde das bedeuten, dass die Funktionen der Vermittlungsstellen (abstrakte Berechtigungsprüfung und Protokollierung) nicht zum Einsatz kommen müssten. Es ist zu prüfen, ob nicht jegliche Kommunikation im NOOTS über Vermittlungsstellen erfolgen sollte. Das hätte zur Folge, dass die abstrakte Berechtigungsprüfung und Protokollierung auch für verwaltungsbereichsinterne Kommunikation eingesetzt werden würde.
[OP_09]	Implikation des 4-Corner-Modell auf Vermittlungsstellen	Hat die Forderung nach einer 4-Corner-Architektur zur Folge, dass in der Kommunikationsstrecke zwischen Data Consumer und Data Provider zwei Vermittlungsstellen zwischengeschaltet werden müssen?
[OP_10}	Zuordnung von Protokolldaten der Vermittlungsstelle zu Inhaltsdaten	Wie ist die Unterstützung der Zuordnung der Protokolldaten der Vermittlungsstelle zu den ihr unbekannten Inhaltsdaten zu berücksichtigen? Gibt es weitere Implikationen?
[OP_11]	Verzeichnisdienst	Welche Komponente liefert die notwendigen Informationen zur Durchführung der abstrakten Berechtigungsprüfung anhand der Kommunikationspartner und des Zwecks der Kommunikation?
[OP_12]	Zusammenwirken mit anderen NOOTS-Komponenten	Das Zusammenwirken zwischen den Vermittlungsstellen und weiteren NOOTS-Komponenten wie dem IDM für Personen und dem IAM für Behörden muss im Rahmen der Konzeption der Vermittlungsstellen berücksichtigt werden.

Offener Punkt	Bezeichnung	Beschreibung
[OP_13]	Datenprotokollierung	Die Vermittlungsstelle muss u.a. nach §7 Abs.2 IDNrG eine Protokollierung durchführen. Zu klären ist, welche Daten (Metadaten, verschl. Inhaltsnachricht) protokolliert werden müssen.
[OP_14]	Speicherung von Protokolldaten	Es muss geklärt werden, ob es Anforderungen gibt, die eine Vorgabe dazu machen, wie die Speicherung der Protokolldaten (gem. §9 IDNrG) zu erfolgen hat.

3.8.4.2 Zukünftige Handlungsfelder

Tabelle 59: Übersicht zukünftiger Handlungsfelder - Vermittlungsstellen

Handlungs-feld	Bezeichnung	Beschreibung	Grob-planung
[HF_01]	Relevanz und Implikation "4-Corner-Modell"	Bewertung der Notwendigkeit eines 4-Corner-Modells in der Registermodernisierung und ggfs. Erfassung von sich daraus ableitenden Anforderungen in Abstimmung mit dem Kompetenzteam Recht & Datenschutz.	Q1 2023
[HF_02]	Untersuchung Transportinfra-struktur	Erfassung und Bewertung der Erkenntnisse zur Zukunftsfähigkeit und Skalierbarkeit von OSCI & XTA und Erarbeitung von Handlungsbedarfen in Abstimmung mit dem Projekt "OSCI-Studie"	Q1 2023
[HF_03]	Anbindung Datenschutz-cockpit	Untersuchung des Zusammenwirkens der Vermittlungsstellen mit dem Datenschutzcockpit in Abstimmung mit dem Umsetzungsprojekt "Datenschutzcockpit"	Q1 2023

Handlungs-feld	Bezeichnung	Beschreibung	Grob-planung
[HF_04]	Grobkonzept Vermittlungs-stellen	Erstellung eines Grobkonzepts zu den Vermittlungsstellen.	Q2 2023
[HF_05]	Entscheidungs-vorlage Vermittlungs-stellen	Erstellung einer Entscheidungsvorlage für den IT-PLR zu den Vermittlungsstellen.	Q2 2023
[HF_06]	Umsetzung Vermittlungs-stellen	Unterstützung bei der Erstellung eines Projektauftrags zur Umsetzung der Vermittlungsstellen.	Q3 2023

3.9 Intermediäre Plattformen

3.9.1 Management Summary

Um der Once-Only-Verpflichtung der SDG-VO zum grenzüberschreitenden Nachweisaustausch mit dem EU-Ausland nachzukommen, setzt Deutschland auf den Einsatz von Intermediären Plattformen. Diese dienen als Mittlerinnen zwischen dem NOOTS und dem EU-OOTS, indem sie Nachweisabfragen aus dem EU-Ausland in nationale Abfragen umwandeln und in das NOOTS weiterleiten, und umgekehrt. Dafür implementieren sie die im jeweiligen System genutzten Technologien und Prozesse.

Dank der Bündelung der EU-spezifischen Anforderungen und Aufgaben für die Anbindung an das EU-OOTS in zentralen Intermediären Plattformen müssen deutsche Nachweislieferanten und deutsche Online-Services diese nicht jeder einzeln umsetzen, sodass Umsetzungsaufwand eingespart wird.

Dabei ist zwischen zwei Typen von Intermediären Plattformen zu unterscheiden. Beide Typen werden in diesem Konzept näher beschrieben. Die hier enthaltenen konzeptionellen Vorgaben sind unabhängig von der Anzahl und Zuständigkeit der Intermediären Plattformen beider Typen, die noch separat festgelegt werden müssen. Dem Typ Intermediärer Plattformen, der dem EU-Ausland gegenüber als Nachweislieferant auftritt und somit die deutschen Register vertritt, obliegt es, den ausländischen Nutzenden zu authentifizieren, den für den gewünschten Nachweistyp zuständigen deutschen Datendienst zu ermitteln sowie den Nutzenden einen Preview des Nachweises darzustellen.

Der zweite Typ Intermediärer Plattformen, der für deutsche abrufende Stellen Nachweise aus dem EU-Ausland anfordert, ist in zwei Ausprägungen denkbar. Um eine größtmögliche Entlastung der Online-Services zu gewährleisten, schlägt dieses Konzept eine komplette Übernahme aller anfallenden Aufgaben durch die Intermediäre Plattform vor, d.h. die Kommunikation mit den Nutzenden und den zentralen EU-Verzeichnissen zur Ermittlung des passenden Nachweistyps und des dafür zuständigen Dienstes im EU-Ausland. Sollten die Online-Services dies selbst übernehmen wollen und können, muss die Intermediäre Plattform mindestens jedoch die technische Abwicklung des Nachrichtenaustauschs mit dem ausländischen Nachweislieferanten sowie die entsprechend notwendigen Transformationsaufgaben durchführen.

3.9.2 Überblick

3.9.2.1 Verwendung und Ziel des Konzepts

Das vorliegende technische Konzept für Intermediäre Plattformen beschreibt den Einsatz Intermediärer Plattformen für die Anbindung deutscher zuständiger Behörden an den grenzüberschreitenden Nachweisaustausch nach Art. 14 der Single Digital Gateway-Verordnung (SDG-VO) aus technischer Perspektive.

Dabei gibt es übergreifende Aspekte, die bei Intermediären Plattformen für alle Arten von zuständigen Behörden relevant sind. Daneben gibt es jedoch auch Funktionen Intermediärer Plattformen, die nur für Nachweisanbieter (im Anwendungsfall „Abruf eines Nachweises aus dem Ausland bei einem deutschen Nachweislieferanten“) und für Nachweise anfordernde Behörden (im Anwendungsfall „Abruf bei einem Nachweislieferanten im Ausland“) relevant sind. Diese verschiedenen Kategorien von Aufgaben Intermediärer Plattformen werden daher getrennt beschrieben und ergänzen sich. Die enthaltenen technischen Festlegungen zur Nutzung Intermediärer Plattformen in Deutschland sind Bestandteil der Technischen Entwurfsdokumentation des nationalen technischen Systems (NOOTS) für den Nachweisabruf.

Das vorliegende Konzept richtet sich primär an drei Zielgruppen:

- Für die Beteiligten an der Architekturkonzeption der Registermodernisierung verdeutlicht es, wie die Komponente „Intermediäre Plattform“ in Deutschland ausgestaltet werden wird und welche Schnittstellen zu anderen Komponenten sich daraus ergeben.
- Für die Stellen, die für die Bereitstellung und den Betrieb einer Intermediären Plattform in Frage kommen, ermöglicht es eine informierte Entscheidung, ob sie diese Rolle übernehmen können.
- Für zuständige Behörden im Sinne des Art. 14 SDG-VO, die ihre Anbindung an das EU-OOTS planen, ermöglicht es eine Einschätzung, welche Aspekte der Anbindung sie an eine Intermediäre Plattform delegieren können und welche zusätzlichen Aufgaben ggf. für sie durch die Nutzung einer Intermediären Plattform entstehen.

3.9.2.2 Rahmenbedingungen

Der europäische Gesetzgeber fordert in SDG-VO die Errichtung eines technischen Systems für den grenzüberschreitenden Austausch von Nachweisen (EU-OOTS), an das die zuständigen Behörden der Mitgliedstaaten nach Art. 14 der SDG-VO angeschlossen werden müssen. Die Anforderungen an das EU-OOTS werden durch die zugehörige Durchführungsverordnung zu Art. 14 der SDG-VO vom 5.8.2022 (im Folgenden DVO) und die begleitende Technische Entwurfsdokumentation (TDD) weiter konkretisiert. Sie lassen den Mitgliedstaaten erhebliche Umsetzungsspielräume, so dass eine eigenständige Konzeption für die deutsche Anbindung an das EU-OOTS notwendig ist.

Zugleich hat der IT-Planungsrat mit Beschluss 2021/05 vom 17.03.2021 ein übergreifendes Zielbild der Registermodernisierung definiert, dass die Anbindung an das EU-OOTS als eines von mehreren Zielen beinhaltet. Zur Umsetzung dieses Zielbilds soll eine nationale Infrastruktur für Registerdatenabrufe geschaffen werden (siehe folgende Abbildung), die als NOOTS bezeichnet wird.

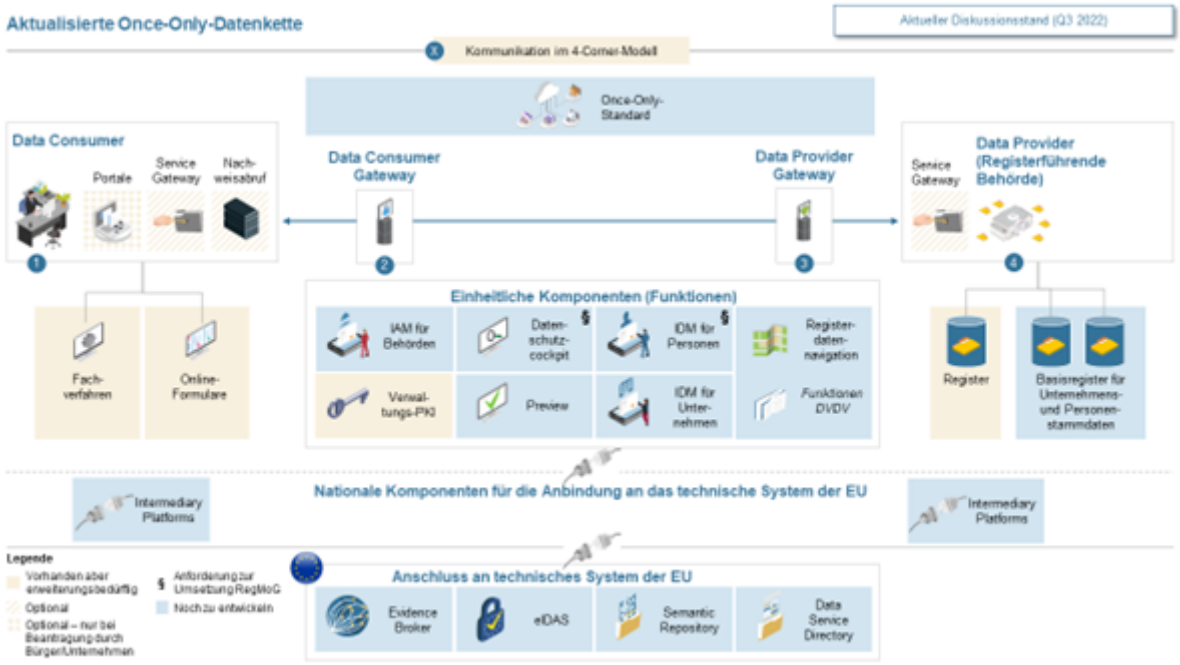


Abbildung 35: Aktualisierte Once-Only-Datenkette (aktueller Diskussionsstand Q3 2022)

Der IT-Planungsrat legt mit dem Beschluss 2022/34 vom 10.11.2022 ferner fest, bei der Anbindung zuständiger Behörden an das EU-OOTS sogenannte Intermediäre Plattformen verpflichtend einzusetzen. Das vorliegende Konzept wurde gemeinsam von den Kompetenzteams EU-Interoperabilität und Architektur der Gesamtsteuerung Registermodernisierung erarbeitet und erläutert die dahinterstehende Konzeption näher.

Kerngedanke ist, mit Intermediären Plattformen eine Zwischenschicht zu schaffen, die nach außen in Richtung des EU-OOTS und nach innen in Richtung des NOOTS spiegelbildliche Funktionen übernimmt.

Für die Anbindung von Nachweislieferanten bedeutet das, dass die Intermediäre Plattform nach außen in Richtung der EU deutsche Data Services gemäß der Anschlussbedingungen des EU-OOTS bereitstellt, zugleich aber gegenüber deutschen Registern als reguläre nachweisabrufende Stelle über das NOOTS auftritt. Auf diese Weise können EU-OOTS und NOOTS sinnvoll zusammengedacht werden und für die deutschen Nachweislieferanten entsteht für die Erfüllung der SDG-Verpflichtungen kein technischer Mehraufwand gegenüber der reinen NOOTS-Anbindung. Für die Anbindung nachweisanfordernder Behörden bedeutet es analog, dass die Behörden die Nachweise bei der Intermediären Plattform anfordern können, die dann selbst wiederum die Nachweise über das EU-OOTS anfordert. Die folgenden Kapitel erläutern diese Überlegungen näher.

Da Intermediäre Plattformen nur einen Teil der Aufgaben im Rahmen der EU-Anbindung übernehmen können und im innerstaatlichen Nachweisabruf in der hier vorgestellten Form nicht sinnvoll sind, diskutiert das Konzept zudem, welchen Nutzen der ergänzende Aufbau zentraler Strukturen auf Seiten der Nachweisanbieter in bisher vollständig dezentralisierten, z.B. kommunalen, Registern haben kann.

3.9.3 Kontext

3.9.3.1 Einführung der zentralen Begriffe

Die Begriffe Evidence Provider, Evidence Requester und Intermediäre Plattform werden in diesem Konzept entsprechend den Definitionen aus der Durchführungsverordnung zu Art. 14 der SDG-VO verwendet.

- **Nachweise anfordernde Behörde, oder auch nachweisanfordernde Behörde (Evidence Requester)** bezeichnet die Behörde, die einen Nachweis über das EU-OOTS anfordert.
- **Nachweislieferant (Evidence Provider)** bezeichnet die Behörde, die den betreffenden Nachweis bereitstellt. Dies kann unmittelbar die registerführende Stelle sein; in bestimmten Kontexten aber auch ein Spiegelregister oder Abrufportal, an das seinerseits mehrere registerführende Stellen angeschlossen sind (siehe auch Kapitel 3.9.3.3).
- **Zuständige Behörde (Competent Authority)** im Sinne des Art. 14 SDG-VO ist der Oberbegriff für Nachweise anfordernde Behörde und Nachweislieferanten.

- Die Durchführungsverordnung lässt den Mitgliedstaaten weitgehende Freiheit, ihre Behörden direkt oder über von ihnen zu gestaltende **Intermediäre Plattformen** mit dem EU-OOTS zu verbinden. In diesem Konzept wird dargestellt, wie diese Möglichkeit in Deutschland genutzt werden soll.
- Evidence Provider und/oder Intermediärer Plattformen stellen technische Dienste bereit, über die bei ihnen Nachweise abgerufen werden können. Diese Dienste werden als **Datendienst (Data Service)** bezeichnet. Eine Stelle kann mehrere Data Services anbieten, z.B. für unterschiedliche Nachweistypen.
- Die grenzüberschreitende Kommunikation erfolgt im EU-OOTS nicht direkt zwischen den angeschlossenen Behörden, sondern vermittelt über sogenannte **eDelivery-Zugangspunkte (eDelivery Access Points).** Jede am EU-OOTS beteiligte Stelle ist innerstaatlich mit einem eDelivery Access Point verbunden; die eDelivery Access Points untereinander übernehmen den grenzüberschreitenden Teil der Kommunikation.
- Beim innerstaatlichen Nachweisabruf über das NOOTS entsprechen die Rollen **Data Consumer und Data Provider** analog den Rollen Evidence Requester und Evidence Provider im EU-OOTS.

3.9.3.2 Wichtige Rahmenbedingungen von EU-OOTS und NOOTS

Das EU-OOTS und das NOOTS sind Systeme für Nachweisabrufe zwischen öffentlichen Stellen. Sie unterscheiden sich jedoch in einigen wichtigen Aspekten. Insbesondere unterstützt das NOOTS eine deutlich größere Breite unterschiedlicher Nachweisabrufe als das EU-OOTS. Die folgende Tabelle zeigt einen Vergleich von Aspekten des EU-OOTS und des NOOTS, die für das vorliegende Konzept relevant sind.

Tabelle 60: Vergleich von Aspekten des EU-OOTS und des NOOTS

EU-OOTS	NOOTS
Grenzüberschreitendes System aller EU-Mitgliedstaaten	Innerdeutsches System
Ausschließlich synchrone Nachweisabrufe, die unmittelbar und vollautomatisiert beantwortet werden können	Synchrone und asynchrone Nachweisabrufe

EU-OOTS	NOOTS
Anfragen werden ausschließlich aus Online-Services ausgelöst, für deren Nutzung ein Nachweis zu erbringen ist.	Anfragen können von Online-Services oder von Fachverfahren auf Behördenseite ausgelöst werden.
Zur Ermittlung des gesuchten Datendienstes muss erst das Verzeichnis ermittelt werden, in dem Datendienste dieses Mitgliedstaats abgelegt sind (verteilte Datenhaltung) und dann dort der gesuchte Datendienst abgefragt werden. Ein analoges verteiltes Modell gilt zudem auch für die Ermittlung der Nachweistypen (siehe unten).	Es existiert eine einheitliche Instanz der Registerdatennavigation, durch deren Aufruf der gesuchte Datendienst ermittelt werden kann.
Da unterschiedliche Mitgliedstaaten die gleiche abstrakte Tatsache durch unterschiedliche Nachweistypen dokumentieren können, muss zunächst ermittelt werden, welcher Nachweistyp aus dem konkreten EU-Mitgliedstaat abgerufen werden soll. Dabei muss die Antwort nicht eindeutig sein und die Auswahl der tatsächlich gewünschten Nachweistypen kann eine Nutzerentscheidung erfordern.	Der abzurufende Nachweistyp ist vorab bekannt.
Bei der Ermittlung des gesuchten Datendienstes kann es sein, dass Zusatzangaben der Nutzenden notwendig werden, um den gesuchten Datendienst zu ermitteln. Je nach Konfiguration des jeweiligen Verzeichnisdienstes können jedoch auch mehrere mögliche Datendienste zurückgeliefert werden, unter denen die Nutzenden eine Auswahl treffen müssen.	Bei der Ermittlung des gesuchten Datendienstes kann es sein, dass Zusatzangaben der Nutzenden notwendig werden, um den gesuchten Datendienst zu ermitteln. Zumindest mit diesen Zusatzattributen ist die Antwort der Registerdatennavigation stets eindeutig.
Die abgerufenen Nachweise müssen den Nutzenden in der Regel zur Bestätigung angezeigt werden, bevor sie für das Verfahren genutzt werden können. Ausnahmen von der Preview-Verpflichtung können im europäischen oder mitgliedstaatlichen Recht definiert werden.	Das NOOTS soll bei nutzerinitiierten Nachweisabrufen eine Preview vorsehen. Nach aktuellem Stand der Diskussion wird die Aufgabe, eine Preview anzubieten, voraussichtlich im Regelfall beim Online-Service bzw. dem dahinterstehenden Portal liegen. Der Mechanismus des EU-OOTS wird in jedem Fall wegen der

EU-OOTS	NOOTS
Die Preview muss vor der grenzüberschreitenden Übermittlung des Nachweises erfolgen. Es erfordert daher eine Weiterleitung der Nutzenden vom Online-Service auf eine Preview-Umgebung, die im EU-Mitgliedstaat des Evidence Providers bereitgestellt wird.	notwendigen Synchronisation zweier paralleler Kommunikationskanäle als sehr aufwändig und störungsanfällig und zudem wegen der Weiterleitung als ungünstig für die Nutzerfahrung bewertet und soll daher nicht so ins NOOTS übernommen werden.
Die Identifikationsnummer (IDNr) wird in der grenzüberschreitenden Kommunikation nicht genutzt.	Es werden Nachweisabrufe mit und ohne Identifikationsnummer unterstützt. Perspektivisch sollen bei Nachweisabrufen zu natürlichen Personen Abrufe mit IDNr der Regelfall werden.
Es findet keine auf den einzelnen Abruf bezogene Berechtigungsprüfung der Behörde statt.	Bei Datenabrufen unter Nutzung der IDNr ist gemäß §7 Abs. 2 IDNr-Gesetz eine abstrakte Berechtigungsprüfung zwingend, bei der Vermittlungsstellen anhand der Metadaten des Abrufs prüfen, ob für den angegebenen Zweck und die angegebenen Kommunikationspartner ein entsprechender Eintrag in einem Vermittlungs- bzw. Verzeichnisdienst vorliegt. Eine solche Prüfung kann auch für andere Datenabrufe über das NOOTS vorgegeben werden.
Die grenzüberschreitende Kommunikation nutzt das Transportverfahren AS4.	Eine Entscheidung über das oder die zulässigen Transportverfahren wurde noch nicht getroffen. Aufgrund der Notwendigkeit, Kommunikation mit vollständiger Ende-zu-Ende-Verschlüsselung zu unterstützen, kommt ein Einsatz von AS4 derzeit jedoch nicht in Frage.
Die grenzüberschreitende Kommunikation nutzt das Exchange Data Model (EDM) als generischen Once-Only-Datenabrufstandard.	Die Kommunikation wird eine für Deutschland angepasste Version des deutschen Exchange Data Model (DE-EDM) als generischen Once-Only-Datenabrufstandard nutzen, um den Besonderheiten und dem breiteren Scope des NOOTS Rechnung zu tragen.

EU-OOTS	NOOTS
Den rechtlichen Rahmen für den Nachweisabruf definieren die SDG-VO und die zugehörige DVO; eine entsprechende Ergänzung im deutschen Recht zur Regelung der datenschutzrechtlichen Aspekte ist in Planung	Es gibt derzeit noch keine übergreifende Rechtsgrundlage für das NOOTS, aber mit dem IDNrG und der XBasisdatenVO liegen Bestandteile vor.

Verschiedene andere Besonderheiten der beiden Systeme (z.B. die Möglichkeit, im europäischen Kontext zunächst den im jeweiligen EU-Mitgliedstaat einschlägigen Nachweistyp mittels des Nachweisdienstes [Evidence Broker] zu ermitteln) werden hier nicht weiter dargestellt, da sie keine Auswirkungen auf das vorliegende Konzept haben.

Bei der Konzeption des NOOTS wird als eines der zentralen Architekturprinzipien verfolgt, eine möglichst weitgehende Übereinstimmung mit dem EU-OOTS zu erreichen und nur bei Vorliegen schwerwiegender Gründe vom europäischen Vorbild abzuweichen. Wie diese Gegenüberstellung zeigt, ist jedoch zum aktuellen Stand bereits absehbar, dass eine vollständige Konvergenz beider Systeme nicht erreicht werden kann und es sowohl bei den Prozessen als auch bei den eingesetzten Technologien in einigen Bereichen notwendige Diskrepanzen geben müssen wird. Aus der Perspektive von Registern, die Nachweise über beide Systeme bereitstellen müssen, besteht damit die Gefahr doppelter Aufwände für separate Anbindungen. Das vorliegende Konzept soll mit den Intermediären Plattformen als „Managerinnen des Übergangs zwischen beiden Systemen“ eine bessere Alternative zu diesem Szenario aufzeigen.

3.9.3.3 Wichtige Rahmenbedingungen der nationalen Registerwelt

Die nationale Registerwelt in Deutschland ist heterogen und besteht aus vielen unterschiedlichen fachlichen Registern bzw. Registertypen, die teilweise in mehreren hundert Instanzen vorhanden sind. Um dieses heterogene Umfeld besser verstehen zu können, wird im Folgenden eine Klassifizierung der unterschiedlichen Register aus der Perspektive einer datenabrufenden Stelle vorgenommen.

Zentralregister sind an einer zentralen Stelle (Bundesebene) errichtet worden. Sie existieren nur einmal und führen einen vollständigen Datenbestand, der für Abrufe von Registerdaten

genutzt werden kann. Beispiele für Zentralregister sind das nationale Waffenregister, das Fahreignungsregister und das Ausländerzentralregister.

Landesregister sind auf Landesebene organisiert. Daher existieren hier mehrere Instanzen des gleichen Registertyps, die jeweils Daten für den betreffenden Zuständigkeitsbereich enthalten (typischerweise ein Register pro Bundesland).

Dezentrale, häufig **kommunale Register** sind kleinteiliger organisiert; hier existiert eine Vielzahl von dezentralen Instanzen, die wiederum die entsprechenden Daten für den jeweiligen Zuständigkeitsbereich vorhalten. In einigen Fällen müssen Datenabrufe dann bei den einzelnen dezentralen Instanzen erfolgen. Andere Informationsverbünde wie das Meldewesen haben allerdings als ergänzende Strukturen **Spiegelregister** oder **Abrufportale** geschaffen, die zum Zugriff auf Registerdaten kontaktiert werden können. Spiegelregister führen dabei Kopien der Daten aus einer ganzen Reihe dezentraler Register zusammen und können so eigenständig Registerabfragen beantworten. Abrufportale dienen lediglich als einheitlicher Zugang, rufen die Daten aber für jede konkrete Abfrage einzeln bei den an sie angeschlossenen dezentralen Registern ab. Für die anfragende Stelle ist diese Kommunikation mit den dahinterstehenden Registerinstanzen jedoch in beiden Fällen transparent, so dass Spiegelregister und Abrufportale für die datenabrufenden Stellen nach außen wie Landes- bzw. Zentralregister wirken. Sowohl für Spiegelregister als auch für Abrufportale ist entscheidend, dass sie aufgrund rechtlicher Regelungen als zuständige Nachweislieferanten für bestimmte Konstellationen festgelegt sind.

Da es bei der Umsetzung des Once Only-Prinzips um die Umsetzung von Registerdatenabrufen geht, steht bei der vorgestellten Klassifikation der Register im Vordergrund, bei welcher Stelle Nachweisdaten abgerufen werden können bzw. müssen. Dabei bedeutet eine Zentralisierung von Daten für die Beantwortung von Anfragen jedoch nicht zwingend, dass die Daten auch zentral gepflegt werden. So übernimmt z.B. ein Spiegelregister typischerweise einfach zyklisch die Daten der angeschlossenen Registerinstanzen, und die eigentliche Datenpflege erfolgt dort. Aber auch bei vollständig zentralisierten Registern kann die Verantwortung für die Datenpflege auf verschiedene Stellen aufgeteilt sein, die z.B. über ein Pflegeinterface oder auch über standardisierte Fachnachrichten aus ihren lokalen Fachverfahren Aktualisierungen im zentralen Register anstoßen können.

3.9.3.4 Wichtige Rahmenbedingungen auf Seiten der Online-Services

Da der grenzüberschreitende Nachweisabruf gemäß SDG-VO für Antragsverfahren und nicht für Fachverfahren vorgesehen ist, zählen zu den datenabrufenden Stellen ausschließlich Online-Services, die Verfahren nach Art. 14 SDG-VO umsetzen, bzw. Antragsportale, sofern entsprechende Online-Services auf diesen laufen. Gemeinsam haben diese datenabrufenden Stellen daher, dass sie über eine Anwenderschnittstelle verfügen und damit zwingend im Internet über einen Browser erreichbar sind, was sie von Nachweislieferanten unterscheidet, die teilweise nur über das Verwaltungsnetz erreichbar sind.

Ansonsten zeichnen sich die Evidence Requester jedoch über eine große Heterogenität aus, sowohl was ihre Fachlichkeit angeht als auch ihren Aufbau und ihre Reichweite: Es sind Online-Services auf Bundes-, Landes- und Kommunalebene darunter, die als Einzel-Lösung, als Einer für Alle (EfA)-Lösung oder als um ein Frontend ertüchtigte Fachanwendung den Nutzenden angeboten werden können. Dazu kommen als Sonderfälle behördlich beauftragte Anbieter, wie zum Beispiel das Bewerbungsportal Hochschulstart.

Behördliche Online-Services in Deutschland müssen sich an den Anforderungen des Online-Zugangsgesetzes messen, die durch die Stufe 3 des OZG-Reifegradmodells weiter operationalisiert werden. Dabei ist wichtig, dass Stufe 3 noch keine Umsetzung des Once Only-Prinzips erfordert. Online-Services sind also bisher in der Regel nicht rechtlich verpflichtet, einen innerstaatlichen Nachweisabruf zu ermöglichen, auch wenn sie unter Art. 14 SDG-VO fallen und damit zukünftig einen grenzüberschreitenden Abruf ermöglichen müssen.

3.9.3.5 Wichtige Annahmen

Dieser Konzeptionserstellung liegen folgende Annahmen über das NOOTS nach dem derzeitigen Konzeptionsstand zugrunde:

Für innerdeutsche Nachweisabrufe im NOOTS wurde die Verantwortlichkeit für die Preview beim Data Consumer festgelegt. Daraus ergibt sich aus Sicht des Data Consumer eine Ungleichbehandlung für deutsche und europäische Nachweise, denn bei grenzübergreifenden Nachweisabrufen muss die Preview immer im Land des Nachweislieferanten angeboten werden.

Bei innerdeutschen Nachweisabrufen sind die Nachweislieferanten frei, je nach ihrem Reifegrad, die Nachweise entweder als Dokument (z.B. als PDF) oder als strukturierte Daten

zu versenden. Eine zentrale Stelle, die die unterschiedlichen Nachweise in Dokumente verwandelt, ist im NOOTS nicht vorgesehen. Da grenzübergreifende Nachweisabrufe jedoch zumindest ergänzend die Übermittlung eines Dokumentenformats, wie bspw. PDF erfordern, soweit kein gesamteuropäisch harmonisiertes Datenformat genutzt wird, müssen von einem deutschen Nachweislieferanten übermittelte strukturierte Nachweise vor der grenzüberschreitenden Übertragung umgewandelt werden (was die Intermediäre Plattform übernehmen kann, dazu im weiteren Verlauf dieses Konzepts mehr).

Des Weiteren nimmt dieses Konzept gemäß der aktuellen Konzeption des NOOTS an, dass Data Consumer die Nachweisabrufe und die dafür notwendigen Benutzerdialoge und Funktionen, wie die Preview, selbst umsetzen. Eine Delegation dieser Aufgaben an eine zentrale Komponente wird zwar als Möglichkeit diskutiert, hier aber nicht angenommen (siehe aber den letzten Abschnitt von Kapitel 3.9.4.4 zur Erläuterung der Auswirkungen, die eine Änderung dieser Annahme auf Intermediäre Plattformen für nachweisabrufende Behörden hätte).

3.9.4 Fachliches Konzept (Anforderungen & Architektur)

3.9.4.1 Grundidee und Vorteile der Intermediären Plattform

Wie im vorangegangenen Kapitel dargestellt, nutzen EU-OOTS und NOOTS in Teilen unterschiedliche Prozesse und Technologien. Zusammen mit der dezentralen und heterogenen Registerlandschaft und den vielfältigen Online-Services in Deutschland birgt diese Ausgangslage das Risiko hoher und unnötiger Aufwände, wenn alle betroffenen Register und Online-Services separate Anbindungen an beide Systeme umsetzen müssen. Daher ist es sinnvoll, für die Kopplung der beiden Systeme die im EU-OOTS explizit eingeräumte Möglichkeit zu nutzen, Intermediäre Plattformen einzurichten.

Neben der Verringerung des Umsetzungsaufwands ermöglicht diese Zentralisierung der Umsetzung der EU-Vorgaben auch ein schnelleres Vorgehen als ein alternativer Ansatz, bei dem im Extremfall jedes einzelne Register und jeder Online-Service separat entsprechend ertüchtigt werden müsste. Der Dringlichkeit der Anbindung deutscher Register und Online-Services an das europäische EU-OOTS bis 12.12.2023 kann so mittels der Anbindung über Intermediärer Plattformen besser begegnet werden. Da mit den Änderungen und Anpassungen des europäischen Systems bis Ende 2023 und auch darüber hinaus zu rechnen ist, hilft eine Anbindung über Intermediäre Plattformen zudem, eine gewisse Entkopplung

zu erreichen und diese Anpassungen in der Regel schnell umzusetzen, ohne Mehraufwand bei den einzelnen angeschlossenen Behörden zu erzeugen.

Aus Perspektive der Gesamtarchitektur wäre es ideal, wenn Intermediäre Plattformen so gestaltet werden können, dass für die angeschlossenen Online-Services und Register kein Unterschied zwischen nationalen und grenzüberschreitenden Nachweisabrufen besteht und dadurch aus Perspektive der betroffenen Behörden kein technischer Zusatzaufwand für die EU-Anbindung entsteht. Wie im Folgenden näher erläutert wird, lässt sich dieses Ziel für Register vollständig erreichen, während Intermediäre Plattformen für sich genommen Online-Services nur von einem Teil der EU-spezifischen Funktionalität entlasten können (siehe den letzten Abschnitt von Kapitel 3.9.4.4 zu einer möglichen Alternative mit weitergehenden Entlastungsmöglichkeiten).

3.9.4.2 Übergreifende Anforderungen

Alle Intermediären Plattformen haben als eine zentrale Funktion, die technische Heterogenität zwischen EU-OOTS und NOOTS zu überbrücken, die sich auf drei Ebenen zeigt.

Auf der Ebene des Transportprotokolls nutzt das EU-OOTS ausschließlich AS4, während das NOOTS einen oder mehrere noch festzulegende, voraussichtlich von AS4 abweichende Standards (wie OSCI) nutzen wird. Die Intermediären Plattformen müssen daher in allen beteiligten Transportprotokollen kommunizieren können und Nachrichten, die auf einem Transportweg eingehen, korrekt auf dem anderen Weg weitergeben können.

Darüber hinaus nutzt das NOOTS auf der Ebene des Nachrichtenmodells ein von EU-OOTS abgeleitetes Modell, das sich jedoch nach aktuellem Stand ebenfalls in manchen Aspekten von der EU-Vorgabe unterscheiden bzw. darüber hinausgehen wird. Zudem können die Vorgaben für die als Nachrichtenanhang übermittelten Nachweisdaten zwischen beiden Systemen abweichen. Daher müssen die Intermediären Plattformen grundsätzlich auch auf dieser Ebene ein technisches Mapping zwischen den Datenmodellen vornehmen. Dies gilt noch verschärft, falls eine Intermediäre Plattform übergangsweise, innerstaatlich mit bestehenden Fachstandards statt dem NOOTS-Nachrichtenmodell kommunizieren sollte (siehe hierzu den Abschnitt „Innerstaatlicher Nachweisabruf über bilaterale Anbindung oder bestehende Informationsverbünde“ in Kapitel 3.9.4.7). Insbesondere für diese Aufgabe ist es zwingend erforderlich, dass die Intermediäre Plattform auf die Inhalte der einzelnen

übermittelten Nachrichten zugreifen kann, um diese ggf. zur Überbrückung von Differenzen in den Nachrichtenmodellen transformieren zu können.

Zudem nutzen EU-OOTS und NOOTS unterschiedliche Mechanismen zur Authentifizierung und Autorisierung der im System aktiven Behörden. Das EU-OOTS verlässt sich in der 4-Corner-Kommunikation darauf, dass die Mitgliedstaaten sicherstellen, dass nur zulässige und vertrauenswürdige Teilnehmer an die jeweiligen Access Points angebunden werden; dafür ist eine entsprechende Absicherung der Kommunikation zwischen einer Intermediären Plattform und ihrem Access Point nötig. Innerstaatlich tritt die Intermediäre Plattform, je nach Typ, entweder als Nachweislieferant oder als datenabrufende Stelle auf und muss daher nach der Zugriffslogik des NOOTS über entsprechende Rechte für diese Rolle verfügen und auch ihrerseits wiederum die Berechtigung ihrer Kommunikationspartner überprüfen.

Alle Intermediären Plattformen müssen zudem die über sie erfolgenden Datenübermittlung protokollieren und dabei sowohl die relevanten innerstaatlichen Vorgaben als auch die spezifischen Protokollierungsanforderungen des EU-OOTS beachten.

3.9.4.3 Anforderungen an Intermediäre Plattformen für Nachweislieferanten

Überblick

Diesem Kapitel liegt die Annahme zugrunde, dass die Intermediäre Plattform von einer öffentlichen Stelle betrieben wird, die insbesondere dafür zuständig ist, die Datendienste für den Nachweisabruf bereitzustellen. Dafür müsste die Intermediäre Plattform rechtlich für grenzüberschreitende Abrufe selbst als Nachweislieferant agieren oder rechtlich geregelt sein, dass der Abruf beim Nachweislieferanten über die Intermediäre Plattform erfolgt.

Die Intermediäre Plattform stellt für Anfragen aus dem europäischen Ausland den Datendienst bereit, der Nachweise nach den Regeln des EU-OOTS ausliefert (Data Service für das EU-OOTS). Sie hält die Nachweisdaten jedoch nicht selbst vor, sondern fordert diese anlassbezogen über das NOOTS von der Stelle an, die im NOOTS für die Bereitstellung dieser Nachweise zuständig ist. Dabei nutzt die Intermediäre Plattform für den innerstaatlichen Abruf ausschließlich der Mechanismen des NOOTS, so dass für die in Deutschland zuständigen Data Provider kein Mehraufwand entsteht.

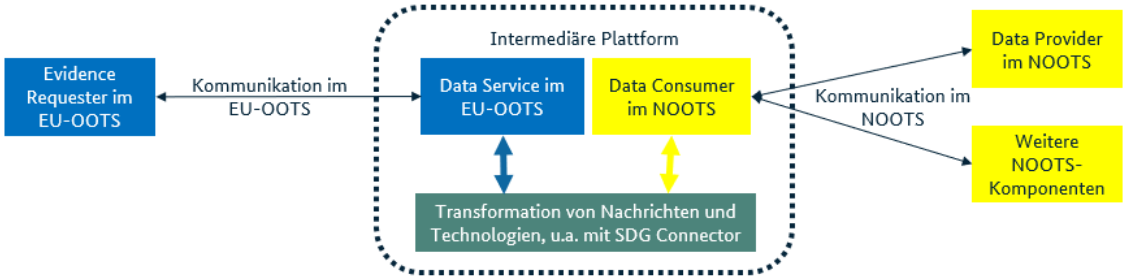


Abbildung 36: Einordnung einer Intermediären Plattform für Nachweislieferanten im Kontext des EU-OOTS und des NOOTS

Abbildung 36 stellt die Grundidee für einen konkreten Abruf dar, an dem immer eine Intermediäre Plattform und ein einzelner Data Provider beteiligt sind. Der eigentliche Mehrwert der Intermediären Plattform entsteht jedoch dadurch, dass viele unterschiedliche Data Provider des NOOTS sich an die gleiche Intermediäre Plattform anschließen können, sofern dies rechtlich zulässig ist. Die Aufwände für die Unterstützung der EU-spezifischen Prozesse und Technologien fallen dann nur pro Intermediärer Plattform und nicht mehr pro Data Provider an.

Die Intermediäre Plattform kann jedoch nicht alle Aufgaben der Register übernehmen. Um systematisch zu erfassen, welche Aufgaben Kernaufgaben eines Registers sind und welche Aufgaben an wen delegiert werden können, wurden drei Kategorien für die Aufgaben gebildet.

- **Datenhoheit und Datenpflege**: Die Datenhoheit liegt immer bei den eigentlichen registerführenden Stellen, die die originären Daten halten und deren Pflegeprozesse sie verantworten. Sie müssen dafür sorgen, dass die fachlich richtigen Daten in den Registern eingespielt und nach den Vorgaben des jeweiligen Registers aktuell gehalten werden. Diese Aufgabe kann von der registerführenden Stelle nicht delegiert werden. Da EU-OOTS und NOOTS nur dem Abruf, aber nicht der Pflege von Registerdaten dienen, wird diese Aufgabendimension im Folgenden nicht weiter betrachtet.
- **Datenbereitstellung**: Die Datenbereitstellung übernimmt die Beantwortung von Anfragen zum Registerinhalt und macht die im Register geführten Daten für einen Nachweisabruf verfügbar. Im einfachsten Fall wird auch diese Aufgabe von der registerführenden Stelle selbst übernommen. Anders als die Datenhoheit kann sie jedoch grundsätzlich auch auf zentrale Strukturen delegiert werden, wenn es dafür eine entsprechende fachrechtliche Grundlage gibt. Ein typisches Beispiel hierfür sind

Spiegelregister und Abrufportale, die nach außen die Beantwortung von Registerabfragen übernehmen. Sie übernehmen die eigentlichen Daten jedoch von den an sie angeschlossenen dezentralen Registern, bei denen die Datenhoheit verbleibt. Das potenzielle Auseinanderfallen beider Ebenen ist der Grund dafür, dass man die Stelle, die nach außen die Beantwortung von Nachfragen übernimmt, als Data Provider (NOOTS) bzw. Evidence Provider (EU-OOTS) bezeichnet und nicht einfach vom Anschluss der registerführenden Stellen selbst spricht. Eine Übertragung der Datenbereitstellung erfordert eine explizite rechtliche Regelung, dass die jeweilige Stelle für diese Aufgabe zuständig ist. Existiert eine solche Regelung, wird die betreffende Stelle selbst Data bzw. Evidence Provider; die Aufgabe kann nicht von einer reinen Intermediären Plattform ohne derartige Berechtigung übernommen werden.

- **Nachweiskommunikation und -präsentation**: Eine dritte Gruppe von Aufgaben lassen sich unter der Kategorie Nachweiskommunikation und -präsentation zusammenfassen. Bei diesen Aufgaben handelt es sich um technische Aufgaben, die die vom Evidence Provider bereitgestellten Nachweise entsprechend den spezifischen Technologien und Prozessen des jeweiligen Informationsverbunds – hier des EU-OOTS – verfügbar zu machen sowie ggfs. die Interaktion mit den Nutzenden durchzuführen. Diese Aufgaben lassen die fachlich vom Evidence Provider gelieferten Daten inhaltlich unverändert und können daher als unterstützende Aufgaben auch an eine Intermediäre Plattform als Hilfsinfrastruktur delegiert werden. Sie stehen im Mittelpunkt des aktuellen Konzepts.

Um die im vorangegangenen Abschnitt ausgeführten Vorteile bei der Anbindung an das EU-OOTS zu erreichen, strebt dieses Konzept an, die grundsätzlich delegierbaren Aufgaben aus dem Bereich Nachweiskommunikation und Nachweispräsentation so weit wie möglich auf die Intermediären Plattformen zu übertragen.

Anforderungen im Einzelnen

Aus Perspektive des EU-OOTS ist die zentrale Anforderung an eine Intermediäre Plattform, geeignete Dienste zum Abruf der Nachweisinformationen aus den angeschlossenen Registern bereitzustellen (im Folgenden Data Services). Diese Data Services müssen entsprechend den Anforderungen der Durchführungsverordnung zu Art. 14 SDG-VO und der technischen Entwurfsdokumentation des EU-OOTS ausgestaltet werden. Einige wichtige Aspekte dieser Vorgaben werden hier im Überblick zusammengefasst.

Data Services sind Dienste, die den Abruf von Nachweisen spezifischer Nachweistypen ermöglichen. Sie müssen dafür im zuständigen Data Service Directory (DSD) registriert und

auf Transportebene jeweils über einen AS4 Access Point erreichbar sein, der allen anderen Access Points des EU-OOTS bekannt ist. Data Services stellen für den Nachweisabruf eine Schnittstelle bereit, die im Exchange Data Model (EDM) der Technical Design Documents definiert ist. Diese Schnittstelle sieht einen Nachrichtentyp vor, mit dem der Evidence Requester beim Data Service einen Nachweis anfordern kann, und mehrere Nachrichtentypen für die Antwort des Data Service:

- Übermittlung des angefragten Nachweises
- Fehlermeldung, weil der Nachweis nicht bereitgestellt werden kann
- Fehlermeldung mit Preview-URL, auf die die Nutzenden weitergeleitet werden können (mehr dazu im Folgenden)
- (optional) Fehlermeldung, weil der Nachweis derzeit nicht bereitgestellt werden kann, mit einer Indikation des Zeitpunkts, zu dem er voraussichtlich verfügbar sein wird

Da der Data Service in unserem Fall von einer Intermediären Plattform bereitgestellt wird, die selbst keine Registerdaten vorhält, muss die Intermediäre Plattform vor einer Nachweisübermittlung zunächst selbst einen entsprechenden Registerdatenabruf durchführen. Dazu führt sie einen innerstaatlichen Datenabruf beim betreffenden Register über das NOOTS durch, für den die entsprechenden Vorgaben aus der Architektur des NOOTS u.a. zum einzusetzenden Datenaustauschstandard und Transportmechanismus gelten. Sie muss dafür die relevanten Informationen aus der Anfrage über das EU-OOTS entnehmen und in eine Anfrage über das NOOTS umwandeln und umgekehrt die Antwortnachricht über das NOOTS in das Nachrichtenmodell des EU-OOTS transformieren.

Beide Nachrichtenmodelle sehen vor, dass die eigentlichen Nachweisinformationen im Erfolgsfall als Anhang der Antwortnachricht übertragen werden. In zwei Fällen kann es dabei notwendig sein, dass die Intermediäre Plattform auch eine Umwandlung des übertragenen Nachweises selbst vornimmt:

- Wenn für den betreffenden Nachweistyp ein EU-weit harmonisiertes Datenformat existiert, aber der nationale Evidence Provider über das NOOTS eine andere strukturierte Darstellung liefert, transformiert die Intermediäre Plattform den Nachweis in das harmonisierte Format.
- Wenn der Evidence Provider ein strukturiertes Datenformat liefert, das jedoch spezifisch für Deutschland ist und nicht auf einem EU-weit harmonisierten Datenformat basiert,

muss zusätzlich eine leicht darzustellende Lesefassung des Nachweises übermittelt werden (siehe Art. 15 Abs. 2 lit. e DVO). Liefert der Evidence Provider keine solche Fassung mit, muss sie in der Intermediären Plattform erzeugt (z.B. im PDF-Format) und bei der Antwortnachricht über das EU-OOTS ergänzt werden.

Das EU-OOTS sieht als Regelfall vor, dass die Nutzenden den Nachweis vor der grenzüberschreitenden Übermittlung einsehen und die Übermittlung freigeben müssen (Preview, siehe Art. 14 Abs. 3 lit. f SDG-VO). Auf die initiale Anfrage eines Nachweises reagiert der Data Service daher in der Regel zunächst mit einer Fehlermeldung, die eine fallspezifische Preview-URL enthält. Die Intermediäre Plattform muss die ursprüngliche Anfrage und die zugehörige Preview-URL vorhalten, bis die URL genutzt wird oder ein Timeout eintritt. Der Evidence Requester leitet die Nutzenden dann zu dieser Preview-URL weiter. Die Intermediäre Plattform muss für die Preview unter der übermittelten URL eine geeignete Nutzeroberfläche im Internet bereitstellen (Preview-Space). Sie authentifiziert die auf die Preview-URL weitergeleiteten Nutzenden aus Sicherheitsgründen im nationalen Kontext, ruft die entsprechenden Nachweisinformationen über das NOOTS ab und stellt sie den Nutzenden zur Freigabe dar. Dabei erzeugt die Intermediäre Plattform eine Preview-ID, die sie ihrer Antwort beifügt und unter der die Entscheidung der Nutzenden gespeichert wird. Nach Ende der Preview werden die Nutzenden wieder in die Umgebung des Evidence Requesters zurückgeleitet. Haben sie die Übermittlung des Nachweises bestätigt, stellt der Evidence Requester eine erneute Anfrage zur Nachweisübermittlung, die dieses Mal vom Data Service mit der eigentlichen Nachweisübermittlung beantwortet wird.

Aufgrund der komplexen und verteilten Registerlandschaft in Deutschland ist es möglich, dass die Intermediäre Plattform weitere Informationen von den Nutzenden benötigt, um die richtige Registerinstanz ermitteln zu können, die nicht Teil der ursprünglichen Anfrage sind. In diesem Fall können die fehlenden Angaben während der Interaktion in der Preview-Umgebung unmittelbar von den Nutzenden erhoben werden.

Es kann Datenabrufe geben, in denen die Notwendigkeit der Preview durch europäisches oder mitgliedstaatliches Recht ausgeschlossen wurde (siehe Art. 14 Abs. 5 SDG-VO); dies wird vom Evidence Requester in der initialen Anfragenachricht gekennzeichnet. In diesem Fall kann der Data Service grundsätzlich bereits die erste Anfrage unmittelbar mit der Übermittlung des betreffenden Nachweises beantworten. Wenn die Intermediäre Plattform aber Zusatzangaben der Nutzenden benötigt, um das richtige Register für den Datenabruf zu ermitteln, kann auch in diesen Fällen eine Weiterleitung der Nutzenden auf die Nutzeroberfläche der Intermediären Plattform angefordert werden (Art. 14 Abs. 2 i.V.m. Art.

11 Abs. 3 DVO). Die Nutzenden können diese Weiterleitung ablehnen; es ist jedoch zulässig, dass der Nachweisabruf in diesen Fällen auch fehlschlagen kann.

Das EU-OOTS bietet die optionale Möglichkeit, bei einem nicht verfügbaren Nachweis einen Zeitpunkt anzugeben, zu dem dieser verfügbar sein wird (Art. 15 Abs. 5 DVO). Gedacht ist dieser Mechanismus für Verzögerungen von wenigen Stunden bis Tagen, sodass die Nutzenden ggf. mit der Ausführung des eigentlichen Antragsverfahrens warten können, um den Nachweis zu einem späteren Zeitpunkt über das EU-OOTS in das Verfahren einbeziehen zu können. Sinnvoll ist ein solches Szenario insbesondere dann, wenn Registerdaten schrittweise digitalisiert werden und die Möglichkeit besteht, aktiv angeforderte Daten in diesem Prozess zu priorisieren und zuerst zu digitalisieren. Es handelt sich explizit um einen optionalen Mechanismus, der aus der übergreifenden Architekturperspektive der Registermodernisierung nur geringen Mehrwert bringt. Seine Umsetzung liegt daher vollständig im Ermessen der jeweiligen Intermediären Plattform in Abstimmung mit den angeschlossenen Registern.

Die Kommunikation im EU-OOTS erfolgt über das Internet, während die Data Consumer des NOOTS in der Regel nur über gesicherte Verwaltungsnetze zu erreichen sind. Eine direkte Anbindung der Data Consumer würde also zudem eine unter Sicherheitsaspekten nicht gewünschte massive Erhöhung der Exposition im Internet bedeuten. Eine weitere zentrale Aufgabe von Intermediären Plattformen für Nachweislieferanten ist daher, die Zahl der Netzübergänge möglichst gering zu halten und diese zentral abzusichern. Für die Absicherung des Übergangs zwischen dem Internet und verwaltungseigenen Netzen in Deutschland sind die entsprechenden Vorgaben des BSI zu berücksichtigen, siehe auch Kapitel 3.9.5.2.

3.9.4.4 Anforderungen an Intermediäre Plattformen für nachweisanfordernde Stellen

Überblick

In diesem Kapitel wird davon ausgegangen, dass die Intermediäre Plattform Online-Services dabei unterstützt, Nachweisabrufe über das EU-OOTS vorzunehmen, siehe Abbildung 37.

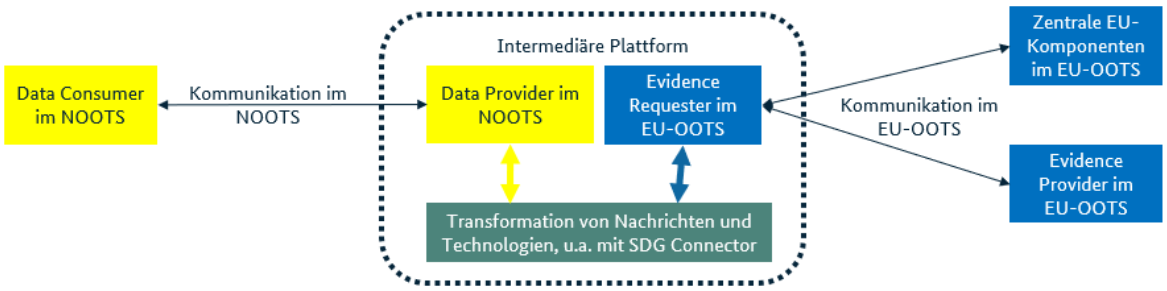


Abbildung 37: Einordnung einer Intermediären Plattform für datenabrufende Stellen im Kontext des EU-OOTS und des NOOTS

Dabei sind grundsätzlich zwei unterschiedliche, aufeinander folgende Phasen zu unterscheiden:

- Vorbereitung des Nachweisabrufs: Zunächst sind eine Reihe von Schritten notwendig, um den richtigen Data Service und weitere Parameter für den Abruf unter Nutzung der entsprechenden Verzeichnisdienste zu ermitteln. In diesem Teilprozess kann an verschiedenen Stellen eine Interaktion mit den Nutzenden notwendig sein.
- Durchführung des Nachweisabrufs: Anschließend erfolgt der eigentliche Nachweisabruf im 4-Corner-Modell über das EU-OOTS. In der Regel ist es in diesem Teilprozess zudem nötig, die Nutzenden parallel auf eine Preview-Umgebung im Mitgliedstaat des Data Service weiterzuleiten und auf den Abschluss der dortigen Interaktion zu warten.

Grundsätzlich ist aus Sicht der Gesamtarchitektur empfehlenswert, dass eine nachweisanfordernde Behörde beide Teilprozesse an eine Intermediäre Plattform delegiert, da so zentral auf wenigen Intermediären Plattformen der SDG-konforme Ablauf des Nachweisabrufs umgesetzt und langfristig aufrechterhalten werden kann.

Für Nutzende hat dies zur Folge, dass er insgesamt auf mindestens drei Umgebungen geleitet wird: Den Online-Antrag, das Frontend der Intermediären Plattform und die Preview-Umgebung im Mitgliedstaat des EU-Nachweislieferanten (siehe dazu im Detail auch „Mehrstufige Weiterleitung“ in Kapitel 3.9.4.8). Dazu kommen ggf. noch die separaten Oberflächen der Authentifizierungsmechanismen. Da diese Umgebungen nicht denselben Ursprung haben, ist von unterschiedlichem Aufbau und Design auszugehen. Da dies aus der Perspektive der Nutzerführung nicht optimal ist, mögen einige Online-Services und große Portale es vorziehen, die Nutzerdialoge im ersten Teilprozess selbst umzusetzen. Dies sollte zulässig sein, sofern sie sich an den vorgegebenen Ablauf halten, sowohl was die Nutzerinteraktion als auch die dazwischen anfallenden Backend-Prozess-Schritte anbelangt.

Anforderungen im Einzelnen

Die zu durchlaufenden Schritte und die entsprechende Unterstützung der Intermediären Plattform sind hier dargestellt. Dabei zeigt die Spalte „Alternativ im Online-Service möglich“, ob die Aufgabe auch direkt vom Online-Service wahrgenommen werden kann; dann sollten allerdings in der Regel alle Schritte des ersten Teilprozesses vollständig direkt im Online-Service umgesetzt werden.

Tabelle 61: Übersicht Schritte bei EU-Nachweisabruf durch deutschen Online-Services mit Intermediärer Plattform

Nr.	Beschreibung	Nutzerinteraktion oder Backend-Aktion	Alternativ im Online-Service
1	Online-Service leitet die Nutzenden für den Nachweisabruf auf die Intermediäre Plattform weiter	Nutzerinteraktion	Entfällt in diesem Fall
2	Intermediäre Plattform fragt bei den Nutzenden das Ursprungsland des Nachweises ab	Nutzerinteraktion	Ja
3	Intermediäre Plattform fragt beim Evidence Broker Registry den für das gewünschte Land zuständigen Evidence Broker ab	Backend	Ja
4	Intermediäre Plattform fragt bei Evidence Broker den oder die möglichen gewünschten Nachweistyp(en) ab	Nutzerinteraktion	Ja
5	Intermediäre Plattform lässt die Nutzenden aus mehreren möglichen Nachweistypen auswählen und nimmt Entscheidung auf (wenn nötig)	Nutzerinteraktion	Ja
6	Intermediäre Plattform fragt bei Data Service Directory Registry das für den gewählten Nachweistyp zuständige Data Service Directory ab	Backend	Ja

Nr.	Beschreibung	Nutzerinteraktion oder Backend-Aktion	Alternativ im Online-Service
7	Intermediäre Plattform fragt bei Data Service Directory die zuständige Stelle für den gewünschten Nachweistyp an	Backend	Ja
8	Intermediäre Plattform erfasst von den Nutzenden die nötigen Zusatzattribute für die Zuständigkeitsermittlung im DSD (wenn nötig)	Nutzerinteraktion	Ja
9	Intermediäre Plattform übermittelt die erfassten Zusatzattribute für die Zuständigkeitsermittlung im DSD (wenn nötig)	Backend	Ja
10	Intermediäre Plattform lässt die Nutzenden aus mehreren möglichen Nachweislieferanten auswählen und nimmt Entscheidung auf (wenn nötig)	Nutzerinteraktion	Ja
11	Intermediäre Plattform löst initialen Nachweisabruf bei Nachweislieferanten aus	Backend	Nur über IP möglich
12	Intermediäre Plattform leitet die Nutzenden auf die Umgebung des Mitgliedstaats des Nachweislieferanten weiter	Nutzerinteraktion	Ja
13	Intermediäre Plattform löst erneuten Nachweisabruf bei Nachweislieferanten aus	Backend	Nur über IP möglich
14	Intermediäre Plattform nimmt Nachweis auf	Backend	Nur über IP möglich
15	Intermediäre Plattform übergibt Nachweis an Online-Service	Backend	Nur über IP möglich

Nr.	Beschreibung	Nutzerinteraktion oder Backend-Aktion	Alternativ im Online-Service
16	Intermediäre Plattform nimmt die Nutzenden wieder in Empfang und lässt sie entscheiden, ob sie einen erneuten Nachweisabruf beginnen oder den Vorgang abschließen und zum Antrag zurückkehren möchten	Nutzerinteraktion	Ja
17	Intermediäre Plattform leitet die Nutzenden zurück zum Online-Service	Nutzerinteraktion	Entfällt in diesem Fall

Eine Funktionalität, welche die Intermediäre Plattform bereithalten muss, um Schritt 4 erfolgreich ausführen zu können, ist die Übersetzung des deutschen Nachweistyps in einen EU-Sachverhalt („requirement“), für den sich dann beim Evidence Broker wiederum das ausländische Äquivalent abfragt. Auf diese Weise muss der Online-Service selbst fachlich nicht bestimmen, um welchen Sachverhalt es ihm beim Nachweis geht, sondern kann – wie bei deutschen Nachweisen auch – auf den ihm bekannten deutschen Nachweistyp verweisen. Da ein Nachweistyp allerdings mehrere Sachverhalte umfassen kann, muss die Intermediäre Plattform ein fachlich informiertes Verzeichnis aufsetzen und pflegen, dass die fachlich relevanten Sachverhalte den Nachweistypen zuordnet.

Nachweisabrufdienst im NOOTS als Alternative

Im Gegensatz zur Registerseite ist es bei Online-Services auch unter Nutzung Intermediärer Plattformen nicht möglich, dass die Abläufe für NOOTS- und EU-OOTS-Abläufe identisch sind, weil der europäische Prozess zusätzliche Nutzerinteraktionen vorsieht, die der Online-Service entweder selbst umsetzen oder durch eine zusätzliche Weiterleitung auf eine Oberfläche der Intermediären Plattform abdecken muss. Dadurch kann keine Transparenz bzgl. der Art des Abrufs geschaffen werden; beide Varianten müssen explizit unterstützt werden und erzeugen damit Zusatzaufwände auf Seiten der Online-Services.

Eine Alternative hierzu wäre möglich, wenn Online-Services den Schritt des Nachweisabrufes auch im NOOTS an einen separaten Nachweisabrufdienst delegieren würden, der für die entsprechenden Schritte eine eigene Oberfläche bereitstellt. Hier würde

der Online-Service die Nutzenden zum Nachweisabruf immer an diesen Dienst weiterleiten und von dort die Nachweise über eine einheitliche Schnittstelle erhalten. Die „Weiche“ zwischen EU- und NOOTS-Abrufen und die unterschiedlichen Prozessabläufe und Nutzerinteraktionen könnten dort gekapselt werden.

Dieses Konzept ist zunächst so gestaltet, dass es keinen solchen zentralen Nachweisabrufdienst gibt. Sollte dies jedoch in der übergreifenden Architektur anders entschieden werden, wären die dargestellten Prozessschritte mit Auswirkungen auf die Nutzerinteraktion besser in einem solchen Nachweisabrufdienst als in der Intermediären Plattform aufgehoben. Die Intermediäre Plattform für nachweisabrufende Stellen könnte dann eine reine Backend-Komponente sein, die nur die übergreifenden Anforderungen aus Kapitel 3.9.4.2 umsetzt und ihrerseits vom Nachweisabrufdienst genutzt würde.

3.9.4.5 Verpflichtende Nutzung, Zahl und Zuschnitt Intermediärer Plattformen

Aufgrund der dargestellten Vorteile bei der Nutzung Intermediärer Plattformen hat der Lenkungskreis Registermodernisierung dem IT-Planungsrat empfohlen, bei der Erarbeitung der weiteren Anbindungskonzeption von einer Verpflichtung zur Nutzung einer Intermediären Plattform zur Anbindung deutscher zuständiger Behörden an das EU-OOTS auszugehen. Dadurch wird auch eine einheitliche und klare Architektur für die Anbindung geschaffen.

Das hier vorgestellte technische Konzept für Intermediäre Plattformen ist unabhängig von der separaten Frage über die Zahl der in Deutschland genutzten Intermediären Plattformen sowie deren Zuschnitt bzw. die Aufteilung der an sie angebundenen zuständigen Behörden.

Zum aktuellen Zeitpunkt sind keine Anforderungen bekannt, die eine bestimmte Zahl oder einen bestimmten Zuschnitt von Intermediären Plattformen zwingend notwendig machen würden. Da das EU-OOTS die deutsche Identifikationsnummer nicht verwendet (siehe auch Kapitel 3.9.4.7), ist das IDNrG nicht einschlägig. Bei der Planung von Zahl und Zuschnitt ist dennoch zu berücksichtigen, dass die Intermediären Plattformen für die Erfüllung ihrer Aufgaben Zugriff auf die übermittelten Nachweisinhalte benötigen. Daher muss entweder durch die Aufteilung der Kommunikation zwischen verschiedenen Intermediären Plattformen, durch geeignete Schutzmechanismen innerhalb der Plattform, oder durch rechtliche und organisatorische Maßnahmen sichergestellt werden, dass die Gefahr einer unzulässigen Profilbildung ausgeschlossen ist.

Das hier vorliegende Konzept erfordert auch keine zwingende Trennung von Intermediären Plattformen für Nachweislieferanten und für Nachweis abrufende Behörden. Wie dargestellt verbindet beide ein Basis Set gemeinsamer Anforderungen, das durch unterschiedliche fallspezifische Anforderungen ergänzt wird. Es ist eine Gestaltungsmöglichkeit der Umsetzung, ob deshalb für beide Richtungen der Kommunikation getrennte Intermediärer Plattformen geschaffen werden („Zwillingslösung“) oder einzelne Intermediäre Plattformen direkt für beide Fälle ausgelegt werden.

Die Offenheit des Konzepts bzgl. der Zahl der Intermediären Plattformen ermöglicht es bei Bedarf, die beabsichtigte Pflicht zur Nutzung einer Intermediären Plattform mit den Bedürfnissen des Einzelfalls in Übereinstimmung zu bringen. Wenn es aufgrund spezifischer Anforderungen notwendig wäre, könnte im Extremfall z.B. auch eine separate Intermediäre Plattform nur für die Anbindung eines einzelnen Registers oder eines einzelnen Portals für Online-Services geschaffen werden. Es sollte dabei allerdings bedacht werden, dass die spezifischen Vorteile dieses Modells umso stärker zum Tragen kommen, je stärker die jeweilige Intermediäre Plattform eine Bündelung von Anbindungen für unterschiedliche Register übernehmen kann.

3.9.4.6 Übergreifende Facharchitektur für Intermediärer Plattformen

Logischer Aufbau der Intermediären Plattform (mit SDG-Connector)

Abbildung 38 zeigt den möglichen Aufbau von Intermediären Plattformen, um die genannten Aufgaben und Funktionen zu erfüllen.

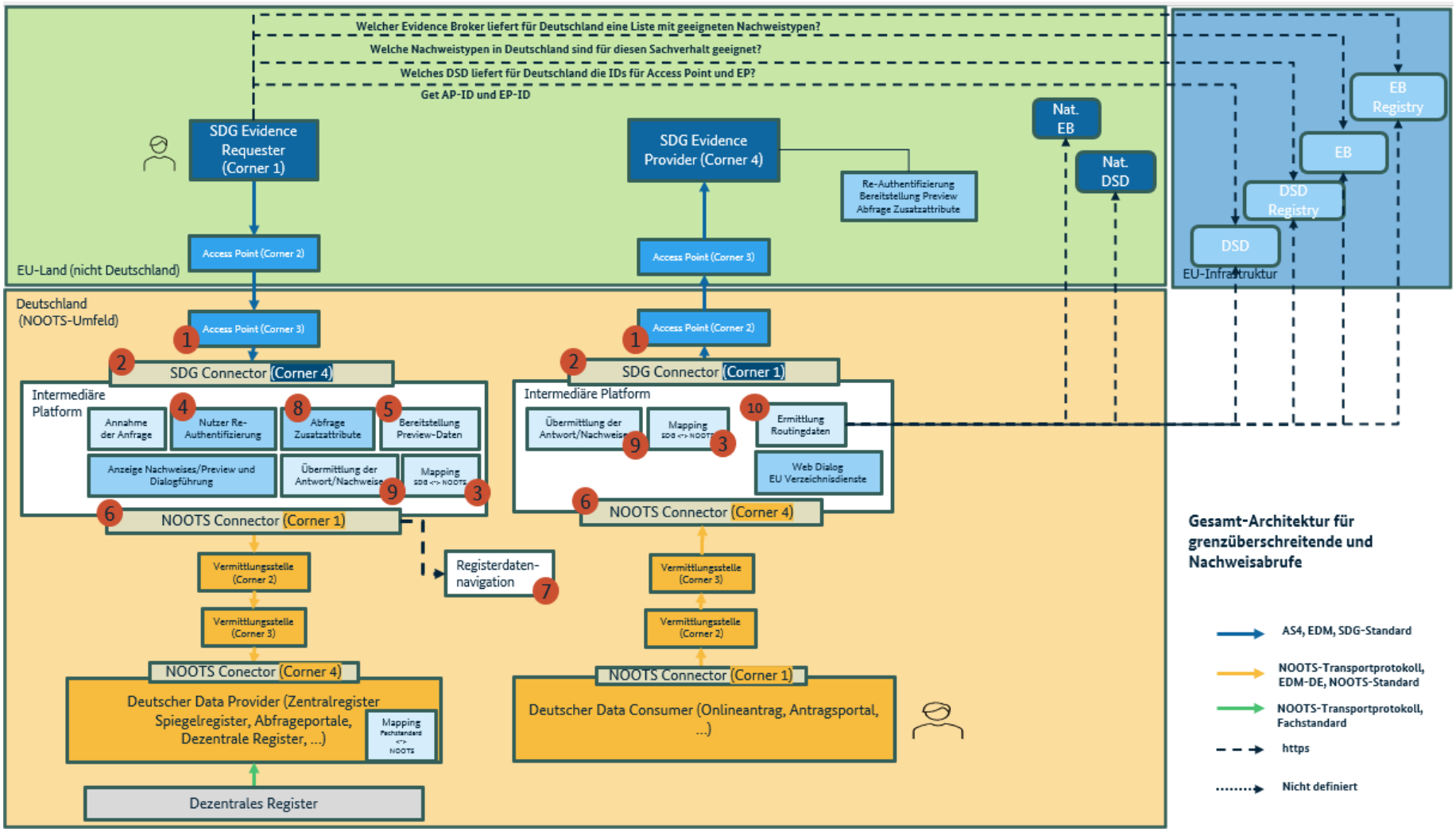


Abbildung 38: Logischer Aufbau der Intermediären Plattformen & Einbindung in grenzüberschreitenden Nachweisabrufen.

Tabelle 62: Übersicht Funktionen der Intermediären Plattform und relevante Komponenten des NOOTS

Nr. (Abbildung 38)	**Name des Elements**	**Erläuterung**
1	Access Point	Der „Access Point“ stellt die Schnittstelle für die zugehörige Intermediäre Plattform auf Transportebene bereit. In Corner 3 gibt er eingehende Anfragenachrichten an die Intermediäre Plattform weiter und gibt die Antwortnachrichten (einschließlich der abgefragten und von der Intermediären Plattform bereitgestellten Nachweise) an die anfragende Stelle im EU-Ausland weiter. In Corner 2 leitet er die Nachrichten entsprechend in umgekehrter Richtung weiter.
2	SDG-Connector	Der “SDG-Connector“ implementiert das Exchange Data Model (EDM) des EU-OOTS. Er nutzt den Access Point für die AS4-Kommunikation mit den anderen Access Points des EU-OOTS. In seiner Rolle als Corner 4 nimmt er Anfragen aus dem EU-Ausland entgegen und stellt die aus dem nationalen Kontext abgefragten Nachweise für den ausländischen Evidence Requester gemäß dem EDM zur Verfügung. Als Corner 1 verhält er sich wie ein Evidence Requester im Sinne des EU-OOTS und versendet Nachweisanfragen.
3	Mapping SDG <-> NOOTS	„Mapping SDG <-> NOOTS“ wandelt die eingegangene Anfragenachricht im EDM des EU-OOTS in eine Anfrage über das NOOTS um und umgekehrt.
4	Nutzer Re-Authentifizierung	Die „Nutzer Re-Authentifizierung“ verantwortet die Authentifizierung der Nutzenden und greift dafür ggf. auf weitere Komponenten (z.B. eID-Server) zurück.

Nr. (Abbildung 38)	Name des Elements	Erläuterung
5	Bereitstellung Preview-Daten	„Bereitstellung Preview-Daten“ ermittelt mit Hilfe der Komponente „NOOTS Connector (Corner 1)“ die Nachweisdaten.
6	NOOTS Connector	Der „NOOTS Connector (Corner 1)“ implementiert das nationale Nachrichtenmodell des NOOTS und verhält sich wie ein Data Consumer im Sinne des NOOTS, um den Nachweis von dem nationalen Evidence Provider abzufragen. Für die Ermittlung des zuständigen Evidence Providers im nationalen Kontext verwendet die Komponente dabei die Registerdatennavigation.
7	Registerdatennavigation	Die „Registerdatennavigation“ ist eine eigenständige Komponente des NOOTS, die auf Grundlage des benötigten Nachweistyps und weiterer Routingparameter (vgl. Zusatzattribute) den zuständigen Data Service in Deutschland und dessen Adressdaten ermittelt.
8	Abfrage Zusatzattribute	Die Komponente „Abfrage Zusatzattribute“ stellt einen Dialog zur Verfügung, um optional notwendige Zusatzattribute für die Ermittlung des richtigen Evidence Providers bei den Nutzenden abzufragen. Die ermittelten Zusatzattribute werden von der Intermediären Plattform zur Abfrage der Registerdatennavigation genutzt.
9	Übermittlung der Antwort/Nachweise	„Übermittlung der Antwort/Nachweise“ mappt mit Hilfe der Komponente „Mapping SDG <-> NOOTS“ die NOOTS Nachweisdaten in EU-OOTS Nachweisdaten bzw. umgekehrt.
10	Ermittlung Routingdaten	Über „Ermittlung Routingdaten“ werden über die zentralen Broker-Dienste der EU die für das jeweilige Land zuständigen Verzeichnisse abgefragt und anschließend

Nr. (Abbildung 38)	Name des Elements	Erläuterung
		der benötigten Nachweistyp sowie die Kontaktdaten des dafür zuständigen Data Services ermittelt.

Zu beachten ist, dass der hier vorgestellte Komponentenaufbau der Illustration der notwendigen Funktionalitäten einer Intermediären Plattform dient und nicht als normativ zu verstehen ist. Auch eine andere interne Strukturierung einer Intermediären Plattform ist zulässig, solange die gleiche Funktionalität erreicht wird.

Die Darstellung der innerstaatlichen Kommunikation der Intermediären Plattform ist ebenfalls nur illustrativ zu verstehen. So ist zum aktuellen Zeitpunkt noch nicht entschieden, ob in allen Fällen Vermittlungsstellen zu nutzen sind und ob OSCI in allen Fällen als Transportstandard genutzt wird. Für den innerstaatlichen Kommunikationsablauf gilt die jeweils gültige Fassung der Architekturvorgaben des NOOTS.

Rolle des SDG-Connectors

Das vorliegende Konzept erlaubt durch Nutzung Intermediärer Plattformen bereits eine starke Bündelung der Umsetzung der EU-spezifischen Technologien und entlastet so die einzelnen zuständigen Behörden. Allerdings ist zum aktuellen Zeitpunkt noch keine Entscheidung über die Anzahl und den Zuschnitt der Intermediären Plattformen getroffen worden. Auch wenn diese wesentlich geringer als die Zahl der zuständigen Behörden sein wird, bleibt damit das Risiko doppelter Implementierungsaufwände, wenn unterschiedliche Intermediäre Plattformen die Übersetzungsaufgaben zwischen EU-OOTS und NOOTS parallel umsetzen müssen.

Der IT-Planungsrat hat daher mit Beschluss 2022/34 festgelegt, für diese Übersetzungsaufgaben eine wiederverwendbare Komponente zu schaffen, die dann von unterschiedlichen Intermediären Plattformen integriert und genutzt werden kann. Dementsprechend zeigt die idealtypische Facharchitektur einer Intermediären Plattform in Abbildung 38 bereits die Verortung dieses SDG-Connector.

Der SDG-Connector dient dabei als Basiskomponente für das technisch-funktionale Mapping des Nachweisdatenaustausches im Kommunikationspattern des EU-OOTS auf das

noch zu präzisierende Nachweisaustauschformat im NOOTS. Er kann dabei für beide hier betrachteten Kommunikationsrichtungen über Intermediärer Plattformen und ggf. auch von weiteren Komponenten genutzt werden. Der SDG-Connector soll perspektivisch ein Produkt des IT-Planungsrats werden und in Kooperation mit anderen EU-Mitgliedstaaten hinsichtlich der EU-OOTS Interaktionsprinzipien konzeptionell spezifiziert und idealerweise kollektiv weiterentwickelt werden (z.B. im Rahmen der Connecting Europe Facility). Die Gesamtsteuerung Registermodernisierung erprobt und härtet das Konzept des SDG-Connector derzeit im Rahmen mehrerer Erprobungsprojekte mit anderen Mitgliedstaaten.

Zuordnung von Access Points zu Intermediären Plattformen

Die grenzüberschreitende Anfrage eines Evidence Requester bei einem Data Service erfolgt immer unter Nutzung des AS4-Transportprotokolls, das ein 4-Corner-Modell voraussetzt. Der Evidence Requester kontaktiert zunächst einen AS4 Access Point in seinem Mitgliedstaat, dieser kontaktiert einen AS4 Access Point im Mitgliedstaat des Data Services, und dieser gibt die Nachricht an den Data Service weiter. Die technische Entwurfsdokumentation (TDD) des EU-OOTS enthält detaillierte Vorgaben, wie die Access Points zu konfigurieren sind, da die AS4-Technologie selbst hier eine große Zahl von Optionen lässt. Das EU-OOTS verwendet aktuell keine Discovery-Mechanismen für Access Points, so dass in jedem Access Point die Kontaktdaten aller anderen Access Points des EU-OOTS konfigurativ hinterlegt werden müssen.

Die Mitgliedstaaten sind frei bei der Zahl und dem Zuschnitt der jeweiligen AS4 Access Points (Art. 3 Abs. 3 DVO). Die Routing-Logik des EU-OOTS verlangt lediglich, dass ein bestimmter Data Service stets über den gleichen Access Point erreichbar ist. Damit wäre es grundsätzlich möglich, dass eine Intermediäre Plattform für verschiedene von ihr bereitgestellte Data Services unterschiedliche Access Points nutzt. Allerdings ist kein Mehrwert dieses Ansatzes erkennbar, da er die Komplexität weiter steigern würde, so dass hier davon ausgegangen wird, dass eine Intermediäre Plattform ihre gesamte Kommunikation über den gleichen Access Point abwickelt.

Umgekehrt ist es grundsätzlich möglich, dass ein Access Point zur Anbindung mehrerer Intermediärer Plattformen dient. Da jede eingehende Nachricht eine Kennzeichnung des angefragten Data Service enthält, könnten die Anfragen vom Access Point eindeutig der jeweils relevanten Intermediären Plattform zugeordnet werden. Zum aktuellen Zeitpunkt kann nicht ausgeschlossen werden, dass eine solche Bündelung im Einzelfall genutzt wird.

Sie erscheint jedoch im Regelfall unter Betriebsgesichtspunkten nicht sinnvoll: Wenn eine Störung der Kommunikation mit dem EU-OOTS auftritt, wird in vielen Fällen nicht unmittelbar erkennbar sein, ob die Fehlerursache auf Seiten des Access Points oder bei der dahinterstehenden Intermediären Plattform liegt. Daher verspricht es für den laufenden Betrieb Vorteile, wenn jede Intermediäre Plattform genau einen ihr exklusiv zugeordneten Access Point nutzt und beide von der gleichen Organisation verantwortet werden. Dies soll daher im Folgenden als Normalfall angenommen werden.

3.9.4.7 Spezifische Aspekte der Facharchitektur für Intermediärer Plattformen für Nachweislieferanten

Registrierung der Data Services der Intermediären Plattform im europäischen Data Service Directory (DSD)

Bei verteilten Registerlandschaften wie in Deutschland können häufig mehrere Evidence Provider die gleichen Typen von Nachweisen ausstellen, und es muss im Einzelfall ermittelt werden, welcher Evidence Provider für die konkrete Anfrage zuständig ist. Dies kann sich z.B. bei einer regionalen Gliederung aus dem Wohnort der betroffenen Person ableiten, aber auch komplexeren Zuständigkeitslogiken folgen (siehe zu einer ausführlicheren Erläuterung dieser Herausforderung im innerstaatlichen Kontext auch das Kapitel 3.1 zur Registerdatennavigation im NOOTS).

Das EU-OOTS ermöglicht es in diesen Fällen, zunächst über das zuständige Data Service Directory (DSD) eine Liste aller in Frage kommenden Evidence Provider zu ermitteln und die Nutzenden daraus auswählen zu lassen. Dies wurde jedoch für Registerlandschaften wie etwa in Deutschland als unzureichend angesehen, da die Nutzenden ggf. unter Tausenden von Registerinstanzen auswählen müssten und auch nicht unbedingt mit der jeweiligen Zuständigkeitslogik der Verwaltung vertraut sind. Daher wurden u.a. auf deutsche Vorschläge hin zwei Mechanismen im EU-OOTS ermöglicht, mit denen die tatsächlich zuständige Registerinstanz genauer ermittelt werden kann.

1. Wenn die Mitgliedstaaten jeden ihrer Evidence Provider für einen bestimmten Nachweistyp einzeln im zuständigen DSD eintragen, können sie dort Zusatzattribute festlegen, die zur eindeutigen Ermittlung der richtigen Instanz genutzt werden können (Art. 5 Abs. 3 lit. b DVO). Das DSD übermittelt die Kategorien der benötigten Zusatzattribute an den aufrufenden Online-Service, der sie bei den Nutzenden abfragt

und anschließend wieder an das DSD übergibt, das damit den Kommunikationspartner ermitteln kann.

2. Wenn die Mitgliedstaaten Intermediäre Plattformen nutzen, die über ihre Preview-Umgebung direkt mit den Nutzenden interagieren, können auch dort von der Intermediären Plattform benötigte Zusatzattribute abgefragt und dann genutzt werden, um über mitgliedstaatspezifische Mechanismen die konkret zuständige Registerinstanz zu ermitteln.

Da beide Mechanismen alternative Lösungen für das gleiche Problem ermöglichen, ist es sinnvoll, für die nationale Umsetzung in Deutschland eine unnötige Dopplung zu vermeiden. Für Deutschland wird dabei die zweite Lösung präferiert, da hierdurch eine klare Entkopplung der Ebenen erreicht werden kann: Auf EU-Ebene müssen nur Daten über die Data Services der Intermediären Plattformen publiziert werden; Daten und Mechanismen zur innerstaatlichen Zuständigkeitsermittlung können hingegen auf das NOOTS beschränkt bleiben und auf dessen Zwecke hin optimiert werden. Daher sollen Zusatzattribute, die für die Zuständigkeitsfindung notwendig sind, in Deutschland immer über die jeweilige Intermediäre Plattform bei den Nutzenden abgefragt und anschließend für die Zuständigkeitsermittlung mit der Registerdatennavigation genutzt werden. Im Data Service Directory werden keine Data Services der einzelnen Evidence Provider und deren Zuständigkeitslogiken hinterlegt, sondern nur die Data Services der Intermediären Plattformen. Der Betreiber einer Intermediären Plattform muss entsprechend dafür Sorge tragen, dass die Daten zu den von ihr bereitgestellten Data Services im DSD jederzeit aktuell sind.

Exkurs: Europäisches oder nationales Data Service Directory (DSD)

Das EU-OOTS lässt den Mitgliedstaaten ein Wahlrecht, ihre Data Services in der zentralen europäischen Instanz des Data Service Directory bereitzustellen oder einen eigenen nationalen Dienst anzubieten, der die DSD-Schnittstelle für Abfragen bereitstellt (Art. 8 DVO). Die Entscheidung muss einheitlich für alle Data Services eines Mitgliedstaats getroffen werden.

Der IT-Planungsrat hat sich in Beschluss 2022/22 auf Vorschlag der Gesamtsteuerung Registermodernisierung dafür ausgesprochen, den Weg eines nationalen DSD zu gehen und eine entsprechende Schnittstelle in der nationalen Registerdatennavigation

vorzusehen. Hintergrund dieser Entscheidung war, dass auf Basis des damals vorliegenden Entwurfs der Durchführungsverordnung zu Art. 14 der SDG-VO nur der hier dargestellte Lösungsweg 1 allgemein möglich erschien: Eine Abfrage von Zusatzattributen durch eine Intermediäre Plattform war nur in Fällen mit Preview vorgesehen, so dass Lösungsweg 2 in allen Fällen ohne Preview unmöglich gewesen wäre. Damit wäre es für eine vollständige Umsetzung der SDG-Verpflichtungen in jedem Fall notwendig gewesen, eine Zuständigkeitsfindung über das DSD zu ermöglichen. Um eine sehr aufwändige Pflege nationaler Zuständigkeitslogiken im europäischen DSD zu vermeiden, war es daher sinnvoller, diese Rolle der nationalen Registerdatennavigation zu übertragen, die diese Informationen ohnehin pflegen muss.

Die Ausgangssituation hat sich gegenüber dem damaligen Stand jedoch wesentlich verändert, da in die finale Fassung der Durchführungsverordnung kurzfristig noch die Möglichkeit eingeführt wurde, auch in Fällen ohne Preview eine Weiterleitung der Nutzenden anzufordern (Art. 14 Abs. 2 i.V.m. Art. 11 Abs. 3 DVO). So können auch in diesen Fällen Zusatzattribute in einer Intermediären Plattform erhoben werden. Kommen die Nutzenden dieser Aufforderung nicht nach und ist das zuständige Register, ohne die benötigten Angaben nicht zu ermitteln, darf der Nachweisabruf auch fehlschlagen. Durch diese maßgebliche Veränderung der Anforderungen kann der – an sich vorzugswürdige – Lösungsweg 2 nun tatsächlich universell genutzt und die Zuständigkeitsfindung klar in den Intermediären Plattformen statt im DSD verortet werden.

Obwohl für das vorliegende Konzept Intermediärer Plattformen nicht zwingend, ermöglicht dieser Lösungsweg es auch, auf die aufwändige nationale Implementierung der DSD-Schnittstelle zu verzichten und das zentrale DSD zu nutzen, da ohnehin nur noch die Informationen zu den Data Services der Intermediären Plattformen im DSD bereitgestellt und keine komplexen Zuständigkeitslogiken auf der Ebene des DSD abgebildet werden müssen.

Nutzer-Authentifizierung

Die Intermediäre Plattform muss die im Evidence Request enthaltenen Identitätsdaten mit den vom jeweiligen Nachweislieferanten vorgehaltenen Identitätsdaten abgleichen; nur bei

eindeutiger Übereinstimmung dürfen Preview und Nachweisübermittlung erfolgen (Art. 16 Abs. 2 DVO).

Nachdem die Nutzenden auf die Umgebung der Intermediären Plattform weitergeleitet wurde, kann diese zudem von ihm eine erneute Authentifizierung verlangen (Art. 16 Abs. 1 DVO). In Deutschland sollte dies in allen Fällen vorgesehen werden, da sonst bereits ein missbräuchlicher Zugriff auf die Preview-URL ausreichen würde, damit Dritte unrechtmäßig über die Intermediäre Plattform vertrauliche Nachweisdaten in der Preview-Funktion einsehen können. Es besteht – anders als bei der Authentifizierung auf Seiten des Online-Service – keine explizite Verpflichtung zur ausschließlichen Nutzung eIDAS-notifizierter Authentifizierungsinstrumente; dennoch muss das notwendige Vertrauensniveau für die in der Folge abgerufenen und in der Preview dargestellten Nachweisdaten erreicht werden. Die Authentifizierung sollte so umgesetzt werden, dass sich die Nutzenden pro Sitzung auf einer Intermediären Plattform nur ein einziges Mal authentifiziert und nicht pro Nachweisabruf, sofern mehrere erfolgen.

Innerstaatlicher Nachweisabruf über das NOOTS

Die europäischen Dokumente sind nicht klar in der Frage, ob eine Intermediäre Plattform ggf. selbst Registerdaten (zwischen-)speichern kann, um daraus Anfragen zu beantworten (siehe insbesondere Abschnitt 1.2.7.7 der High-Level-Architecture der TDD, der möglicherweise über die Vorgaben der DVO hinausgeht). Um eine ausreichende Klarheit in der Konzeption zu erhalten, wird für die Umsetzung in Deutschland jedoch konzeptionell festgelegt, dass eine Intermediäre Plattform selbst keine Registerdaten vorhält. Dies schließt nicht aus, dass z.B. ein neues Spiegelregister und eine zugeordnete Intermediäre Plattform innerhalb eines integrierten Projekts entwickelt werden (siehe auch Kapitel 3.9.6.2 zu zentralen Strukturen); auch dann werden diese unterschiedlichen Bestandteile aber zumindest logisch-konzeptionell voneinander unterschieden.

Da eine Intermediäre Plattform also selbst keine Registerdaten vorhält, muss sie die benötigten Nachweisinformationen zur Beantwortung einer Anfrage bei dem zuständigen Evidence Provider abrufen. Hierfür sollen im Normalfall die Mechanismen des NOOTS genutzt werden, die parallel zur Konzeption Intermediärer Plattformen entwickelt werden.

Für den Registerabruf muss die Intermediäre Plattform zunächst bestimmen, welche konkrete Registerinstanz für den konkreten Einzelfall zuständig ist (wenn ein Nachweistyp nicht ohnehin nur von einem Zentralregister geliefert wird). Hierfür ruft die Intermediäre Plattform die nationale Registerdatennavigation auf. Wenn für die Ermittlung der

Zuständigkeit Zusatzangaben notwendig sind, die nicht der originären Anfrage entnommen werden können, dann erhebt die Intermediäre Plattform diese direkt über eine entsprechende Dialogführung bei den Nutzenden.

Anschließend ruft die Intermediäre Plattform die benötigten Nachweisinformationen gemäß den allgemeinen Mechanismen des NOOTS vom zuständigen Evidence Provider ab. Dies beinhaltet die Nutzung des Nachrichtenmodells des NOOTS, die Nutzung der vom NOOTS vorgegebenen Transportstandards und auch die Einhaltung weiterer Vorgaben wie bspw. die Kommunikation über Vermittlungsstellen in den vom IDNrG und der NOOTS-Architektur vorgegebenen Fällen. Die Einzelheiten zu diesen Vorgaben des NOOTS werden parallel zur Konzeption Intermediärer Plattformen durch die Gesamtsteuerung Registermodernisierung entwickelt. Die Intermediäre Plattform muss im Identitäts- und Zugriffsmanagement für Behörden die entsprechenden Rechte erhalten, die für ihre Data Services benötigten Nachweisinformationen über das NOOTS von den eigentlichen Evidence Providern anfordern zu können.

Innerstaatlicher Nachweisabruf über bilaterale Anbindung oder bestehende Informationsverbünde

Da sich das NOOTS erst im Aufbau befindet und die Umsetzung der SDG-Verpflichtungen einer engen Frist unterliegt, kann die Situation eintreten, dass Nachweisinformationen über eine Intermediäre Plattform bereitgestellt werden sollen, bevor ein entsprechender Abruf über das NOOTS möglich ist.

Sofern die relevanten Evidence Provider bereits andere Formen des digitalen Nachweisabrufs unterstützen, ist es in diesen Fällen denkbar, übergangsweise auf diese zurückzugreifen. Bei Zentralregistern ist hier eine direkte bilaterale Anbindung des jeweiligen Registers über dessen bestehende Kommunikationsmechanismen möglich. Bei dezentralen Registern, die bereits Nachweisabrufe ermöglichen, sind die betreffenden Dienste häufig in DVDV verzeichnet. Hier kann die Intermediäre Plattform aus den Angaben der Anfrage und ggf. weiteren, bei den Nutzenden erhobenen Daten den DVDV-Schlüssel des Dienstes der zuständigen Registerinstanz ermitteln und dann über den Fachstandard des bereits existierenden Dienstes die entsprechenden Nachweisinformationen abrufen.

Anders als bei der Nutzung der generischen Mechanismen des NOOTS muss in diesen Fällen die fachliche Zuständigkeitslogik zur Ermittlung des DVDV-Schlüssels in der Intermediären Plattform selbst implementiert werden und zudem für jeden Nachweistyp der jeweilige fachspezifische Standard unterstützt werden; dies erhöht die Aufwände für die Umsetzung

der Intermediären Plattform. Zudem besteht die Gefahr, dass ein solches Provisorium eine zeitnahe Migration auf die NOOTS-Technologien behindert, sobald diese verfügbar sind. Eine Registeranbindung über derartige Legacy-Mechanismen ist daher einer Anbindung über das NOOTS klar unterlegen und sollte nur als letzte Option zur Einhaltung der gesetzlichen Verpflichtungen genutzt werden.

Nachweisabruf über bestehende Systeme des grenzüberschreitenden Nachweisabrufs

In verschiedener Fachlichkeit existieren in der EU bereits etablierte Systeme für den grenzüberschreitenden Nachweisabruf zwischen Behörden mit Blick auf den jeweiligen fachlichen Bedarf. Erfüllt ein solches System die restriktiven Anforderungen des Art. 14 Abs. 10 SDG-VO, entfällt durch sein Vorhandensein die Notwendigkeit einer separaten Anbindung der entsprechenden zuständigen Behörden an das EU-OOTS; diese Fälle sollen hier deshalb nicht weiter betrachtet werden. In allen anderen Fällen ermutigt Erwägungsgrund 6 der DVO Kommission und Mitgliedstaaten, zu prüfen, ob durch eine technische Kopplung der Systeme eine einfachere Umsetzung der Anbindung an das EU-OOTS möglich wird.

Wenn eine solche Kopplung inhaltlich sinnvoll ist, ist zunächst zu klären, ob sie auf europäischer oder mitgliedstaatlicher Ebene erfolgt. Bei der Verbindung zweier gesamteuropäischer Systeme erscheint es zunächst naheliegend, eine zentrale Verbindung auf EU-Ebene anzustreben, wodurch ggf. eine separate Anbindung der über das System erreichbaren Evidence Provider an das EU-OOTS entfallen könnte. Allerdings ist auch denkbar, dass eine rein zentrale Kopplung der Systeme den Anforderungen des EU-OOTS nicht gerecht werden kann. Dies könnte z.B. dann der Fall sein, wenn das bestehende System nur Behörde-zu-Behörde-Abrufe unterstützt, aber im EU-OOTS eine Vorschaupflicht besteht und diese daher nicht über das bestehende System erfüllt werden kann. Auch in diesen Fällen könnte ggf. die bereits bestehende Abrufmöglichkeit für die betreffenden Nachweise noch sinnvoll genutzt werden, indem eine Kopplung auf nationaler Ebene erfolgt. Daher sollte auch bei der Konzeption einer Intermediären Plattform geprüft werden, ob die Nachweise der anzuschließenden Evidence Provider ggf. einfacher abgerufen werden können, indem die Intermediäre Plattform ein bereits bestehendes europäisches System zum Nachweisabruf nutzt, an das der Evidence Provider bereits angebunden ist. Dies muss aber stets im Einzelfall mit Blick auf die konkreten Evidence Provider beurteilt werden, die über die spezifische Intermediäre Plattform angebunden werden sollen.

Keine Nutzung der Identifikationsnummer im EU-OOTS und Möglichkeiten der Nutzung durch Intermediäre Plattformen

Die Stammdaten, die im EU-OOTS zu einer Person übermittelt werden, basieren auf dem jeweiligen Datensatz des von den Nutzenden eingesetzten, eIDAS-konformen Authentifizierungsinstruments (in Deutschland in der Regel der eID des Personalausweises, des elektronischen Aufenthaltstitels oder der eID-Karte für Bürgerinnen und Bürger des Europäischen Wirtschaftsraums). Dieser Datensatz enthält bei in Deutschland ausgestellten Authentifizierungsinstrumenten nicht die Personen-Identifikationsnummer nach dem IDNrG, die daher im EU-OOTS auch nicht übermittelt und grenzüberschreitend nicht genutzt wird.

Allerdings sieht das NOOTS für die Zukunft den Datenabruf unter Nutzung der IDNr bei natürlichen Personen als den Regelfall vor. Es ist daher grundsätzlich denkbar, dass die Intermediäre Plattform mit den aus der Anfrage verfügbaren Personendaten über den Identitätsdatenabruf die zur Person gehörige IDNr ermittelt, um sie für den anschließenden Nachweisabruf zu nutzen, soweit dies rechtlich zulässig ist. Auch in diesen Fällen würde die IDNr jedoch nur für den innerstaatlichen Nachweisabruf der Intermediären Plattform beim zuständigen Register genutzt und nicht in der grenzüberschreitenden Antwort weitergegeben werden, solange die von Deutschland notifizierten Authentifizierungsinstrumente die IDNr nicht zu den dort enthaltenen Personendaten zählen.

Gesamtüberblick: Der Ablauf eines Nachweisabrufs aus dem EU-Ausland von einem deutschen Evidence Provider

Das Sequenzdiagramm im Anhang (Abbildung 40) beschreibt die Kommunikation zwischen einem europäischen Evidence Requester und einem deutschen Evidence Provider über eine Intermediäre Plattform anhand des folgenden Beispiels: Ein in Deutschland geborener Staatsbürger benötigt für die Eheschließung in den Niederlanden einen Nachweis aus Deutschland über seine Geburt.

Zur Vereinfachung der Darstellung wurden die Access Points sowie die Vermittlungsstellen (siehe auch Kapitel 3.9.4.6 und insbesondere Abbildung 38) weggelassen.

Die folgende Tabelle fasst die Einzelschritte erläuternd zusammen, um eine Übersicht zu erhalten.

Tabelle 63: Erläuterung der Sequenzschritte eines Nachweisabrufs aus dem EU-Ausland

Schritte	Beschreibung
[010] – [130]	Diese Schritte beschreiben die Kommunikation zwischen den Nutzenden und einem Evidence Requester im EU-Ausland (z.B. ein Online-Service), sowie die Kommunikation zwischen dem Evidence Requester und den zentralen, von der EU bereitgestellten Komponenten (im Kontext des EU-OOTS). Zuletzt hat der Evidence Requester die Informationen, welcher Nachweistyp in Deutschland abgefragt und über welche Intermediäre Plattform die Abfrage gestellt werden soll. Voraussetzung hierfür ist, dass die Intermediäre Plattform entsprechend im EU-DSD für den entsprechenden Nachweistyp registriert/konfiguriert ist.
[140] – [150]	Mit diesen Schritten beginnt die Kommunikation mit den von DE bereitgestellten Komponenten. Hier erfolgt die (erste) Anfrage im EU-OOTS an die zuständige IP.
[160] – [250]	Wenn eine Nutzerinteraktion auf Seiten der Intermediären Plattform notwendig ist, lehnt die Intermediäre Plattform die erste Abfrage ab und gibt mit der Fehlermeldung eine URL der Intermediären Plattform zurück, auf die die Nutzenden weiterzuleiten sind. Dort wird er im nationalen Kontext authentifiziert (190-200) und es können ggf. notwendige Zusatzattribute von ihm abgefragt werden (210-240, siehe dazu auch Abbildung 40, Punkt 8). Parallel muss der Evidence Requester eine erneute Abfrage stellen (250). Dieser wird von der Intermediären Plattform der ursprünglichen Abfrage zugeordnet (260) und erst weiterbearbeitet, wenn die notwendige Nutzerinteraktion bis Schritt 240 erfolgt ist.
[270] – [280]	Hier findet die Kommunikation der IP mit der Registerdatennavigation statt, um den richtigen Evidence Provider im NOOTS zu ermitteln (vgl. Abbildung 40, Punkt 7).
[290]	Die Daten des eingegangenen SDG-Requests werden auf NOOTS Informationen gemappt (vgl. Abbildung 40, Punkt 3).
[300] – [310]	Die IP tritt nun im NOOTS als Data Consumer auf, erzeugt einen Request im Kontext des NOOTS und schickt die Anfrage an den ermittelten Evidence Provider (vgl. Abbildung 40, Punkt 6), der den Nachweis bereitstellt.

Schritte	Beschreibung
[320] – [330]	Wenn eine Preview erforderlich ist, zeigt die Intermediäre Plattform den Nutzenden den Nachweis an und holt ihre Bestätigung ein, dass die Nachweisübermittlung fortgesetzt werden soll.
[340]	Wurden die Nutzenden auf eine Weboberfläche der Intermediären Plattform weitergeleitet, werden sie hier wieder zum ursprünglichen Online-Service des Evidence Requester zurückgeleitet.
[350] – [370]	Der Nachweis wird an den Evidence Requester im EU-Ausland übermittelt, der ihn nun für das Antragsverfahren nutzen kann. Die Intermediäre Plattform kann die Session-Daten löschen, da der Vorgang für sie abgeschlossen ist.

Der dargestellte Ablauf setzt voraus, dass für die Zuständigkeitsermittlung bei einem bestimmten Nachweistyp oder für die Identifikation des korrekten Datensatzes in einem Registertyp immer die gleichen Zusatzattribute notwendig sind (wenn überhaupt), sodass diese dem Dienst der Intermediären Plattform vorab bekannt sind und auf Basis des in der ursprünglichen Anfrage genannten Nachweistyps von den Nutzenden eingefordert werden können.

Sollten die benötigten Zusatzattribute sich von Fall zu Fall unterscheiden, muss die Intermediäre Plattform die Abfrage der Registerdatennavigation bzw. des Evidence Provider vorziehen und initial bereits vor der Entscheidung durchführen, ob eine Nutzerinteraktion notwendig ist (also vor Schritt 160). Die Intermediäre Plattform könnte dann dynamisch auf Basis der Antwortnachrichten von Registerdatennavigation bzw. Evidence Provider entscheiden, ob und ggf. welche Zusatzattribute im Einzelfall abgefragt werden müssen. Die aktuelle Konzeption der Registerdatennavigation sieht vor, dass die Registerdatennavigation fehlende Zuständigkeitsparameter zur Laufzeit als Fehler zurückgeben kann, so dass auch ein solcher Ablauf möglich wäre (siehe Kapitel 3.1 Registerdatennavigation). Ob auch Evidence Provider im NOOTS die Möglichkeit erhalten sollen, im Falle fehlender Informationen einen spezifischen Fehler zurückzugeben, der die benötigten Zusatzattribute enthält und für einen solchen Ablauf genutzt werden könnte, muss im Rahmen der weiteren Konzeption des deutschen Nachrichtenmodells noch entschieden werden.

3.9.4.8 Spezifische Aspekte der Facharchitektur für datenabrufende Stellen

Autorisierung der Intermediären Plattform zur Nutzung der zentralen Dienste des EU-OOTS

Intermediäre Plattformen haben sich möglicherweise an zwei Stellen als legitime Kommunikationspartner im EU-OOTS ausweisen: Bei der Kommunikation mit den zentralen europäischen Verzeichnisdiensten (Evidence Broker und Data Service Directory) und beim eigentlichen Nachweisabruf. In letzterem Fall verwendet die IP einen zugelassenen Access Point, dem die EU-Kommunikationspartner vertrauen, da sie davon ausgehen, dass national sichergestellt wurde, dass nur berechtigte Behörden den Access Point nutzen können.

Bei der Kommunikation mit den zentralen EU-Komponenten wird jedoch kein Access Point verwendet, sondern Anfragen direkt über eine REST-Schnittstelle gestellt. Die technische Entwurfsdokumentation (TDD) des EU-OOTS lässt derzeit noch offen, welche Form der Authentifizierung die zentralen Dienste hier erwarten. Der aktuelle Diskussionsstand in den Sub-Groups TDD und Security der EU SDG Coordination Group geht zum Zeitpunkt der Erstellung dieses Konzepts davon aus, dass vollständig auf eine Authentifizierung verzichtet wird, weil die Informationen in den zentralen Diensten allgemein zugänglich sein sollen. Sollte diese Frage jedoch anders entschieden werden, muss die Intermediäre Plattform für nachweisanfordernde Behörden die entsprechenden Mechanismen umsetzen, um die zentralen Dienste abfragen zu können.

Dynamische Ermittlung der zuständigen Verzeichnisdienste

Um für EU-Partner auffindbar zu sein, müssen die Mitgliedstaaten dafür sorgen, dass ihre Nachweise und Dienste in einem Verzeichnis geführt werden. Sie haben dabei aber die Wahl, ob sie die zentralen EU-Verzeichnisse (Evidence Broker und Data Service Directory) nutzen wollen oder eigene nationale Verzeichnisse zur Verfügung stellen. Da sich die zuständigen Verzeichnisse also zwischen den Mitgliedstaaten unterscheiden und sich ggf. auch über die Zeit hinweg ändern können, muss die Intermediäre Plattform bei jedem Nachweisabruf ermitteln, welche konkreten Verzeichnisse sie anzufragen hat. Dies geschieht über die beiden EU-Komponenten Evidence Broker Registry und Data Service Directory Registry mit folgenden Anfragen:

1 Die Intermediäre Plattform fragt beim Evidence Broker Registry, welcher Evidence Broker für das gewünschte Land zuständig ist. Mögliche Antworten:

a. EU Evidence Broker

b. Jeweiliger nationaler Evidence Broker

2 Die Intermediäre Plattform fragt beim Data Service Directory Registry, welches Data Service Directory für das gewünschte Land zuständig ist. Mögliche Antworten:

a. EU Data Service Directory

b. Jeweiliges nationales Data Service Directory

Mehrstufige Weiterleitung

Beim Einsatz von Intermediären Plattformen werden die Nutzenden, ausgehend vom ursprünglichen Online-Service, zweimal weitergeleitet: einmal innerhalb Deutschlands vom Online-Service zur Intermediären Plattform, ein weiteres Mal zur Preview-Umgebung im Mitgliedstaat des Nachweislieferanten.

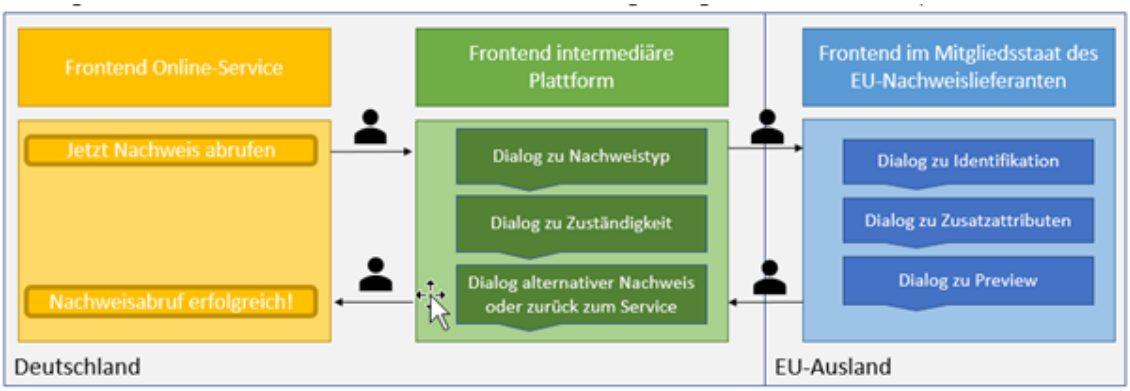


Abbildung 39: Zweistufige Nutzerweiterleitungen beim Einsatz von Intermediären Plattformen

Der Online-Service muss in seinem Frontend keine für den EU-Nachweisabruf spezifischen Dialoge vorhalten. Es genügt ein nutzerfreundlicher Absprung in die IP-Umgebung sowie im Erfolgsfall eine Erfolgsmeldung oder alternativ im Nicht-Erfolgsfall ein entsprechender Hinweis, was die Nutzenden alternativ tun können.

Das aktuelle Konzept geht davon aus, dass ein Aufruf der Intermediären Plattform pro Nachweistyp erfolgt; da es aber sein kann, dass die Nutzenden sich (nacheinander) mehrere Alternativen von Nachweistypen oder Nachweislieferanten in der Preview anschauen möchten, empfiehlt es sich vorzusehen, dass die Nutzenden nach der Interaktion mit dem Nachweislieferanten erst wieder auf die Intermediäre Plattform zurückgeleitet werden, um dort zu entscheiden, was sie als nächstes tun möchten.

Denkbar ist aber auch, dass die Intermediäre Plattform für mehrere Nachweistypen auf einmal aufgerufen wird. Dies wäre vor allem dann vorteilhaft, sollte auf der Intermediären Plattform eine erneute Authentifizierung der Nutzenden anfallen. Daher ist diese Entscheidung in der Feinkonzeption in Anbetracht der gesamten Nutzererfahrung zu treffen.

In jedem Fall sollte der Nutzerdialog in der Intermediären Plattform so aufgesetzt sein, dass die Nutzenden keine manuelle Änderung der geforderten Nachweistypen vornehmen können, die der Online-Service beim Aufruf der IP mitgibt; die Auswahl bezieht sich allein auf zulässige Alternativen.

Hinweis: Sollte der EU-Nachweislieferant gemäß dem für seinen Nachweistyp festgelegten Vertrauensniveau eine eIDAS-konforme Nutzer-Authentifizierung durchführen, kann es sein, dass die Nutzenden auf die Umgebung eines Drittanbieters umgeleitet werden; dies ist in der obigen Abbildung nicht dargestellt.

Die Intermediäre Plattform muss sicherstellen, dass sie die Backend-Kommunikation mit dem Data Service (die über die Access Points im 4-Corner-Modell erfolgt) und die Weiterleitung der Nutzenden auf die Preview-Umgebung im Mitgliedstaat des Evidence Providers richtig aufeinander abstellt. Die Weiterleitung der Nutzenden ist erst möglich, wenn der initiale Evidence Request vom Data Service beantwortet wurde, da die fallspezifische Preview-URL mit der Antwort bereitgestellt wird. Sobald die Nutzenden weitergeleitet werden, sollte die Intermediäre Plattform nun einen erneuten Evidence Request stellen. Dieser wird vom Data Service offengehalten und beantwortet, sobald die Nutzenden die Entscheidung über die Bestätigung der Preview getroffen haben; auf diese Weise muss die Intermediäre Plattform selbst keine Kenntnis davon haben, wo sich die Nutzenden auf Seiten der Preview-Umgebung im Prozess befinden.

Nutzer-Authentifizierung

Nachweisabrufe über das EU-OOTS setzen zwingend eine Authentifizierung unter Nutzung eines notifizierten eIDAS-Authentifizierungsinstruments voraus (Art. 11 Abs. 1 DVO). Die Intermediäre Plattform muss daher eine entsprechende Authentifizierung sicherstellen, bevor sie auf Ersuchen der Nutzenden einen Nachweisabruf auslösen kann. Um im Interesse der Nutzerfreundlichkeit wiederholte Authentifizierungen zu vermeiden, sollte die Intermediäre Plattform zunächst prüfen, ob der Online-Service die Nutzenden bereits authentifiziert hat. Da eine Single-Sign-On Lösung mit einer Weitergabe der Anmeldedaten der Nutzenden im eIDAS-Kontext aufgrund datenschutzrechtlicher Vorgaben nicht

möglich ist, sollte der Online-Service auf die bekannte Praxis setzen, die Information über die erfolgreiche Authentifizierung der Antragstellenden zu bestätigen, indem der Online-Service den Request (Abfrage eines Nachweises) mit Hilfe des technischen Zertifikats des Online-Service signiert. Die Intermediäre Plattform kann die Signatur prüfen und dadurch, bei erfolgreicher Prüfung, von einer sicheren Authentisierung der Antragstellenden ausgehen. Die Anmeldedaten selbst erhält die Intermediäre Plattform dabei nicht; die für den Nachweisabruf benötigten Personendaten entnimmt sie stattdessen aus den Nutzdaten des Requests. Dieses Vorgehen kann bei Bedarf auch in einer Kette von aufeinanderfolgenden Diensten genutzt werden, wenn diese Dienste jeweils der Authentisierung des Online-Service vertrauen sollen.

Im Fall, dass die Nutzenden im Online-Service noch nicht authentifiziert wurden, führt die Intermediäre Plattform die Authentifizierung selbst durch. In beiden Szenarien sollte die Authentifizierung für die Dauer der gesamten Sitzung erhalten bleiben.

Statische oder dynamische Regelung der Preview-Verpflichtung

Nach Art. 14 Abs. 5 SDG-VO entfällt die Verpflichtung zur Preview der abgerufenen Nachweise, wenn dies durch eine entsprechende europarechtliche oder mitgliedstaatliche Vorschrift bestimmt wird. Während dies bei europarechtlichen Vorschriften eindeutig ist, enthalten weder die SDG-VO noch der Durchführungsrechtsakt zu Art. 14 SDG-VO explizite Vorgaben dazu, wie mit möglicherweise unterschiedlichen Regelungen in den beteiligten mitgliedstaatlichen Rechten umzugehen ist. Die DVO sieht jedoch immerhin vor, dass die Nachweis-anfordernde Behörde oder ihre Intermediäre Plattform in ihrem Evidence Request kennzeichnen muss, ob die Preview nach ihrer Rechtsauffassung notwendig oder entbehrlich ist (Art. 13 Abs. 1 lit. k DVO). Daher muss für jede Intermediäre Plattform festgelegt werden, wie sie diese Information wiederum von der für die Beurteilung originär zuständigen Nachweis anfordernden Behörde erhält.

Es herrscht die Annahme, dass Ausnahmen von der Preview-Verpflichtung nach Art. 14 Abs. 5 SDG-VO, falls sie auftreten, in der Regel den Abruf bestimmter Nachweistypen in bestimmten Verfahren als Ganzes betreffen werden und langfristig stabil bleiben. Solange dies der Fall ist, können derartige Sonderfälle zwischen der zuständigen Behörde und dem Betreiber der Intermediären Plattform auf organisatorischem Weg kommuniziert werden. Die Ausnahmefälle werden dann konfigurativ in der Intermediären Plattform hinterlegt, die dann eine entsprechende Kennzeichnung der Evidence Requests in diesen Fällen vornimmt. Entsprechend der Wertung der Art. 14 SDG-VO kennzeichnet die Intermediäre Plattform in

allen Fällen, für die keine explizite Ausnahme konfiguriert ist, eine Preview in der Anfrage als "notwendig".

Nur dann, wenn Ausnahmen von der Preview-Pflicht an spezifische Umstände des jeweiligen Einzelfalls anknüpfen würden, müsste die Schnittstelle zwischen Online-Service und Intermediärer Plattform es beim einzelnen Aufruf ermöglichen, zu kennzeichnen, dass im konkreten Fall keine Preview vorgesehen ist. Dieser Fall wird hier als unwahrscheinlich angesehen und daher nicht weiter ausgestaltet.

Gesamtüberblick: Der Ablauf des Abrufs eines deutschen Evidence Requester mit einer Intermediären Plattform im EU-Ausland

Das Sequenzdiagramm im Anhang (Abbildung 41) beschreibt die Kommunikation zwischen einem deutschen Data Consumer und einem europäischen Evidence Provider (in der Abbildung SDG Evidence Provider genannt) über eine Intermediäre Plattform anhand des folgenden Beispiels: Ein im EU-Ausland geborener Staatsbürger benötigt für die Eheschließung in Deutschland einen Nachweis aus dem EU-Ausland über seine Geburt.

Zur Vereinfachung der Darstellung wurden die Access Points weggelassen.

Die folgende Tabelle fasst die Einzelschritte erläuternd zusammen, um eine Übersicht zu erhalten.

Tabelle 64: Erläuterung der Sequenzschritte des Abrufs eines europäischen Nachweises aus Deutschland

Schritte	Beschreibung
[010] – [070]	Diese Schritte beschreiben den Beginn des Nachweisabrufs auf der Umgebung des Data Consumers. Dieser ruft die Intermediäre Plattform mit einer Anfrage zur Nachweiserbringung aus dem EU-Ausland äquivalent zu einem bestimmten deutschen Nachweistyp auf und leitet die Nutzenden an die (ihnen fest zugeordnete) Intermediäre Plattform weiter.
[080] – [140]	Auf der Intermediären Plattform ermittelt die IP zunächst intern, welcher Sachverhalt gemäß der EU-Systematik nachzuweisen ist. Anschließend ermittelt sie beim Evidence Broker Registry, welcher Evidence Broker für das gewünschte Land zuständig ist, und fragt diesen nach den verfügbaren Nachweistypen für den Sachverhalt. Im Falle von mehreren Optionen, lässt die Intermediäre Plattform den Nutzenden eine auswählen.
[150] – [240]	Die Intermediäre Plattform ermittelt anschließend im Data Service Directory Registry das zuständige Data Service Directory. Bei diesem fragt sie den zuständigen Data-Service an. Sind hierfür Zusatzattribute

Schritte	Beschreibung
	vonnöten, erfragt sie diese bei den Nutzenden. Gibt es mehrere mögliche Evidence Provider/Data-Services lässt die Intermediäre Plattform den Nutzenden darunter einen auswählen.
[250] – [280]	Die Intermediäre Plattform unternimmt ein Mapping des NOOTS Requests, den sie vom Data Consumer erhalten hat, in einen EU-OOTS-Request und sendet ihn den zuständigen Evidence Provider/Data-Service im EU-Ausland. Hierbei erfolgt die (erste) Anfrage im EU-OOTS.
[290] – [470]	Der EU Evidence Provider nimmt den Request entgegen und prüft zunächst, ob ihm bereits eine Preview zu dieser ID vorliegt. Ist das nicht der Fall, sendet er einen Link an die Intermediäre Plattform, über die die Nutzenden in ihre Umgebung geleitet werden. Hier re-authentifiziert der Evidence Provider die Nutzenden, wenn nötig (300-370). Wenn die übergebenen Identitätsdaten nicht ausreichen, um den Datensatz der betroffenen Person eindeutig zu identifizieren, fragt der EU Evidence Provider bei den Nutzenden Zusatzattribute ab. Anschließend zeigt er den Nutzenden eine Preview des Nachweises und gibt diesen die Möglichkeit, dessen Verwendung zuzustimmen oder sie abzulehnen. Bei dieser Interaktion sind weder Data Consumer noch IP beteiligt. Am Ende dieses Abschnitts werden die Nutzenden zurück auf die Intermediäre Plattform geleitet.
[480] – [520]	Die Zustimmung der Nutzenden zur Preview löst einen erneuten Nachweisabruf durch die IP beim Evidence Provider aus. Da diesem unter der entsprechenden Anfrage-ID diesmal eine Bestätigung der Nutzenden vorliegt, sendet sie den Nachweis an die Intermediäre Plattform (510). Haben die Nutzenden der Preview nicht zugestimmt, haben sie die Wahl, entweder einen anderen Nachweistyp oder Evidence Provider zu wählen oder zum Antrag zurückzukehren (im Diagramm nicht dargestellt).
[530] – [580]	Die Intermediäre Plattform leitet die Nutzenden zurück in die Umgebung des Data Consumers und übergibt auch die Session ID, unter der die Zustimmung des Users gespeichert ist. Dies löst eine erneute Nachweis-Anfrage seitens des Data Consumers bei der IP aus, die dieses Mal von der IP mit der Zusendung des Nachweises beantwortet wird.

3.9.4.9 Abgrenzungen

Im Kontext von Hilfsdiensten der Infrastruktur sind neben Intermediären Plattformen bei Registerdatenabrufen weitere Arten von Komponenten relevant, die hier daher zur Vermeidung von Missverständnissen von Intermediären Plattformen abgegrenzt werden sollen.

Service Gateway

Ein Service Gateway ist ein technischer Zugang zu einem Dienst, der über ein definiertes Protokoll und festgelegte Nachrichten die Funktionen dieses Dienstes für eine anfragende Stelle zugänglich macht. Jedes Register, das seine Funktionen (z.B. Erteilung einer Auskunft/eines Nachweises) in einer elektronischen Form zur Verfügung stellen will, braucht mindesten einen Service Gateway (SGW) um diese verfügbar machen zu können.

Auch Intermediäre Plattformen können Service Gateways zur Umsetzung einzelner Schnittstellen nutzen.

Vermittlungsstelle (Data Consumer Gateway/Data Provider Gateway)

Eine Vermittlungsstelle ist ein Dienstleister, der im NOOTS Transportaufgaben übernimmt und zugleich eine Kontrollfunktion nach § 7 Abs. 2 IDNrG ausübt, in dem er – ohne Kenntnis der Nachrichteninhalte – eine abstrakte Berechtigungsprüfung der über die Vermittlungsstelle übertragenen Nachweisabrufe vornimmt. Ihr Einsatz ist für bereichsübergreifende Datenübermittlungen unter Nutzung der Identifikationsnummer im Rahmen der Maßgaben des IDNrG zwingend vorgeschrieben. In der Architektur des NOOTS ist noch keine Entscheidung gefallen, ob sie ggf. auch für andere Arten von Registerabrufen zu nutzen sind. Bei Nutzung von Vermittlungsstellen entsteht für Datenabrufe im NOOTS ebenfalls eine 4-Corner-Architektur, in der die Vermittlungsstellen eine ähnliche Basisfunktion wie die AS4 Access Points im EU-OOTS übernehmen, die aber noch um den Kontrollaspekt erweitert wird. Vermittlungsstellen werden innerstaatlich – je nachdem, von welchem Endpunkt der Kommunikation sie genutzt werden – auch als Data Consumer Gateway bzw. Data Provider Gateway bezeichnet und sollten nicht mit den o.g. Service Gateways verwechselt werden.

Vermittlungsstellen müssen strikt von Intermediären Plattformen getrennt werden, da sie keine Kenntnis der Nachrichteninhalte erlangen dürfen und daher die in diesem Konzept vorgestellten Aufgaben Intermediärer Plattformen nicht übernehmen können. Für den innerstaatlichen Nachweisabruf über das NOOTS müssen Intermediäre Plattformen jedoch Vermittlungsstellen nutzen, soweit dies nach den Vorgaben des IDNrG und der NOOTS-Architektur vorgesehen ist (siehe Kapitel 3.8).

3.9.5 Technische Aspekte

Die im Folgenden dargestellten nicht-funktionen Aspekte müssen im Rahmen der Konzeption einzelner Intermediärer Plattformen weiter konkretisiert und mit

entsprechenden Schutzbedarfsfeststellungen unterlegt werden. Dennoch sollen an dieser Stelle bereits Hinweise auf einige besonders wichtige Aspekte gegeben werden, die in der späteren Detailkonzeption zwingend zu berücksichtigen sind.

3.9.5.1 Datenschutz

Die Intermediäre Plattform ist eine Infrastrukturkomponente, die Registerabrufe unterstützt. Sie benötigt dafür Zugriff auf personenbezogene Informationen zur Person, die um den Registerabruf ersucht, und auf die in der Registerantwort enthaltenen personenbezogenen Informationen. Die Kritikalität dieser Angaben ist auch mit Blick auf die konkret angeschlossenen Register und die von ihnen übermittelten Arten von Informationen zu bewerten. In jedem Fall handelt es sich bei Intermediären Plattformen jedoch um eine sensible Infrastruktur, die gegen einen Missbrauch dieser Daten abgesichert werden muss. Hierzu gehört auch, dass durch geeignete Maßnahmen sicher ausgeschlossen werden muss, dass Daten aus verschiedenen Registerabrufen über die gleiche Intermediäre Plattform zusammengeführt und so für eine unzulässige Profilbildung missbraucht werden können.

3.9.5.2 IT-Sicherheit

Auch aus der Perspektive der IT-Sicherheit sind hohe Anforderungen an Intermediäre Plattformen zu stellen.

Das EU-OOTS bietet für Intermediärer Plattformen und/oder Evidence Provider keine Möglichkeit, die Berechtigung einer Registerabfrage aus dem Ausland im Rahmen einer abstrakten Berechtigungsprüfung im Einzelfall vor der Datenübermittlung zu plausibilisieren. Die entsprechende Verantwortung wird von der Durchführungsverordnung bei den anfragenden Behörden verortet, die die Rechtmäßigkeit ihrer Anfragen sicherstellen müssen, und bei den jeweiligen Mitgliedstaaten, die sicherstellen müssen, dass nur zuständige Behörden Zugriff auf das EU-OOTS erhalten. Im Mitgliedstaat des Evidence Provider muss die Anfrage dann grundsätzlich als zulässig betrachtet werden. Diese aus deutscher Sicht mit Blick auf IT-Sicherheit kritische Vorgabe lässt sich nicht auf der Ebene einer Intermediären Plattform revidieren. Bei der Umsetzung einer Intermediären Plattform muss jedoch darauf geachtet werden, die potenziellen Folgen dieses Designs so gering wie möglich zu halten.

Nach aktuellem Kenntnisstand bedingt dies mindestens zwei Aspekte, die bei der weiteren Ausgestaltung Intermediärer Plattformen zu beachten sind. Zunächst müssen alle Anfragen

aus dem EU-OOTS als legitim betrachtet und von der Intermediären Plattform über das NOOTS weitergegeben werden. Dafür muss die Intermediäre Plattform im NOOTS eine entsprechende Stellung mit weitreichenden Zugriffsrechten auf Register erhalten. Dabei muss jedoch strikt darauf geachtet werden, dass jede Intermediäre Plattform trotzdem nur die Zugriffsrechte erhält, die für ihre jeweiligen Data Services notwendig sind, und nicht jede Intermediäre Plattform pauschal privilegierten Zugriff auf alle Data Provider des NOOTS erhält. Zudem sollte bei der Konzeption einer Intermediären Plattform geprüft werden, welche Möglichkeiten existieren, zumindest ex-post anhand einer Auswertung von Protokolldaten Hinweise auf ungewöhnliches Abrufverhalten einzelner Evidence Requester zu erhalten und so potenzielle Missbrauchsfälle zumindest nachträglich verfolgen zu können.

Bei der umgekehrten Richtung, dass deutsche nachweisanfordernde Behörden über die Intermediäre Plattform Nachweise aus dem europäischen Ausland anfordern, können die Mechanismen des NOOTS zum Identitätsmanagement von Behörden und zur abstrakten Berechtigungsprüfung genutzt werden, um sicherzustellen, dass die betreffende Behörde auf die Intermediäre Plattform zugreifen und im Rahmen ihrer Zuständigkeit grundsätzlich die betreffende Art von Nachweisen anfordern darf. Solange die übergreifenden NOOTS-Mechanismen noch nicht vollständig zur Verfügung stehen, ist dies ggf. durch lokale Maßnahmen der Intermediären Plattform zum gleichen Zweck zu ergänzen.

Bei der Umsetzung einer Intermediären Plattform ist zudem zu beachten, dass die Durchführungsverordnung zu Art. 14 der SDG-Verordnung in einigen sicherheitsrelevanten Bereichen unmittelbare Vorgaben macht (Art. 17, 28f DVO). So stellt die DVO explizite Vorgaben zu Art und Umfang der Protokollierung auf, die neben die ohnehin in Deutschland bereits bestehenden Anforderungen ebenfalls erfüllt werden müssen (Art. 17 DVO). Hierzu gehört auch, dass eine technische Möglichkeit verfügbar sein muss, Protokolldaten ggf. im Rahmen der Aufklärung eines grenzüberschreitenden Missbrauchsverdachts für andere Behörden bereitzustellen. Zudem sind die Mitgliedstaaten u.a. verpflichtet, für die innerstaatliche Kommunikation der Intermediären Plattform mindestens ein mit dem grenzüberschreitenden AS4-Transportprotokoll vergleichbares Sicherheitsniveau zu garantieren (Art. 28 Abs. 4 lit. a DVO).

Aufgrund der Konstruktion des EU-OOTS müssen Intermediäre Plattformen aus dem Internet erreichbar sein. Zugleich kommunizieren Intermediäre Plattformen mit den angeschlossenen zuständigen Behörden in Deutschland über gesicherte Verwaltungsnetze. Hieraus ergibt sich die Notwendigkeit eines sicheren Managements des betreffenden

Netzübergangs, für das alle entsprechenden Vorgaben des BSI einzuhalten sind. Durch die Nutzung Intermediärer Plattformen kann diese Aufgabe zumindest auf eine kleinere Zahl von abzusichernden Systemen beschränkt werden, da nicht jeder anschlusspflichtige Evidence Provider selbst im Internet exponiert werden muss (während die Online-Services in der umgekehrten Richtung qua ihrer Natur ohnehin ebenfalls im Internet erreichbar sein müssen).

3.9.5.3 Verfügbarkeit, Antwortzeit und Last

Für die Verfügbarkeit der Intermediären Plattform müssen die Vorgaben aus Art. 27 der Durchführungsverordnung zu Art. 14 SDG-VO beachtet werden. Dort wird normiert, dass das EU-OOTS rund um die Uhr betrieben wird und eine Mindestverfügbarkeit der Access Points und der Preview-Umgebungen – und damit in diesem Fall der sie bereitstellenden Intermediären Plattformen – von 98% normiert. Dabei werden planmäßige Wartungen gem. Abs. 27 Abs. 2 DVO nicht in die Bewertung der Verfügbarkeit einbezogen.

Wichtig zum Verständnis dieser Anforderung ist, dass sie sich nur auf die Verfügbarkeit des Access Points und der Intermediären Plattform selbst beziehen und nicht zwingend bedeuten, dass auch eine Verfügbarkeit von 98% für Nachweisabrufe erreicht wird: Für einen erfolgreichen Abruf müssen auch der initiierende Online-Service und das die Nachweisdaten letztlich liefernde Register verfügbar sein. Für die Verfügbarkeit dieser Komponenten macht die Durchführungsverordnung jedoch keine pauschalen Vorgaben, sondern überlässt deren Regelung noch zu entwickelnden Service Level Agreements zwischen Kommission und Mitgliedstaaten (Art. 27 Abs. 1 DVO).

Für Antwortzeitverhalten und Lastfähigkeit einer Intermediären Plattform können aktuell noch keine präzisen Anforderungen benannt werden. Es ist jedoch zu beachten, dass Nachweisabrufe im EU-OOTS aus der interaktiven Benutzung eines Online-Antrags heraus erfolgen. Dies erfordert in jedem Fall ausreichend kurze, quasi-synchrone Reaktionszeiten, die von den Nutzenden als Teil eines durchgehenden Antragsflusses akzeptiert werden können. Die Lastfähigkeit einer Intermediären Plattform muss abhängig von der erwarteten Zahl der Abrufe geplant werden, die ihrerseits stark von den im Einzelfall angeschlossenen zuständigen Behörden und der Relevanz, der über die Intermediäre Plattform abgerufenen Nachweisinformationen für grenzüberschreitende Antragsprozesse abhängt und daher im Einzelfall beurteilt werden muss.

3.9.6 Zentrale Evidence Provider/Data Provider für die Anbindung an EU-OOTS und NOOTS

3.9.6.1 Anschlussbedingungen und Grenzen der Unterstützung durch Intermediäre Plattformen

Sowohl das EU-OOTS als auch das NOOTS stellen Anforderungen an die angebundenen Evidence Provider/Data Provider, die derzeit weiter ausgestaltet und zu entsprechenden Anschlussbedingungen führen werden. Für das EU-OOTS erfolgt die weitere Konkretisierung dieser Anforderungen in den auf europäischer Ebene eingerichteten Sub-Groups der EU SDG Coordination Group, für das NOOTS in den Strukturen der Gesamtsteuerung Registermodernisierung.

Es ist bereits jetzt absehbar, dass diese Vorgaben viele Aufgaben im Bereich der Nachweiskommunikation und -präsentation umfassen werden, etwa die Vorgabe des einzusetzenden Datenaustauschstandards und Vorgaben zur Preview. Bei der Kommunikation über das EU-OOTS können diese Aufgaben an eine Intermediäre Plattform delegiert werden; im NOOTS müssen sie jedoch vom Evidence Provider selbst umgesetzt werden.

Darüber hinaus ist jedoch davon auszugehen, dass die Anschlussbedingungen für beide Systeme auch Anforderungen an die Datenbereitstellung umfassen werden, die in keinem Fall delegiert werden können. Dies betrifft insbesondere Anforderungen an die Verfügbarkeit, die für das NOOTS noch definiert werden und für das EU-OOTS laut DVO in noch zu schaffende Service Level Agreements festzuhalten sind. Beide Systeme sollen insbesondere Abrufe aus laufenden Sitzungen eines Online-Antragsprozesses ermöglichen und werden daher aller Voraussicht nach hohe Anforderungen an die Verfügbarkeit aufstellen müssen, weil sonst ggf. die Verfügbarkeit der entsprechenden Antragsprozesse selbst untergraben würde.

Eine Kategorisierung von Aufgaben der Evidence Provider und deren Delegierbarkeit an Intermediäre Plattformen wurde in Kapitel 3.9.4.3 näher ausgeführt.

3.9.6.2 Anschlussstrategien für verschiedene Arten von Registern

Es bleiben daher sowohl im EU-OOTS als auch im NOOTS wesentliche Anforderungen an Evidence Provider bestehen, die nicht delegiert werden können. Vor diesem Hintergrund sollte bewusst entschieden werden, welche Stelle die entsprechende Aufgabe als Evidence

Provider/Data Provider und damit als Systemteilnehmer bei EU-OOTS und NOOTS übernimmt.

Bei den zu treffenden Entscheidungen zu den Registern ist es sinnvoll, diese anhand ihrer Klassifizierung, die in Kapitel 3.9.3.3 erläutert wird, vorzunehmen.

Bei **zentralen Registern** und **Landesregistern** kann die Umsetzung dieser Anforderungen in der Regel unproblematisch unmittelbar bei diesen Registern erfolgen, die damit die Rolle des Evidence Provider/Data Provider unmittelbar übernehmen können.

Bei verteilten, z.B. kommunalen, Registern, für die bereits **Spiegelregister** oder **Abrufportale** eingerichtet wurden, liegt ein wesentlicher Teil der Motivation für die Schaffung dieser zentralen Strukturen gerade in der besseren Umsetzung entsprechender Anforderungen. In diesen Fällen sollte daher aus technischer Sicht in der Regel nicht die einzelne dezentrale Registerinstanz, sondern das entsprechende Spiegelregister oder Abrufportal als Evidence Provider/Data Provider an EU-OOTS und NOOTS angebunden werden. Aus technisch-konzeptioneller Sicht stellen diese Stellen dann den Endpunkt der Kommunikation über das NOOTS dar; ihre Kommunikation mit den angeschlossenen dezentralen Registern erfolgt über einen separaten Informationsverbund. Diese aus technischer Sicht empfohlene Lösung muss jedoch auch durch die rechtliche Stellung des jeweiligen Spiegelregisters oder Abrufportals gedeckt werden.

Die größten Herausforderungen für die Erfüllung der Anschlussbedingungen werden sich jedoch voraussichtlich bei **dezentralen, insbesondere kommunalen Registern** ohne entsprechende zentrale Strukturen stellen. Diese Register müssen grundsätzlich alle Anforderungen des NOOTS zu Datenbereitstellung und Nachweiskommunikation und -präsentation sowie zumindest die Anforderungen des EU-OOTS an Datenbereitstellung, wie etwa Verfügbarkeit, erfüllen. Dies könnte im Einzelfall zu hohen Anpassungslasten bei einer Vielzahl von Registerinstanzen führen. Auf technischer Ebene ist daher in diesen Fällen überlegenswert, ob der Anschluss an die Systeme zum Nachweisabruf als Anlass genommen werden kann, auch hier zentrale Strukturen wie Spiegelregister oder Abrufportale zu schaffen und diesen dann die Rolle als Evidence Provider/Data Provider zu übertragen. Da Intermediärer Plattformen technisch ähnlich wie eine Abfrageplattform funktionieren, könnten die Lösungen ggf. sogar gemeinsam konzipiert und entwickelt werden. Bei der Entscheidung über die Schaffung neuer zentraler Strukturen sind allerdings neben technischen und wirtschaftlichen Aspekten auch organisatorische sowie rechtliche Vorgaben der jeweiligen Fachlichkeit zu beachten. Die Entscheidung über die

Notwendigkeit der Schaffung zentraler Strukturen muss daher in den Gremienstrukturen der jeweiligen Fachlichkeit verbleiben.

3.9.7 Ausblick & Weiterführende Aspekte

Das vorliegende Konzept verdeutlicht die Vorteile einer Anbindung an das EU-OOTS über Intermediäre Plattformen, konkretisiert deren Ausgestaltung für Deutschland und gibt Hinweise für den ggf. ergänzend sinnvollen Aufbau neuer zentraler Evidence Provider. Es füllt damit den technischen Teil der übergreifenden Konzeption Intermediärer Plattformen aus.

Für ein Gesamtkonzept zu Intermediären Plattformen müssen seitens der Gesamtsteuerung Registermodernisierung zudem Vorgaben zu den organisatorischen, rechtlichen und finanziellen Dimensionen Intermediärer Plattformen gemacht werden. Wegen des engen Zeitplans zur Umsetzung der Verpflichtungen aus der SDG-Verordnung sollte die Erarbeitung dieser Aspekte und die Klärung von Zuschnitt und betrieblicher Verantwortlichkeit für die zu schaffenden Intermediären Plattformen hinsichtlich einer ersten Umsetzung parallel vorangetrieben werden.

Um die in diesem Konzept erläuterten Funktionen ausführen zu können, müssen die Intermediären Plattformen mit gewissen Befugnissen ausgestattet werden: Intermediäre Plattformen für Nachweislieferanten brauchen die Befugnis, einen Data Service anbieten zu dürfen sowie Nachweisdaten im Zuge der Preview-Bereitstellung zwischenspeichern zu dürfen. Intermediäre Plattformen für nachweisabrufende Stellen wiederum müssen im NOOTS Nachweise anfordern dürfen. Ob es hierfür rechtlich nötig oder sinnvoll ist, Intermediäre Plattformen direkt als Evidence Provider bzw. Consumer zu deklarieren, ist im Rahmen einer rechtlichen Analyse zu klären.

Aus technischer Perspektive ist zudem zeitnah zu klären, ob zur Schaffung vollständiger Transparenz zwischen innerstaatlichen und europäischen Nachweisabrufen ggf. doch ein separater Nachweisabrufdienst in Betracht gezogen wird. Sollte dies der Fall sein, würde sich die Umsetzung Intermediärer Plattformen für nachweisanfordernde Stellen entsprechend vereinfachen (siehe letzter Abschnitt in 3.9.4.4).

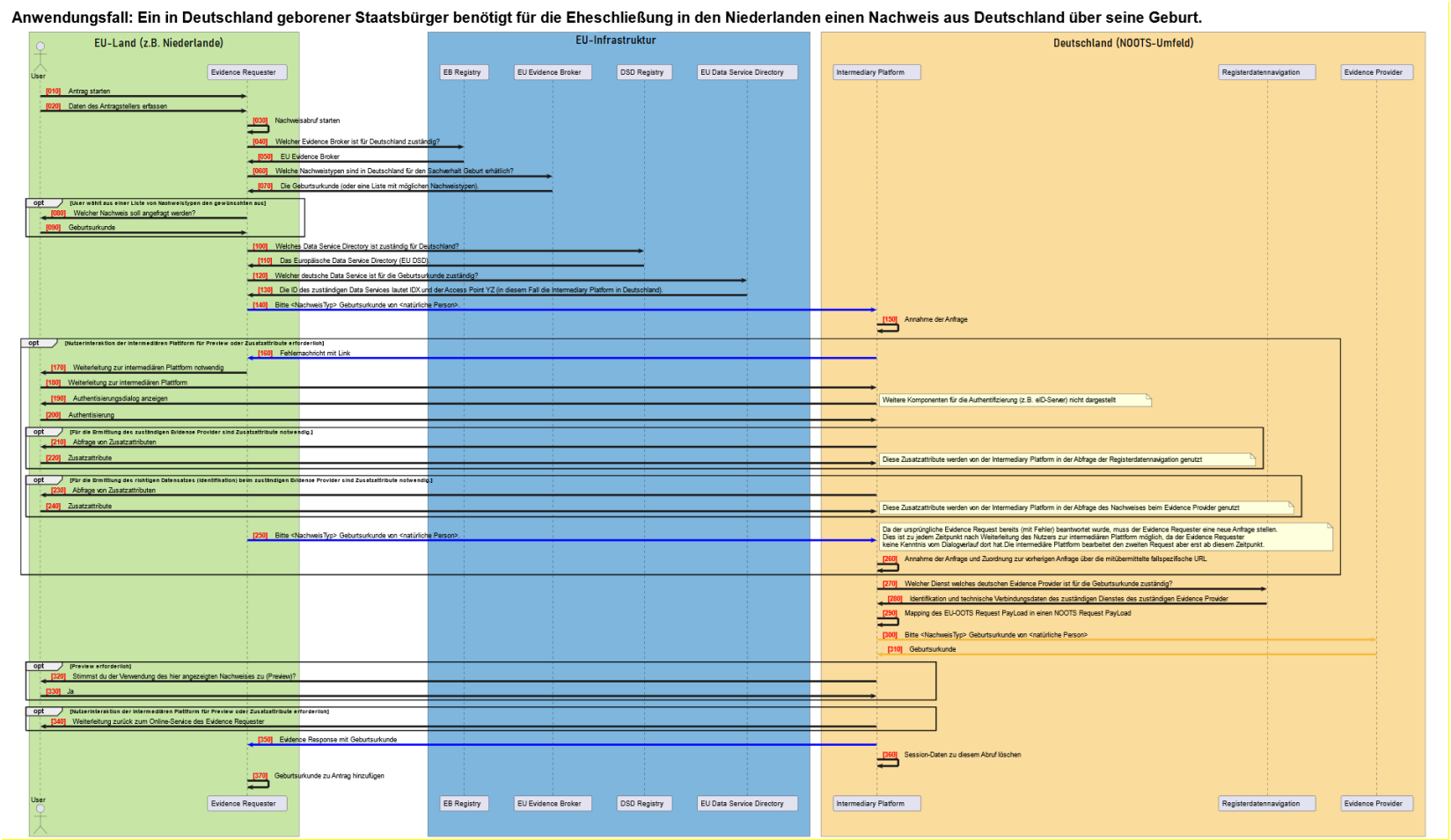


Abbildung 40: Sequenzdiagramm für einen Beispielabruf eines Nachweises aus Deutschland

Hinweis: (blaue Pfeile – EU-OOTS Kommunikation über 4-Corner, gelbe Pfeile NOOTS Kommunikation über 4-Corner, schwarze Pfeile – https Kommunikation oder interner Verarbeitungsschritt)

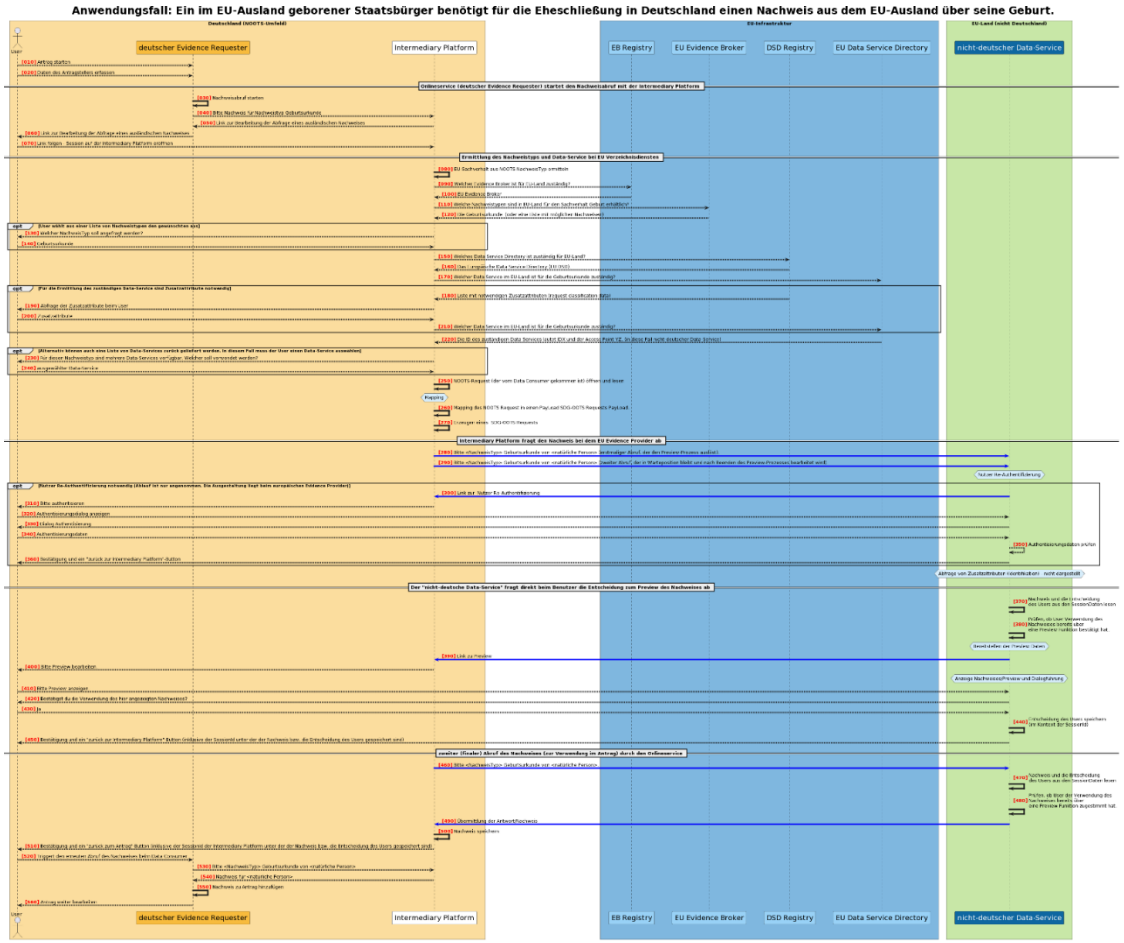


Abbildung 41: Sequenzdiagramm für einen Beispielabruf eines Nachweises aus dem EU-Ausland

Hinweis: (blaue Pfeile – EU-OOTS Kommunikation über 4-Corner, gelbe Pfeile NOOTS Kommunikation über 4-Corner, schwarze Pfeile – https Kommunikation oder interner Verarbeitungsschritt)

3.10 Data Consumer (Evidence Requestor)

3.10.1 Überblick

Da die Konzepte der einzelnen NOOTS-Komponenten im Wesentlichen erst als Entwürfe vorliegen, werden sich für die angeschlossenen Systeme im Verlauf der Weiterentwicklung voraussichtlich noch erhebliche Änderungen ergeben. Diese Änderungen werden entsprechend in dieses Dokument einfließen, sobald sie vorliegen.

Dennoch soll dieses Kapitel einen Überblick über den aktuellen Sachstand geben und ggf. offene Punkte aufdecken und richtet sich an alle IT-Systeme, die über das NOOTS Daten aus nationalen Registern abrufen wollen und fasst zusammen, welche technischen und organisatorischen Maßnahmen getroffen werden müssen, um einen Anschluss an das NOOTS zu gewährleisten. Im NOOTS werden abrufende Systeme als Data Consumer bezeichnet. Dies sind in erster Linie Online-Portale für Bürgerinnen und Bürger und Organisationen und Fachverfahren für Behörden. Darüber hinaus nutzt auch das Statistische Bundesamt das NOOTS für Zugriffe im Rahmen des Registerzensus und es gibt noch nicht spezifizierten Bedarf Wissenschaftlicher Institutionen, über das NOOTS Daten aus den Registern abzurufen.

Neben dem Begriff des Data Consumers im nationalen Kontext, gibt es auch den Begriff des Evidence Requesters im europäischen Kontext. Dieser Begriff wird für Systeme verwendet, die Evidences im Sinne des SDG abrufen. Dies sind grundsätzlich die gleichen Akteure (Online-Portale, Fachverfahren etc.), aber im nationalen Kontext werden über das NOOTS nicht zwangsweise vordefinierte Nachweise abgerufen, sondern das NOOTS ermöglicht Datenabrufe im Allgemeinen.

Die technischen Anschlussbedingungen der unterschiedlichen Data Consumer wird durch die Registermodernisierung homogenisiert und sollte daher im Folgenden für alle Data Consumer identisch sein. D.h. der Zugriff auf Registerdaten durch eine Behörde mittels eines Fachverfahrens gestaltet sich im Wesentlichen identisch zum Abruf von Registerdaten im Zuge eines Onlineantrags. Falls es für einzelne Data Consumer unterschiedliche Voraussetzungen - insbesondere organisatorische - geben sollte, werden diese besonders hervorgehoben.

3.10.2 Anschlussbedingungen NOOTS Komponenten

Die folgende Tabelle enthält alle zum aktuellen Zeitpunkt bekannten Anschlussbedingungen, die sich aus den Konzepten der einzelnen NOOTS-Komponenten ergeben.

Tabelle 65: Übersicht Data Consumer Anschlussbedingungen

NOOTS-Komponente	**Anschlussbedingungen für Data Consumer**	**Bemerkung**
Registerdaten-navigation	Der Data Consumer muss sich im RDN-eigenen IAM registrieren.	Übergangslösung, langfristig soll die zentrale Komponente „IAM für Behörden“ genutzt werden
	Implementierung der RDN Abfrage API. Die Struktur der Abfragen werden dem Once Only Standard folgen. Die Schnittstelle wird sowohl aus den Netzen des Bundes als auch dem Internet erreichbar sein. Die notwendige Verschlüsselung der Anfragen wird voraussichtlich dem Schutzbedarf „hoch“ entsprechen.	Im Zuge der Feinkonzeption wird hierfür ein SDK erarbeitet
Preview	Ein Data Consumer muss Personen und Unternehmen eine Preview der abgerufenen Daten anzeigen können. Der Data Consumer erhält dazu vom Data Provider strukturierte Daten und muss in der Lage sein, diese in menschenlesbarem Format anzuzeigen.	Vorbehaltlich Zustimmung durch den Datenschutz.
IAM für Behörden	Sobald die einheitliche Lösung für IAM für Behörden produktiv gesetzt worden ist, müssen Data Consumer für Authentisierungen und Zugriffsanfragen an Register, NOOTS-	

NOOTS-Komponente	Anschlussbedingungen für Data Consumer	Bemerkung
	Komponenten und die Intermediäre Plattform die geplante einheitliche Lösung für IAM für Behörden nutzen.	
	Bis die einheitliche Lösung für IAM für Behörden produktiv gesetzt worden ist, müssen Data Consumer für Authentisierungen und Zugriffsanfragen an Register, NOOTS-Komponenten und die Intermediäre Plattform die bereits vorhandenen IAM-Lösungen und Konzepten der einzelnen NOOTS-Komponenten nutzen.	Dies betrifft den Zugriff auf IDM für Personen, IDM für Unternehmen, Registerdatennavigation, Abfragen an Registern über Vermittlungsstellen, Datenschutzcockpit und Intermediäre Plattformen.
	Nach Produktivsetzung der einheitlichen Lösung für IAM für Behörden müssen Data Consumer für alle bereits eingeführten Registeranbindungen in einer Übergangszeit auf diese einheitliche IAM-Lösung umstellen.	Die Dauer der Übergangszeit ist noch zu definieren.
V-PKI	Bei Verschlüsselungen und Siegelungen müssen Data Consumer Zertifikate von Zertifizierungsstellen der V-PKI einsetzen. Das V-PKI Zertifikat muss einen Verweis auf die Zertifikatsrichtlinie für die Registermodernisierung enthalten.	Die Zertifikatsrichtlinie für die Registermodernisierung muss noch erstellt werden.
	Für die geplante einheitliche IAM-Lösung der Registermodernisierung müssen Data Consumer Zertifikate der V-PKI als Identifizierungsmittel einsetzen. Das V-PKI Zertifikat	V-PKI-Zertifikate werden als Identifizierungsmittel eingesetzt, sobald die einheitliche IAM-Lösung für die Registermodernisierung produktiv gesetzt worden ist. Vor Einführung der einheitlichen IAM Lösung ist der Einsatz von V-

NOOTS-Komponente	Anschlussbedingungen für Data Consumer	Bemerkung
	muss einen Verweis auf die Zertifikatsrichtlinie für die Registermodernisierung enthalten.	PKI-Zertifikaten abhängig von den IAM-Lösungen der einzelnen NOOTS-Komponenten. Die Zertifikatsrichtlinie für die Registermodernisierung muss noch erstellt werden.
IDM für Unternehmen	Der Data Consumer muss, sofern fachlich erforderlich, in der Lage sein, Unternehmensbasisdaten vom IDM für Unternehmen auf Basis von Identifikatoren (wie z. B. bundeseinheitliche Wirtschaftsnummer) abzurufen.	
IDM für Personen	Der Data Consumer muss die IDNr der betroffenen Person anhand der persönlichen Identifikationsmerkmale der angemeldeten Nutzenden vor dem Nachweisabruf mittels XBasisdaten abrufen.	Das IDM für Personen ist nur für Nachweise zu verwenden, wenn deren Data Provider im RegMoG benannt sind und seinerseits bereits an das IDM für Personen angeschlossen ist. Für den Anschluss an das NOOTS ist die Anbindung an das IDM für Personen nicht zwingend erforderlich.
	Verwendung der IDNr als Schlüsselparameter im Nachweisabruf.	
Datenschutz-cockpit	Keine Anforderungen an Data Consumer.	Siehe hierzu auch Anforderungen an Data Provider

NOOTS-Komponente	Anschlussbedingungen für Data Consumer	Bemerkung
Vermittlungs-stellen	Klärung und Bereitstellung der Kommunikationsinfrastruktur, sofern noch nicht geklärt und/oder vorhanden.	An Vermittlungsstellen sind Data Consumer anzubinden, wenn sie Nachweise aus einem anderen Verwaltungsbereich unter Verwendung der IDNr abrufen wollen. Der Schnitt der Verwaltungsbereiche existiert derzeit nicht. Die konkrete Implementierung der Vermittlungsstellen sowie der von ihnen genutzten Transportstandards sind noch offen.
	Hinterlegung der eigenen Verbindungsparameter in der Vermittlungsstelle oder einem davon genutzten Verzeichnisdienst, bspw. DVDV, für die sichere Kommunikation mit dem Data Provider.	
	Implementierung des Nachweisabrufstandards unter Verwendung des Transportprotokolls der Vermittlungsstelle.	
Intermediäre Plattformen	Online-Services implementieren deutschen Once-Only Standard	Keine besonderen Anforderungen an Data Consumer im Vergleich zu anderen Data Providern. Der Datenaustausch über IPs sollte für die Consumer transparent sein.
	Online-Services implementieren 4-Corner-Kommunikation über Vermittlungsstellen (Arbeitsthese - zu validieren) mit dem deutschen NOOTS-Transportprotokoll	
	Online-Services signieren Request (Nachweisabruf) mit technischem Zertifikat des OS vor Übergabe an die IP (zur Bestätigung der Authentifizierung der Antragstellenden)	

3.11 Data Provider (Evidence Provider)

3.11.1 Überblick

Da die Konzepte der einzelnen NOOTS-Komponenten im Wesentlichen erst als Entwürfe vorliegen, werden sich für die angeschlossenen Systeme im Verlauf der Weiterentwicklung voraussichtlich noch erhebliche Änderungen ergeben. Diese Änderungen werden entsprechend in dieses Dokument einfließen, sobald sie vorliegen.

Dennoch soll dieses Kapitel einen Überblick über den aktuellen Sachstand geben und ggf. offene Punkte aufdecken. Dieses Kapitel richtet sich ebenfalls an alle IT-Systeme, die Daten im NOOTS zum Abruf bereitstellen. Dies sind in erster Linie registerführenden Behörden. Wenn in einem Fachbereich der Zugriff auf die Registerdaten über Spiegelregister oder Abrufportale erfolgt, so sind diese im Sinne dieses Dokuments Data Provider. In diesem Fall müssen die vorgeschalteten Systeme die untenstehenden Anschlussbedingungen erfüllen.

Neben dem Begriff des Data Providers im Kontext des NOOTS, bezeichnen Evidence Provider Systeme (national oder im EU-Ausland), die Evidences im Sinne des SDG zum Abruf bereitstellen.

3.11.2 Anschlussbedingungen NOOTS Komponenten

Die folgende Tabelle enthält alle zum aktuellen Zeitpunkt bekannten Anschlussbedingungen, die sich aus den Konzepten der einzelnen NOOTS-Komponenten ergeben.

Tabelle 66: Data Provider Anschlussbedingungen

NOOTS-Komponente	Anschlussbedingungen für Data Provider	Bemerkung
Registerdaten-navigation	Kein direkter Anschluss an die RDN, aber um in der RDN für Data Consumer auffindbar zu sein, müssen Data Provider folgende Pflegeverantwortungen erfüllen: Pflege ihrer Behördendaten und ihrer Dienste mit Verbindungsparametern (DVDV) Pflege ihrer Zuständigkeiten (DVZV) Für die beiden o.g. Aufgaben bedarf es dem Benennen und Anlegen von pflegeverantwortlichen Stellen im Pflegesystem der RDN (Zusammenhang mit dem bestehenden DVDV-Pflegesystem wird in der Feinkonzeption ausgearbeitet) Sicherstellen, dass die bereitgestellten Nachweistypen im NOOTS fachlich definiert und mit einer Nachweis-ID versehen sind.	
Preview	Die Preview ist vom Data Consumer zu implementieren, daher ergeben sich hier noch keine direkten Anforderungen an die Data Provider.	Ggfs. werden die Data Provider Hinweise zur lesbaren Darstellung der strukturierten Daten bereitstellen müssen. Dies befindet sich noch in der Diskussion.
IAM für Behörden	Sobald die einheitliche Lösung für IAM für Behörden produktiv gesetzt worden ist, müssen Data Provider für Authentisierungen und Zugriffsanfragen an NOOTS-Komponenten und die	Register werden voraussichtlich keine direkten Schnittstellen zu IAM für Behörden haben. Stattdessen werden Vermittlungsstellen im Rahmen einer abstrakten

NOOTS-Komponente	Anschlussbedingungen für Data Provider	Bemerkung
	Intermediäre Plattform die geplante einheitliche Lösung für IAM für Behörden nutzen	Berechtigungsprüfung Zugriffsanfragen auf Register prüfen.
	Bis die einheitliche Lösung für IAM für Behörden produktiv gesetzt worden ist, müssen Data Provider für Authentisierungen und Zugriffsanfragen an NOOTS-Komponenten und die Intermediäre Plattform die bereits vorhandenen IAM-Lösungen und Konzepten der einzelnen NOOTS-Komponenten nutzen.	Register werden voraussichtlich keine direkten Schnittstellen zu IAM für Behörden haben. Stattdessen werden Vermittlungsstellen im Rahmen einer abstrakten Berechtigungsprüfung die Zugriffsanfragen auf Register prüfen.
	Nach Produktivsetzung der einheitlichen Lösung für IAM für Behörden müssen Data Provider für alle bereits eingeführten Registeranbindungen in einer Übergangszeit auf diese einheitliche IAM-Lösung umstellen.	Register werden voraussichtlich keine direkten Schnittstellen zu IAM für Behörden haben. Stattdessen werden Vermittlungsstellen im Rahmen einer abstrakten Berechtigungsprüfung die Zugriffsanfragen auf Register prüfen. Die Dauer der Übergangszeit ist noch zu definieren.
V-PKI	Bei Verschlüsselungen und Siegelungen müssen Data Provider Zertifikate von Zertifizierungsstellen der V-PKI einsetzen. Das V-PKI Zertifikat muss einen Verweis auf die Zertifikatsrichtlinie für die Registermodernisierung enthalten.	

NOOTS-Komponente	Anschlussbedingungen für Data Provider	Bemerkung
	Für die geplante einheitliche IAM-Lösung der Registermodernisierung müssen Data Provider Zertifikate der V-PKI als Identifizierungsmittel einsetzen. Das V-PKI Zertifikat muss einen Verweis auf die Zertifikatsrichtlinie für die Registermodernisierung enthalten.	Die Zertifikatsrichtlinie für die Registermodernisierung muss noch erstellt werden.
IDM für Unternehmen	Die Quellregister müssen die quellspezifischen Unternehmensdaten an das Basisregister bereitstellen.	V-PKI-Zertifikate werden als Identifizierungsmittel eingesetzt, sobald die einheitliche IAM-Lösung für die Registermodernisierung produktiv gesetzt worden ist. Vor Einführung der einheitlichen IAM Lösung ist der Einsatz von V-PKI-Zertifikaten abhängig von den IAM-Lösungen der einzelnen NOOTS-Komponenten.
	Das Basisregister muss die Abfragen der angebundenen Register zu Unternehmensdaten beantworten.	gem. §5 UBRegG
	Die Kommunikation zwischen dem Basisregister und den berechtigen öffentlichen Stellen für die anlassbezogene Übermittlung von Unternehmensereignissen und Abrufe aus dem Basisregister muss über die standardisierte Schnittstelle XUnternehmen.Basisregister erfolgen.	

NOOTS-Komponente	Anschlussbedingungen für Data Provider	Bemerkung
IDM für Personen	Zufügen der IDNr für alle Personendatensätze, zu denen der Data Consumer Nachweise liefert.	An das IDM für Personen sind nur Data Provider anzubinden, die im RegMoG benannt sind. Für den Anschluss an das NOOTS ist die Anbindung an das IDM für Personen nicht zwingend erforderlich.
	Unterstützung des Nachweisabrufs mittels Once-Only Standard unter Verwendung der IDNr.	
	Protokollierung der Nachweisabrufe gem. IDNrG und Bereitstellung der Protokolldaten für das Datenschutzcockpit über eine XDSC Schnittstelle.	
	Eintrag der Zuständigkeit für die bereitgestellten Nachweise in der Registerdatennavigation.	
	Authentifizierung und Autorisierung der Kommunikationspartner für Nachweisabrufe und XSDC-Abrufe mittels IAM für Behörden.	
Datenschutz-cockpit	Der Data Provider muss die aufeinander aufbauenden Abfragen (Status, Protokoll- und Inhaltsdaten) vom Datenschutzcockpit zu den Datenübermittlungen (unter Nutzung der IDNr.) beantworten.	Gemäß dem Standard XDatenschutzcockpit

NOOTS-Komponente	Anschlussbedingungen für Data Provider	Bemerkung
	Registerführende Stellen und die Registermodernisierungsbehörde müssen die Datenübermittlungen unter der Nutzung der IDNr. protokollieren.	Gemäß RegMoG, Art. 1 §2, §9
Vermittlungs-stellen	Klärung und Bereitstellung der Kommunikationsinfrastruktur, sofern noch nicht geklärt und/oder vorhanden.	An Vermittlungsstellen sind Data Provider anzubinden, wenn sie Nachweise an einen anderen Verwaltungsbereich unter Verwendung der IDNr liefern. Der Schnitt der Verwaltungsbereiche existiert derzeit nicht. Die konkrete Implementierung der Vermittlungsstellen sowie der von ihnen genutzten Transportstandards sind noch offen.
	Hinterlegung der eigenen Verbindungsparameter in der Vermittlungsstelle oder einem davon genutzten Verzeichnisdienst, bspw. DVDV, für die sichere Kommunikation mit dem Data Consumer	
	Implementierung des Nachweisabrufstandards unter Verwendung des Transportprotokolls der Vermittlungsstelle.	
Intermediärer Plattformen	Data Provider implementieren deutschen Once-Only Standard.	Das SDG fordert den Eintrag von Data Providern als Evidence Provider Beim eigentlichen Abruf ergeben sich keine besonderen Anforderungen an Data Provider, falls der Abruf durch eine IP erfolgt.
	Data Provider implementieren 4-Corner-Kommunikation über Vermittlungsstellen mit dem deutschen NOOTS-Transportprotokoll	

NOOTS-Komponente	Anschlussbedingungen für Data Provider	Bemerkung
	Data Provider müssen ihre SDG-relevanten Nachweistypen im Evidence Broker hinterlegen sowie die für sie zuständige IP im DSD	

4 Generischer Nachweisabrufstandard

Kapitel wird als separates Dokument zur Verfügung gestellt.

5 Anhang

5.1 Quellenverzeichnis

Tabelle 67: Beschlüsse des IT-Planungsrats zur Registermodernisierung

Referenz	Dokument	Beschreibung
[IT-PLR-B-01]	IT-PLR Beschluss 2019/03	28. Sitzung des IT-Planungsrats am 12.03.2019: Einrichtung des Koordinierungsprojekts Registermodernisierung unter FF Bund, HH & BY
[IT-PLR-B-02]	IT-PLR Beschluss 2019/23	29. Sitzung des IT-Planungsrats am 27.06.2019: IT-Planungsrat beauftragt das Koordinierungsprojekt mit verschiedenen Aufgaben
[IT-PLR-B-03]	IT-PLR Beschluss 2020/25	32. Sitzung des IT-Planungsrats am 24.06.2020: Kenntnisnahme der Eckpunkte der Registermodernisierung
[IT-PLR-B-04]	IT-PLR Beschluss 2021/05	34. Sitzung des IT-Planungsrats am 17.03.2021: Beschluss des Zielbildes der Registermodernisierung sowie der Umsetzungsplanung
[IT-PLR-B-05]	IT-PLR Beschluss 2021/25	35. Sitzung des IT-Planungsrats am 23.06.2021: Einrichtung des Projekts „Gesamtsteuerung Registermodernisierung“
[IT-PLR-B-06]	IT-PLR Beschluss 2021/35	36. Sitzung des IT-Planungsrats am 29.10.2021: Umsetzungsplanung des Zielbilds der Registermodernisierung
[IT-PLR-B-07]	IT-PLR Beschluss 2022/06	37. Sitzung des IT-Planungsrats am 09.03.2022: Beschluss der Programmplanung inklusive der Meilensteine bis 2025
[IT-PLR-B-08]	IT-PLR Beschluss 2022/22	38. Sitzung des IT-Planungsrats am 22.06.2022: Insb. Beschluss verschiedener Beschlüsse des Lenkungskreises der

Referenz	Dokument	Beschreibung
		Registermodernisierung zur technischen Architektur und Bericht zum aktuellen Umsetzungsstand
[IT-PLR-B-09]	IT-PLR Beschluss 2022/34	39. Sitzung des IT-Planungsrats am 10.11.2022: Bericht zum Umsetzungsstand und NOOTS-Registeranschluss
[IT-PLR-B-01]	IT-PLR Beschluss 2019/03	28. Sitzung des IT-Planungsrats am 12.03.2019: Einrichtung des Koordinierungsprojekts Registermodernisierung unter FF Bund, HH & BY

Tabelle 68: Entscheidungen des IT-Planungsrats zur Registermodernisierung

Referenz	Dokument	Beschreibung
[IT-PLR-E-01]	IT-PLR Beschluss 2022/22 - Entscheidung Reifegradmodell	Entscheidung zur Einführung eines Reifegradmodells für Nachweisabrufe und Ausrichtung des NOOTS auf Reifegrad D
[IT-PLR-E-02]	IT-PLR Beschluss 2022/22 - Entscheidung asynchrone Prozesse	Entscheidung zur Unterstützung asynchroner Prozesse in der Architektur der Registermodernisierung
[IT-PLR-E-03]	IT-PLR Beschluss 2022/22 - Entscheidung Nachweisabrufstandard	Entwicklung eines allgemeinen Standards für den Nachweisabruf für die nationale Registermodernisierung
[IT-PLR-E-04]	IT-PLR Beschluss 2022/22 - Entscheidung nationales DSD	Aufbau eines nationalen Data Service Directory und Nutzung des europäischen Evidence Brokers
[IT-PLR-E-05]	IT-PLR Beschluss 2022/22 - Entscheidung Registerdatennavigation	Entscheidung zur Umsetzung der Komponente Registerdatennavigation als zentralen Routing-Dienst (Routing As a Service) auf Grundlage des Deutschen Verwaltungsdienste Verzeichnis (DVDV)

Referenz	Dokument	Beschreibung
		unter Wiederverwendung von Lösungsansätzen aus FIT-Connect
[IT-PLR-E-06]	IT-PLR Beschluss 2022/34 - Entscheidung EU-OOTS	Entscheidung über die Anbindung der Register und Online-Services an das EU-NOOTS über Intermediärer Plattformen
[IT-PLR-E-07]	IT-PLR Beschluss 2022/34 - Entscheidung NOOTS-Registeranbindung	Entscheidung über die Anbindung der Register an das NOOTS zum Nachweisabruf
[IT-PLR-E-08]	T-PLR Beschluss 2022/34 - Entscheidung SDG-Connector	Entscheidung über die Umsetzung einer standardisiert einheitlich nutzbaren Basiskomponente (sog. SDG-Connector) für die Anbindung des NOOTS - und somit den nationalen Registern und Onlinediensten/Portalen - an das EU-OOTS

Tabelle 69: Dokumente der Europäischen Kommission zur SDG-Umsetzung

Referenz	Dokument	Beschreibung
[EU-01]	OOTS Implementing Act	Festlegung technischer und betrieblicher Spezifikationen des OOTS für den grenzüberschreitenden automatisierten Nachweisabruf und zum Grundsatz der einmaligen Erfassung gemäß der Verordnung (EU) 2018/1724 des Europäischen Parlaments und des Rates
[EU-02]	EU Technical Design Documents (TDDs)	Technische Beschreibung des EU-OOTS - Release Oktober 2022

Tabelle 70: Weiterführende Dokumente zur Registermodernisierung

Referenz	Dokument	Beschreibung
[SQ-01]	Normenkontrollrat Faktencheck Registermoderni-sierung	Bericht des Normenkontrollrat zum Beschluss des Registermodernisierungsgesetzes
[SQ-02]	Kabinettsfassung Registermoderni-sierungsgesetz (Drucksache 19/24226)	Kabinettsfassung des Registermodernisierungsgesetzes
[SQ-03]	Gesamtsteuerung Registermoder-nisierung	Gemeinsamer Arbeitsbereich der Gesamtsteuerung Registermodernisierung

Tabelle 71: Rechtliche Grundlagen und Rahmenbedingungen

Referenz	Dokument	Beschreibung
[RGR-01]	Gesetz zur Einführung und Verwendung einer Identifikationsnummer in der öffentlichen Verwaltung und zur Änderung weiterer Gesetze	Registermodernisierungsgesetz (RegMoG) / Identifikationsnummerngesetz (IDNrG)
[RGR-02]	Gesetz zur Errichtung und Führung eines Registers über Unternehmensbasisdaten und zur Einführung einer bundeseinheitlichen Wirtschaftsnummer für Unternehmen und zur Änderung weiterer Gesetze	Unternehmensbasisdatenregistergesetz (UBRegG)

Referenz	Dokument	Beschreibung
[RGR-03]	Gesetz zur Verbesserung des Onlinezugangs zu Verwaltungsleistungen	Onlinezugangsgesetz (OZG)
[RGR-04]	Gesetz zur Erprobung von Verfahren eines Registerzensus	-
[RGR-05]	Verordnung (EU) 2018/1724 des Europäischen Parlaments und des Rates über die Einrichtung eines einheitlichen digitalen Zugangstors zu Informationen, Verfahren, Hilfs- und Problemlösungsdiensten und zur Änderung der Verordnung (EU) Nr. 1024/2012	Single-Digital-Gateway-Verordnung (SDG-VO)
[RGR-06]	Durchführungsverordnung zur Festlegung technischer und operativer Spezifikationen des technischen Systems für den grenzüberschreitenden automatisierten Austausch von Nachweisen und zur Anwendung des Grundsatzes der einmaligen Erfassung gemäß der Verordnung (EU) 2018/1724 des Europäischen Parlaments und des Rates	EU-Durchführungsverordnung

Referenz	Dokument	Beschreibung
[RGVS-01]	Bayerisches Gesetz zur Ausführung des Bundesmeldegesetzes (BayAGBMG)	Bayrisches Bundesmeldegesetz (BayAGBMG)
[RGVS-02]	Verordnung zur Durchführung von regelmäßigen Datenübermittlungen zwischen Meldebehörden	Erste Bundesmeldedatenübermittlungsverordnung (1. BMeldDÜV)
[RGVS-03]	Verordnung zur Durchführung von regelmäßigen Datenübermittlungen zwischen Meldebehörden	Landesmeldegesetz MV (LMG MV)

Tabelle 72: Weiterführende Quellen Registerdatennavigation

ID	**Quelle**	**Beschreibung**
1	Destatis	Destatis - Verwaltungsinformationsplattform
2	BMI Evidence Survey Zwischenbericht	Auszug aus dem BMI Evidence Survey Zwischenbericht (25.05.2022)
2	OZG	OZG Lexikon
3	ITZBund	ITZBund: DVDV – das Diensteverzeichnis der öffentlichen Verwaltung
4	XRepository	XRepository – XÖV-Standards und Codelisten

ID	Quelle	Beschreibung
5	FIM-Portal	Föderales Informationsmanagement Portal
6	BVA	BVA - Registerlandkarte

5.2 Tabellenverzeichnis

Tabelle 1: Komponentenübersicht und Aufgabenbeschreibung NOOTS 9
Tabelle 2: Übersicht IT-PLR Ziele Registermodernisierung 2023/2025 13
Tabelle 3: Übergreifende Entwurfsentscheidungen 19
Tabelle 4: Überblick Use-Cases 22
Tabelle 5: Prozessschritte Use-Case 1a: Bürgerinitiierter Nachweisabruf im NOOTS 25
Tabelle 6: Prozessschritte Use-Case 1b: Unternehmensinitiierter Nachweisabruf 33
Tabelle 7: Prozessschritte Use-Case 2: Behördeninitiierter Registerdatenabruf 41
Tabelle 8: Prozessschritte Use-Case 3: Abruf von nationalen Nachweisen 47
Tabelle 9: Prozessschritte Use-Case 4: Abruf von europäischen Nachweisen 59
Tabelle 10: Klärungspunkte aus der Use-Case Modellierung 69
Tabelle 11: Annahmen aus der Use-Case Modellierung 79
Tabelle 12: Anforderungen aus der Use-Case Modellierung 81
Tabelle 13: Grobe Zeitplanung 91
Tabelle 14: Annahmen und Rahmenbedingungen für die Konzeption der Registerdatennavigation 92
Tabelle 15: Zentrale Begriffe und deren Zusammenhänge 95
Tabelle 16: Anwender und Systeme 97
Tabelle 17: Use-Case 1: Verbindungsparameter für Nachweis abrufen 99
Tabelle 18: Use-Case 2: Verbindungsparameter für bekannte Behörde abrufen 101
Tabelle 19: Use-Case 3: Nutzende anlegen und Rechte verteilen 102
Tabelle 20: Use-Case 4: Nachweistypen und benötigte Routingparameter pflegen 103
Tabelle 21: Use-Case 5: Bestehende Zuständigkeiten und Verbindungsparameter pflegen 104

Tabelle 22: Use-Case 6: Bestehende Zuständigkeiten und Verbindungsparameter importieren 105
Tabelle 23: Registerdatennavigation - Funktionale Anforderungen 106
Tabelle 24: Registerdatennavigation - Bausteine der Lösungsarchitektur 112
Tabelle 25: Übersicht Schnittstellen der Registerdatennavigation 119
Tabelle 26: Ein- und Ausgabedaten der zwei Funktionen der RDN API 119
Tabelle 27: Vorläufige Einschätzung zum Schutzbedarf der RDN 125
Tabelle 28: Registerdatennavigation - Nichtfunktionale Anforderungen 126
Tabelle 29: Offene Punkte relevant für die Konzeption der Registerdatennavigation 129
Tabelle 30: Use-Case 8: Verbindungsparameter für Nachweis abrufen 141
Tabelle 31: Anforderungen an die RDN für den EU Use-Case 8 143
Tabelle 32: Anwendungsfall (Use-Case) UC-PREVIEW-01 147
Tabelle 33: Anwendungsfall (Use-Case) UC2-PREVIEW-02 149
Tabelle 34: Übersicht der Anforderungen 150
Tabelle 35: Funktionale Anforderungen an IAM für Behörden 164
Tabelle 36: Nichtfunktionale Anforderungen an IAM für Behörden 166
Tabelle 37: Beschreibung der Phasen für die Umsetzung von IAM für Behörden 172
Tabelle 38: Anforderungen an V-PKI (Qualitätskriterium – Funktionale Software) 203
Tabelle 39: Anforderungen an V-PKI – Sonstige Qualitätskriterien entsprechend ISO 25010 205
Tabelle 40: Zuständigkeiten für das Basisregister für Unternehmen innerhalb des Statistischen Bundesamtes 211
Tabelle 41: Übersicht Annahmen IDM Personen 215
Tabelle 42: Übersicht Rahmenbedingungen IDM Personen 216
Tabelle 43: Akteure 217
Tabelle 44: Use-Case 1: IDM für Personen 219
Tabelle 45: Use-Case 10 IDM für Personen 220
Tabelle 46: Nicht-funktionale Anforderung IDM Personen 221

Tabelle 47: Offene Punkte 223
Tabelle 48: Schnittstellen zwischen dem Datenschutzcockpit und externen System sowie Zuordnung zum funktionalen Ablauf 230
Tabelle 49: Zeitplan Vermittlungsstellen 233
Tabelle 50: Weiterführende Dokumente zu den Vermittlungsstellen 234
Tabelle 51: Annahmen - Vermittlungsstellen 234
Tabelle 52: Rahmenbedingungen - Vermittlungsstellen 235
Tabelle 53: Übersicht Anforderungen Vermittlungsstellen 236
Tabelle 54: Übersicht Anwender und Systeme - Vermittlungsstellen 241
Tabelle 55: Use-Case 1: Bereichsübergreifende Datenübermittlung 242
Tabelle 56: Use-Case 2: Protokolldaten bereitstellen 244
Tabelle 57: Use-Case 3: Protokolldaten nach Aufbewahrungsfrist löschen 245
Tabelle 58: Übersicht Offener Punkte Vermittlungsstellen 246
Tabelle 59: Übersicht zukünftiger Handlungsfelder - Vermittlungsstellen 249
Tabelle 60: Vergleich von Aspekten des EU-OOTS und des NOOTS 255
Tabelle 61: Übersicht Schritte bei EU-Nachweisabruf durch deutschen Online-Services mit Intermediärer Plattform 270
Tabelle 62: Übersicht Funktionen der Intermediären Plattform und relevante Komponenten des NOOTS 276
Tabelle 63: Erläuterung der Sequenzschritte eines Nachweisabrufs aus dem EU-Ausland 287
Tabelle 64: Erläuterung der Sequenzschritte des Abrufs eines europäischen Nachweises aus Deutschland 293
Tabelle 65: Übersicht Data Consumer Anschlussbedingungen 306
Tabelle 66: Data Provider Anschlussbedingungen 311
Tabelle 67: Beschlüsse des IT-Planungsrats zur Registermodernisierung 318
Tabelle 68: Entscheidungen des IT-Planungsrats zur Registermodernisierung 319
Tabelle 69: Dokumente der Europäischen Kommission zur SDG-Umsetzung 320
Tabelle 70: Weiterführende Dokumente zur Registermodernisierung 321
Tabelle 71: Rechtliche Grundlagen und Rahmenbedingungen 321

5.3 Abbildungsverzeichnis

Abbildung 1: Übersicht NOOTS Komponenten und Umfeld 8
Abbildung 2: Scope High-Level-Architecture 14
Abbildung 3: Reifegradmodell Registermodernisierung 16
Abbildung 4: Use-Case 1a: Bürgerinitiierter Nachweisabruf 24
Abbildung 5: Use-Case 1b: Unternehmensinitiierter Nachweisabruf 32
Abbildung 6: Use-Case 2: Behördeninitiierter Registerdatenabruf 40
Abbildung 7: Use-Case 3: Abruf von nationalen Nachweisen 46
Abbildung 8: Use-Case 4: Abruf von europäischen Nachweisen 58
Abbildung 9: Sequenzdiagramm Use-Case 3 83
Abbildung 10: Sequenzdiagramm Use-Case 4 84
Abbildung 11: Vereinfachte Darstellung des Architekturmodells als Datenkette zur Umsetzung von "Once Only" 88
Abbildung 12: Zwei Schritte beim Nachweisabruf im NOOTS (Ausschnitt der Once-Only Datenkette) 89
Abbildung 13: Zusammenspiel der Komponenten bei Nachweisabruf aus EU-Ausland mit IP 90
Abbildung 14: Kontextdiagramm Registerdatennavigation 94
Abbildung 15: Modell Registerdatennavigation 94
Abbildung 16: Skizze der RDN-Lösungsarchitektur 111
Abbildung 17: Funktionsbündelung der Registerdatennavigation 117
Abbildung 18: Klassendiagramm für Registerdatennavigation 118
Abbildung 19: Datenfluss von Funktion API-NAT-1 der API RDN Abfrage 121
Abbildung 20: Datenfluss von Funktion API-NAT-2 der API RDN Abfrage 122
Abbildung 21: Entscheidungsvorlage Registerdatennavigation 132
Abbildung 22: Registerdatennavigation API mit gebündelter Funktion 141
Abbildung 23: Überblick über den fachlichen Ablauf bei nationalen Online-Antragsverfahren 152

Abbildung 24: Überblick über den Nachweisabruf aus einem anderem EU-Land 153
Abbildung 25: Klassendiagramm - IAM für Behörden 160
Abbildung 26: Phasen für die Umsetzung von IAM für Behörde 171
Abbildung 27: Darstellung der einheitlichen IAM-Lösung auf Token-Basis (UML-Notation) 175
Abbildung 28: Verworfene Variante IAM auf der Grundlage von OSCI-Intermediären (UML-Notation) 178
Abbildung 29: Funktionsumfang einer PKI-Infrastruktur 187
Abbildung 30: Klassendiagramm für Zertifikate und Schlüssel 194
Abbildung 31: Klassendiagramm V-PKI - Übergreifend im Kontext der Registermodernisierung 198
Abbildung 32: Business Übersicht für IDM für Personen 217
Abbildung 33: Grafische Ablaufbeschreibung im Datenschutzcockpit 229
Abbildung 34: Systemkontext Vermittlungsstellen 235
Abbildung 35: Aktualisierte Once-Only-Datenkette (aktueller Diskussionsstand Q3 2022) 253
Abbildung 36: Einordnung einer Intermediären Plattform für Nachweislieferanten im Kontext des EU-OOTS und des NOOTS 264
Abbildung 37: Einordnung einer Intermediären Plattform für datenabrufende Stellen im Kontext des EU-OOTS und des NOOTS 269
Abbildung 38: Logischer Aufbau der Intermediären Plattformen & Einbindung in grenzüberschreitenden Nachweisabrufen. 275
Abbildung 39: Zweistufige Nutzerweiterleitungen beim Einsatz von Intermediären Plattformen 290
Abbildung 40: Sequenzdiagramm für einen Beispielabruf eines Nachweises aus Deutschland 302
Abbildung 41: Sequenzdiagramm für einen Beispielabruf eines Nachweises aus dem EU-Ausland 303

5.4 Glossar & Abkürzungsverzeichnis

5.4.1 Glossar

Begriff/ Abkürzung	Synonyme/ Langform/Abk.	Begriffsdefinition und Quelle
(eDelivery) Access Point	Deutsch: eDelivery-Zugangspunkt	A communication component that is part of the eDelivery electronic delivery service based on technical specifications and standards, including the AS4 messaging protocol and ancillary services developed under the Connecting Europe Facility Programme and continued under the Digital Europe Programme. The extent that these technical specifications and standards overlap with the ISO 15000-2 standard. Eine Kommunikationskomponente, die Teil des elektronischen Zustelldienstes eDelivery ist und auf technischen Spezifikationen und Normen beruht, einschließlich des AS4-Datenübermittlungsprotokolls und zusätzlicher Dienste, die im Rahmen der Fazilität "Connecting Europe" entwickelt und im Rahmen des Programms "Digitales Europa" fortgeführt wurden, soweit sich diese technischen Spezifikationen und Normen mit der Norm ISO 15000-2 decken. (Quelle: Implementing Act Art. 1 Nr. 4)
Abstrakte Berechtigungs-prüfung		In §7 Abs. 2 IDNrG ist definiert, dass bei der verwaltungsbereichsübergreifenden Datenübermittlung zwischen öffentlichen Stellen, unter Verwendung der IDNr., eine abstrakte Berechtigungsüberprüfung der Datenübermittlung über eine dritte Stelle, sog. Vermittlungsstelle erfolgen muss. Liegt abstrakt eine Übermittlungsberechtigung auf Seiten des Senders oder des Empfängers einer zu übermittelnden Datenübermittlung nicht vor, so erfolgt keine Datenübermittlung. Die Vermittlungsstellen müssen ihre Aufgaben ohne Kenntnis des eigentlichen Nachrichteninhalts erbringen können; dadurch sollen sie lediglich die Metadaten der Datenübermittlung kennen, was die Gefahr einer Profilbildung verringert. Die dritten Stellen prüfen, ob es für den angegebenen Zweck und die angegebenen

Begriff/ Abkürzung	Synonyme/ Langform/Abk.	Begriffsdefinition und Quelle
		Kommunikationspartner einen entsprechenden Eintrag in einem Vermittlungs- bzw. Verzeichnisdienst gibt. Die Vermittlungsstelle muss die Datenübermittlung zudem protokollieren. (Quelle: KT Recht - Prüffrage KT-Arch-003)
AGS	Allgemeiner Gemeinde-schlüssel	8-stelliger Schlüssel zur eindeutigen Identifizierung einer Gemeinde mit den Bestandteilen: Bundesland (2 Stellen), Regierungsbezirk (1 Stelle), Kreis (2 Stellen) und Gemeinde (3 Stellen). (Quelle: Destatis - Glossar AGS)
Antragsverfahren		Verwaltungsverfahren, das nur auf Antrag durchgeführt wird
ARS	Allgemeiner Regional-schlüssel	
Behörde		Konkrete Behörde eines Behördentyps. Eine Behörde führt eine konkrete Registerinstanz und bietet einen technischen Endpunkt an, über den auf diese zugegriffen werden kann. Beispiel: Einwohnermeldeamt Köln (Quelle: KT Architektur - RDN)
Behördentyp		Kategorie von Behörden, die die gleichen Leistungen erbringen und die gleichen Prozesse ausführen. Je nach Fachdomäne gibt es eine oder mehrere Behörden vom selben Behördentyp. Behörden desselben Behördentyps führen Register desselben Registertyps. Behördentypen können auch mehrere Registertypen führen. Beispiel: Meldebehörden (Quelle: KT Architektur - RDN)

Begriff/ Abkürzung	**Synonyme/ Langform/Abk.**	**Begriffsdefinition und Quelle**
Competent Authority	Deutsch: Zuständige Behörde	Any Member State authority or body established at national, regional or local level with specific responsibilities relating to the information, procedures, assistance and problem-solving services covered by this Regulation. Jede Stelle oder Behörde eines Mitgliedstaats auf nationaler, regionaler oder lokaler Ebene mit bestimmten Zuständigkeiten für die unter diese Verordnung fallenden Informationen, Verfahren, Hilfs- und Problemlösungsdienste. (Quelle: Art. 3 Nr. 4 SDG-VO)
Data Consumer	Nachweisanfordernde Stelle	"Data Consumers sind in der Regel Onlinedienste öffentlicher Stellen, die Antragstellenden, die zur Beantragung einer Verwaltungsleistung notwendigen Formulare bereitstellen, diese um Nachweise aus Basisregistern ergänzen und die Formulare zusammen mit den Nachweisen an das zuständige Fachverfahren weiterleiten. Behörden, die Nachweise bzw. Daten aus Basisregistern abrufen, welche zur Aufgabenwahrnehmung erforderlich sind, sind ebenfalls Data Consumers." (Quelle: IT-PLR-Beschluss 2022/06)
Data Consumer Gateway		"Data Consumer Gateway und Data Provider Gateway sind Vermittlungsstellen, die Nachrichten sicher und nachvollziehbar transportieren. Dazu gehört auch die abstrakte Berechtigungsprüfung." (Quelle: IT-PLR-Beschluss 2022/06)
Data Provider	Nachweisliefernde Stellen	"Data-Provider sind registerführende Behörden oder Basisregister, die Nachweise über Antragstellende zur Bearbeitung einer Verwaltungsleistung in einem Fachverfahren ausstellen." (Quelle: IT-PLR-Beschluss 2022/06)

Begriff/ Abkürzung	Synonyme/ Langform/Abk.	Begriffsdefinition und Quelle
Data Provider Gateway		"Data Consumer Gateway und Data Provider Gateway sind Vermittlungsstellen, die Nachrichten sicher und nachvollziehbar transportieren. Dazu gehört auch die abstrakte Berechtigungsprüfung." (Quelle: IT-PLR-Beschluss 2022/06)
Data Model	Deutsch: Datenmodell	An abstraction that organises elements of data, standardises how they relate to one another and specifies the entities, their attributes and the relationship between such entities. Eine Abstraktion, in der Datenelemente organisiert werden und die ihre Beziehungen zueinander standardisiert und die Entitäten, ihre Merkmale und die Beziehungen zwischen diesen Entitäten spezifiziert. (Quelle: Implementing Act Art. 1 Nr. 13)
Data Service	Deutsch: Datendienst	A technical service through which an evidence provider handles the evidence requests and dispatches evidence. Ein technischer Dienst, über den ein Nachweislieferant die Nachweisanfrage bearbeitet und die Nachweise übermittelt. (Quelle: Implementing Act Art. 1 Nr. 12)
Data Service Directory	Abbreviated as DSD Deutsch: Verzeichnis der Datendienste	A registry containing the list of evidence providers and the evidence types they issue together with the relevant accompanying information. Ein Register, das die Liste der Nachweislieferanten und der von ihnen herausgegebenen Nachweisarten zusammen mit den entsprechenden Begleitinformationen enthält (Quelle: Implementing Act Art. 1 Nr. 7)
Datenschutzcockpit	DSC	"Das Datenschutzcockpit (DSC, Art. 2 Registermodernisierungsgesetz (RegMoG)) soll es Bürgerinnen und Bürgern ermöglichen, durchgeführte behördliche

Begriff/ Abkürzung	Synonyme/ Langform/Abk.	Begriffsdefinition und Quelle
		Datenübermittlungen unter Nutzung der Identifikationsnummer (IDNr) nach dem Identifikationsnummerngesetz (IDNrG) nachzuvollziehen und die zur Person erfassten Registerdaten einsehen zu können." (Quelle: IT-PLR-Beschluss 2022/06)
EDM	Exchange Data Model	
eID		Electronic identification as defined in Article 3 point 1 of Regulation (EU) 910/2014, the process of using person identification data in electronic form uniquely representing either a natural or legal person, or a natural person representing a legal person. (Quelle: Explanatory Paper V3.0)
eIDAS Node	Deutsch: eIDAS-Knoten	A node as defined in Article 2, point (1), of Implementing Regulation (EU) 2015/1501 and complying with the technical and operational requirements laid down in and on the basis of that Regulation. Ein Knoten im Sinne von Artikel 2 Nummer 1 der Durchführungsverordnung (EU) 2015/1501, der die technischen und operativen Anforderungen erfüllt, die in dieser Verordnung und auf deren Grundlage festgelegt sind. (Quelle: Implementing Act Art. 1 Nr. 5)
Electronic Identification means	Deutsch: Elektronisches Identifizierungsmittel	A material and/or immaterial unit, containing person identification data and which is used for authentication for an online service. Eine materielle und/oder immaterielle Einheit, die Personenidentifizierungsdaten enthält und zur Authentifizierung bei Online-Diensten verwendet wird. (Quelle: Implementing Act Art. 1 Nr. 9)

Begriff/ Abkürzung	**Synonyme/ Langform/Abk.**	**Begriffsdefinition und Quelle**
Entity		A 'thing', such as a vessel, a geographic location, a sensor, a map or something more abstract like an incident, an event or an observation. (Quelle: (EU) TDDs - Version Dezember 2021)
Evidence	Deutsch: Nachweis	Any document or data, including text or sound, visual or audiovisual recording, irrespective of the medium used, required by a competent authority to prove facts or compliance with procedural requirements referred to in point (b) of Article 2(2). Alle Unterlagen oder Daten, einschließlich Text- oder Ton-, Bild- oder audiovisuellen Aufzeichnungen, unabhängig vom verwendeten Medium, die von einer zuständigen Behörde verlangt werden, um Sachverhalte oder die Einhaltung der in Artikel 2 Absatz 2 Buchstabe b genannten Verfahrensvorschriften nachzuweisen. (Quelle: SDG-VO Art. 3 Nr. 5) Nachweise sind Unterlagen und Daten jeder Art unabhängig vom verwendeten Medium, die zur Ermittlung des Sachverhalts geeignet sind. (Quelle: § 5 Absatz 1 Satz 2 EGovG Bund-Entwurf) Vorschlag: die deutsche Definition zu dem deutschen Begriff Nachweis verschieben und nicht nur als Übersetzung von evidence auflisten, vor allem, da hier auf das EGovG verwiesen wird.
Evidence Broker	EB Deutsch: Nachweisdienst	A service allowing an evidence requester to determine which evidence type from another Member State satisfies the evidence requirement for the purposes of a national procedure. Ein Dienst, der es einer nachweisanfordernden Behörde ermöglicht, festzustellen, welche Nachweisart aus einem anderen EU-Mitgliedstaat die Anforderungen an die Nachweise für die Zwecke eines nationalen Verfahrens erfüllt

Begriff/ Abkürzung	Synonyme/ Langform/Abk.	Begriffsdefinition und Quelle
		(Quelle: Implementing Act Art. 1 Nr. 8)
Evidence Provider	Abbreviated as EP Deutsch: Nachweislieferant	A competent authority as referred to in Article 14(2) of Regulation (EU) 2018/1724 that lawfully issues structured or unstructured evidence. Eine zuständige Behörde im Sinne des Artikels 14 Absatz 2 der Verordnung (EU) 2018/1724, die strukturierte oder unstrukturierte Nachweise rechtmäßig ausstellt. (Quelle: Implementing Act Art. 1 Nr. 2)
Evidence Requester	Abbreviated as ER Deutsch: Nachweise anfordernde Behörde	A competent authority responsible for one or more of the procedures referred to in Article 14(1) of Regulation (EU) 2018/1724. Eine zuständige Behörde, die für eines oder mehrere der in Artikel 14 Absatz 1 der Verordnung (EU) 2018/1724 genannten Verfahren verantwortlich ist. (Quelle: Implementing Act Art. 1 Nr. 3)
Evidence Survey		Die Evidence Survey ist eine zentrale Erhebung durch die EU-Kommission, die durch innerstaatliche Vorarbeiten vorbereitet wird. Ziel der Evidence Survey ist die Identifikation von Nachweisen für den automatisierten grenzüberschreitenden Austausch zu SDG-relevanten Verfahren. Für die Erstellung der Evidence Survey müssen innerstaatliche Vorarbeiten erfolgen, die hier „Deutsche Erhebung Evidence Survey“ genannt werden. Die deutsche Erhebung für die Evidence Survey wird durch den nationalen SDG-Koordinator gesteuert. Die Bearbeitung obliegt dem Kompetenzteam EU-Interoperabilität. Die Prüfung und Freigabe der deutschen Angaben für die EU KOM erfolgt durch die fachlich und rechtlich zuständigen Stellen.
Evidence Type	Deutsch: Nachweisart Nachweistyp	A category of structured or unstructured evidence with a common purpose or content. Eine Kategorie von strukturierten oder unstrukturierten Nachweisen mit einem

Begriff/ Abkürzung	Synonyme/ Langform/Abk.	Begriffsdefinition und Quelle
		gemeinsamen Zweck oder einem gemeinsamen Inhalt. (Quelle: Implementing Act Art. 1 Nr. 17)
Explanatory Paper		Begleitdokument, welches Aufschluss über den Anwendungsbereich des Anhang 2 der SDG-Verordnung gibt. Die zu betrachtenden Richtlinien aus Artikel 14 sind bislang nicht im Explanatory Paper enthalten. Die Mitgliedstaaten haben die EU KOM darauf hingewiesen, dass für die Auslegung der Richtlinien ein vergleichbares Dokument hilfreich wäre; eine entsprechende Ergänzung erfolgt möglicherweise.
Fachlicher Dienst		Logische Gruppierung technischer Dienste, die denselben Nachweistyp liefern. Beispiel: NOOT_Melderegister (Quelle: KT Architektur - RDN)
Fachverfahren		Technisch: IT-Anwendung zur Unterstützung oder Ausführung einer speziellen Verwaltungsaufgabe Juristisch: fachrechtliche Verwaltungsverfahren
Front office		Verfahrensschnittstelle, die es den Nutzenden ermöglicht, mit der zuständigen Behörde von der Identifizierung der Nutzenden bis zum Abschluss eines Online-Verfahrens zu interagieren. (Quelle: Explanatory Paper V3.0)
führendes Register		Ein Nachweis wird von einer durch geltendes Recht berechtigten Stelle ausgestellt. Führendes Register für diesen Nachweis ist das Register, aus dem die berechtigte Stelle die Daten bezieht/in das sie diese speichert.
IAM für Behörden		"Das IAM für Behörden ermöglicht die technische Authentifizierung von Behörden

Begriff/ Abkürzung	Synonyme/ Langform/Abk.	Begriffsdefinition und Quelle
		durch die Prüfung von Zertifikaten sowie die Überprüfung der Gültigkeit durch einen bereitgestellten Onlinedienst der V-PKI." (Quelle: IT-PLR-Beschluss 2022/06)
IDM für Unternehmen	Identitätsmanagement für Unternehmen	Das Identitätsmanagement für Unternehmen befasst sich mit der registerübergreifenden eindeutigen Identifikation der Unternehmen anhand einer bundeseinheitlichen Wirtschaftsnummer. Die Bundeseinheitliche Wirtschaftsnummer wird durch das Bundeszentralamt für Steuern vergeben und von der W-IdNr.-Datenbank des Bundeszentralamtes für Steuern bereitgestellt.
IDM für Personen	Identitätsmanagement für Unternehmen	"Das IDM für Personen (Art. 1 RegMoG) stellt die IDNr eines Bürgers bzw. einer Bürgerin und weitere Basisdaten zur Person bereit." (Quelle: IT-PLR-Beschluss 2022/06)
IDNr	Identifikationsnummer	Die Identifikationsnummer nach § 139b der Abgabenordnung, die nach dem IDNr-Gesetz als zusätzliches Ordnungsmerkmal in allen von der Registermodernisierung betroffenen Register eingeführt wird mit dem primären Zweck, die Daten einer natürlichen Person in einem Verwaltungsverfahren eindeutig zuordnen zu können.
Implementing Act	IA, DVO, Durchführungsverordnung, Implementing Regulation	Durchführungsverordnungen der Kommission dienen der einheitlichen Umsetzung von EU-Rechtsvorschriften. Zu diesem Zweck hat die Kommission zu Art. 14 SDG-VO (vgl. Art. 14 Abs. 9 SDG-VO) die Durchführungsverordnung (EU) 2022/1463 der Kommission vom 5. August 2022 zur Festlegung technischer und operativer Spezifikationen des technischen Systems für den grenzüberschreitenden automatisierten Austausch von Nachweisen und zur Anwendung des Grundsatzes der einmaligen Erfassung gemäß der Verordnung (EU) 2018/1724 des Europäischen Parlaments und des Rates erlassen.

Begriff/ Abkürzung	**Synonyme/ Langform/Abk.**	**Begriffsdefinition und Quelle**
Incident	Deutsch: Vorfall	A situation where the OOTS is not performing, fails to transmit the evidence or transmits evidence that has not been requested, or where the evidence has changed or been disclosed during the transmission, as well as any breach of security referred to in Article 29. Eine Situation, in der das technische System (OOTS) die Leistung nicht erbringt, die Nachweise nicht übermittelt oder Nachweise übermittelt, die nicht angefordert wurden, oder in der die Nachweise während der Übermittlung verändert oder offengelegt wurden, sowie jede Verletzung der Sicherheit gemäß Artikel 29. (Quelle: Implementing Act Art. 1 Nr. 18)
Intermediary Platform Intermediäre Plattform	IP	A technical solution acting in its own capacity or on behalf of other entities such as evidence providers or evidence requesters, depending on the administrative organisation of Member States in which the intermediary platform operates, and through which evidence providers or evidence requesters connect to the common services referred to in Article 4(1) or to evidence providers or evidence requesters from other Member States. Eine technische Lösung, die je nach der Verwaltungsorganisation der Mitgliedstaaten, in denen die Intermediäre Plattform tätig ist, in Erfüllung eigener Aufgaben oder im Namen anderer Behörden wie Nachweislieferanten oder Nachweise anfordernden Behörden tätig wird und über die Nachweislieferanten oder Nachweise anfordernde Behörden mit den in Artikel 4 Absatz 1 genannten gemeinsamen Diensten oder mit Nachweislieferanten oder Nachweise anfordernden Behörden aus anderen Mitgliedstaaten verbunden werden. (Quelle: Implementing Act Art. 1 Nr. 6)
LAU	Lokale Verwaltungseinheiten	Der europäische Schlüssel, um Gemeinden zu identifizieren. "Um der Nachfrage nach Statistiken auf lokaler Ebene gerecht zu werden, unterhält Eurostat ein

Begriff/ Abkürzung	Synonyme/ Langform/Abk.	Begriffsdefinition und Quelle
		System lokaler Verwaltungseinheiten (LAUs), das mit der NUTS kompatibel ist. Diese LAU sind die Bausteine der NUTS und umfassen die Gemeinden und Kommunen der Europäischen Union." (Quelle: Eurostat - LAU)
Lawfully issued		"von einer staatlich ermächtigten Institution ausgestellt"
Nachweis		siehe "Evidence".
Nachweistyp		Ein fachliches Objekt, um einen Sachverhalt nachzuweisen. Dabei kann es sich um ein (elektronisches) Dokument oder eine Datenstruktur handeln. Ein Nachweistyp wird von Registern desselben Registertyps ausgestellt. Ein Nachweistyp wird von einem fachlichen Dienst geliefert. Siehe auch "Nachweis" und "Evidence". Beispiel: Meldenbescheinigung (Quelle: KT Architektur - RDN) Nachweistypen dienen zur Klassifikation von Nachweisen nach gemeinsamem Zweck oder Inhalt. Nachweistypen sind selbst keine Nachweise, aber Nachweise gehören zu einem Nachweistyp. Beispiel: Alle konkreten Geburtsurkunden sind Ausprägungen zum Nachweistyp "Geburtsurkunde".
Nachweisanfordernde Stellen		siehe "Data Consumer"
Nachweisliefernde Stelle		siehe "Data Provider"

Begriff/ Abkürzung	**Synonyme/ Langform/Abk.**	**Begriffsdefinition und Quelle**
Nationales Once-Only-Technical-System	NOOTS	Das OOTS, welches auf nationaler Ebene für Deutschland entwickelt wird, da es nationale Anforderungen gibt, die vom EU-OOTS nicht abgedeckt werden können. (Quelle: IT-PLR-Beschluss 2022/06) Das NOOTS ist ein System aus technischen Komponenten, Schnittstellen und Standards sowie organisatorischen und rechtlichen Regelungen, das öffentlichen Stellen den rechtskonformen Abruf von elektronischen Nachweisen aus den Registern der deutschen Verwaltung ermöglicht. Über einen Anschluss an das europäische Once-Only-Technical-System (EU-OOTS) wird ein Austausch von Nachweisen mit dem EU-Ausland ermöglicht. (Quelle: KT Architektur - HLA)
(EU) Once-Only Technical System	Deutsch: Technisches System zur einmaligen Erfassung Kurzform für deutsche Texte: "EU-OOTS" Abbreviated as (EU) OOTS	The technical system for the cross-border automated exchange of evidence referred to in Article 14(1) of Regulation (EU) 2018/1724. Das technische System für den grenzüberschreitenden automatisierten Austausch von Nachweisen gemäß Artikel 14 Absatz 1 der Verordnung (EU) 2018/1724. (Quelle: Implementing Act Art. 1 Nr. 1)
Online-Leistung / Online-Service	Online-Dienst	Digitalisiertes Verwaltungsverfahren
Portal		Siehe "Procedure Portal"
Preview (Space), der	Deutsch: Vorschaubereich	A functionality that enables the user to preview the requested evidence as referred to in Article 15(1), point (b)(ii). Eine Funktion, die es den Nutzenden ermöglicht, die angeforderten Nachweise gemäß Artikel 15 Absatz 1 Buchstabe b Ziffer ii vorab einzusehen. (Quelle: Implementing Act Art. 1 Nr. 14)

Begriff/ Abkürzung	**Synonyme/ Langform/Abk.**	**Begriffsdefinition und Quelle**
Procedural requirements	PR, verfahrensbezogene Nachweisanforderungen	Aus den erforderlichen Nachweisen ergeben sich Procedural Requirements (PR), auf Deutsch bestimmte (abstrakte) verfahrensbezogene Nachweisanforderungen genannt. Beispiel: Der erforderliche Nachweis "Ausweisdokument" hat die übergeordnete Nachweisanforderung „Nachweis der Identität“.
Procedure	Deutsch: Verfahren	A sequence of actions that must be taken by users to satisfy the requirements, or to obtain from a competent authority a decision, in order to be able to exercise their rights as referred to in point (a) of Article 2(2). Eine Abfolge von Maßnahmen, die die Nutzenden ergreifen müssen, um den Anforderungen zu entsprechen oder einen Beschluss einer zuständigen Behörde zu erwirken, um ihre Rechte nach Artikel 2 Absatz 2 Buchstabe a ausüben zu können. (Quelle: SDG-VO Art. 3 Nr. 3)
Procedure Portal	Deutsch: Verfahrensportal	A webpage or a mobile application where a user can access and complete an online procedure referred to in Article 14(1) of Regulation (EU) 2018/1724. Eine Webseite oder eine mobile Anwendung, über die die Nutzenden Zugang zu einem Online-Verfahren im Sinne von Artikel 14 Absatz 1 der Verordnung (EU) 2018/1724 haben und es abschließen können. (Quelle: Implementing Act Art. 1 Nr. 19)
Register		Liste der Datenbestände aus der Anlage zu Art 1 §1 RegMoG
Registerdatennavigation	RDN	Komponente im Zielbild und zentraler Routingdienst des NOOTS. Liefert auf Anfrage die Information, von welchem technischen Dienst einer Behörde ein gesuchter Nachweistyp abgerufen werden kann. Dazu übermittelt die RDN notwendige Verbindungsparameter.

Begriff/ Abkürzung	Synonyme/ Langform/Abk.	Begriffsdefinition und Quelle
		(Quelle: KT Architektur)
registerführende Stelle		Registerführende Stelle zu einem Register ist die Behörde/das Basisregister, die/das rechtlich zur Führung des Registers berechtigt oder verpflichtet ist.
Registerinstanz		Eine Kategorie von IT-Systemen, die Daten der Verwaltung speichern und elektronische Nachweise ausstellen können. Registerinstanzen desselben Registertyps werden von Behörden desselben Behördentyps geführt. Register desselben Registertyps bieten denselben fachlichen Dienst zur Ausstellung desselben elektronischen Nachweistyps an. Beispiel: Melderegister (Quelle: KT Architektur - RDN)
Registertyp		Ein IT-System, welches von einer Behörde geführt wird. Registerinstanzen betreiben technische Endpunkte, über die von ihnen erstellte Nachweise abgerufen werden können. Beispiel: Melderegister der Stadt Köln (Quelle: KT Architektur - RDN) Registertypen dienen zur Klassifikation von Registern nach nach gemeinsamem Zweck oder Inhalt. Registertypen sind selbst keine Register, aber Register gehören zu einem Registertyp. Beispiel: Alle konkreten Melderegister sind Ausprägungen zum Registertyp "Melderegister".
Reifegradmodell Nachweisabruf		Modell zur Beschreibung von möglichen Reifegraden, in denen ein Nachweis in den Registern der deutschen Verwaltung vorliegen kann. Das Modell umfasst die Stufe A (Offline), die Stufe B (Elektronisch übermittelte Nachweise), die Stufe C (Elektronisch auswertbare Nachweise) und die Stufe D (bedarfsgerecht übermittelte Informationen). (Quelle: KT Architektur)

Begriff/ Abkürzung	Synonyme/ Langform/Abk.	Begriffsdefinition und Quelle
Routingparameter		Je Nachweistyp festgelegte Informationen zur Ermittlung des für die Ausstellung des Nachweises zuständige Stelle. Beispiel: Postleitzahl (Quelle: KT Architektur - RDN)
SDG	Single-Digital Gateway	"The single digital gateway facilitates online access to information, administrative procedures, and assistance services that EU citizens and businesses may need in another EU country." (Quelle: Europäische Kommission - SDG)
SDG-OOTS		Hinweis: Dieser Begriff wird nicht verwendet. Siehe führender Begriff "(EU) Once-Only Technical System".
SDG-Procedure		Siehe "Procedure".
SDG Regulation	SDG-Verordnung, SDG-VO	Regulation (EU) 2018/1724 of the European Parliament and of the Council of 2 October 2018 establishing a single digital gateway to provide access to information, to procedures and to assistance and problem-solving services and amending Regulation (EU) No 1024/2012.
SDG1-Relevanz		Nationale Verfahren auf LeiKa-Ebene werden bei Erfüllung der in Anhang I der SDG-VO definierten Kriterien als SDG-1-relevant bezeichnet. Der Evidence Survey erhebt keine Informationen zur SDG1-Relevanz. SDG1-relevant sind Informationsbereiche im Zusammenhang mit Bürgern.
SDG2-Relevanz		Nationale Verfahren auf LeiKa-Ebene werden bei Erfüllung der in Artikel 14 der SDG-VO definierten Kriterien als SDG2-relevant bezeichnet. Die Zahl 2 bezieht sich dabei auf den Anhang 2 der SDG-Verordnung, wenngleich von Artikel 14 mehr als nur die in Anhang 2 aufgeführten 21 SDG-Verfahren betroffen sind,

Begriff/ Abkürzung	Synonyme/ Langform/Abk.	Begriffsdefinition und Quelle
		nämlich auch die Verfahren nach den Richtlinien 2005/36/EG, 2006/123/EG, 2014/24/EU und 2014/25/EU werden hier als SDG2-relevante Verfahren bezeichnet.
Semantic Repository	Deutsch: Semantischer Datenspeicher	A collection of semantic specifications, linked to the evidence broker and the data service directory, composed of definitions of names, data types and data elements associated with specific evidence types to ensure mutual understanding and cross-lingual interpretation for evidence providers, evidence requesters and users, when exchanging evidence through the OOTS. Ein Archiv semantischer Spezifikationen, die mit dem Nachweisdienst und dem Verzeichnis der Datendienste verknüpft sind und aus Definitionen von Namen, Datentypen und Datenelementen bestehen, die mit bestimmten Nachweisarten verbunden sind, um das gegenseitige Verständnis und die sprachenübergreifende Auslegung für Nachweislieferanten, Nachweise anfordernde Behörden und Nutzenden beim Austausch von Nachweisen über das OOTS sicherzustellen. (Quelle: Implementing Act Art. 1 Nr. 10)
Service Gateways	SGs	Service Gateways (SGs) sind optionale Produkte, die die Anbindung von Data Consumers und Data-Providern an das NOOTS vereinfachen und beschleunigen können. Sie bündeln Authentifizierung und Autorisierung, Schemavalidierung, Protokollübersetzung oder Datentransformation. Data Consumers und Data-Provider können Anbindungen wahlweise über eigene Schnittstellen/Komponenten oder über SGs umsetzen. (Quelle: IT-PLR-Beschluss 2022/06)
Structured Evidence	Deutsch: Strukturierter Nachweis	Any evidence in electronic format required for the procedures listed in Article 14(1) of Regulation (EU) 2018/1724 that is organised in predefined elements or fields that have a specific meaning and technical format allowing for

Begriff/ Abkürzung	Synonyme/ Langform/Abk.	Begriffsdefinition und Quelle
		processing by software systems, supplemented by the metadata elements of the OOTS generic metadata model referred to in Article 7(1) of this Regulation and either in compliance with the OOTS data model for the relevant evidence type as referred to in Article 7(2) of this Regulation, or accompanied by a human-readable version. Ein Archiv semantischer Spezifikationen, die mit dem Nachweisdienst und dem Verzeichnis der Datendienste verknüpft sind und aus Definitionen von Namen, Datentypen und Datenelementen bestehen, die mit bestimmten Nachweisarten verbunden sind, um das gegenseitige Verständnis und die sprachenübergreifende Auslegung für Nachweislieferanten, Nachweise anfordernde Behörden und Nutzenden beim Austausch von Nachweisen über das OOTS sicherzustellen. (Quelle: Implementing Act Art. 1 Nr. 15)
Technical Design Documents	Abbreviated as TDD Deutsch: Technische Entwurfs-dokumentation	A set of detailed and non-binding technical documents, drawn up by the Commission in cooperation with Member States in the framework of the EU SDG Coordination Group referred to in Article 29 of Regulation (EU) 2018/1724 or any sub-groups referred to in Article 19 of this Regulation, which includes but is not limited to, a high-level-architecture, exchange protocols, standards and ancillary services that support the Commission, Member States, evidence providers, evidence requesters, intermediary platforms and other entitites concerned in establishing the OOTS in compliance with this Regulation. Eine Reihe detaillierter und unverbindlicher technischer Dokumente, die von der Kommission in Zusammenarbeit mit den Mitgliedstaaten im Rahmen der Koordinierungsgruppe für das Zugangstor gemäß Artikel 29 der Verordnung (EU) 2018/1724 oder etwaiger Untergruppen gemäß Artikel 19 dieser Verordnung erstellt werden und die unter anderem eine oberste Ebene der Architektur,

Begriff/ Abkürzung	Synonyme/ Langform/Abk.	Begriffsdefinition und Quelle
		Austauschprotokolle, Normen und Zusatzdienste umfassen, die die Kommission, die Mitgliedstaaten, die Nachweislieferanten, die Nachweise anfordernden Behörden, die Intermediären Plattformen und andere betroffene Behörden bei der Einrichtung des OOTS im Einklang mit dieser Verordnung unterstützen. (Quelle: Implementing Act Art. 1 Nr. 11)
Technischer Dienst	Data Service	Unter dem technischen Dienst wird die konkrete Implementierung eines fachlichen Dienstes zur Ausstellung eines Nachweises bei einer konkreten Registerinstanz verstanden. Andere technische Dienste, die Softwarekomponenten anbieten, sind im Kontext dieses Konzepts nicht gemeint. Für den Abruf von Nachweisen von einem technischen Dienst sind Verbindungsparameter erforderlich. Beispiel: Dienstinstanz von NOOTS_Meldebescheinigung für die Stadt Köln (Quelle: KT Architektur - RDN)
Unstructured Evidence	Deutsch: Unstrukturierter Nachweis	Evidence in electronic format required for the procedures listed in Article 14(1) of Regulation (EU) 2018/1724 that is not organised in predefined elements or fields that have specific meaning and technical format, but is supplemented by the metadata elements of the OOTS generic metadata model referred to in Article 7(1) of this Regulation. Nachweise in elektronischem Format, die für die in Artikel 14 Absatz 1 der Verordnung (EU) 2018/1724 genannten Verfahren erforderlich sind und die nicht in vordefinierten Elementen oder Feldern organisiert sind, die eine bestimmte Bedeutung und ein bestimmtes technisches Format haben, sondern durch die Metadatenelemente des allgemeinen Metadatenmodells des OOTS gemäß Artikel 7 Absatz 1 der vorliegenden Verordnung ergänzt werden. (Quelle: Implementing Act Art. 1 Nr. 16)

Begriff/ Abkürzung	**Synonyme/ Langform/Abk.**	**Begriffsdefinition und Quelle**
User	Deutsch: Nutzende	Bürgerinnen und Bürger der EU oder eine natürliche Person mit Wohnsitz in einem Mitgliedstaat der EU sowie eine juristische Person mit eingetragenem Sitz in einem EU-Mitgliedstaat.
Verbindungs-parameter		Die Gesamtheit aller Informationen, die benötigt werden, um einen Technischen Dienst zu nutzen. Dazu gehört mindestens die URL des Dienstes, Zertifikate, etc. Beispiel: Dienstinstanz von NOOTS_Meldebescheinigung für die Stadt Köln & Zertifikat des Einwohnermeldeamts Köln (Quelle: KT Architektur - RDN)
Verwaltungs-Public-Key-Infrastructure	V-PKI	"Die Verwaltungs-Public-Key-Infrastructure (V-PKI) stellt eine zertifikatsbasierte Infrastruktur für elektronische Signatur und Verschlüsselung zum Schutz der Vertraulichkeit, Integrität und Authentizität in der digitalen Kommunikation zur Verfügung." (Quelle: IT-PLR-Beschluss 2022/06)
Verwaltungs-verfahren		Ein Verwaltungsverfahren liefert oder benötigt Nachweise. Es kann, muss sich aber dabei nicht um eine Leistung handeln. Beispiel: „Meldedatensatz zum Abruf Bereitstellung“ (elektronische Meldebescheinigung) (Quelle: KT Architektur - RDN)
Zentrale Dienste (des EU-OOTS)	Central Services	Evidence Broker (siehe Begriffsdefinition oben) Data Service Directory (siehe Begriffsdefintion oben) Semantic Repository (siehe Begriffsdefintion oben) Von der europäischen Kommission bereitgestellte zentrale Komponenten des EU-OOTS. Sie dienen alle als "Nachschlagewerke"

Begriff/ Abkürzung	Synonyme/ Langform/Abk.	Begriffsdefinition und Quelle
		und verarbeiten selbst keine personenbezogenen Daten.

5.4.2 Abkürzungsverzeichnis

AGS	Allgemeiner Gemeindeschlüssel
API	Application Programming Interface
BMI	Bundesministerium des Innern und für Heimat
BVA	Bundesverwaltungsamt
DE4A	Digital Europe for All
DVDV	Deutsches Verwaltungsdiensteverzeichnis
eIDAS	electronic IDentification, Authentication and trust Services
EUR	Euro
FITKO	Föderale IT-Kooperation
IDNr	Identifikationsnummer
IDNrG	Identifikationsnummerngesetz
IT-PLR	IT-Planungsrat
EU-KOM	Europäische Kommission
KoSIT	Koordinierungsstelle für IT-Standards
KT	Kompetenzteam
Mio.	Millionen
Mrd.	Milliarden
NdB	Netze des Bundes
NKR	Nationaler Normenkontrollrat
OOTS	Once-Only-Technical-System
OZG	Onlinezugangsgesetz
PVOG	Portalverbund Online-Gateway
RegMoG	Registermodernisierungsgesetz

RDN	Registerdatennavigation
SDG	Single Digital Gateway
SDG-VO	SDG-Verordnung
URI	Uniform Resource Identifier
ZuFi	Zuständigkeitsfinder