Freie Hansestadt Bremen

IT-Planungsrat
Digitale Zukunft gestalten

Governikus KG

dataport

Prüfauftrag zu Baustein 5 „OZG PLUS Postfach“ und Baustein 6 „Autorisierungsmodul“

Erweiterung der Bausteine 1 – 4 auf dem Weg zu einem Einheitlichen Unternehmenskonto

Inhaltsverzeichnis

1 Management Summary

Im Rahmen der Erstellung des Basiskonzepts zu einem Einheitlichen Unternehmenskonto wurde festgestellt, dass dieses um Funktionalitäten, die in den Bausteinen 5 „OZG-PLUS-Postfach“ und 6 „Autorisierungsmodul“ münden, erweitert werden muss. Ziel der Erweiterung um die beiden Bausteine ist es, eine wirtschaftliche und funktionale Adaption des Einheitlichen Unternehmenskontos in allen Ländern zu ermöglichen sowie den Grundstein für eine ganzheitliche Digitalisierung von Business-to-Government-Beziehungen zu setzen.

Ebenso wurde vereinbart, dass diese Bausteine im Wege der arbeitsteiligen OZG-Umsetzung von Bremen zunächst im Wege eines Prüfauftrags vor der eigentlichen Umsetzung zu betrachten sind. Vereinbart war das Ziel eines selbstständigen Betriebs, unabhängig von den Bausteinen 1 bis 4.

Die Trennung in funktionale Bausteine, die möglichst lose gekoppelt sind, stellt so generell die flexible Weiterentwicklung sicher. Da heute noch nicht abgesehen werden kann, welche Anforderungen noch entstehen, wenn das System erst einmal etabliert ist, kann diese Art der Umsetzung als Blaupause für zukünftige Erweiterungen dienen.

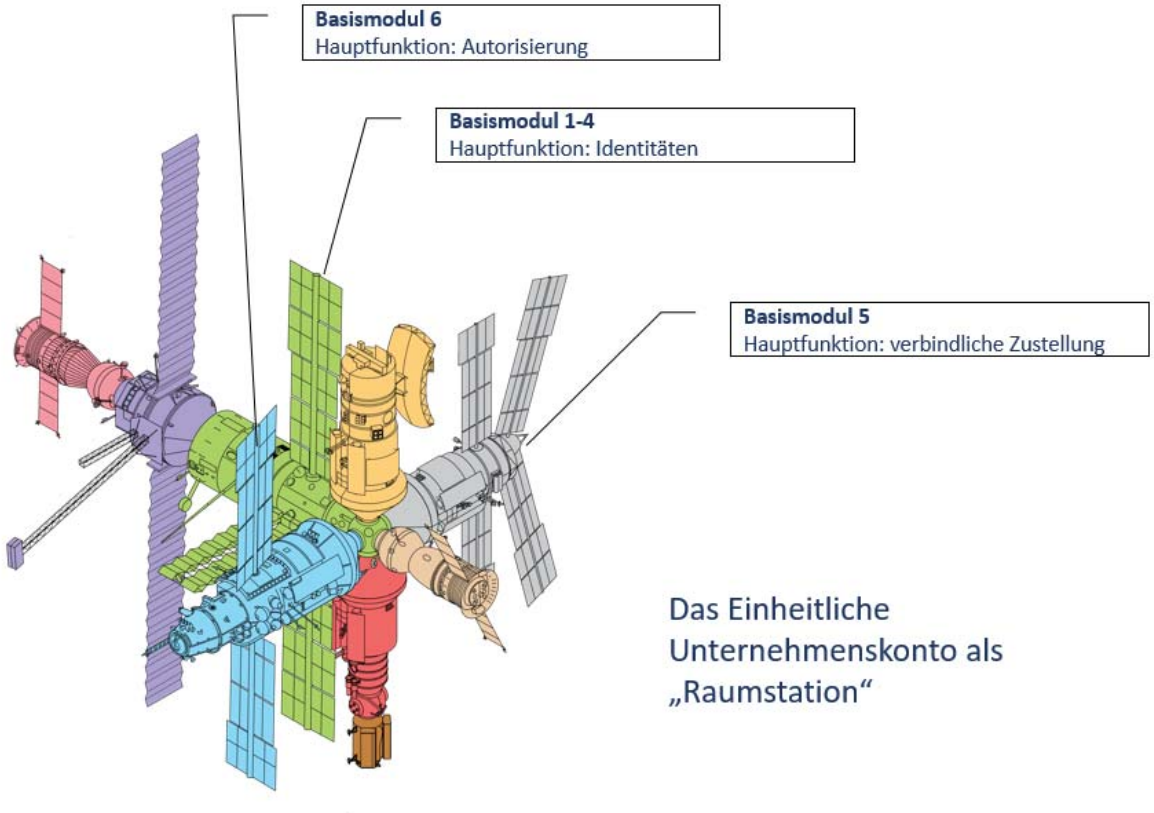

Abbildung 1: Das Einheitliche Unternehmenskonto als „Raumstation“

Bei der Architektur des Gesamtsystems sind wir davon ausgegangen, dass es auch in Zukunft weitere Anforderungen geben kann, die weitere Module erfordern. Genau deswegen ist es so entscheidend, die bestehenden Funktionsblöcke abzugrenzen und zu benennen sowie klar umrissene und standardisierte Schnittstellen zu beschreiben.

Auch wenn das Einheitliche Unternehmenskonto deutlich weniger komplex ist als eine Raumstation; sei doch der folgende Vergleich erlaubt. Internationale Raumstationen sind deswegen so erfolgreich umgesetzt worden, weil diese sogar Nationen-übergreifend entwickelt werden

konnten und nicht alles aus einer Hand kommen muss. Auch Bayern und Bremen sind gemeinsam in der deutschen Raumfahrt aktiv; mit MT Aerospace aus dem Raumfahrtkonzern OHB sind Standorte in Bremen und Augsburg erfolgreich.

Der Prüfauftrag zu den Bausteinen 5 „OZG-PLUS-Postfach“ und 6 „Autorisierungsmodul“ konnte erfolgreich durchgeführt werden. Hinsichtlich der Ziele des Prüfauftrags wurde festgestellt, dass die Machbarkeit der Umsetzung für die Bausteine 5 und 6 gegeben ist.

Eine genaue Umsetzung der Bausteine 5 und 6 im Zusammenspiel mit den Bausteinen 1 bis 4 ist in der Feinkonzeptionsphase zu definieren.

2 Kurzdarstellung der Bausteine

Das Angebot eines Einheitlichen Unternehmenskontos auf der Basis der sechs Bausteine bietet eine hohe funktionale Flexibilität bei der Entwicklung von digitalen Verwaltungsleistungen. Es erhöht die Nutzerfreundlichkeit, da die Anforderungen der verschiedenen Organisationen abgebildet werden können und ein Fokus auf offenen Standards liegt.

Die folgende Tabelle zeigt, welche Funktionalitäten durch die Bausteine 5 und 6 für das Einheitliche Unternehmenskonto ergänzt werden und welchen Mehrwert die Erweiterung um die beiden Bausteine bietet. Die Tabelle dient der verständlichen Darstellung, welche Funktionen die Bausteine 5 und 6 liefern. Die Angaben basieren auf den aktuellen Erkenntnissen und sollen in keinster Weise die Bausteine 1 - 4 in ihrer Sinnhaftigkeit und ihrem Funktionsumfang schmälern.

Rubrik	Feature	Bemerkungen[1]
Allgemein	Verwendung etablierter, offener Standards (Empfehlung IT-PLR zu XTA)	Governikus KG dataport
Allgemein	Maschine-zu-Maschine-Kommunikation	Governikus KG dataport *2
Allgemein	starke Vertraulichkeit ermöglichen (Verschlüsselung, kein Teilen des privaten Schlüssels)	Governikus KG dataport
Allgemein	Nachvollziehbarkeit/Nachweisbarkeit/Quittungsmechanismus (auch nach offenen Standards)	Governikus KG dataport
Postfach	Postfach als Rückkanal (Ablage von Nachrichten und Bescheiden), erreichbar webbasiert über ein Portal oder über Maschine-zu-Maschine-Kommunikation	*2 Governikus KG
Postfach	Wechsel des Postfachs (z.B. durch Weiterleitung)	Governikus KG
Postfach	Auswahl eines abweichenden Empfängers bei Antragsstellung	Governikus KG
Postfach	Funktions- bzw. Gruppenpostfächer	Governikus KG
Postfach	Poststellenfunktion/Fachsoftware-Anbindung (Empfangsmodul)	Governikus KG
Postfach	Notifikationen bei neuen Nachrichten	*2 Governikus KG
Postfach	Notifikationen bei noch nicht abgerufenen Nachrichten	Governikus KG
Postfach	Unterstützung von verschiedenen Transportinfrastrukturen	Governikus KG
Postfach	Nutzung des Rückkanals für Antworten von der Organisation an die Verwaltung	Governikus KG

[1] Die Bemerkungen zu den Bausteinen 1 bis 4 wurden entnommen aus „Basiskonzept Unternehmenskonto“ und „Machbarkeitsstudie für ein sogenanntes ELSTER Unternehmenskonto“.

[2] In Baustein 1-4 auch vorhanden

Autorisierung	Abwesenheitsvertretung innerhalb des Unternehmens (Urlaub, Krankheit)	dataport
Autorisierung	Vertretung durch Dritte (Architekt, Notar)	dataport *3
Autorisierung	Zugriffssteuerung auf Postfächer innerhalb einer Organisation ermöglichen	dataport
Autorisierung	Fachliche/organisatorische Berechtigungs-steuerung innerhalb des Unternehmens	dataport
Autorisierung	Verwaltung der Mitarbeiter eines Unterneh-mens	dataport
Autorisierung	Möglichkeit zur Einrichtung von Berechti-gungsgruppen innerhalb eines Unterneh-mens	dataport
Autorisierung	Möglichkeit für Anbieter digitaler Verwal-tungsleistungen, die Nutzung auf bestimmte Unternehmen zu beschränken	dataport
Autorisierung	Möglichkeit, Rollen für eine digitale Verwal-tungsleistung zu definieren	dataport

Tabelle 1: Übersicht Funktionalitäten

[3] In Baustein 1-4 teilweise vorhanden

3 Vision

Das Einheitliche Unternehmenskonto, welches neben den Unternehmen auch andere Organisationen, wie Behörden und Vereine sowie Stiftungen, umfasst, kann nur erfolgreich sein, wenn eine ganzheitliche Digitalisierung angestrebt wird.

Eine ganzheitliche Digitalisierung umfasst die Digitalisierung der Verwaltungsleistung im Großen und Ganzen mit Blick auf den gesamten Prozess und die Möglichkeit für die Unternehmen, ihre Prozesse, Zuständigkeiten und organisatorischen Regelungen abzubilden.

Die jahrelange Erfahrung beim Digitalisieren von Verwaltungsleistungen hat gezeigt, dass ein Großteil der digitalen Verwaltungsleistungen nicht als reine Antragsformulare dargestellt werden können. Die Komplexität bestimmter Verwaltungsleistungen erfordert eine flexible, nutzerzentrierte Entwicklung, um den Endanwendern die Nutzung so einfach wie möglich zu gestalten und die Erfahrung zu liefern, dass der Kontakt zur Verwaltung einfach und schnell vonstattengeht.

Dieses Ziel wird nicht erreicht, indem die bereits vorhandenen Papierprozesse nur in elektronische Antragsformulare übertragen werden. Das Potenzial für Optimierungen, gerade auch bei den Arbeitsschritten, die in der Verwaltung ablaufen, wird hier verschenkt.

Um für Unternehmen smarte, digitale Verwaltungsleistungen anbieten zu können, sind Funktionalitäten erforderlich, die über die angebotenen Funktionen der Bausteine 1 bis 4 hinausgehen. Die ganzheitliche Digitalisierung und der flächendeckende Erfolg des Einheitlichen Unternehmenskontos können nur erreicht werden, indem die Bausteine 5 und 6 mit angeboten werden.

Die Bausteine 5 und 6 sind Bestandteile des Einheitlichen Unternehmenskontos und ganzheitlich, in Verbindung mit den Bausteinen 1 bis 4, als ein organisatorisch zusammengehörendes System anzusehen. Eine einheitliche Nutzerführung und ein einheitliches Design werden hier das Gefühl des Anwenders stärken, mit *einem* System zu agieren.

Eine lose Koppelung der einzelnen Bausteine untereinander und die Reduzierung der Abhängigkeiten sollte die Bestrebung sein, da so eine einfache Integration weiterer zukünftig notwendiger Bausteine, wie z.B. eine Bezahlungskomponente, ermöglicht werden kann. Gerade in der heutigen schnelllebigen Zeit sollte die Erweiterbarkeit um weitere Bausteine 7 – n gewährleistet sein, um flexibel auf neue Gegebenheiten reagieren zu können.

4 Auftrag des IT-Planungsrats

Die Ziffern 5 und 6 des Beschlusses des IT-Planungsrats vom Januar 2020 stellen die Grundlage für den Prüfauftrag zu den Bausteinen 5 und 6 dar. Aus diesem Beschluss geht in Ziffer 1 ebenfalls deutlich hervor, dass das Einheitliche Unternehmenskonto die Bausteine 1 bis 6 umfasst und sollte eine Beauftragung der Bausteine 5 und 6 erfolgen, diese zusammen mit den Bausteinen 1 – 4 als ein System angesehen werden sollten.

Beschluss des IT-Planungsrates 2020/01

1. Der IT-Planungsrat stimmt der Einrichtung eines einheitlichen Unternehmenskontos auf Basis des vom Koordinierungsprojekt Unternehmenskonto vorgelegten Basiskonzepts mit den Bausteinen 1-6 zu. Der IT-Planungsrat dankt dem Koordinierungsprojekt Unternehmenskonto für die geleistete Arbeit.

2. Der IT-Planungsrat richtet als Nachfolger des derzeitigen Koordinierungsprojektes Unternehmenskonto ein länderoffenes Steuerungsprojekt Unternehmenskonto unter Federführung Bayerns und Bremens ein und beauftragt dieses zum 01.02.2020 mit der Umsetzung des Unternehmenskontos entsprechend der inhaltlichen, organisatorischen und zeitlichen Vorgaben des Basiskonzepts.

3. Der IT-Planungsrat beauftragt das Land Bayern im Rahmen des Projekts „EKONA 2“ (Elster Konten für Alle) mit der Bereitstellung der vier Bausteine MEIN UP 1.0, NEZO, NEZOP und Postfach 2.0.

4. Der IT-Planungsrat erteilt hierfür aus seinem bestehenden Digitalisierungsbudget eine Finanzierungszusage entsprechend der vom Koordinierungsprojekt Unternehmenskonto vorgelegten Kostenschätzung.

5. Der IT-Planungsrat stellt fest, dass das einheitliche Unternehmenskonto zur flexiblen wirtschaftlichen und funktionalen Adaption in den Ländern über die optionalen Bausteine erweitertes Postfach und Autorisierungsmodul verfügen sollte, die durch Bund und Länder genutzt werden können.

6. Der IT-Planungsrat erteilt dem Land Bremen aus seinem bestehenden Digitalisierungsbudget entsprechend der im Basiskonzept vorgelegten Kostenschätzung eine Finanzierungszusage, um innerhalb von 3 Monaten die Prüfaufträge unter Einbeziehung des Bayerischen Landesamtes für Steuern (ELSTER) im Sinne einer arbeitsteiligen Umsetzung des OZG für die Bausteine 5 und 6 zu erfüllen.

7. Vorbehaltlich eines positiven Ergebnisses der Prüfaufträge unter Ziffer 6 wird der IT-Planungsrat bei der weiteren Beauftragung der Entwicklung von selbstständig betreibbaren Bausteinen 5 und 6 die arbeitsteilige Umsetzung des OZG berücksichtigen und dem Land Bremen einen entsprechenden Auftrag erteilen.

8. Der IT-Planungsrat bittet den Bund, die dafür notwendigen dauerhaften rechtlichen Regelungen zeitnah zu schaffen.

5 Baustein 5 „OZG-PLUS-Postfach“

Auf dem Weg hin zu digitalen Verwaltungsprozessen muss es Bürgern und Organisationen in jeder Größe möglich sein, auf analoge Strecken, wie z.B. Zustellung über den Postweg, zu verzichten. Es gibt einige erfolgreiche Beispiele für die durchgehende Nutzung von elektronischen Verfahren, allen voran ist sicher der elektronische Rechtsverkehr zu nennen. Die durchgehende Nutzung dieser Verfahren lässt sich in den meisten Fällen durch entsprechende Verfahrensvorschriften erklären und dürfte der Grund dafür sein, dass elektronische Zustellverfahren i.d.R. nur innerhalb einer Fachdomäne existieren. Der fachübergreifende Ansatz „De-Mail“ konnte sich jedoch aus anderen Gründen nicht durchsetzen, die hier nicht gesondert betrachtet werden sollen.

Das Bayerische Landesamt für Steuern hat mit ELSTER und dem Ansatz des Einheitlichen Unternehmenskontos eine zentrale Fragestellung der Digitalisierung von Verwaltungsverfahren, die „elektronische Unternehmensidentifizierung“, beantwortet. In diesem Rahmen wird auch das Unternehmenspostfach angeboten, welches sicher ein erster richtiger Schritt ist, aber für die einheitliche Umsetzung eines OZG-PLUS-Postfaches für alle Fachdomänen noch nicht alle Anforderungen erfüllt. Im Folgenden werden die Anforderungen an ein solches Postfach zusammenfassend dargestellt. In den späteren Abschnitten entwerfen wir ein Postfach, das diesen Anforderungen genügen kann. Dabei betrachten wir immer auch, welche Anwendungen und Projekte des IT-Planungsrates bereits existieren und welche Empfehlungen der IT-Planungsrat herausgibt, um doppelte Entwicklungen von Standards oder Software zu vermeiden.

Um unseren Vorschlag auf Umsetzbarkeit und Nutzerfreundlichkeit hin zu prüfen, orientieren wir uns in diesem Prüfbericht an einer User Journey, die in Kapitel 5.3 beschrieben wird.

5.1 Anforderungen

5.1.1 Allgemeine Anforderungen

Berücksichtigung bestehender IT-Planungsrat-Anwendungen und -Protokolle

Die E-Government-Vorhaben des IT-Planungsrats umfassen Steuerungs- und Koordinierungsprojekte, Anwendungen sowie Maßnahmen zur Verbesserung der Rahmenbedingungen. Sie dienen als Basisbausteine zur Weiterentwicklung der bürger- und unternehmensfreundlichen digitalen Verwaltung. Auf die bestehenden Anwendungen und Projekte des IT-Planungsrats zu achten, heißt Doppelinvestitionen zu vermeiden und Zeit zu sparen, da bereits vorhandene Bausteine besser weiterentwickelt als neuentwickelt werden sollten.

Im Kontext elektronischer Nachrichten sind insbesondere die folgenden Anwendungen und Projekte des IT-Planungsrates zu berücksichtigen:

- Steuerungsprojekt „Weiterentwicklung DVDV 2.0“ (siehe auch: https://www.it-planungsrat.de/DE/Projekte/Anwendungen/DVDV_2_0/dvdv_2_0_node.html)
- Anwendung Governikus (siehe auch https://www.it-planungsrat.de/DE/Projekte/Anwendungen/Governikus/governikus_node.html)
- LeiKa Plus (siehe auch: https://www.it-planungsrat.de/DE/Projekte/Anwendungen/LeiKaPlus/leiKaPlus_node.html)
- SAFE (siehe auch https://www.it-planungsrat.de/DE/Projekte/Anwendungen/SAFE/sAFE_node.html)

- FIM (siehe auch https://www.it-planungsrat.de/DE/Projekte/Anwendungen/FIM/fim_node.html)
- XÖV Standardisierung (siehe auch: https://www.it-planungsrat.de/DE/Projekte/AbgeschlosseneProjekte/XOEV_Standardisierung/XOEV_Standardisierung_node.html)

Verwendung offener Standards

Die Architekturrichtlinie des Bundes 2019 empfiehlt die Nutzung von offenen Standards. Der Empfehlung folgend, muss der Zugang zu Postfächern durch offene Standards möglich sein. Für die Beurteilung, was als „offener Standard" gelten kann, wird die Definition der Free Software Foundation Europe („FSFE") zugrunde gelegt.

Im Sinne der Definition können die folgenden Standards eingesetzt werden, da diese ohne Restriktionen aufruf- und nutzbar sind:

- OSCI
- XTA 2
- SAML
- XACML
- IMAP
- HTTP

Ggf. werden weitere Standards vor der Umsetzung gegen die Definition der FSFE geprüft.

Die Standards „ELSTER-Transfer" und „ERiC", sofern diese als Standards zu betrachten sind, fallen *nicht* in die Kategorie „offene Standards" und sollten daher nicht vom IT-Planungsrat zur Verwendung empfohlen werden.

5.1.2 Technische Anforderungen

Der Betrieb von modernen Lösungsangeboten wird i.d.R. über verteilte Systeme gelöst. Über diesen Ansatz wird es möglich, abhängig von Lastanforderungen gezielt zu skalieren. Die technischen Komponenten müssen verteilt installierbar sein. Die in diesem Prüfauftrag beschriebene Architektur wird auch für den Betrieb in Containerumgebungen, wie z.B. Docker bzw. Kubernetes, vorbereitet sein und kann auf diese Weise unabhängig vom unterstützten Betriebssystem eines Rechenzentrums verwendet werden.

Aktualisierbarkeit, Wartbarkeit und Pflege stehen im Vordergrund des Systemdesigns. Da ein hybrides Betriebsmodell, also zentrale und dezentrale Komponenten, angestrebt wird, sind diese Aspekte von besonderer Bedeutung.

Das Systemdesign muss aufgrund der zu erwartenden Last gut zu skalieren sein und ausfallsicher betrieben werden können. Bei Schnittstellen ist der konsequente Einsatz von offenen und etablierten Standards erforderlich. Grundlegende Anforderungen an das System, wie zum Beispiel 3-Tier-Architektur und die Berücksichtigung der im IT-Grundschutz vorgeschlagenen Maßnahmen, sind selbstverständlich.

5.1.3 Fachliche Anforderungen

In Rahmen dieses Prüfauftrags wird die strukturierte, antragsbezogene Kommunikation zwischen Unternehmen bzw. Organisationen und Verwaltung betrachtet.

Mit dem elektronischen Emissionshandel, bei dem die von Anlagenbetreibern begutachteten CO_2-Emissionswerte elektronisch an die DEHSt übermittelt werden müssen, wurde eines der ersten Verfahren etabliert, das auf vollständig elektronische Umsetzung der Business-to-

Government-Kommunikation[4] setzt. Seit 2005 sind viele weitere elektronische Kommunikationsszenarien dazugekommen. Sowohl die Anforderungen als auch die Erwartungshaltung der Stakeholder an Kommunikationsinfrastrukturen sind enorm gewachsen.

Die Anforderungen lassen sich grob in die drei Bereiche „*Gesamtsystem*“, „*Empfangsmodul*“ und „*Sendemodul*“ untergliedern.

Für das *Gesamtsystem* lassen sich die Anforderungen wie folgt zusammenfassen:

- Strukturierte Daten übermitteln/Abgrenzung: es geht nicht um unstrukturierte Kommunikation
- Große und kleine Unternehmen berücksichtigen
- Statusbenachrichtigungen
- Offene, etablierte Standards berücksichtigen
- Sicherheit im Design
  - Sichere-Sender-Identifikation (Bedarf an sicheren Verzeichnisdiensten)
  - Sichere-Empfänger-Identifikation (ELSTER-ID)
  - starke Vertraulichkeit ermöglichen (Verschlüsselung)
  - starker Integritätsschutz
  - Ausfallsicherheit
  - Nachvollziehbarkeit/Nachweisbarkeit/Quittungsmechanismen
- Rechtsverbindliche Zustellung ermöglichen

Das *Empfangsmodul* ist der Einstiegspunkt für das Unternehmen bzw. die Organisation. Neben dem besonderen Augenmerk auf Benutzerfreundlichkeit werden die folgenden Anforderungen gestellt:

- Unternehmen müssen die Möglichkeit erhalten, den Zugriff ihrer Mitarbeiter auf Postfächer zu steuern.
- Vertretungsregelung, d.h. über einen bestimmten Zeitraum hinweg kann ein Mitarbeiter im Auftrag eines anderen handeln. Die Einrichtung einer Vertretungsregelung erfolgt über einen dazu berechtigten Administrator.
- Funktionspostfächer, d.h. eine bestimmte Gruppe von Mitarbeitern eines Unternehmens, bspw. der Betriebsrat, kann adressiert werden. Nur die Mitarbeiter, die dieser Gruppe zugeordnet sind, können die entsprechenden Nachrichten lesen.
- Im Konzept muss berücksichtigt werden, dass Mitarbeiter ungeplant aus einer Organisation ausscheiden können. In diesen Fällen müssen Maßnahmen ergriffen werden können, um auf entsprechende Nachrichten zuzugreifen.
- Urlaubsvertretung, d.h. über einen bestimmten Zeitraum hinweg kann ein Mitarbeiter im Auftrag eines anderen Mitarbeiters (Kollegen) handeln. Die Einrichtung einer Urlaubsvertretung erfolgt durch den zu Vertretenden („Urlaubsübergabe“).
- Poststellenfunktion/Fachsoftware-Anbindung
- Unterstützung von Vertrauensniveaus

[4] https://www.it-planungsrat.de/SharedDocs/Downloads/DE/Projekte/Anlagen_Blaupause/Anlage_A14_Anwendungen_auf_Basis_OSCI.pdf

Für das *Sendemodul* lassen sich die Anforderungen wie folgt zusammenfassen:

- Unterstützung von verschiedenen Transportinfrastrukturen
- Einfache Anbindung
- Repository für Fachdomänen und gekoppelte Transportwege

5.1.4 Sicherheitsanforderungen

Insbesondere die Vertraulichkeit und die Integrität der Nachrichten sind durch das System zu gewährleisten. Dabei muss auch beachtet werden, dass eventuell nicht einmal der Betreiber selbst Kenntnis von Nachrichteninhalten erlangen darf.

Deswegen sind bereits zur Designphase Maßnahmen zu analysieren, die die Sicherheitsanforderungen umsetzen. Das System wird also die Grundsätze „Security by Design“ und „Privacy by Design“ berücksichtigen. Im Kontext elektronischer Nachrichten können diese nur auf Basis von kryptografischen Konzepten umgesetzt werden. Rein organisatorische Maßnahmen sind i.d.R. zu schwach und deswegen ungeeignet, Schutzziele konsequent durchzusetzen.

Die Vertraulichkeit der Daten einerseits und die Anforderung an Funktions- und Gruppenpostfächer andererseits müssen auf einem Kryptokonzept basieren. Vor allem dürfen die Benutzer nicht dazu verleitet werden, Schlüsselmaterial zu teilen, um so fehlende Funktionen des Systems zu kompensieren.

Um zum Beispiel Vertreterregeln auch kryptografisch umzusetzen, werden sogenannte *Proxy re-encryption Schemes* eingesetzt, die es erlauben, einen für eine Person A verschlüsselten Text so für Person B umzuschlüsseln, dass der Proxy (also die Institution, die die Umschlüsselung vornimmt) keine Information über den unverschlüsselten Text erhält. Auch für die Anforderung, dass mehrere Personen einen Geheimtext entschlüsseln können, ohne sich einen gemeinsamen geheimen Schlüssel zu teilen, gibt es Lösungen. Um dies effizient umzusetzen, kann auf sogenannte *Attribute-based encryption Schemes* zurückgegriffen werden.

„Für die beschriebenen Funktionalitäten existieren bereits etablierte kryptographische Verfahren, deren Sicherheit mathematisch nachgewiesen ist und die bereits in Kryptobibliotheken implementiert wurden, so dass eine einfache Umsetzung ermöglicht wird.“, erläutert Herr Prof. Dr. Marian Margraf vom Institute of Computer Science der Freien Universität Berlin auf Rückfrage durch Governikus.

Das zwingend erforderliche Kryptosystem / Schlüsselmanagement wird die folgenden Anforderungen berücksichtigen:

- Die Benutzer des Systems sind keine Techniker, man darf keine technischen Kenntnisse voraussetzen.
- Es sollen größtenteils Systeme verwendet werden, die bereits vorhanden sind. Konkret: Es sind Sicherheitsfunktionen der Endgeräte zu nutzen. Der Besitz oder die Benutzung von Kartenlesern oder Karten ist keine Voraussetzung.
- „Ende-zu-Ende“-Sicherheit - wobei die Enden nicht immer natürliche Personen sind, sondern auch Institutionen oder Systeme sein können.
- PKI-basiert
- Vertreterregelung ermöglichen
- Gruppenfunktion, d.h. eine Gruppe von Menschen kann einen Ciphertext entschlüsseln, die Gruppe teilt sich aber keinen gemeinsamen privaten Schlüssel
- Nutzer können mehrere Geräte nutzen, sollten aber mittels ELSTER-ID nur einmal identifiziert werden müssen.

5.2 Annahmen / Entwurfsentscheidungen

Wir gehen in diesem Entwurf von einem Kommunikationsschema aus, das aus vier Schritten bzw. Strecken besteht (siehe Abb. 1). Die Kommunikationsinitiierung erfolgt dabei durch die Organisation durch Aufruf einer digitalen Verwaltungsleistung (Strecke #1). Wir gehen weiter davon aus, dass über den Rückkanal Nachrichten, z.B. Bescheide, elektronisch an das Sendemodul übermittelt werden (Strecke #2). Anders als bei ELSTER, erfolgt diese Übermittlung nach offenen Standards und berücksichtigt dabei bereits vorhandene Szenarien und bestehende Infrastrukturen. Als notwendigen dritten Schritt (Strecke #3) sehen wir eine Übermittlung der Nachricht durch das Sendemodul an das Empfangsmodul vor. Auch hierbei werden wieder offene Standards eingesetzt (OSCI, ggf. AS4). Die Zustellung der Nachricht an den Empfänger (Strecke #4) erfolgt in Schritt vier.

Der Empfänger einer Nachricht ist die Organisation, die im Fall eines Unternehmens durch eine beliebige Anzahl von Mitarbeitern vertreten werden kann. Hier sehen wir das Erfordernis, neben einer Vertretungsregelung auch die Berechtigungen und Weiterleitungsmöglichkeiten für Gruppen- und Funktionspostfächer zu implementieren. Die Funktionen des OZG-PLUS Postfachs sollten nicht hinter den im Unternehmen etablierten E-Mail-Möglichkeiten zurückbleiben. Die Vertretungsregelung erfolgt über die Anbindung des Moduls 6 (Autorisierungsmodul).

Die Postfachfunktion kann mittels Status- und Benachrichtigungsfunktionen über den Zustand eines Verfahrens informieren. Die eigentliche Bearbeitung eines Vorgangs bleibt aber immer Sache der digitalen Verwaltungsleistung. Dementsprechend werden Ergänzungen durch den Antragsteller über die Strecke #1 (Kommunikationsinitiierung) an die Verwaltung übermittelt. Perspektivisch ist zu prüfen, ob es möglich sein soll, aus dem Postfachdienst die Kommunikation für einen laufenden Vorgang zu führen. Dann müsste die Verwaltungsleistung ebenfalls über ein Postfach verfügen und die Nachrichtentypen wären entsprechend zu erweitern.

Unter Organisationen verstehen wir in diesem Entwurf zunächst juristische Personen, also Unternehmen, Vereine und Behörden.

Die hier getroffenen Annahmen weichen bewusst nicht von dem vom Bayerischen Landesamt für Steuern skizzierten Szenario ab, um die Anforderungen an das OZG-PLUS-Postfach und dessen einheitliche Umsetzung herauszustellen.

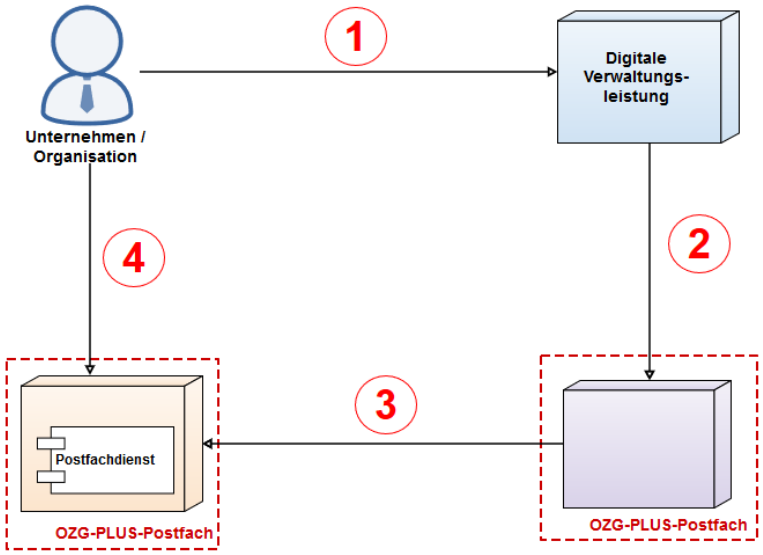

Abbildung 2: Kommunikationsschema

5.2.1 Rollen und Akteure

Im Postfachsystem sind die folgenden Akteure zu berücksichtigen:

- *Digitale Verwaltungsleistung*
  Dieser Akteur steht für die Anforderungen, die seitens einer digitalen Verwaltungsleistung auftreten können. Es handelt sich also um die Belange des Betriebs seitens der Verwaltung, sowie die sich daraus ergebenden Anforderungen aus Datenschutz- und Compliance Aspekten.
- *Unternehmen/Organisation*
  Das Unternehmen/die Organisation nimmt eine digitale Verwaltungsleistung in Anspruch, will elektronisch adressierbar sein und komfortablen Zugriff auf die elektronischen Nachrichten haben. „Komfortabel“ hängt in dem Fall von mehreren Faktoren ab. Wir sehen die beiden Anforderungen, dass auf das System sowohl per Fachsoftware als auch mittels Web-Oberfläche zugegriffen werden soll.
- *Hersteller von Verwaltungssoftware*
  Hersteller von Verwaltungssoftware sind diejenigen, die die Postfachdienste anbinden müssen. Insbesondere ist es für diese Gruppe wichtig, offene und gut dokumentierte Standards nutzen zu können. Auch ist die Verfügbarkeit von Beispielen und Bibliotheken für die Hersteller essenziell. Stabilität und Governance der Schnittstellen spielen für Softwarehersteller eine entscheidende Rolle.
- *Behördliche Stellen*
  Dieser Akteur steht für die IT-Entscheider und Architekten. Die Gruppe muss besonders gut informiert und unterstützt werden, um eine hohe Akzeptanz des Gesamtsystems zu erreichen.
- *Betreiber von Infrastrukturen, Betreiber bereits etablierter Kommunikationssysteme*
  Wie bereits an verschiedenen Stellen ausgeführt, ist es absolut erforderlich, bestehende Systeme zu betrachten und zu analysieren, welche Anforderungen über diese Gruppe eingebracht werden. Das Ziel eines einheitlichen Systems in der Business to Government-Kommunikation ist nur durch Umsetzung dieser Anforderungen zu erreichen. Übergangsweise müssen leichtgewichtige Brücken in die Kommunikationsszenarien gebaut werden, um wenigstens alle fachlichen Domänen bedienen zu können.

5.2.2 Mengengerüst

Bereits heute, mit in Teilen erfolgter Umsetzung des OZG, werden jährlich große Mengen an Nachrichten elektronisch zwischen Unternehmen und Behörden ausgetauscht. Geht man davon aus, dass in den kommenden Jahren entsprechend dem OZG-Katalog eine große Anzahl an weiteren Verwaltungsleistungen digitalisiert werden soll, so ist mit einer weiter steigenden Zahl von Transaktionen zu rechnen. Die nachstehenden beiden Abbildungen unterstreichen die Anforderung an die Skalierbarkeit des Systems.

Zwar können die Transaktionszahlen zwischen Verwaltungsleistungen stark variieren, aber in Summe müssen sowohl steigende als auch konstant hoch bleibende Transaktionszahlen abgewickelt werden können.

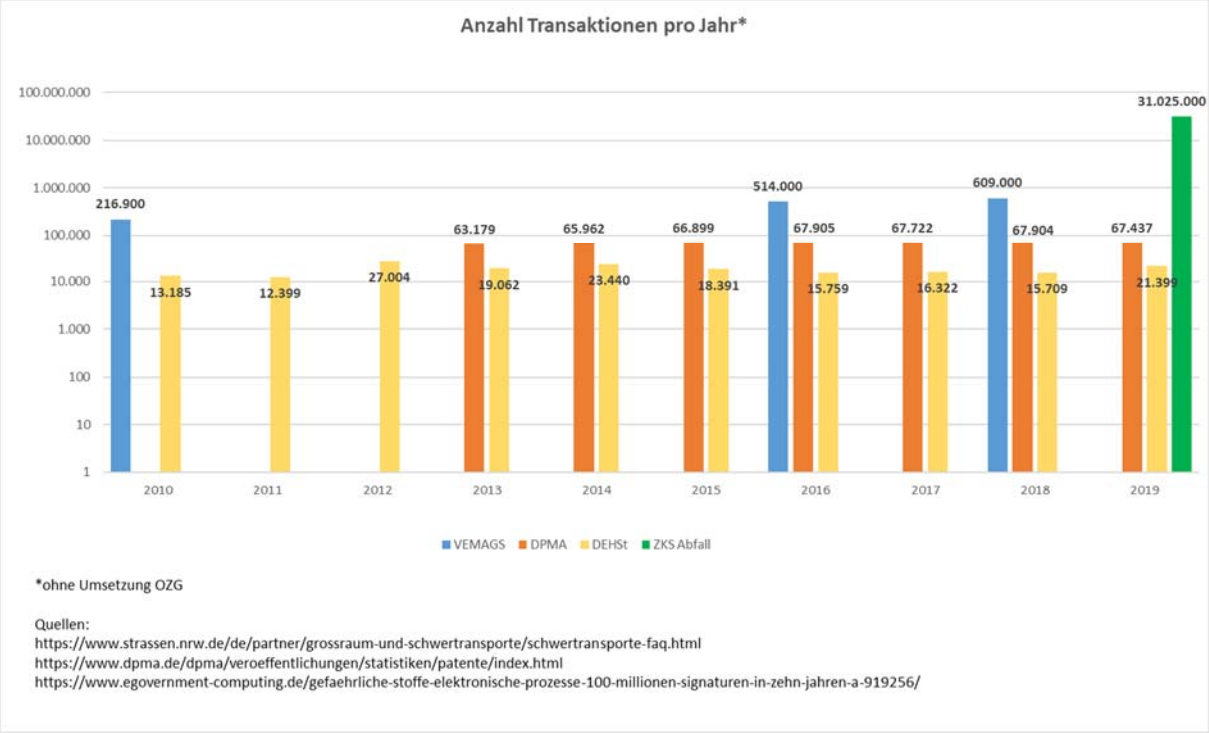

Abbildung 3: Transaktionszahlen ausgewählter Verwaltungsleistungen

Mit weiterer Umsetzung des OZG werden fast 3,5 Millionen Unternehmen digitale Verwaltungsleistungen nutzen können. Die dabei zu erwartenden Transaktionszahlen werden nicht nur durch die großen Unternehmen mit zahlreichen Mitarbeitern beeinflusst, sondern vor allem auch durch die große Anzahl an klein- und mittelständischen Unternehmen, wie Abbildung 4 veranschaulicht.

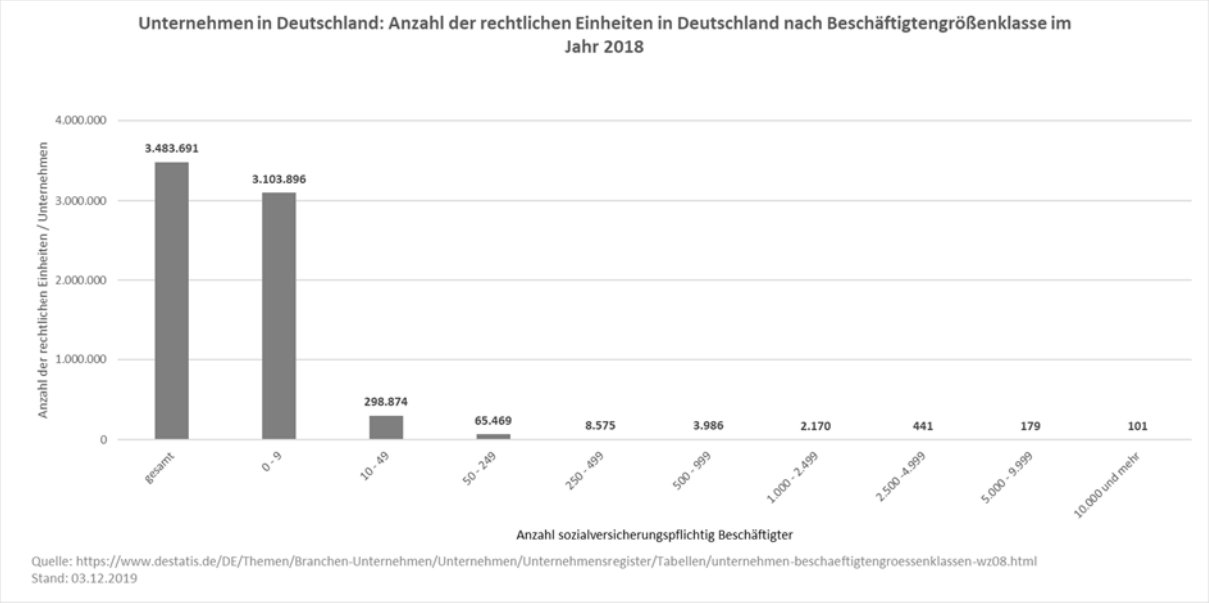

Abbildung 4: Anzahl der Unternehmen in Deutschland

Im Interesse der Akzeptanz für diese Verwaltungsleistungen erscheint es unbedingt ratsam, die dabei verwendeten Technologien, Protokolle, Datenbanken und Hardwarekomponenten so zu wählen, dass das von den Systemen zu bewältigende Transaktionsvolumen (Anzahlen von Benutzern, Empfängersystemen und Nachrichten sowie die durchschnittliche Größe der einzelnen Nachrichten) skalierbar und hochverfügbar ist. Aufgrund der zu erwartenden Lastzahlen ist ein dezentraler Betrieb zu empfehlen.

VEMAGS

Über das Elektronische Verfahrensmanagement Großraum- und Schwertransporte (VEMAGS) wurden in den ersten 5 Jahren bereits 1 Million Anträge gestellt. Diese Zahl hat sich in den folgenden 5 Jahren noch einmal verdoppelt, so dass nach 10 Jahren der elektronischen Antragsstellung über 3 Millionen Anträge über das System abgewickelt wurden. Aus den vorliegenden Zahlen ergibt sich im Schnitt ein jährliches Antragsvolumen von 450.000 Stück. Es handelt sich jedoch nur um einen einfachen Mittelwert; in 2018 stieg die Zahl der Anträge auf über 600.000 an.

DPMA

Seit 2013 können Patente beim Deutschen Patent- und Markenamt (DPMA) elektronisch angemeldet werden. Im Schnitt werden jährlich rund 66.000 Anträge gestellt.

DEHSt

Seit dem Start des elektronischen Emissionshandels im Jahr 2010 liegt die jährliche Nachrichtenanzahl konstant bei rund 18.000. Die vergleichsweise geringe Zahl an Transaktionen sollte nicht darüber hinwegtäuschen, dass von knapp 1.900 Unternehmen pro Jahr damit im Schnitt 500 Millionen Euro erzielt werden.

ZKS Abfall

Mit aktuell täglich 85.000 abzuwickelnden Dokumenten gehört die Entsorgung von gefährlichen Abfällen über das Portal ZKS Abfall zu den transaktionsstarken Anwendungen. Die Anmeldung kann bereits seit dem 1. April 2010 elektronisch erfolgen und wurde am 1. Februar 2011 verpflichtend für alle am Prozess Beteiligten eingeführt. In den ersten 10 Jahren sind dabei über 100 Millionen Transaktionen abgewickelt worden.

5.3 User Journey: Zustimmung zur Kündigung schwerbehinderter Menschen

Der nachstehend beschriebene Anwendungsfall ist dem Themenbereich „Unternehmensführung und -entwicklung“ und da speziell der Geschäftslage „Arbeitgeber sein“ des OZG-Umsetzungskatalogs entnommen und wird exemplarisch als User Journey in diesem Prüfbericht verwendet.

Für die Darstellung der User Journey gehen wir von folgenden Annahmen aus: Die digitale Verwaltungsleistung ist vollständig elektronisch abbildbar und erfordert neben einer Anmeldung mit einem Organisationskonto auch eine Autorisierung. Die Zustellung an private Postfächer ist Gegenstand eines gesonderten Projektes zur Interoperabilität von Servicekonten und soll in diesem Dokument nicht detailliert betrachtet werden. Für die User Journey bedeutet das, dass wir die Zustellung an eine private Person als gelöst betrachten.

Anwendungsfall

Anton hat einen mittelständischen Betrieb mit mehreren Fertigungsanlagen und beschäftigt in seinem Unternehmen mehrere schwerbehinderte Personen. Aus wirtschaftlichen Gründen muss er die Hälfte seiner Fertigungsanlagen außer Betrieb setzen und entsprechend Personal entlassen. Davon ist auch der schwerbehinderte Mitarbeiter *Dieter* betroffen. *Anton* muss vor der Kündigung von *Dieter* einen Antrag auf Zustimmung zur Kündigung eines schwerbehinderten Arbeitsnehmers beim zuständigen Integrationsamt in Celle stellen. *Anton* beauftragt seine Mitarbeiterin *Hilde* aus dem Personalbüro mit der Antragstellung. *Hilde* ruft die Internetseite des Integrationsamtes auf, füllt den Antrag im Servicebereich elektronisch aus und übermittelt ihn an das Integrationsamt zur Feststellung.

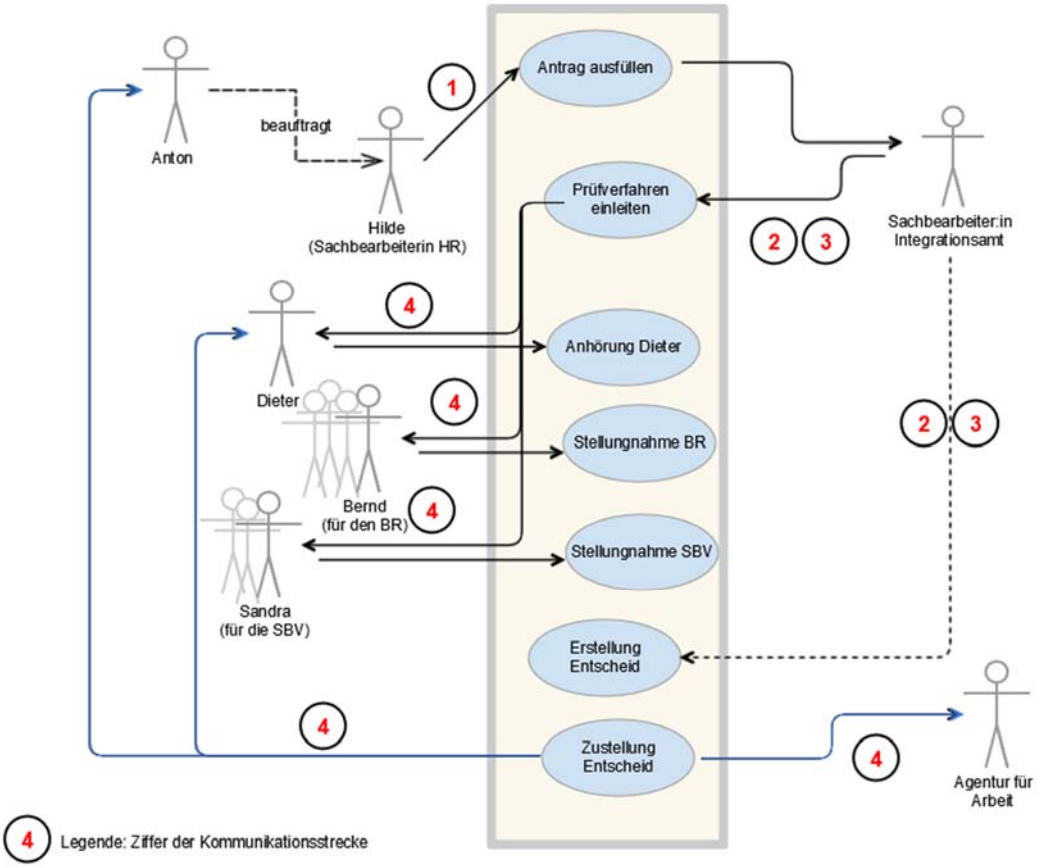

Abbildung 5: User Journey im Anwendungsfall „Kündigung schwerbehinderter Menschen“

Zur Feststellung hört das Integrationsamt den schwerbehinderten Arbeitnehmer *Dieter* an, indem es ihm einen Fragebogen in sein Postfach zustellt. Außerdem sind Stellungnahmen des Betriebsrats (BR) und der Schwerbehindertenvertretung (SBV) aus *Antons* Firma erforderlich. Deshalb stellt das Integrationsamt zum einen eine entsprechende Nachricht in das Funktionspostfach des BR, die von *Bernd* in seiner Rolle als ein Mitglied des BR abgeholt wird. Zum anderen wird vom Integrationsamt eine weitere Nachricht in das Funktionspostfach der SBV gestellt, die dort von *Sandra* in ihrer Rolle als ein Mitglied der SBV abgeholt wird.

Nachdem das Integrationsamt die Rückmeldungen von *Dieter*, *Bernd* und *Sandra* erhalten hat, wird über den Antrag zur Zustimmung zur Kündigung von *Dieter* entschieden.

Der Entscheid wird in elektronischer Form an *Anton* und *Dieter* übermittelt; die Agentur für Arbeit wird ebenfalls vom Integrationsamt informiert.

5.4 Funktionalitäten

Die folgende Grafik gibt einen Überblick über das vorgeschlagene OZG-PLUS-Postfach-System.

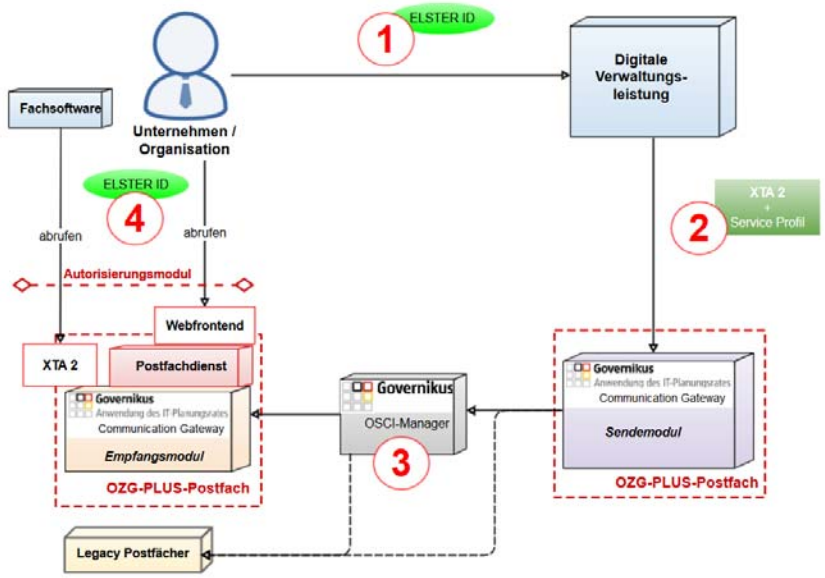

Abbildung 6: Schema OZG-PLUS-Postfach

Die vorgeschlagene Lösung besteht aus etablierten Standards und vorhandenen Bestandteilen aus den Projekten und Anwendungen des IT-Planungsrats. Das System besteht im Wesentlichen aus den (Sub)Modulen „Sende-/Empfangsmodul“ und „Postfachdienst“, die bezogen auf ihren Funktionsumfang im Folgenden kurz beschrieben werden.

5.4.1 Sende-/Empfangsmodul

Sende- und Empfangsmodul werden über das Protokoll XTA 2 angesprochen. XTA 2 ist dabei bewusst so konzipiert, dass es unabhängig vom Nachrichteninhalt den Nachrichtentransport übernehmen kann. Das Sendemodul nimmt einen Transportauftrag von der digitalen Verwaltungsleistung entgegen. Die digitale Verwaltungsleistung markiert den Transportauftrag mit weiteren Metadaten, die für die Zustellung erforderlich sind. XTA 2 sieht vor, dass Service Profile existieren, die die für bestimmte Szenarien benötigten Metadaten und Verarbeitungsregeln definieren. Für das OZG-PLUS-Postfach muss mindestens ein Service Profil erstellt werden. Die Rollen in diesem Szenario sind wie folgt:

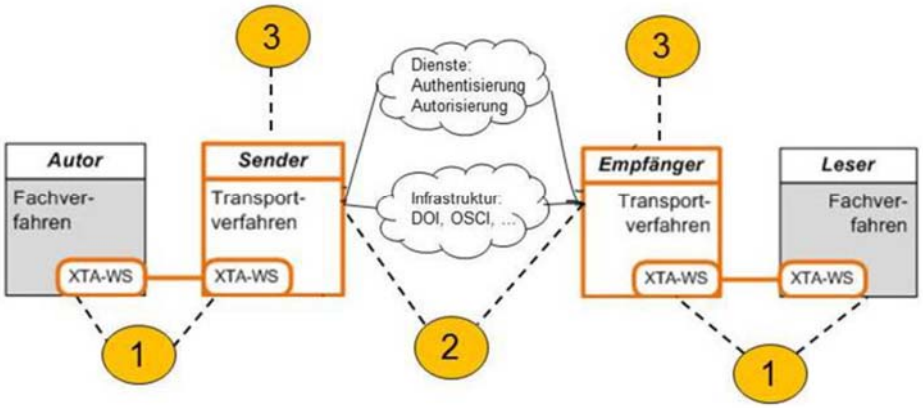

Abbildung 7: Infrastruktur der Nachrichtenübermittlung aus XTA Spezifikation

- Autor: Digitale Verwaltungsleistung
- Leser: Unternehmen
- Sender: Sendemodul
- Empfänger: Empfangsmodul

Insbesondere ist im Standard XTA das Instrument von Quittungen vorgesehen. „Durch Quittungen soll der Sender in die Lage versetzt werden, Auskunft über Ereignisse geben zu können, an denen er nicht notwendigerweise direkt beteiligt ist. Gedacht ist hier an die Ereignisse bei der Abarbeitung eines Transportauftrags innerhalb der entsprechenden Transportinfrastruktur. Für den Auftraggeber eines Transports ist in vielen Fällen diese Auskunftsfähigkeit seines Transport-Dienstleisters von großer Wichtigkeit.“[5] Das Sendemodul unterstützt nur den asynchronen Versand von Nachrichten.

Das Modul 5 kann hier zu wesentlichen Teilen durch bestehende Infrastrukturkomponenten und Standards umgesetzt werden.

5.4.2 Postfachdienst

Funktionspostfächer können durch den Administrator an die spezifischen Gegebenheiten im Unternehmen angepasst angelegt werden. In unserem Anwendungsfall wären das z.B. ein Postfach für den Betriebsrat, die Schwerbehindertenvertretung und die Personalabteilung. Diese Funktionspostfächer können durch die digitale Verwaltungsleistung direkt adressiert werden. Die „Adressen“ dieser Postfächer können z.B. im Rahmen eines Formulars abgefragt werden.

Auch Mitarbeiterpostfächer können durch einen Administrator angelegt werden. Diese Postfächer werden ebenfalls direkt durch die digitale Verwaltungsleistung adressiert. Die Adresse des Postfachs kann im Zuge der Authentifizierung bei der Antragsstellung übermittelt werden oder auch durch Abfrage in einem Formular. Für Mitarbeiterpostfächer gibt es eine Vertreterregelung, die durch einen Administrator freigeschaltet wird.

Der Postfachdienst bedient sich im Hintergrund des Empfangsmoduls; die Bereitstellung an Fachsoftware erfolgt über XTA 2-Aufrufe. Die Darstellung als Web-UI muss allerdings erstellt werden. Dabei wird sich die Ansicht des Postfachdienstes an den Darstellungen bekannter Web-Mail-Software orientieren, das entspricht den Nutzererwartungen.

[5] Spezifikation XTA 2 (Version 3)

Das nachfolgende Beispielbild zeigt einen intuitiven Ansatz für die Darstellung eines Postfaches.

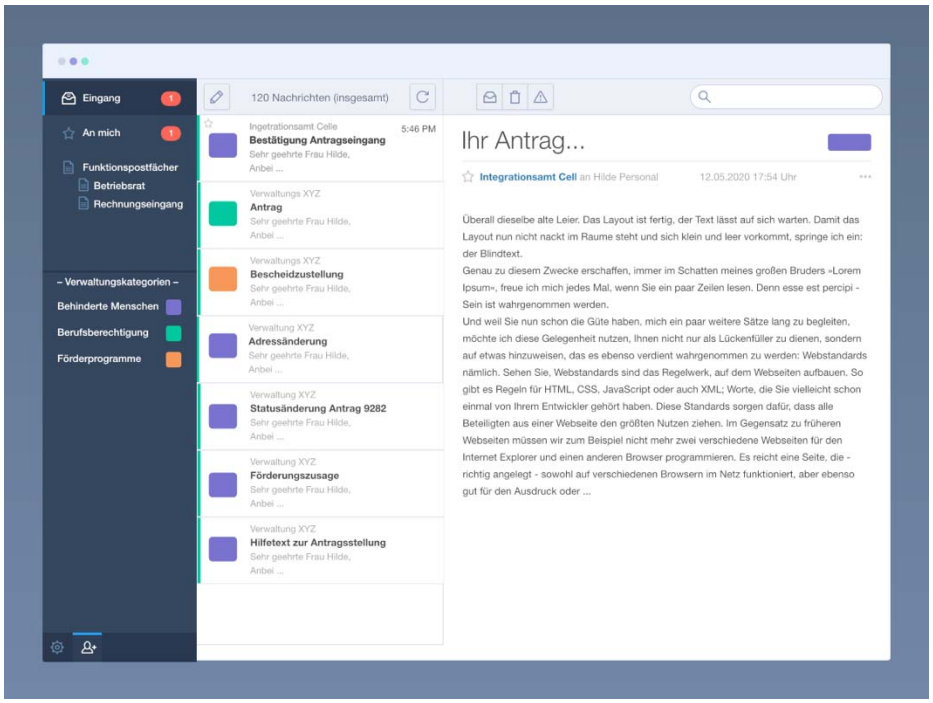

Abbildung 8: Beispiel Postfach

Insbesondere kann der Benutzer in der Oberfläche die Ordner sehen, auf die er Zugriff hat. Die Ordner sind eine Darstellung, die Benutzer aus anderer Software kennen, sie sind aber nur ein visuelles Mittel, Nachrichten anhand von bestimmten Kriterien zu gruppieren. Wir sehen die drei folgenden Gruppen, diese Liste ist noch nicht abschließend:

- *Gruppe „Meine Nachrichten“*
  In dieser Gruppe sind alle Nachrichten, die an diesen Mitarbeiter direkt gingen.
- *Gruppe „Meine Funktionspostfächer/Vertretungen“*
  In dieser Gruppe werden alle Nachrichten in entsprechenden Ordnern angezeigt, die entweder zu einem zugeordneten Funktionspostfach gehören oder die dem jeweiligen Mitarbeiter vertretungsweise zugeordnet sind.
- *Gruppe „Verwaltungskategorien“*
  Wir sehen vor, dass jede digitale Verwaltungsleistung beim Versenden einer Nachricht diese mit der eigenen LeiKa-Leistungsgruppe markiert. Auf diese Weise können die Nachrichten entsprechend der Verwaltungskategorie in unserer User Journey „Behinderte Menschen“ gefiltert werden. Diese Gruppierungen können ggf. als Berechtigung vergeben werden.

Neben den oben beschriebenen Funktionen zur Nachrichtenverwaltung werden im Postfachdienst Einstellungen angeboten. Diese unterscheiden sich in „persönliche Einstellungen“ und „Systemeinstellungen“.

In den persönlichen Einstellungen kann der Benutzer unter anderem

- Urlaubsvertretungen eintragen,
- Benachrichtigungsfunktionen einstellen,
- Regeln einstellen zur spezifischen Weiterleitung.

Diese Funktionen sind im Wesentlichen aus dem Umgang mit E-Mails bekannt und erleichtern den Einstieg.

Zum Bereich für „Systemeinstellungen“ haben nur Mitarbeiter Zugang, die über entsprechende Berechtigungen verfügen. Dort können Einstellungen vorgenommen werden, die systemweit Geltung haben. Insbesondere können hier Verbindungsparameter eingestellt werden, wenn eine eigene Infrastruktur betrieben wird.

5.4.3 Zukünftige Ausbaustufen

Die Systeme sollten sich anhand von Anwenderbedürfnissen weiterentwickeln. Wir gehen davon aus, dass, sobald der einseitige Kanal zum Unternehmen/zur Organisation etabliert ist, der Bedarf an Antwortmöglichkeiten entsteht. Es sollte dann eine benutzerfreundliche Kommunikation der Unternehmen mit der Verwaltung ermöglicht werden (z.B. für die Nachlieferung von Nachweisen bzw. Dokumenten).

Dabei wären insbesondere die folgenden Anforderungen zu betrachten:

- Die Unternehmen müssen die Möglichkeit erhalten, rechtsverbindlich und sicher digital mit der Verwaltung über das einheitliche Postfach zu kommunizieren.
- Die Unternehmen müssen die Möglichkeit erhalten, per Uploadfunktion Anhänge an die Verwaltung zu senden.

5.5 Technische Umsetzung

Das in Abbildung 6 dargestellte Schema zeigt die Komponenten und Kommunikationsstrecken, die im Workflow mit dem OZG-PLUS-Postfach zum Einsatz kommen und nachfolgend beschrieben werden.

5.5.1 Anbindung Verzeichnisdienste

Vor dem Versand einer Nachricht muss vom Sendemodul die Adresse des zuständigen Postfachs ermittelt werden. Dazu wird auf einen Verzeichnisdienst zugegriffen, in dessen Datenbank alle infrage kommenden Empfänger-Postfächer inklusive der Zugriffsdaten (z.B. URL, Verschlüsselungszertifikate, weitere Meta-Daten, wie ggf. ELSTER-ID) verzeichnet sind.

Eine mögliche Lösung wäre die Nutzung des etablierten und föderal betriebenen Deutschen Verwaltungsdiensteverzeichnisses (DVDV). Momentan werden im DVDV lediglich Dienstleistungen der öffentlichen Verwaltung gelistet, hier müsste eine Anpassung bzw. Erweiterung um Adressdaten der Organisationen durchgeführt werden.

5.5.2 Strecke #1 Organisation => digitale Verwaltungsleistung

Unternehmen bzw. Mitarbeiter von Unternehmen authentifizieren sich an einem zentralen ELSTER-Identifizierungsdienst (z.B. per Zertifikat, Stick, Personalausweis usw.) und nehmen die Kommunikation mit einem Online-Portal der Verwaltung auf, über welches sie eine digitale Verwaltungsleistung beantragen. Die ELSTER-ID dient dazu, vorhandene Infrastrukturen, wie Servicekonten, Portale oder Behördenkonten, miteinander zu verknüpfen und weiterverwenden zu können.

Die von ELSTER für Organisationen ausgegebenen Zertifikate werden gleichermaßen für die Authentisierung als auch die Verschlüsselung der übermittelten Daten verwendet. Die ELSTER-ID könnte daher nicht nur als zertifikatsbasiertes Authentisierungsmittel auf Strecke #1 bei der Beantragung einer digitalen Verwaltungsleistung genutzt werden, sondern auch zur Verschlüsselung der Rückgabedaten auf der Strecke #4 zwischen dem Empfangsmodul des OZG-PLUS-Postfachs und der Organisation.

5.5.3 Strecke #2 digitale Verwaltungsleistung => Sendemodul

Das Portal, auf dem die Digitale Dienstleistung beantragt wurde, übermittelt seine Nachrichten (Bescheide, Rückfrage usw.) ggf. direkt in einem maschinenlesbaren Format an das Sendemodul des OZG-PLUS-Postfachs. Hierfür wird XTA 2 als Schnittstelle zwischen Fach- und Transportverfahren eingesetzt.

XTA 2 standardisiert die elektronische Übermittlung von Daten im E-Government durch zwei Ansätze auf unterschiedlichen Ebenen:

Durch das Modul der Service Profile werden die Anforderungen an Datenschutz und Datensicherheit, z.B. bzgl. der Integrität oder Authentizität, für einen Transport definiert und damit einheitlich konfiguriert (siehe Abbildung 9).

Durch das Modul des XTA-Webservice (XTA-WS) wird die Übermittlung von Daten, also der Transport selbst, standardisiert: Durch die Spezifikation von Webservices wird die Vereinheitlichung der Schnittstellen zwischen digitaler Verwaltungsleistung und Transportverfahren (auch innerhalb eines Landes und Rechenzentrums) erreicht. Die öffentliche Verwaltung hat so die Möglichkeit der funktionalen Steuerung (siehe Abbildung 9).

Die beiden Module „Service Profile“ und „XTA-WS“ beziehen sich konzeptionell stark aufeinander, es ist aber dennoch möglich, sie unabhängig voneinander einzusetzen.

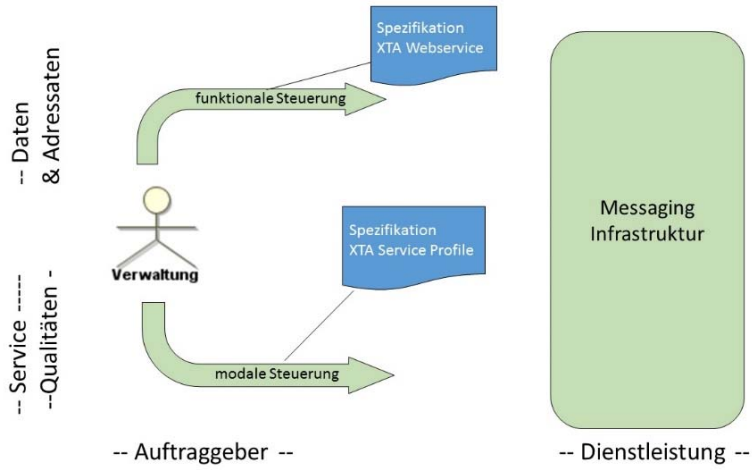

Abbildung 9: Die zwei Dimensionen der Steuerung der IT-Dienstleistung

In der *MessageMetaData* befinden sich Informationen, wie z.B. die Leistungsgruppe aus dem LeiKa-Katalog einer digitalen Verwaltungsleistung; in unserer User Journey wäre das „Behinderte Menschen“. Zusätzlich werden dort noch Aktenzeichen, ausstellende Behörde und weitere noch zu definierende Informationen eingetragen. Über den internen Kanal wird die Nachricht an das Governikus Communication Gateway (GCG), das Sendemodul, per XTA-WS übergeben.

Das GCG übernimmt dann für die digitale Verwaltungsleistung die Transportaufgaben, wie beispielsweise den Aufbau der Containerstruktur, die technische Adressierung, die Transportverschlüsselung und die Transportsignatur.

5.5.4 Strecke #3 Sendemodul => Empfangsmodul

Auf der Strecke #3 zwischen Sende- und Empfangsmodul erfolgt eine asynchrone Kommunikation, d.h. das Empfangsmodul holt die Nachrichten aus dem OSCI-Manager. Über den externen Kanal wird die Kommunikation zwischen GCG und OSCI-Manager über OSCI-Transport durchgeführt. Der OSCI-Manager übernimmt den gesicherten Transport der Nachricht an das Empfangsmodul, das wiederum ein GCG ist.

Im europäischen Rahmen wird AS4 als Transportprotokoll für eDelivery eingesetzt. AS4 könnte alternativ als Transportprotokoll auf der Strecke #3 eingesetzt werden. Governikus ist an der Entwicklung von Access Points für das GCG und AS4 Transport involviert und beobachtet die Entwicklung engmaschig. Daher ist es in unserer Lösung möglich, alternativ bzw. zu einem späteren Zeitpunkt auch AS4 Transport zu implementieren. Noch ist AS4 allerdings nicht so weit entwickelt wie OSCI und in Deutschland auch noch nicht so etabliert, daher präferieren wir OSCI für den Transport auf Strecke #3.

5.5.5 Strecke #4 Empfangsmodul => Organisation

Das GCG im Empfangsmodul dient als temporärer Speicher der Nachrichten, die entweder automatisch vom Postfachdienst übernommen oder direkt über XTA 2 von einer Fachsoftware der jeweiligen Organisation abgeholt werden.

Der Postfachdienst ist eine Datensenke, in der alle Nachrichten für Organisationen gespeichert werden. Es gibt pro Organisation nur einen Postfachdienst.

5.5.5.1 Webfrontend

Eine Subkomponente innerhalb der Empfangsmoduls ist das Webfrontend, welches den Zugriff auf den Postfachdienst über einen Browser ermöglicht. Es zeigt den vom Autorisierungsmodul zugelassenen Nutzern die empfangenen Nachrichten an.

Über das Webfrontend können Standardfunktionen ermöglicht werden, z.B. Auflisten von Nachrichten, Lesen, Löschen, Betrachten und Herunterladen von Dateien, also Funktionen, die von einem herkömmlichen E-Mail-Postfach bekannt sind. In einem späteren Ausbauschritt wird auch eine Antwortfunktion integriert.

Idealerweise gibt es hier eine Schnittstelle für die Integration in Mein UP. Entweder greift diese direkt auf das Postfach zu oder es gibt Templates, die in Mein UP integriert werden können.

5.5.5.2 Postfächer

Jede durch eine digitale Verwaltungsleistung versendete Nachricht gibt auch automatisch eine Absenderkategorie mit. Diese Kategorie entspricht den Leistungsgruppen aus dem LeiKa-Katalog. In unserem Anwendungsbeispiel wäre das z.B. „Behinderte Menschen“. Diese Absenderkategorie kann optional für die Autorisierungsentscheidung herangezogen werden und sollte für eine Sortierung bei der Auflistung obligatorisch verwendet werden.

Die Absenderkategorie wird den Nachrichten über die *MessageMetaData* des XTA 2-Protokolls aus der digitalen Verwaltungsleistung mitgegeben.

Die Postfächer sind virtuell und werden durch einen Administrator über eine Postfachverwaltung aktiviert. Bei nicht vorhandenem Postfach gilt entweder ein „Catch-All“, d.h. nur autorisierte Nutzer können die Nachrichten sehen, oder es erfolgt eine Benachrichtigung, wie z.B. „Postfach nicht vorhanden“. In diesem Fall müssen Mechanismen etabliert werden, wie mit der Nachricht weiter zu verfahren ist.

Alle hier geschilderten Postfach-Ressourcen können durch URI’s abgebildet werden, wie z.B. `postfach/ihrunternehmen/behinderte_menschen`

Für den Fall der Maschine-zu-Maschine-Kommunikation können die Nachrichten aus dem GCG abgeholt werden. Die Zugriffsberechtigung wird dabei ebenfalls über das Autorisierungsmodul gesteuert. Für verschlüsselte Nachrichten wird ein OZG-Empfangsadapter zur Entschlüsselung auf Seiten der Fachsoftware der Organisation benötigt.

Es sollte die Option angeboten werden, den Postfachdienst direkt bei den Unternehmen in der eigenen Firmen-IT zu installieren und zu betreiben. Das hätte den Vorteil, dass diese selbst

über die bereitgestellte Speicherplatzgröße und die gewünschte Speicherdauer von Nachrichten entscheiden könnten.

5.5.6 Zusammenspiel von Modul 5 mit den Modulen 1 bis 4

Die IdP-Funktion der Module 1 bis 4 ist die zentrale Schnittstelle zwischen Modul 5 und den Modulen 1 bis 4. Die Anmeldung an Modul 5 erfolgt über das ELSTER-Login. Als Schnittstelle wird hier die von ELSTER bereitgestellte SAML-Anbindung verwendet. Zur Anbindung von Basis-Modulen, wie Modul 5 und 6 es sind, kann die Verwendung von Single Sign-On die Benutzerfreundlichkeit deutlich erhöhen, ohne dabei die Sicherheit des Gesamtsystems herabzusetzen. Die in der Machbarkeitsstudie vorgestellte Variante U2F („Mein UP“ Version 2 und Verwaltungsleistung) kann dabei die Nutzerfreundlichkeit deutlich steigern. Die folgende Grafik ist der Machbarkeitsstudie entnommen und ergänzt. Die Abbildung zeigt die angestrebte Integration.

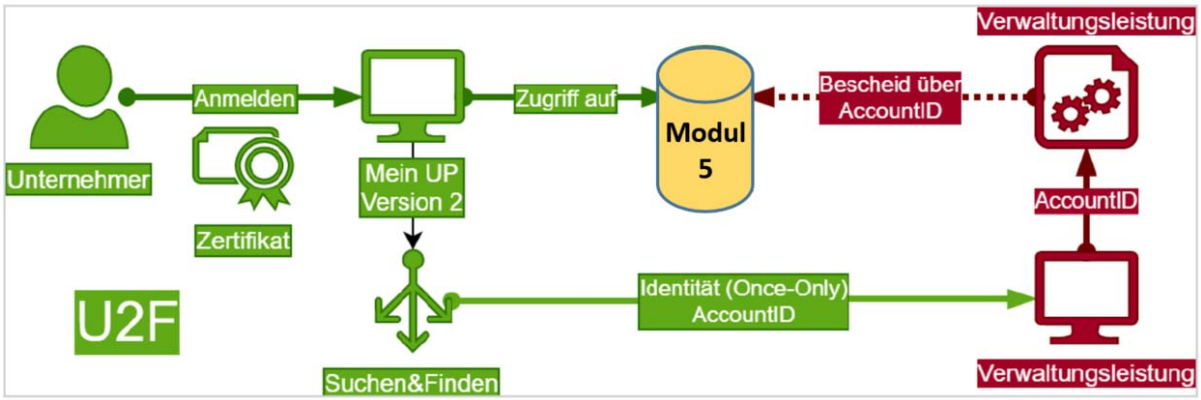

Abbildung 10: Variante U2F („Mein UP“ Version 2 und Verwaltungsleistung)

5.5.7 Zusammenspiel von Modul 5 und 6

Das Modul 6 ist für ein generisches Rechtemanagement ausgelegt und wird in Modul 5 verwendet, um die Zugriffe auf die Ordner im Postfachdienst zu steuern.

Wie in Abschnitt 5.4.2 beschrieben, können drei Gruppierungen von Nachrichten existieren, die der Einfachheit halber im Weiteren als Ordner bezeichnet werden. Der Zugriff auf den Postfachdienst erfolgt entweder durch ein Fachverfahren oder durch die Web-UI. Für die Autorisierungsanfrage ist das aber nicht relevant.

Es existieren die folgenden Gruppierungen

- *Absenderkategorie:*
  Das ist die „Leistungsgruppierung“ aus LeiKa. Diese wird optional zur Autorisierungsentscheidung herangezogen, aber sie wird i.d.R. als Metadatum in einer Nachricht mitgeliefert. Diese Information kann zur Sortierung und Darstellung der Nachrichten genutzt werden.
- *Funktionspostfach:*
  Das Beispiel „Betriebsrat“ stellt ein Funktionspostfach dar. Der Name des Funktionspostfaches kann frei vergeben werden und wird im Antragsverfahren dann entsprechend eingetragen (analog zu E-Mail). Für Funktionspostfächer kann nur ein Administrator Vertretungen eintragen.
- *Mitarbeiterpostfach:*
  Dieses kann für jeden Mitarbeiter vorhanden sein. Hierfür gibt es eine Default-Regel, die besagt, dass der Mitarbeiter die Nachrichten in seinem eigenen Postfach liest. Für dieses Postfach kann der Nutzer Vertretungen eintragen.

Beispielsweise kann der Aufruf eines Ordners, der ein Funktionspostfach repräsentiert, in Modul 5 die in der folgenden Abbildung skizzierte Anfrage an das Modul 6 senden.

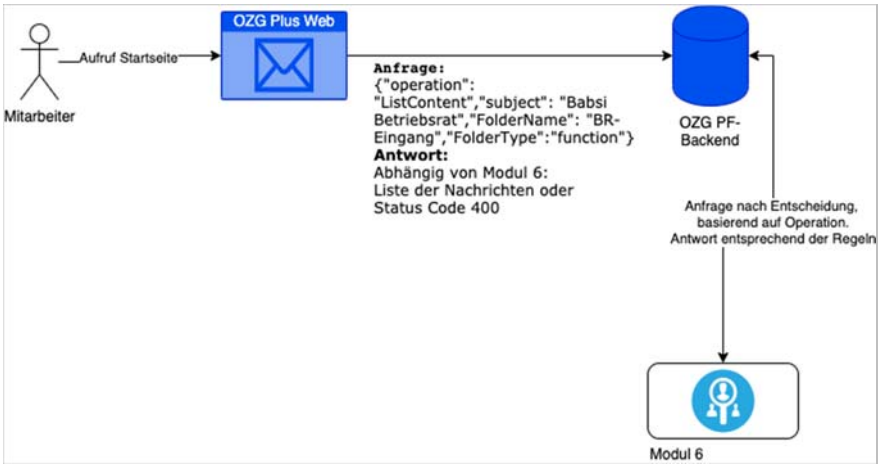

Abbildung 11: Zusammenspiel zwischen Modul 5 und 6

Wie oben zu sehen ist, werden die Zugriffe auf die Ordner durch das Autorisierungsmodul geregelt. Die Regeln in Modul 6 beziehen sich auf die Nachrichten-Gruppen, wie sie in Kapitel 5.4.2 beschrieben wurden, und werden in Modul 5 nach Benutzergruppen oder Rollen ausgewertet. Der Postfachdienst lässt nur Zugriffe zu, für die Modul 6 eine entsprechende Bestätigung sendet. Damit wird verhindert, dass Personen unberechtigten Zugang zu fachfremden Nachrichten bekommen.

Technisch gibt es nur ein Postfach (Speicherort) pro Organisation und die Sortierung in einzelne Postfächer ist virtuell. Die Nachrichten liegen verschlüsselt im Postfach. Der Zugriff auf die Nachrichten wird technisch betrachtet durch den Zugriff auf entsprechendes Schlüsselmaterial abgesichert.

5.6 Infrastruktur/Betrieb

Es wird ein hybrides Betriebsmodell angestrebt. Dieses sieht eine zentrale Instanz des OZG-PLUS-Postfachs vor. Es liegt im Ermessen eines Unternehmens, ein Postfachsystem selbst zu betreiben. Dazu kann der Administrator auf der zentralen Instanz einen entsprechenden Eintrag vornehmen. Bevor das Sendemodul eine Nachricht absendet, wird das OZG-PLUS-Postfach nach dem zuständigen Service angefragt. Dabei kommen die aus dem europäischen eDelivery-Kontext bekannten Services „SMP+SML“ zum Einsatz.

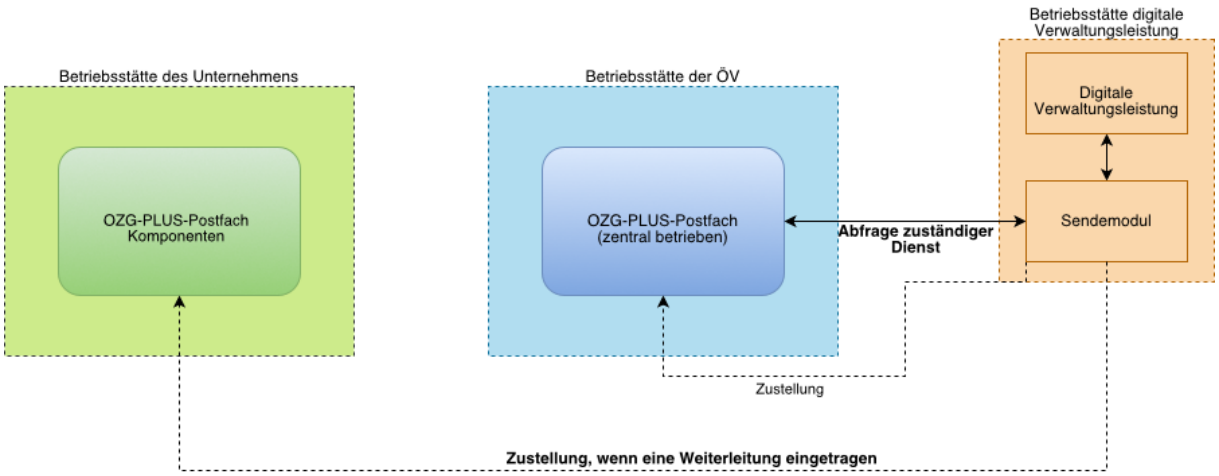

Abbildung 12: Hybrides Betriebsmodell

6 Baustein 6 „Autorisierungsmodul“

Das Autorisierungsmodul bietet verschiedene Funktionalitäten zur Steuerung von Berechtigungen, sowohl auf Seiten des Unternehmens als auch auf Seiten des Anbieters der digitalen Verwaltungsleistung.

Der Baustein 6 bedient somit die Anforderungen, die im Rahmen des Koordinierungsprojektes Unternehmenskonto gemeinsam mit verschiedenen Vertretern von repräsentativen Unternehmen in Workshops erhoben worden sind. Darüber hinaus sind jahrelange Erfahrungen des Nutzerverhaltens in vorhandenen Portalen sowie bei der Entwicklung von digitalen Verwaltungsleistungen eingeflossen.

6.1 Anforderungen/Nutzen

Im Folgenden werden die Funktionalitäten beschrieben, die das Autorisierungsmodul bietet und welchen Vorteil das Einheitliche Unternehmenskonto mit Baustein 6 für die Nutzer darstellt.

6.1.1 Funktionalitäten

Die Funktionalitäten des Autorisierungsmoduls können aus zwei Perspektiven betrachtet werden: Das Modul bietet sowohl Verwaltungsfunktionalitäten für die Unternehmen[6] intern, als auch für die Anbieter von digitalen Verwaltungsleistungen an.

Diese zwei Perspektiven zu berücksichtigen, ist essenziell, da als Anwender nicht nur die Unternehmen, die die Verwaltungsleistungen nutzen wollen, betrachtet werden, sondern auch die Behörden, die ihre Verwaltungsleistungen digital anbieten. Diese stellen ebenfalls Anforderungen an ein Einheitliches Unternehmenskonto, um ihre Verwaltungsleistungen bestmöglich anbieten zu können.

6.1.1.1 Unternehmensperspektive

Das Autorisierungsmodul bietet dem Unternehmen folgende Funktionalitäten:

- *Mitarbeitermanagement*
  Diese Funktion ermöglicht es dem Unternehmen, einen Überblick über alle Mitarbeiter des Unternehmens zu erhalten. So kann das Unternehmen digital erkennen, welcher Mitarbeiter ein ELSTER-Zertifikat für das Unternehmen beantragt hat. Darüber hinaus ist eine Verwaltung dieser Mitarbeiter möglich. Dazu zählt auch das Löschen von Mitarbeitern, die z.B. wegen Kündigung oder Rente aus dem Unternehmen ausscheiden. Weiterhin kann es, im Rahmen der Nutzung einer digitalen Verwaltungsleistung, ermöglicht werden, Workflowprozesse, wie das 4-Augen-Prinzip anzubieten.
- *Berechtigungssteuerung*
  Das Autorisierungsmodul ermöglicht dem Unternehmen, seine internen Zuständigkeiten abzubilden. Viele Unternehmen haben im Koordinierungsprojekt Unternehmenskonto gefordert, dass nicht alle Mitarbeiter jegliche Berechtigung zur Nutzung von Verwaltungsleistungen im Unternehmen erhalten sollen. Dem Unternehmensadministrator ist es hiermit möglich zu entscheiden, welcher Mitarbeiter welche digitalen Verwaltungsleistungen nutzen kann, um z.B. zu verhindern, dass ein für die Fuhrparkanzeige zuständiger Mitarbeiter ebenfalls eine Mutterschutzanzeige oder Schwerbehindertenkündigung durchführen kann. Dies ist insbesondere erforderlich, da die über den Rückkanal (Post-

[6] Der Begriff „Unternehmen“ inkludiert andere Organisationen, wie z.B. Behörden, Stiftungen und Vereine, die ebenfalls Nutzer von digitalen Verwaltungsleistungen sind.

fach) kommenden Informationen hoch sensible Daten enthalten können. Diese Berechtigungen können pro Bereich (z.B. Steuern, Personal, Bauen) oder auf einzelne digitale Verwaltungsleistungen gesetzt werden. Die Berechtigungssteuerung kann auf weitere Berechtigungsstufen runtergebrochen werden, die es dem Administrator ermöglicht differenzierte Berechtigungen wie z.B. lesenden oder schreibenden Zugriff zu gewähren.

- *Berechtigungsgruppen*
  Zur Erleichterung der Berechtigungsvergabe, insbesondere für größere Unternehmen, besteht die Möglichkeit zum Anlegen von Gruppen. Diese fungieren wie klassische Berechtigungsgruppen. Alle Mitarbeiter, die in der Gruppe sind, erhalten implizit die Berechtigung, die diese Gruppe innehat.

  Beispiele:

  Gruppe Arbeitsschutz – Berechtigung für die digitalen Verwaltungsleistungen Arbeitszeitmeldung und Asbestmeldung

  Gruppe Personal – Berechtigung auf Personaldienste wie z.B. Mutterschutzanzeige

- *Vertretungsregelung*
  Dem Unternehmen ist es möglich, zwischen den Mitarbeitern Vertretungen zu organisieren. Dies gilt für Abwesenheitsvertretungen bei Urlaub oder Krankheit. Der vertretende Mitarbeiter hat dann die Berechtigungen des Vertretenen inne. Es wird aber immer deutlich, dass der Mitarbeiter gerade in Vertretung handelt.

- *Postfachzugriff*
  Über das Autorisierungsmodul ist es möglich, die Steuerung der Zugriffe auf vorhandene Funktionspostfächer zu organisieren. Gerade der Rückkanal kann häufig auch sensible Daten beinhalten, auf die nicht alle Mitarbeiter des Unternehmens einen Zugriff haben sollten.

  Beispiel:

  Schwerbehindertengutachten – Erstellung von ärztlichen Gutachten

- *Mandatsübergabe*
  Es ist gängige Praxis, bestimmte Aufgaben innerhalb eines Unternehmens an unabhängige Dritte auszulagern bzw. zu delegieren. Dazu gehören Architekten, Notare oder Anwälte. Es ist im Interesse des Unternehmens, dass diese Personen nur bestimmte Verwaltungsleistungen im Namen des Unternehmens durchführen können und somit auch hier die Berechtigungen beschränkt werden müssen. Zum Beispiel kann ein Architekt nur die Verwaltungsleistungen des Bereiches Bauen (z.B. Bauantrag) nutzen, nicht aber die des Bereiches Personal (z.B. Mutterschutzanzeige). Darüber hinaus wird eine Überprüfung der Vollmachten der handelnden Dritten erfolgen müssen, ob diese tatsächlich vom Unternehmen berechtigt sind.

6.1.1.2 Perspektive Anbieter digitaler Verwaltungsleistungen

Das Autorisierungsmodul bietet dem Anbieter einer digitalen Verwaltungsleistung folgende Funktionalitäten:

- *Zugriffsbeschränkung*
  Ein Anbieter einer digitalen Verwaltungsleistung hat die Möglichkeit, den Zugriff auf diese digitale Verwaltungsleistung zu beschränken und nur bestimmte Unternehmen zu deren Nutzung zuzulassen. Bestimmte digitale Verwaltungsleistungen dürfen nur von Organisationen mit einem berechtigten Interesse genutzt werden. Eine Zugriffsbeschränkung und explizite Freischaltung dieser Organisationen seitens des Anbieters der digitalen

Verwaltungsleistung hat den Vorteil, dass eine Prüfung, ob diese Organisation die digitale Verwaltungsleistung nutzen darf, nur einmal erfolgen muss und nicht bei jeder erneuten Nutzung der digitalen Verwaltungsleistung. Das führt zu einer hohen Zeitersparnis auf Seiten der Verwaltungen, die seit Jahren schon mit geringen Kapazitäten und Personalengpässen umgehen müssen.

Beispiele:

Führerscheinerstantrag - Die Nutzung der digitalen Verwaltungsleistung zur erstmaligen Beantragung eines Führerscheins ist den Fahrschulen vorbehalten.

Die Funktion der Zugriffsbeschränkung bietet insbesondere bei stark nachgefragten Auskunftsverfahren einen Vorteil. Hier wird einmalig geprüft, ob die registrierte Organisation auf die digitale Verwaltungsleistung zugreifen darf und berechtigt ist, die Auskunft zu erhalten. Das bietet den Vorteil, dass diese Auskünfte automatisiert und ohne erneute Prüfung gegeben werden können.

Beispiel Auskunftsverfahren:

Schulregister - Auskunft aus dem Schulregister ist den Ärzten vorbehalten.

Schiffsdatenregister - Auskunft aus dem Schiffsdatenregister für berechtigte Organisationen

ELBE+ (Leitungsanfragen) - Diese digitale Verwaltungsleistung ermöglicht es, digitale Auskünfte über Leitungen zu geben. Diese Anfragen sind nur für Bauunternehmen mit berechtigtem Interesse zugänglich. Ein berechtigtes Interesse besteht, wenn ein Bauvorhaben im angefragten Gebiet geplant ist. Aufgrund der vorherigen Freischaltung der Organisationen, die ein berechtigtes Interesse nachweisen können, kann die Auskunft automatisiert erteilt werden.

- *Rollendefinition*
  Jeder Anbieter einer digitalen Verwaltungsleistung kann dafür Rollen definieren. Diese Rollen können bei der Freischaltung an die Organisationen differenziert vergeben werden. Rollen haben den Zweck, unterschiedliche fachliche Berechtigungen innerhalb einer digitalen Verwaltungsleistung abzubilden.

Alle oben genannten Funktionalitäten sind ein Angebot seitens des Autorisierungsmoduls und nicht verpflichtend von den Anwendern zu nutzen. Das Modul bietet die Möglichkeit, auch komplexe Sachverhalte sowohl auf Seiten der Unternehmen als auch auf Seiten der Anbieter von digitalen Verwaltungsleistungen abzubilden. Diese Flexibilität, bereits vorhandene, durch ein System angebotene Funktionen nutzen zu können, war in der Vergangenheit bei der Entwicklung von digitalen Verwaltungsleistungen immer von Vorteil.

Gerade erst kürzlich konnte in der aktuellen COVID-19-Krisensituation eine digitale Verwaltungsleistung innerhalb von drei Tagen entwickelt und produktiv gesetzt werden. Es wurde gezeigt, dass durch diese Funktionalitäten eine Flexibilität bei der Entwicklung von digitalen Verwaltungsleistungen gegeben ist. Werden diese Funktionalitäten nicht zentral angeboten, muss jede digitale Verwaltungsleistung, die diese Funktionalitäten benötigt, diese selbstständig implementieren. Es ist dann nicht möglich, innerhalb kürzester Zeit eine technische Unterstützung in Krisensituationen bereitzustellen.

6.1.2 Anwendungsfälle

Im Folgenden werden verschiedene Fallbeispiele erläutert, die die Funktionalitäten des Autorisierungsmoduls veranschaulichen. Die Beispiele werden heute schon produktiv betrieben.

6.1.2.1 Bauleitplanung online Beteiligung in Schleswig-Holstein (BOB-SH)

Fachlichkeit

Laut Baugesetzbuch müssen Bauvorhaben im öffentlichen Raum durch eine Stadt oder Gemeinde in einem systematischen Verfahren vorab durchgeplant werden. Der dabei entstehende Plan (Bauleitplan) wird anschließend als Anleitung für den Bau verwendet. Die Bauleitpläne werden von der Stadt bzw. der Gemeinde aufgestellt. Zu einem Bauleitplan gehören der Flächennutzungsplan und der Bebauungsplan.

Rechtliche Grundlagen

Das Baugesetzbuch besagt in den §§3, 4 BauGB, dass die Öffentlichkeit sowie Behörden, deren Aufgabengebiete durch das Bauvorhaben berührt sind, bei der Bauleitplanung zu beteiligen sind. Das heißt, dass die Bauleitpläne öffentlich bekannt gemacht werden müssen, um Bürgern, Behörden und Trägern öffentlicher Belange (TöB) eine Einsicht sowie Stellungnahme zu ermöglichen.

Laut Bekanntmachungsverordnung in Schleswig-Holstein kann diese Beteiligung auch online erfolgen. Dafür wurde die digitale Verwaltungsleistung BOB-SH geschaffen.

Anforderung 1 – Nutzung des Servicekontos für Behörden und Unternehmen (Organisationskonto)

Alle Organisationen, die mit der digitalen Verwaltungsleistung agieren, müssen über ein Servicekonto verfügen. Das heißt, BOB-SH hat keine eigene Benutzerverwaltung, sondern nutzt die angebotenen Servicekonten. Es handelt sich bei den Nutzern sowohl um Behörden als auch Unternehmen.

Die Behörden, wie Gemeinden und Städte, stellen die Planungsdokumente online und eröffnen das Beteiligungsverfahren. Andere Gemeinden bzw. Städte sowie TöBs können ihre Stellungnahme dazu abgeben. Die TöBs sind z.B. Kirchen, Strom-, Gas- und Wasserversorgungsunternehmen.

Dem Bürger steht die digitale Verwaltungsleistung zur Information und Stellungnahme ohne Registrierung zur Verfügung.

Anforderung 2 – Schutz des Zugriffs auf die digitale Verwaltungsleistung für bestimmte Organisationen

Wie aus den Ausführungen ersichtlich wird, ist die digitale Verwaltungsleistung nur von bestimmten Organisationen (Behörden und TöBs) nutzbar. Aus diesem Grund schützt der Anbieter der digitalen Verwaltungsleistung diese vor unbefugten Zugriffen. Grund dafür ist, dass nur öffentliche Stellen ein Beteiligungsverfahren starten, sowie nur Behörden und TöBs Stellungnahmen dazu abgeben können und nicht jedes Unternehmen, welches ein Organisationskonto besitzt.

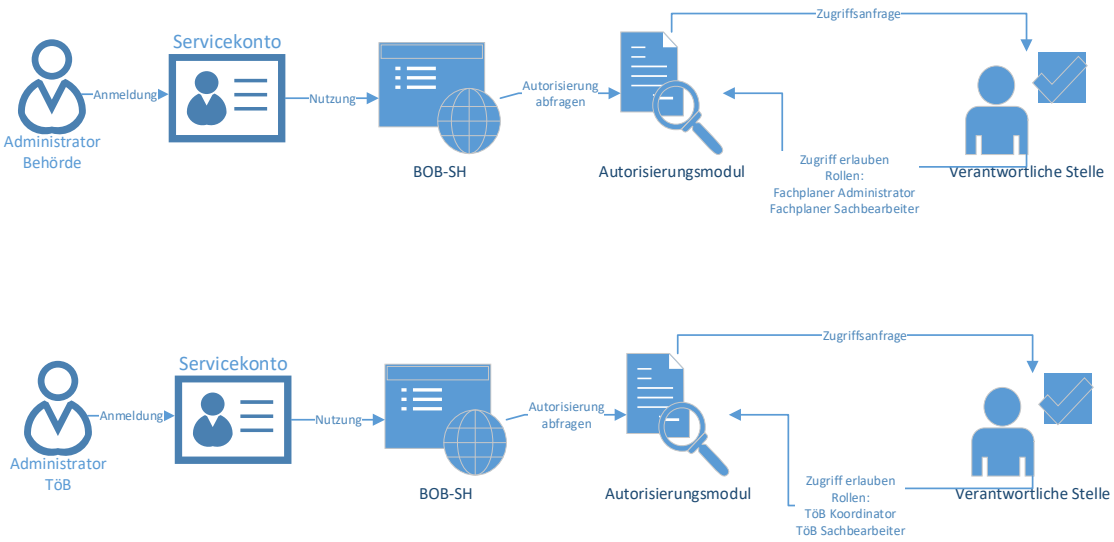

Abbildung 13: Darstellung Zugriffsschutz Verwaltungsleistung, Resource Owner schützt

Würde die digitale Verwaltungsleistung für jeden Inhaber eines Organisationskontos offen zur Verfügung stehen, müsste die Gemeinde bei jeder Stellungnahme prüfen, ob dieser überhaupt berechtigt ist Stellungnahmen abzugeben. Diese kontinuierliche Überprüfung erzeugt erheblichen Mehraufwand bei den sowieso schon überlasteten Verwaltungen.

Anforderung 3 – Unterschiedliche Berechtigungen innerhalb der digitalen Verwaltungsleistung

Neben den Freischaltungen einzelner Organisationen für die digitale Verwaltungsleistung, werden den Behörden und TöBs unterschiedliche Rollen zugewiesen. Die Rollen haben unterschiedliche Berechtigungen in der digitalen Verwaltungsleistung, das heißt mit den einzelnen Rollen können verschiedene Funktionalitäten bedient werden.

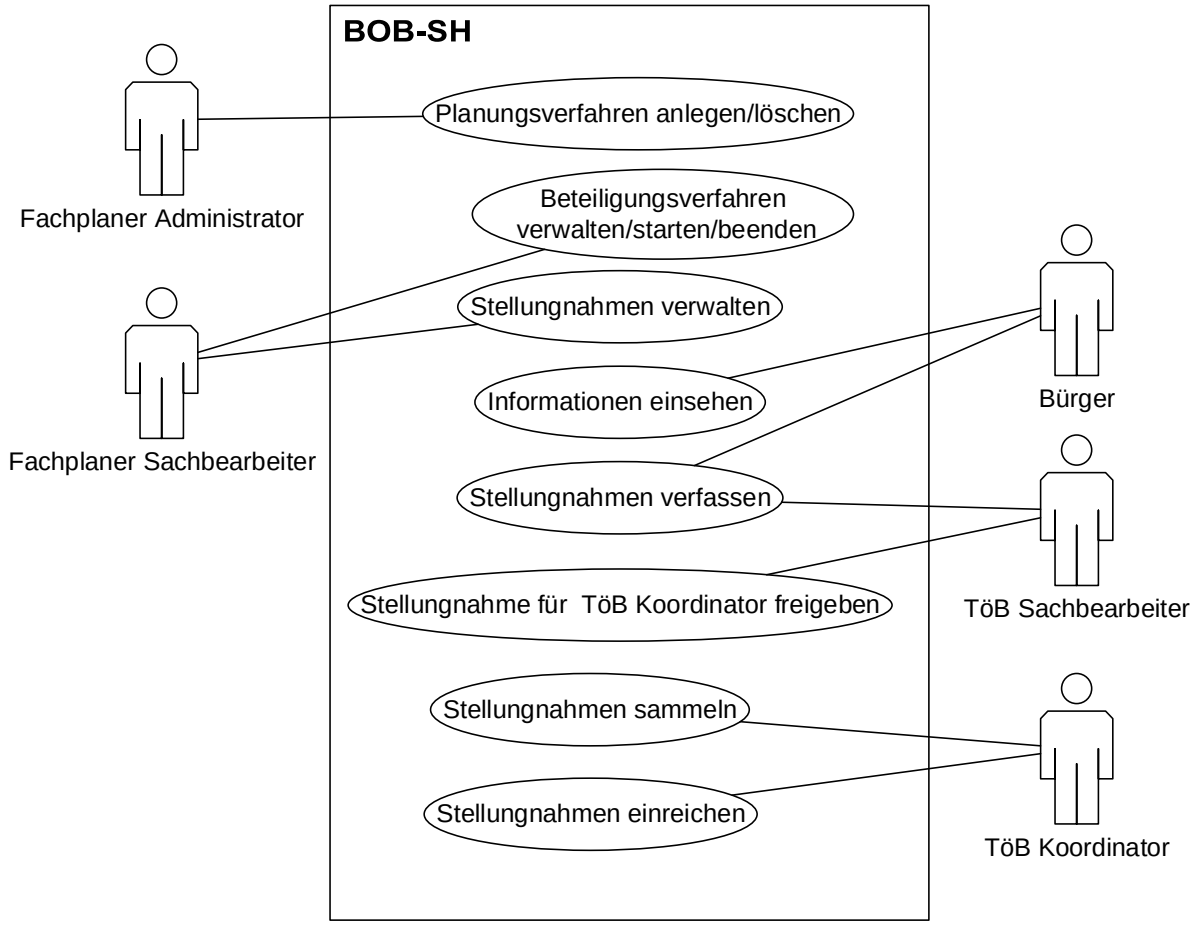

Abbildung 14: Unterschiedliche Berechtigungen am Beispiel BOB-SH

Anforderung 4 – Beschränkung des Zugriffs für einzelne Mitarbeiter bzw. Gruppen seitens der Organisation

Des Weiteren ist es im Interesse der Organisation, dass nicht alle Mitarbeiter Stellung zu den Bauleitplänen nehmen können. Deshalb hat ein Administrator eines Unternehmens die Möglichkeit, nur bestimmten Mitarbeitern Zugriff auf die digitale Verwaltungsleistung zu gewähren und eine entsprechende Rolle zuzuweisen. Der Administrator kann sich aus dem Rollenset bedienen, welches dem Unternehmen bzw. der Behörde von dem Anbieter der digitalen Verwaltungsleistung gegeben wurde.

Anforderung 5 – Rückkanal an mehrere Mitarbeiter, Funktionspostfächer

Der ToB-Koordinator sammelt alle Stellungnahmen der ToB-Sachbearbeiter seiner Organisation und gibt diese gemeinsam frei zur Bewertung durch die planende Behörde. Die Bewertungen der Stellungnahmen gehen an das zugehörige Postfach der Organisation. Hier ist es wichtig, dass eine Zustellung an ein Funktionspostfach erfolgen kann, auf welches alle zuständigen Mitarbeiter einen Zugriff haben.

6.1.2.2 Ambulantes COVID-19 Monitoring – Schleswig-Holstein

Im Rahmen der aktuellen COVID-19 Krise hat sich gezeigt, wie wertvoll die oben genannten Funktionalitäten sind. So konnte eine digitale Verwaltungsleistung innerhalb kürzester Zeit entwickelt und bereitgestellt werden.

Bei dem Fallbeispiel handelt es sich um ein ambulantes COVID-19 Monitoring, mit dem infizierte Patienten, die nicht stationär aufgenommen wurden, betreuen zu können.

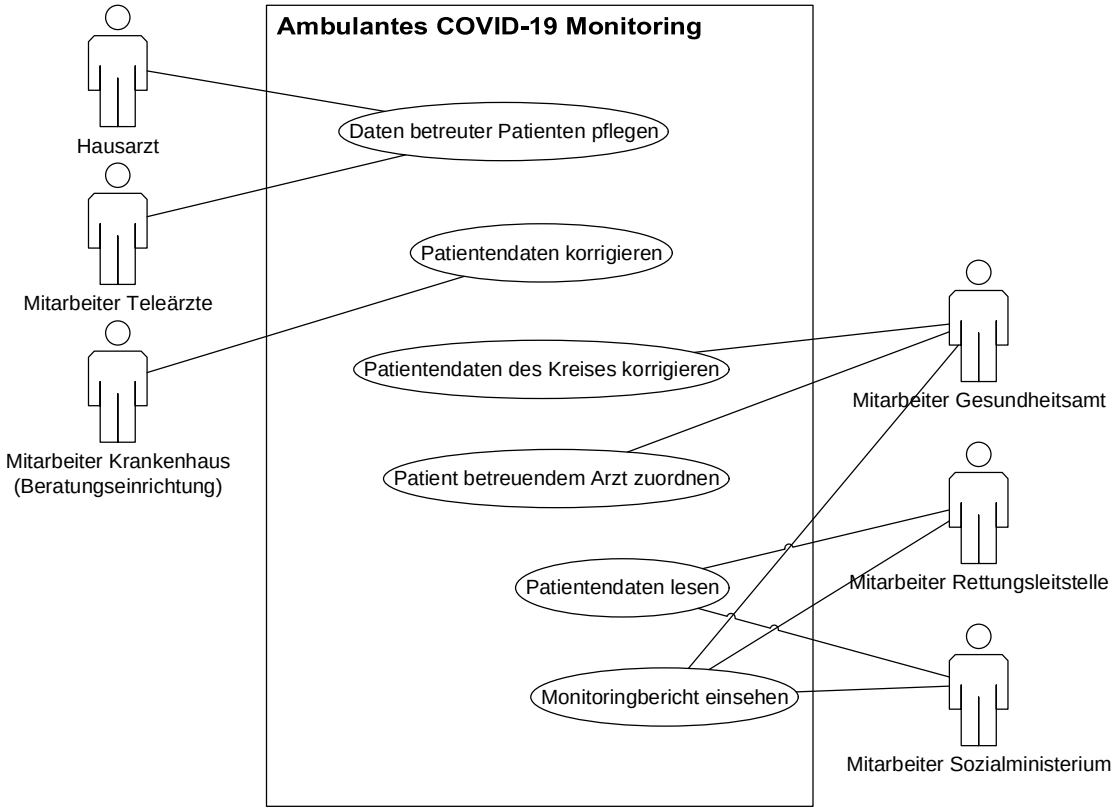

Abbildung 15: Fallbeispiel ambulantes COVID-19 Monitoring

Es wird deutlich, dass die digitale Verwaltungsleistung verschiedene Funktionalitäten benötigt:

- Perspektive Anbieter der digitalen Verwaltungsleistung
  - Rollen mit unterschiedlichen Berechtigungen in der digitalen Verwaltungsleistung
  - Beschränkung des Zugriffs auf die digitale Verwaltungsleistung wegen sensibler Daten
- Unternehmensperspektive
  - Fachliche Zuordnung der digitalen Verwaltungsleistung, damit nicht jeder Mitarbeiter im Unternehmen die sensiblen Daten melden und einsehen kann

6.2 Technische Umsetzung

In den folgenden Abschnitten werden die konzeptionellen Grundzüge und die Grobarchitektur für eine technische Umsetzung des Moduls beschrieben. Um den Rahmen dieses Dokuments zum Prüfauftrag nicht zu sprengen, wird hier lediglich stark vergröbert und auf abstrakter Ebene der Lösungsentwurf skizziert. Viele Aspekte zum Entwurf können auf diesem Abstraktionsniveau bestenfalls angerissen werden.

6.2.1 Grundlagen des Konzeptansatzes

Das abstrakte Modell des Autorisierungsmoduls, d.h. die Begriffe, Funktionen und Regeln, die die konzeptionelle Grundlage des Moduls und seiner Interaktion mit anderen Komponenten festlegen, orientiert sich an den Paradigmen der Konzepte zur „attribut- und regelbasierten

Zugriffssteuerung“. Diese etablierten und gereiften Autorisierungsmodelle liefern die grundsätzlichen Architekturmuster, die genügend Raum für eine Ausgestaltung bieten, um den aktuellen und künftigen Anforderungen an die Autorisierungssteuerung eines bundesweiten Organisationkontos gerecht zu werden.

Das zugrunde gelegte Modell basiert zwar auf den Elementen des allgemeinen ABAC-Konzepts[7], prägt es aber spezieller und einschränkender aus und geht an einigen Stellen darüber hinaus. Insbesondere werden Elemente des rollenbasierten RBAC-Grundmusters zur Reduzierung der konzeptionellen Komplexität mit den ABAC-Mustern kombiniert.

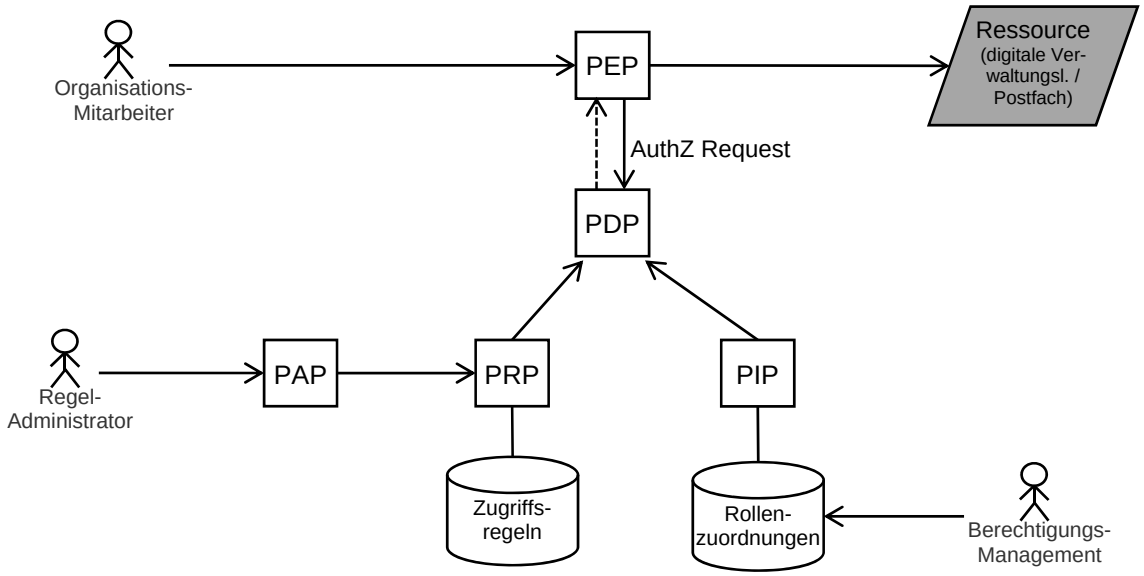

Abbildung 16: Abstraktes Modell zu Attribute-Based Access Control (ABAC)

Ein wesentliches Prinzip des ABAC-Modells ist die Trennung von Entscheidung und Durchsetzung der Zugriffsregeln: Während die Auswertung der Regeln und schlussendliche Entscheidung, ob auf eine Ressource zugegriffen werden darf, an eine spezielle Instanz (Policy Decision Point, PDP) delegiert wird, liegt die Verantwortung für die tatsächliche Durchsetzung der Entscheidung, also der Abweisung oder der Zugriffsgestattung, bei einer eigenen Instanz (Policy Enforcement Point, PEP).

In Abbildung 16 ist dargestellt, dass der Zugriff eines Nutzers auf die digitale Verwaltungsleistung (Ressource) grundsätzlich über eine PEP-Instanz erfolgt. Der PEP delegiert die Entscheidung über die Zugriffserlaubnis an eine PDP-Instanz, indem er eine Autorisierungsanfrage versendet. Bestandteil der Anfrage (Policy Request) sind Informationen zur adressierten Ressource, zum Nutzer und dessen Eigenschaften (insb. Rollen) und ggf. zur Zugriffsoperation (z.B. Ausführen, Lesen oder Schreiben).

Der PDP beschafft sich die passende, gespeicherte Berechtigungsregel (Policy) zur Ressource und trifft auf Basis der Rollen, die dem authentifizierten Nutzer oder dessen Organisation zugeordnet sind, seine Entscheidung. Während der PEP innerhalb des Portalsystems angesiedelt ist, realisiert das Autorisierungsmodul den PDP.

[7] Attribute based access control, siehe z.B. ABAC-NIST-Publication

6.2.1.1 Elemente zur Berechtigungssteuerung

Um eine Berechtigung eines Nutzers zu steuern, also den Zugriff auf eine Ressource (digitale Verwaltungsleistung oder Postfach) zu gestatten oder zu verwehren, stehen im attribut- und regelbasierten Modell zwei Elemente zur Verfügung:

- *Berechtigungsregeln (Policy)*
  Mit den Berechtigungsregeln können Nutzer aufgrund ihrer Eigenschaften (Rollen) zur Nutzung berechtigt oder ausgeschlossen werden. Typischerweise wird eine Erlaubnis an die Inhaberschaft einer oder mehrerer Rollen geknüpft.
- *Zuordnung* von Rollen
  Durch Zuweisen oder Entziehen von Rollen an einen Nutzer oder dessen Organisation wird beeinflusst, ob die Auswertung einer Berechtigungsregel zu einer positiven oder negativen Entscheidung führt.

Regeln und Rollenzuordnungen ergänzen sich daher. Die Änderungen von Regeln und Zuordnungen sind aber in verschiedenen Hoheiten bzw. Verantwortungsbereichen angesiedelt.

6.2.1.2 Basiskonzepte Rollenkontext und Ressource

Das Fachkonzept zur technischen Umsetzung definiert einige begriffliche Konzepte, die dazu dienen, Anforderungen bezüglich Einfachheit und Optionalität erfüllen zu können. Die wichtigsten Eigenschaften, die die Profilierung des allgemeinen ABAC-Konzeptes widerspiegeln, sollen hier kurz angerissen werden.

Der Begriff Ressource aus dem ABAC-Muster bezeichnet allgemein digitale Entitäten, deren Zugriffe zu autorisieren sind. Dieses fachliche Modell profiliert genau drei Ausprägungen einer Ressource:

- *Service*
  Eine konkrete, durch eine Behörde direkt oder indirekt bereitgestellte Web-Applikation, die eine bestimmte digitale Verwaltungsleistung realisiert (Online-Dienst).
- *Abstrakter* Service
  Repräsentiert eine logische Verwaltungsleistung (z.B. auf Basis LeiKa bzw. FIM-Prozesskatalog) und nicht eine reale Bereitstellung in Form einer Web-Applikation. Zweck ist die Schaffung der Möglichkeit zur generellen Berechtigung aller konkreter Services, die diesen Service-Typ realisieren - unabhängig vom Ort der Bereitstellung bzw. der bereitstellenden Behörde.
- *Inbox*
  Ein logisches Postfach einer Organisation, ggf. ergänzt um ein Klassifizierungsmerkmal.

Zu jeder Ressource – unabhängig von ihrem konkreten Typ – gibt es genau eine verantwortliche Stelle (Resource Owner), der es allein obliegt, die Zugriffsregeln festzulegen.

Das fachliche Modell zum Prüfauftrag definiert ein weiteres Konzept zur ABAC-Profilierung, welches durch den Begriff Rollenkontext ausgedrückt wird. Ein Rollenkontext repräsentiert den Geltungsbereich für Rollendefinitionen, er liefert einen Namensraum sowie ein zugehöriges organisatorisches Modell.

Einerseits können alle Ressourcen (s.o.) einen Rollenkontext bilden, d.h. es können in ihrem Geltungsbereich Rollenbezeichner festgelegt werden. Des Weiteren sind eigenständige Rollenkontexte vorgesehen, deren Rollen allgemeinerer Natur sind und für Autorisierungsentscheidungen bei unterschiedlichen digitalen Verwaltungsleistungen potenziell relevant sind. Beispiele für solche eigenständigen Rollen sind „Freier Träger nach Sozialgesetzbuch VIII“ oder „Notar“.

6.2.1.3 Verantwortungsbereiche des Berechtigungsmanagements

Eine gründlichere Betrachtung der Fachlichkeit offenbart, dass es mehrere Verantwortungsbereiche für das Management von Berechtigungen gibt. Verknüpft mit diesen Bereichen sind unterschiedliche Zwecke und Ziele hinsichtlich Erteilung oder Verweigerung von Berechtigungen:

- *Verantwortungsbereich der digitalen Verwaltungsleistung*
  Die verantwortliche Stelle für die Verwaltungsleistung, i.d.R. die dienstanbietende Behörde (Resource Owner), hat das Interesse, ihren Dienst vor unautorisierten Zugriffen zu schützen. Dazu legt sie Berechtigungsregeln (Policies) fest, mit denen ausgedrückt wird, wer bzw. mit welchen Rollen ein Nutzer welche Operation des Dienstes nutzen darf.
- *Verantwortungsbereich der Organisation*
  Dagegen hat die Organisation ggf. das Interesse, zu regeln, welche ihrer Mitarbeiter welche Verwaltungsleistung in Anspruch nehmen dürfen. Eine Organisation kann somit Zugriffsberechtigungen, die die Organisation selbst zwar innehat, optional für ihre Mitarbeiter differenziert beschränken.
- *Verantwortungsbereich für das Attestieren von Rollen*
  Jenseits der nutzenden Organisation und der dienstanbietenden Behörde gibt es Stellen, zu deren Aufgaben es zählt, von ihnen verantwortete Rollen zu attestieren. Diese qualifizierenden Stellen überprüfen, ob eine Organisation begründet Anspruch auf bestimmte Rollen besitzt und weisen bei positiver Prüfung diese der Organisation dauerhaft zu.

  Qualifizierende Stellen sind für eine oder mehrere Rollen zuständig, d.h. sie sind für einen bestimmten Rollenkontext verantwortlich, in dessen Geltungsbereich Rollen definiert werden. Diese Rollen sind typischerweise dienstübergreifend relevant und können von mehreren Berechtigungsregeln referenziert werden.

Stellen innerhalb dieser drei Bereiche teilen sich somit die Verantwortung für das Management der Berechtigungen – jede mit eigenem Ziel und unterschiedlichen Befugnissen zur Änderung von Rollenzuordnungen oder Berechtigungsregeln.

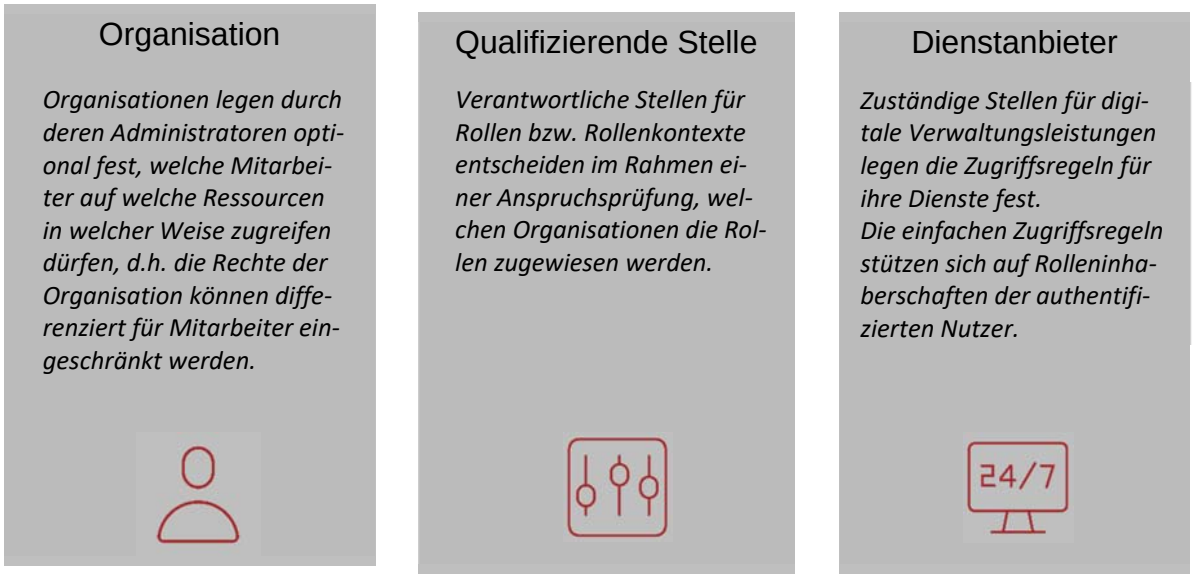

Abbildung 17: Die drei logischen Verantwortungsbereiche im Berechtigungsmanagement

6.2.1.4 Zuordnung von Rollen

Die Entscheidung, ob ein Nutzer für den Zugriff auf eine Ressource berechtigt ist, ergibt sich aus dem Zusammenspiel von Berechtigungsregeln (Policy) der Ressource und den Rollen, die dem Nutzerkonto zugeordnet sind. Der Vorgang einer Berechtigung ist daher gleichbedeutend mit einer Zuweisung einer Rolle an ein Nutzerkonto.

Diese Facharchitektur definiert folgende Prinzipien hinsichtlich der Rollenzuordnung:

- Grundsätzlich werden an Organisationskonten zugewiesene Rollen an deren Mitarbeiter implizit übertragen (Role Propagation), d.h. im Allgemeinen erbt ein Nutzer die Rechte seiner Organisation. Beim Ressourcentyp „Inbox“ (Funktionspostfächer) findet dagegen keine implizite Rollenübertragung statt.
- Optional kann eine Organisation jedoch differenzierte Berechtigungen für seine Mitarbeiter vorsehen. Dazu kann die Organisation durch ihren Administrator den Standardmodus für die Rollenübertragung deaktivieren und stattdessen die Rollen, die der Organisation zugeordnet sind, differenziert an Mitarbeiterkonten zuweisen.
- Für alle Rollen bzw. deren übergeordnete Rollenkontexte existieren verantwortliche Stellen. Diese Stellen definieren die Rollen des von ihnen verantworteten Kontextes.
- Nur diese Stellen sind autorisiert, die von ihnen verantworteten Rollen zwecks Berechtigung an Organisationen zuzuweisen. Zuweisungen direkt an Mitarbeiterkonten sind durch diese Stellen nicht möglich.
- Folgende Typen von für Rollen verantwortliche Stellen (Role Context Owner) sieht die Facharchitektur vor:
    1. Zuständige Stelle für bereitgestellte digitale Verwaltungsleistung
    2. Zuständige Stelle für Verwaltungsleistungstyp
    3. Zuständige Stelle für eigenständige Rollen
    4. Organisation als Inhaber eines Postfachs

6.2.1.5 Profilierung der Zugriffsregeln

Das allgemeine Konzept zur attribut- und regelbasierten Zugriffssteuerung (ABAC) wird an einigen Stellen zur Reduzierung der Komplexität deutlich eingeschränkt. Beispiele für profilierende Einschränkungen sind:

- *Zuordnung von Ressource zu Policies*
  Jede Ressource referenziert genau eine Policy (Satz von Berechtigungsregeln). Ein zeitaufwändiges und semantisch komplexes Identifizieren betroffener Policies entfällt.

  Jedoch können Policies einer Ressource von anderen Ressourcen derselben verantwortlichen Stelle referenziert werden (geteilte Nutzung) - analog einem symbolischen Link im Dateisystem, sofern die in der Policy referenzierten Attribute in dem Kontext zur Verfügung stehen (s.u.).
- *Regelausprägungen*
  Die Policies sind einfach strukturiert, ohne hierarchische Beziehungen und Gruppierungen. Es gibt lediglich eine oder mehrere Regeln, die optional Operationen zugeordnet werden können.
- *Eingeschränkte Rollensätze*
  Als in Regeln referenzierte Rollen stehen lediglich Rollen aus dem Kontext der Ressource oder übergreifender Rollenkontexte zur Verfügung. Der Regeleditor unterstützt entsprechend bei der Rollenauswahl.

Ein grafischer Regeleditor berücksichtigt diese und weitere Einschränkungen. Er ist einfach, intuitiv und unmissverständlich zu bedienen. Er verhindert die Festlegung nichtvalider Regeln.

6.2.1.6 Systemunterstützung für Berechtigungsmanagement

Ein wichtiger Aspekt ist das Management der Aktivitäten zur Berechtigungserteilung, also das Zuweisen oder Entziehen von Rollen. Da eine große Zahl an Nutzern und zuständigen Stellen für digitale Verwaltungsleistungen existiert, ist eine Systemunterstützung bei der Verwaltung und Abarbeitung von Berechtigungsaufgaben erforderlich, die mit einem adäquaten organisatorischen Modell korrespondiert. Delegation und Dezentralisierung sind zu berücksichtigende Aspekte, um die Berechtigungsverwaltung skalierbar und damit handhabbar zu gestalten.

Die durch das Autorisierungsmodul realisierte Systemunterstützung erfolgt durch ein Management von impliziten Berechtigungsanträgen in Form von einfachen Workflow-Tasks. Die PDP-Komponente, die die Berechtigungsregeln (Policies) für die Entscheidungsfindung auswertet, verfügt über das Wissen, aufgrund welcher fehlenden Rollen eine Berechtigungsentscheidung ggf. negativ beschieden wurde und welche Stelle für diese Rollen verantwortlich ist. Diese Informationen werden genutzt, um ein teilautomatisiertes Management zur Rollenanspruchsprüfung zu initiieren (Abbildung 18).

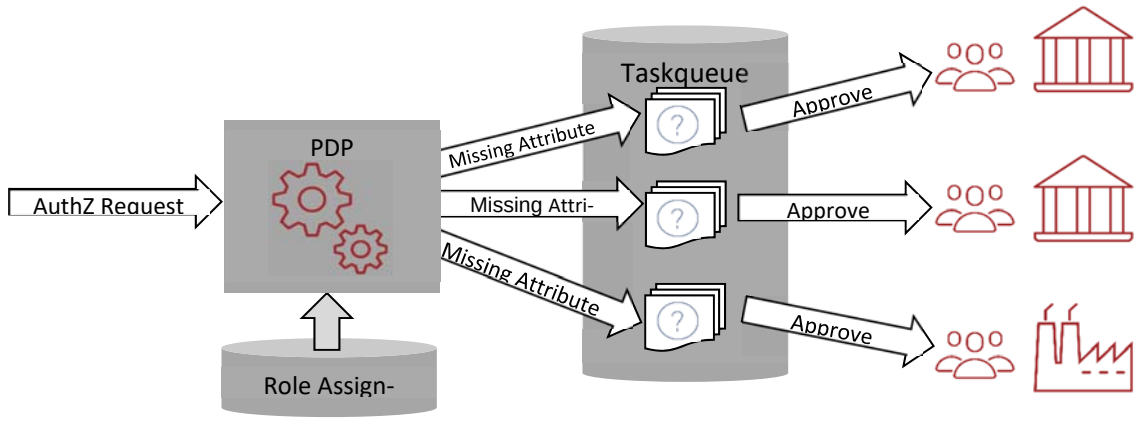

Abbildung 18: Schematische Darstellung zur teilautomatisierten Berechtigungsverwaltung

Auf Aspekte wie Routing der Workflow-Tasks inkl. Delegation und Dezentralisierung oder die Unterdrückung wiederholter Tasks kann auf diesem Detaillierungsniveau nicht eingegangen werden.

6.2.2 Immanente Anwendungsfälle und Akteure

Fachprozessbezogene Szenarien, die den fachlichen Nutzen des Autorisierungsmoduls im OZG-Kontext aufzeigen, sind im Abschnitt 6.1.2 beispielhaft beschrieben. In Abgrenzung dazu realisiert das Autorisierungsmodul seine systemeigenen, immanenten Anwendungsfälle für das Berechtigungsmanagement.

Anhand der Ansätze und Prinzipien der hier skizzierten Facharchitektur lassen sich Anwendungsfälle und Akteure (kanonische Rollen im System) des logischen Gesamtsystems „Autorisierungsmodul“ ableiten. Einige Akteure lassen sich dabei zu abstrakten Rollen zusammenfassen.

Die nach aktueller Analyse identifizierten immanenten Anwendungsfälle des Autorisierungsmoduls sind in Abbildung 19 dargestellt. Exemplarische sollen konkrete Besetzungen der abstrakten Rollen genannt werden.

- Die abstrakte Rolle „Resource Owner“ wird wahrgenommen durch

- Mitarbeiter einer Behörde, die für eine bereitgestellte digitale Verwaltungsleistung verantwortlich ist
- Mitarbeiter einer öffentlichen Stelle, die zuständig ist für einen Verwaltungsleistungstyp (z.B. LeiKa-Leistungsobjekt)
- Administrator einer Organisation, der die Funktionspostfächer seiner Organisation verantwortet

- Die abstrakte Rolle „Role Context Owner“ wird wahrgenommen durch Mitarbeiter, die entweder die Rolle „Resource Owner“ (s.o.) oder „Autonomous Context Owner“ (s.u.) innehaben (s.o.).
- Die Rolle „Autonomous Context Owner“ wird wahrgenommen durch Mitarbeiter einer öffentlichen Stelle, in deren Verantwortlichkeit sich eigenständige (nicht an Ressourcen gebundene) Rollendefinitionen befinden (z.B. „Freier Träger“ oder „Notar“).
- Die Rolle „Organization Admin“ wird wahrgenommen durch Mitarbeiter einer Organisation, die autorisiert sind, das Berechtigungsmanagement inkl. Gruppenverwaltung stellvertretend für die Organisation durchzuführen. Die Zuweisung der Administrator-Rolle erfolgt durch Beantragungs- und Freischaltungsprozesse analog der heutigen ELSTER-Registrierung.

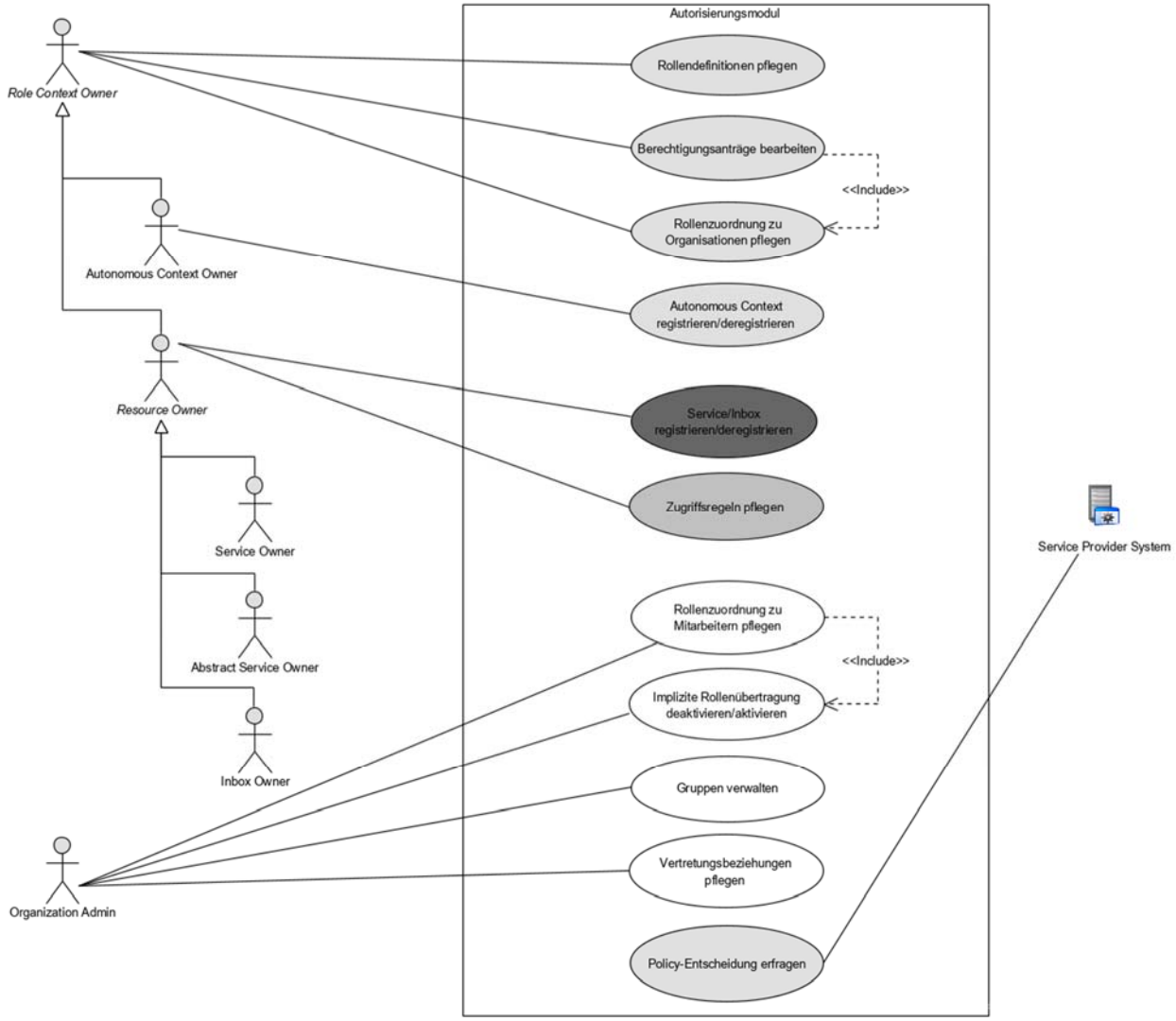

Abbildung 19: Systemeigene Anwendungsfälle und abstrakte Akteure

6.2.3 Architekturskizze

Der im Rahmen dieses Prüfauftrags entwickelte Architekturentwurf besitzt zwar nicht den für eine Implementierungsvorgabe notwendigen Reife- und Detaillierungsgrad, umreißt aber bereits wesentliche Prinzipien und Muster:

- Das Autorisierungsmodul bildet zwar mit dem Identity Provider (IdP) vom ELSTER-Organisationskonto einen fachlich zusammenhängenden Systemverbund, realisiert aber die Funktionen zur Autorisierung als ein eigenständiges, mit dem ELSTER-IdP lose gekoppeltes System (Architekturmuster Self-contained System, ScS).
- Dem ScS-Muster entsprechend, realisiert das Autorisierungsmodul auch eigenständig die Web-Dialoge seiner immanenten Anwendungsfälle. Das Design der Dialoge wird dazu vollständig von „Mein ELSTER“ (bzw. „MUP“) übernommen, um ein aus Nutzersicht geschlossenes System zu realisieren.
- Die Schnittstelle des PDP (Berechtigungsregel-Entscheidungsinstanz) zu den Portalen mit den digitalen Verwaltungsleistungen wird als hochskalierbare und hochverfügbare Komponente innerhalb des Autorisierungsmoduls implementiert.
- Die fachliche Kopplung der Verwaltungsportale (in der Rolle SAML Service Provider) mit dem Autorisierungsmodul basiert auf der AccountID aus der vom ELSTER-IdP ausgestellten SAML-Assertion. Im Falle von für die Portale pseudonymisierten IDs ist eine Depseudonymisierung, z.B. auf Basis eines verschlüsselten SAML-Attributs mit den depseudonymisierten IDs oder einer Depseudonymisierungsschnittstelle, vorzusehen.

Das Diagramm in Abbildung 20 zeigt die Grobarchitektur mit Fokus auf dem Zusammenspiel aller beteiligten Systeme, insbesondere dem ELSTER-IdP und den Verwaltungsportalen, die die digitalen Verwaltungsleistungen bereitstellen.

Gemäß Anforderungen ist die Nutzung des Autorisierungsmoduls durch die Verwaltungsportale optional. Nur Portale, die eine PEP-Komponente mit ihrer „Türsteher“-Funktion realisieren und mit dem Autorisierungsmodul interagieren, sind in diesem Zusammenhang betroffen. Die Entscheidung darüber obliegt der zuständigen Behörde für eine Verwaltungsleistung (Service Owner).

6.2.3.1 Vertrauensbeziehungen

Zwischen den Systemen ELSTER-IdP, Autorisierungsmodul und Verwaltungsportal bestehen transitive Vertrauensbeziehungen in einem Dreiecksverhältnis. Das Autorisierungsmodul nimmt genau wie alle Verwaltungsportale die Rolle eines SAML Service Provider ein – das bidirektionale Vertrauen basiert technisch auf dem Austausch der SAML-Metadaten und der Public-Key-Infrastruktur.

6.2.3.2 Integration der Rollen in SAML-Assertion

Aus mehreren Gründen wäre es vorteilhaft, wenn die Rollen eines Nutzers bezogen auf eine bestimmte digitale Verwaltungsleistung in die vom ELSTER-IdP ausgestellte SAML-Assertion im Rahmen der Nutzer-Authentifizierung bereits integriert werden. Rolleninhaberschaften könnten so in Form von SAML-Attributen bereits direkt zum Service Provider (Portal oder Dienstimplementierung) weitergereicht werden.

Erforderlich ist dazu eine Schnittstelle des Autorisierungsmoduls, die vom ELSTER-IdP im Zuge der Assertion-Ausstellung bedient wird. Nach erfolgreicher Authentifizierung des Nutzers übermittelt der IdP die AccountID sowie den URI der beabsichtigten Verwaltungsleistung (sofern im Authentisierungs-Request enthalten). Das Autorisierungsmodul liefert im Anschluss

genau die Rollen zurück, die in dem Kontext durch die entsprechenden Zugriffsregeln spezifiziert und dem Nutzer bzw. dessen Organisation auch zugeordnet sind (Schnittmengenbildung).

Dieses Muster ist im Kontext von Identity Providern durchaus üblich - das Autorisierungsmodul nimmt dabei gegenüber dem IdP die Rolle eines ergänzenden, vertrauenswürdigen „Attribute Providers“ ein. Diese Variante hinsichtlich der Kopplung von IdP und Autorisierungsmodul als Attribute Provider bietet u.a. folgende fachlich/technische Vorteile:

- Dadurch, dass eine Dienstimplementierung den Satz von Rollen direkt im Zugriff hätte, könnte die Applikation ergänzend zur Berechtigungsanfrage einfache Is-in-Role-Checks vornehmen, z.B. um ein UI-Element sichtbar oder unsichtbar zu schalten.
- Dienste, die einen abstrakten Verwaltungsleistungstyp mit Zugriffsregeln realisieren, aber selbst keinen PEP implementieren, können normalerweise nicht vom Organisationsadministrator differenziert für Mitarbeiter zugriffsbeschränkt werden. Mit einer Attribute-Provider-Kopplung könnte aber die SAML-Ausstellung vom IdP bereits verwehrt werden, sodass kein Zugriff für einen nicht-autorisierten Mitarbeiter möglich wäre.

Im Zuge der Feinkonzeption sollte eine Präzisierung dieses Ansatzes vorgenommen werden. Z.B. sind Aspekte zu Caching, synchron/asynchrones (reaktive) Schnittstellen-Design oder Standard- und Fehlerverhalten näher zu betrachten.

6.2.3.3 Innere Architektur und Technologie-Stack

Die konkrete Implementierungstechnologie und Bereitstellungsform ist unabhängig von dem grundsätzlichen Architekturentwurf. Allerdings wird davon ausgegangen, dass aufgrund der hohen Anforderung an Verfügbarkeit, Robustheit und Skalierung moderne Virtualisierungsformen der Bereitstellung (Container-Orchestrierung) Anwendung finden werden.

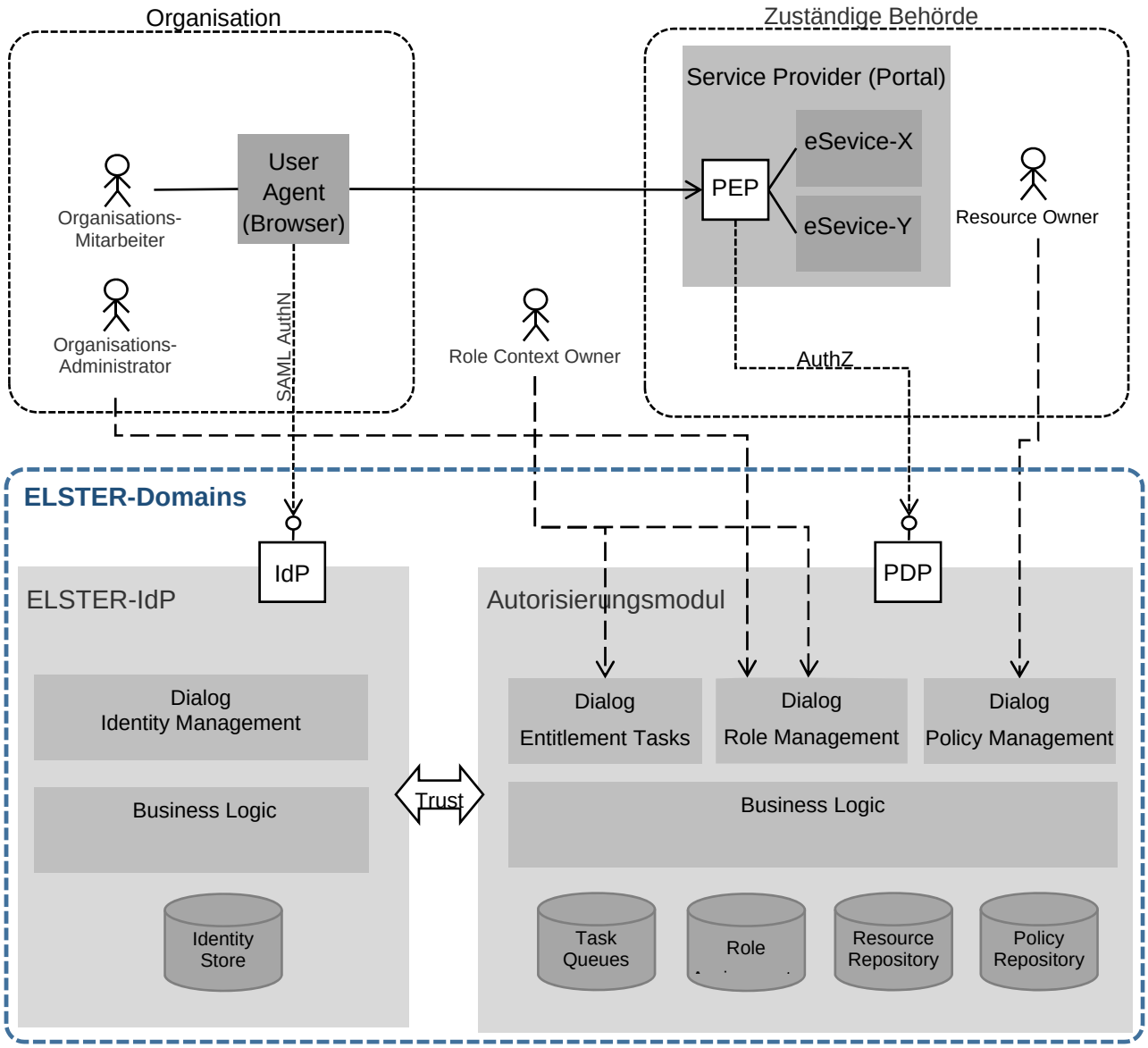

Abbildung 20: Architekturskizze zum Autorisierungsmodul und Einbettung ins Gesamtsystem

6.2.4 Schnittstellen

6.2.4.1 Autorisierungsmodul / ELSTER-IdP

- *SAML-Authentisierung der Web-Dialoge (obligatorisch)*
  Die Authentisierung an den Web-Dialogen des Autorisierungsmoduls erfolgt analog den anderen Verwaltungsportalen über die SAML-Schnittstelle (Web Browser SSO Profile) des ELSTER-IdP (NEZO-Schnittstelle).
- *Deprovisionierung (obligatorisch)*
  Die Deprovisionierung gelöschter ELSTER-Konten erfolgt über die bereits vorhandenen NEZO-Mechanismen von ELSTER (mittels SAML Name Identifier Management Protocol).
- *Attribute-Provider für Rollenverknüpfungen (optional)*
  Für die im Abschnitt 6.2.3.2 beschriebene Integration der Rollenzuordnungen in die SAML-Assertion fungiert das Autorisierungsmodul gegenüber dem ELSTER-IdP als so-

genannter Attribute Provider. Dazu stellt das Autorisierungsmodul eine Schnittstelle bereit, die dem IdP für einen authentifizierten Nutzer dessen aktuelle Rollenzuordnungen bezogen auf eine bestimmte Verwaltungsleistung übermittelt.

- *Pull-Schnittstelle für „Liste der Mitarbeiter einer Organisation“ (optional)*
  Für die Konfiguration der Berechtigungen der Mitarbeiter sowie das Gruppenmanagement sind dem Autorisierungsmodul die Nutzerkonten zu einer Organisation bekannt zu machen. Verschiedene Möglichkeiten bestehen, um dies zu erreichen. Denkbar ist eine Toolunterstützung für Organisationsadministratoren zum Versenden von Deeplinks an Mitarbeiter, um Referenzen auf Konten in das Autorisierungsmodul abzubilden.

  Aus Komfortgründen besser und für den lose gekoppelten Systemverbund aus IdP und Autorisierungsmodul angemessener wäre eine vom ELSTER-IdP bereitgestellte Schnittstelle, die dem Autorisierungsmodul eine Liste mit den Konten zu einer Organisation liefert. Eine mögliche Ausprägung wäre z.B. die standardisierte SCIM2-GetUsers-Schnittstelle.

6.2.4.2 Autorisierungsmodul / Service Provider (obligatorisch)

- *PDP-Schnittstelle*
  Die PDP-Maschinenschnittstelle, die von den PEP-Komponenten der Portale für die Autorisierungsentscheidung aufgerufen wird, wird sich nach gegenwärtiger Einschätzung an der aktuellen Version des „OASIS XACML REST Profil“ orientieren, wobei die Spezifikation zwecks Vereinfachung weiter einschränkend profiliert werden wird.

  Die Authentifizierung der PDP-Schnittstelle wird auf den vom ELSTER-IdP an das Verwaltungsportal herausgegebenen SAML-Assertions basieren. Nach gegenwärtigem Entwurfsstand erfolgt die Autorisierung an der PDP-Schnittstelle über OAuth2 mit SAML-Assertion (OAuth 2.0 SAML Bearer Assertion Flow).

6.3 Infrastruktur und Betriebsmodell

Das fachliche Modell hinter dem beschriebenen Architekturentwurf impliziert ein zentrales Betriebsmodell für das Autorisierungsmodul. Rollendefinitionen, Rollenzuordnungen sowie Zugriffsregeln sind Entitäten, für die eine zentrale Speicherung im hohen Maße angebracht, wenn nicht gar erforderlich ist. Das Autorisierungsmodul ist daher als zentral betriebenes System, das mit dem ELSTER-IdP über wenigen Schnittstellen lose gekoppelt ist, vorgesehen.

Die physische Lokalisierung des Systems ist eine betriebliche Frage, die von der eigentlichen Software-Architektur entkoppelt ist. Der Betrieb der Module kann innerhalb eines Rechenzentrums erfolgen oder in sicher vernetzten, verteilten Rechenzentren, wie es ja bereits im Consent-Verbund der Fall ist.

Obwohl durch den Architekturentwurf nicht zwingend vorgegeben, wird als Infrastruktur-Technologie eine zeitgemäße Container-Orchestrierung (Kubernetes-Cluster mit Docker-Containern) empfohlen. Diese Technologie bietet einerseits ein hohes Maß der Robustheit und Verfügbarkeit und gestattet andererseits eine flexible, bedarfsgerechte Skalierung der Systemressourcen.

7 Meilensteinplanung

Die Meilensteinplanung erfolgte auf Grundlage der vorhandenen Anforderungen und technischen Entwürfen. Im Rahmen der Umsetzung wird mit einer Feinkonzeptionsphase gestartet, die eine detaillierte technische Umsetzung sowie die Aufbereitung der Anforderungen umfasst. Parallel zur Feinkonzeption und Priorisierung der Anforderungen kann die Realisierung starten.

Es wird die Annahme getroffen, dass nach erfolgreichem IT-Planungsratsbeschluss eine Beauftragung erfolgt und die Arbeiten im August 2020 starten können.

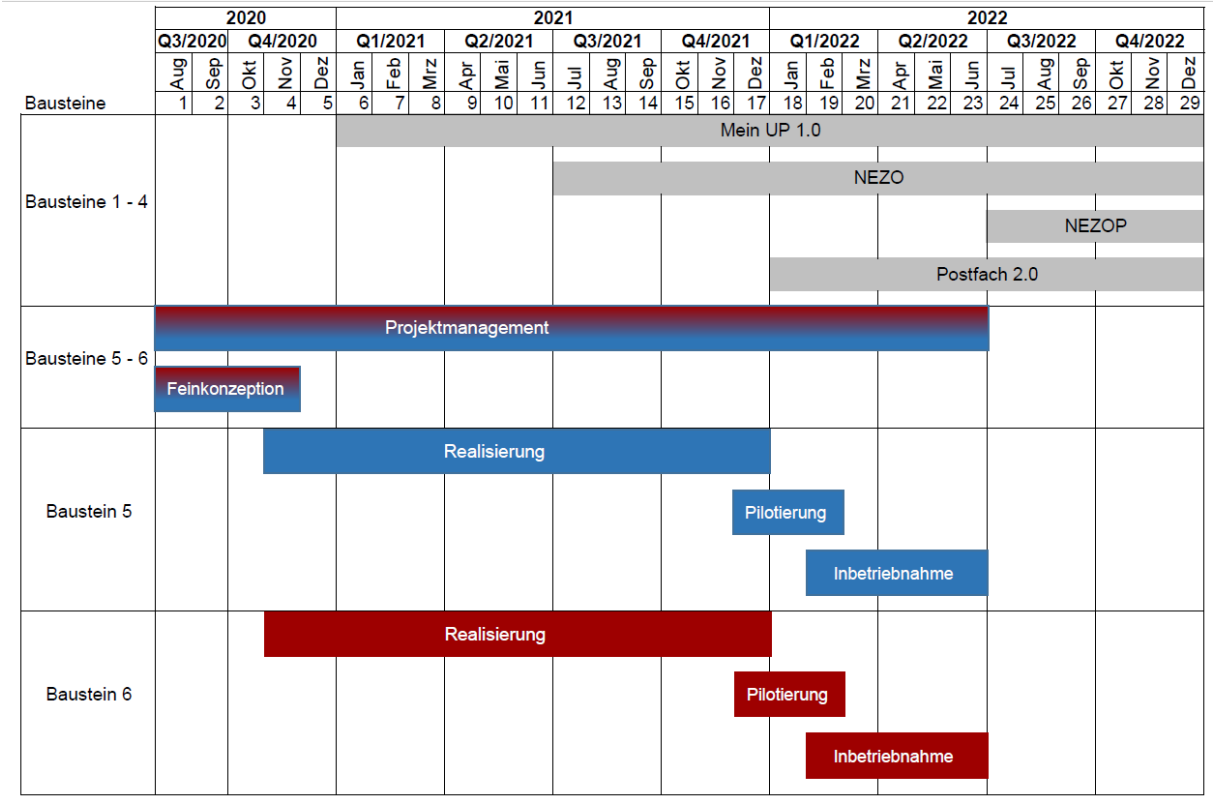

Abbildung 21: Grobe Meilensteinplanung für Module 5 und 6

8 Kostenschätzung

Grundlage der Schätzung sind die oben identifizierten Anforderungen bzw. Funktionen und designten Architekturskizzen.

Die Kosten für die beiden Module teilen sich in die Realisierungskosten und die Betriebskosten und werden im Folgenden dargestellt.

Zusätzlich zu diesen Kosten wird eine Vollzeitstelle bei dem Land Bremen i.H.v. circa 120.000 €/Jahr die übergreifende Koordination und Kommunikation übernehmen.

8.1 Modul 5 „OZG-PLUS-Postfach“

8.1.1 Realisierungsaufwand

Die folgende Tabelle zeigt die einzelnen Positionen der Kosten für die Realisierung des Bausteins 5:

Leistung	**Kosten**
Projektmanagement Stellvertretende Projektleitung	170.000 €
Feinkonzeption Detaillierte Konzeption der Anforderungen und Umsetzung	180.000 €
Realisierung Umsetzung inklusive Test	1.300.000 €
Pilotierung Pilotierung im kleineren Rahmen	130.000 €
Inbetriebnahme inklusive Abnahme durch den Auftraggeber	200.000 €
Summe	**1.980.000 €**

Tabelle 2: Kosten für die Realisierung Baustein 5

8.1.2 Betriebskosten

Der Schätzung der Betriebskosten liegen grob geschätzte Annahmen und Preise zugrunde und entsprechen einem zentralen Betrieb des Bausteins 5.

Leistung Modul 5	**Kosten**
Kubernetes Cluster Produktion inkl. techn. Betrieb Produktion mit hohem Schutzbedarf in einer Zone mit erweiterter Sicherheit	410.000 €
Kubernetes Cluster Qualitätssicherung inkl. techn. Betrieb QS mit normalen Schutzbedarf in einer Zone mit Standard-Sicherheit	160.000 €
Summe	**570.000 €**

Tabelle 3: Kosten für den Betrieb von Baustein 5

8.2 Modul 6 „Autorisierungsmodul“

8.2.1 Realisierungsaufwand

Die folgende Tabelle zeigt die einzelnen Positionen der Kosten für die Realisierung des Autorisierungsmoduls:

Leistung	**Kosten**
Projektmanagement Kontinuierliches Projektmanagement/Projektleitung	170.000 €
Feinkonzeption Detaillierte Konzeption der Anforderungen und Umsetzung	180.000 €
Realisierung Umsetzung inklusive Test	2.500.000 €
Pilotierung Pilotierung im kleineren Rahmen	130.000 €
Inbetriebnahme inklusive Abnahme durch den Auftraggeber	200.000 €
Summe	**3.180.000 €**

Tabelle 4: Kosten für die Realisierung Baustein 6

8.2.2 Betriebskosten

Der Schätzung der Betriebskosten liegen grob geschätzte Annahmen und Preise zugrunde und entsprechen einem zentralen Betrieb des Bausteins 6.

Leistung Modul 6	**Kosten**
Kubernetes Cluster Produktion inkl. techn. Betrieb Produktion mit hohem Schutzbedarf in einer Zone mit erweiterter Sicherheit	330.000 €
Kubernetes Cluster Qualitätssicherung inkl. techn. Betrieb QS mit normalen Schutzbedarf in einer Zone mit Standard-Sicherheit	140.000 €
Summe	**470.000 €**

Tabelle 5: Kosten für den Betrieb von Baustein 6

8.3 Weiterentwicklung der Module

Für die Weiterentwicklung der Module wird ein Change Prozess für neue Anforderungen eingerichtet. Sind Erweiterungen bzw. Änderungen an den Modulen erwünscht, muss ein Einsteuern dieser über einen strukturierten Change Request erfolgen. Dieser Change Request wird in einem festgelegten Prozess bewertet und priorisiert.

9 Prämisse

Es wird davon ausgegangen, dass die Gesetzesänderung der AO und des OZGs Erfolg hat.

10 Organisationsstruktur des Steuerungsprojektes und Anforderungsmanagement in der Betriebsphase

Vorbehaltlich einer Beauftragung Bremens, soll das Anforderungsmanagement für die Bausteine 5 und 6 in der Betriebsphase wie folgt gestaltet sein:

Unter Federführung Bremens werden die Anforderungen zur Weiterentwicklung für die Bausteine 5 und 6 unter Einbindung von Bund und Ländern erhoben und definiert.

Geplant ist hierfür ebenfalls eine Beiratsfunktion aus Wirtschaft und Verwaltung, im Sinne von „users first“. Gespräche mit möglichen Teilnehmern sind bereits geführt worden.

Die mögliche Organisationsstruktur des gesamten Steuerungsprojektes Bausteine 1 bis 6 wurde bereits im Basiskonzept Einheitliches Unternehmenskonto beschrieben. Auf dieser Basis wird nach Beauftragung der Umsetzung der Bausteine 5 und 6 eine finale Organisationsstruktur zwischen Bremen und Bayern abgestimmt.

11 Glossar

Begriff	Erläuterung
ABAC	*Attribute-Based Access Control*, abstraktes Modell zur attributbasierten Zugriffskontrolle
Anbieter digitaler Verwaltungsleistung	Unter einem Anbieter für eine digitale Verwaltungsleistung wird meist eine Behörde verstanden, die eine ihrer Leistungen, den Nutzern online zur Verfügung stellt.
AS4	*Applicability Statement 4* ist eine von der Organization for the Advancement of Structured Information Standards (OASIS) entwickelte Schnittstelle, die sich insbesondere für den Austausch von elektronischen Daten im Business-to-Business-Bereich (B2B) eignet.
Bauleitplanung	Planungswerkzeug zur Lenkung und Ordnung der städtebaulichen Entwicklung einer Gemeinde.[8]
BOB-SH	Das Projekt *Bauleitplanung Online-Beteiligung für Schleswig-Holstein* steht allen Kommunen zur Verfügung, um die Beteiligung in der Bauleitplanung komplett medienbruchfrei im Internet durchzuführen.
Business to Government	Beschreibt die Beziehungen und Transaktionen zwischen Unternehmen und der Verwaltung.
Change Request	Ein Change Request bezeichnet eine Änderungsanfrage. Hier ist ein Änderungsauftrag an einem bestehenden Produkt gemeint, welches in einem strukturierten Prozess bewertet und priorisiert wird.
COVID-19	*Corona Virus Disease 2019* - bezeichnet die Erkrankung, die durch SARS-CoV-2 ausgelöst wird.[9]
DEHSt	Die *Deutsche Emissionshandelsstelle* ist beim Bundesamt für Umwelt angesiedelt und zuständig für den Handel mit Zertifikaten für den Ausstoß des klimaschädlichen Kohlendioxids. https://www.dehst.de/DE/startseite/startseite-node.html
Digitale Verwaltungsleistung	Eine Digitale Verwaltungsleistung ist eine online angebotene Leistung der Verwaltung zur ort- und zeitunabhängigen Nutzung durch die Bürger und Organisationen. Diese Leistungen können reine Antragsformulare sein. In den meisten Fällen sind diese Leistungen komplexer und nicht mehr in Anträgen darstellbar.
Einheitliches Unternehmenskonto	Unter dem Begriff Einheitliches Unternehmenskonto wird ein Angebot eines Nutzerkontos für Organisationen (Unternehmen, Vereine, Stiftungen, Behörden) verstanden, welches die Bausteine 1-6 umfasst.

[8] https://de.wikipedia.org/wiki/Bauleitplanung

[9] https://www.bundesregierung.de/breg-de/themen/coronavirus/informationen-zum-coronavirus-1734932

ELSTER-Transfer	ELSTER-Verfahren, das für den sicheren Datenaustausch zwischen der Steuerverwaltung und zum Beispiel Kommunen verantwortlich ist. Die Nutzer von ELSTER-Transfer sind derzeit hauptsächlich Kommunen, Kammern, Universitäten, Versicherungen, Banken, Anstalten, Dienstleister, Verbände oder Behörden. Bei ELSTER-Transfer handelt es sich um eine etablierte, aber proprietäre Lösung zum Datenaustausch mit der Steuerverwaltung.
ERiC	Der *Elster Rich Client* stellt Softwareentwicklern eine C-Schnittstellenbibliothek für den ELSTER-Zugriff durch Drittanbieter-Steueranwendungen zur Verfügung.
FIM	*Föderales Informationsmanagement*, Steuerungsprojekt des IT-Planungsrats
FSFE	Die *Free Software Foundation Europe* ist eine gemeinnützige, regierungsunabhängige Organisation, die sich seit 2001 für die Belange freier Software einsetzt.
Governikus	Mit der Anwendung *Governikus des IT-Planungsrates* stehen Bund, Ländern und Kommunen wichtige Bausteine und Basiskomponenten für Digitalisierungsvorhaben im gesamten Lebenszyklus elektronischer Kommunikation, Dokumente und Daten zur Verfügung. Das Leistungsspektrum der Anwendung Governikus wurde im Laufe der Jahre erheblich erweitert. Ursprünglich als Middleware für die Datenübermittlung auf Basis des OSCI-Transportprotokolls konzipiert, bei dem bereits Signaturen und Kryptografie sowie die Authentisierung eine große Rolle spielten, enthält die Anwendung inzwischen Produkte und Funktionsmodule für die Handlungsfelder eID, sichere Datenübermittlung, Ver- und Entschlüsselung, elektronische Signaturen und Siegel und deren Verifikation sowie TR-ESOR-konforme Beweiswerterhaltung.
Kubernetes	Eine ursprünglich von Google entwickelte Open-Source-Plattform zur Orchestrierung von Containern. Sie gestattet das automatisierte Einrichten, Skalieren, Betreiben und Warten containerisierter Anwendungen und unterstützt Container-Engines, wie Docker, und zahlreiche Cloud-Computing-Plattformen.
LeiKa	Der *Leistungskatalog der öffentlichen Verwaltung* verzeichnet alle in Deutschland durch die öffentliche Verwaltung (in sämtlichen Ebenen) angebotenen Verwaltungsleistungen und liefert dazu einheitliche Beschreibungen.
OASIS	*Organization for the Advancement of Structured Information Standards*, technisches Komitee für Kommunikationsdienste, welches u.a. AS4 entwickelte.
OAuth2	*Open Authorization 2.0, offener Protokollstandard für API-Autorisierung*

OSCI	*Online Services Computer Interface* ist ein im Auftrag der öffentlichen Verwaltung unter Beteiligung von Partnern aus Verwaltung und Industrie entwickelter Protokollstandard für die sichere, vertrauliche und rechtsverbindliche Übertragung elektronischer Daten im E-Government. OSCI gewährleistet dabei die klassischen Schutzziele Integrität, Authentizität, Vertraulichkeit und Nachvollziehbarkeit und kommt häufig in unsicheren Netzen zum Einsatz, etwa dem Internet, bietet aber durch seine ergänzenden Funktionen auch in sicheren Netzen Vorteile und sorgt insbesondere für Verbesserungen in der Interoperabilität. OSCI bildet inzwischen die technische Basis für E-Government in Deutschland.
OZG	Das *Online-Zugangsgesetz* des Bundes verpflichtet die öffentliche Verwaltung von Bund und Ländern, ihre Dienstleistungen bis spätestens 2022 über Verwaltungsportale elektronisch anzubieten.
PDP	Policy Decision Point
PEP	Policy Enforcement Point
PEPPOL	Im Rahmen des EU-Projekts *Pan-European Public Procurement On-Line* wurde ein Standard für grenzüberschreitende öffentliche Beschaffungsverfahren innerhalb der Europäischen Union erarbeitet. Viele europäische Länder haben PEPPOL inzwischen als Standard für die Realisierung von eRechnung implementiert.
RBAC	*Role-Based Access Control*, abstraktes Modell zur rollenbasierten Zugriffskontrolle
SAML	Security Assertion Markup Language
Servicekonto	Nutzerkonto im Sinne des OZG
SML	*Service Metadata Locator* is a component of CEF eDelivery that is responsible for Dynamic Service Location: in order to send a message, the Access Point of a Sending Party needs to discover where the information about a Receiving Party is stored. The Service Metadata Locator (SML) serves this purpose, and guides the Access Point of the Sending Party towards this location, which is called the Service Metadata Publisher (SMP).In other words, the SML is used to retrieve/add/update/delete information about the Receiving parties and SMPs location on a Domain Name System (DNS). The SML is a centralised component.
SMP	*Service Metadata Publisher* is a component of CEF eDelivery that is responsible for Capability Lookup: once the Access Point of the Sending Party discovered the address of the Receiving Party's SMP (Service Metadata Publisher), it is able to retrieve the required information to interoperate with the Receiving Party (i.e. metadata). SMP are registers of the message exchange capabilities and location of parties (i.e. metadata). SMP's are usually used in a distributed way.
TöB	Träger öffentlicher Belange
VEMAGS	Das *VErfahrensMAnagement für Großraum- und Schwertransporte* ist ein internetbasiertes Online-Genehmigungsverfahren für Großraum- und Schwertransporte der 16 Bundesländer und des Bundes.

Vertretung	In diesem Prüfauftrag werden im Wesentlichen drei Arten von Vertretung unterschieden. Das erste ist die Abwesenheitsvertretung und ist gekennzeichnet durch eine zeitlich begrenzte Vertretung innerhalb einer Organisation (üblicherweise Urlaub, Krankheit, etc.). Die zweite Art der Vertretung entsteht durch das Ableben oder das unerwartetes Ausscheiden einer Person innerhalb einer Organisation und ist gekennzeichnet durch eine zumeist ungeplante, nicht begrenzte Vertretung bzw. Übernahme der Rolle/Rechte/Aufgaben. Davon zu unterscheiden ist die dritte Art der Vertretung, die sogenannte Unternehmensvertretung durch eine andere Person oder Organisation außerhalb der zu vertretenden Organisation (üblicherweise durch Steuerberater, Notare, Insolvenzverwalter etc.).
XACML	*eXtensible Access Control Markup Language*, OASIS-Standard zu Darstellung und Verarbeitung von Autorisierungs-Policies
XÖV	Der Standard *XML in der öffentlichen Verwaltung* dient dem elektronischen Datenaustausch auf Basis von XML und SOAP. XÖV wird durch die Koordinierungsstelle für IT-Standards (KoSIT) betreut und hat sich zum Protokollstandard für das deutsche E-Government entwickelt. XÖV gewährleistet Integrität, Authentizität, Vertraulichkeit und Nachvollziehbarkeit und schafft damit die Grundlagen für Interoperabilität.
XTA	*XÖV Transport Adapter* ist ein vom IT-Planungsrat empfohlener, fachunabhängiger Interoperabilitätsstandard, der Webservices für die Anbindung von IT-Fachapplikationen an eine technische Infrastruktur für Nachrichtenübermittlung (Transportverfahren) definiert. Ergänzend bietet XTA Definitionen für Struktur und Semantik in Form von sog. „Service Profilen“ an, mit denen eine Fachlichkeit die durch sie geforderten Service-Qualitäten für die Nachrichten- und Datenübermittlung vorgeben kann.
ZKS-Abfall	Über die *Zentrale Koordinierungsstelle Abfall* wird bundesweit der Datenverkehr zu Entsorgungsnachweisen und Begleitscheinen gemäß elektronischem Abfallnachweisverfahren zwischen Wirtschaft und Behörden geführt.

12 Abbildungsverzeichnis

13 Tabellenverzeichnis