IT-PLANUNGSRAT

25.09.2026

Föderale Zielarchitektur für Postfach- und Kommunikationslösungen

Zielarchitektur (Version 1.1)

Bauplan einer modernen Kommunikationsinfrastruktur für Privatpersonen, private Organisationen und öffentliche Stellen

Die vorliegende Zielarchitektur Version 1.1 wurde unter Berücksichtigung des bislang eingegangenen Feedbacks erstellt. Da einzelne Abstimmungen weiterhin stattfinden, können sich im weiteren Verlauf noch vereinzelt Anpassungen an den dargestellten Inhalten ergeben.

Titel	Dokumentenart	Inhalt
Überblick und Handlungsempfehlungen	Klammerdokument	Übergreifende Zusammenfassung des Vorhabens und Darstellung strategischer Implikationen
Zielarchitektur (Version 1.1)	**Begleitdokument**	**Fortschreibung der auf die Ziele des Vorhabens ausgerichteten Zielarchitektur**
Übergreifende Transitionsstrategie	Begleitdokument	Transitionsstrategie zur schrittweisen Überführung bestehender Postfachlösungen in die ZaPuK-Infrastruktur
Rechtsgutachten	Begleitdokument	Prüfung der rechtlichen Rahmenbedingungen sowie Ableitung von Handlungsempfehlungen für die Umsetzung

Nutzungsbedingungen

Die Inhalte dieses Dokumentes unterliegen der Creative Commons Namensnennung 4.0 International Public License (CC BY 4.0).

Inhaltsverzeichnis

1 Einleitung 5
1.1 Umfang, Geltungsbereich und Abgrenzung 7
1.2 Methodisches Vorgehen bei der Architekturentwicklung 8
2 Strategische Positionierung und Einordnung 11
2.1 Zielbild 11
2.2 Architekturziele 11
2.3 Architekturprinzipien 12
2.4 Einordnung in das Ökosystem der Deutschland-Architektur sowie des D-Stacks 14
2.5 Einordnung in das Ökosystem des Matrix-Standards 17
3 Geschäftsarchitektur 19
4 Zielbild für Entwicklung, Betrieb und Governance 20
4.1 Zentrale Softwareentwicklung 21
4.1.1 Backend-Komponenten 21
4.1.2 Frontend: Zentraler Postfach-Zugang für Privatpersonen und Organisationen 23
4.1.3 Softwareentwicklung von Umsystemen und Lösungen Dritter 25
4.1.4 Allgemeine Festlegungen zur Softwareentwicklung 26
4.2 Zentraler Betrieb 27
4.2.1 Entscheidungstreiber 27
4.2.2 Überblick 28
4.2.3 Backend-Komponenten 29
4.2.4 Frontend: Zentraler Postfach-Zugang für Privatpersonen und Organisationen 37
4.3 Governance des ZaPuK-Kommunikationsverbunds 38
5 IT-Architektur 41
5.1 Überblick und Architekturmodell 41
5.2 Applikationssicht 44
5.2.1 Infrastrukturnutzende Systeme 46
5.2.2 Kerninfrastruktur 47
5.2.3 Unterstützende externe Systeme 54
5.3 Informationssicht 55

5.4 Architekturentscheidungen 56
5.4.1 Infrastrukturtopologie und Betriebsmodelle 58
5.4.2 Postfächer und Postfachzugänge 59
5.4.3 Funktionspostfächer und Vorgangsräume 60
5.4.4 Kommunikations- und Verschlüsselungsschicht 64
5.4.5 Authentisierung und Autorisierung 65
5.4.6 Adressierung und Adressverzeichnis 67
5.4.7 Interoperabilität 69
5.4.8 Verhältnis zu angrenzenden nationalen und EU-Vorhaben 70
5.4.9 Anschlussbedingungen und Föderationskontrolle 72
5.4.10 Malware-Prüfung unter Ende-zu-Ende-Verschlüsselung 73
5.4.11 Metadatenreduktion 74
5.4.12 Nichtabstreitbarkeit und Abstreitbarkeit 75
5.4.13 Schlüsselwiederherstellung 77
5.4.14 Archivierung unter Ende-zu-Ende-Verschlüsselung 77
5.5 Zusammenwirken der Komponenten 78
5.5.1 Adressierung von Organisationen und Berufsträgern 78
5.5.2 Adressierung von Privatpersonen 79
5.5.3 Automatisierte Nachrichteneinlieferung (M2M) 81
5.5.4 Beweissichere Übermittlung 81
5.5.5 Funktionspostfach und Vorgangsraum 83
5.6 Zentrale vs. dezentrale Betriebsmodelle für Organisationen 84
Glossar 89
Abbildungsverzeichnis 90
Tabellenverzeichnis 91
Abkürzungsverzeichnis 92

1 Einleitung

Dieses Dokument beschreibt die föderale **Zielarchitektur Postfach- und Kommunikationslösungen (ZaPuK)** in Version 1.1. Die ZaPuK ist eine moderne, modulare und föderierte Client-Server-Architektur zur sicheren, Ende-zu-Ende-verschlüsselten (E2EE) Kommunikation zwischen Privatpersonen, privaten Organisationen und öffentlichen Stellen, mit moderner User-Experience, in Echtzeit und nativer Anwendbarkeit auf mobilen Endgeräten. Sie setzt dabei konform zum Deutschland-Stack (D-Stack)[1] auf offene Standards wie das REST-basierte offene Matrix-Protokoll in Kombination mit IPv6 und HTTPS/TLS 1.3 für die Transport- und Kommunikationsschicht, verfolgt einen Zero-Trust-Ansatz und integriert zentrale sowie dezentrale Backend- und Client-Komponenten. Die Zielarchitektur realisiert eine konsolidierte, interoperable, hochsichere Kommunikationsinfrastruktur mit als Teil des D-Stacks zentral bereitgestellten Postfachzugängen und -Backends, unterstützt aber auch den Betrieb eigener Systeme durch Dritte. Privatpersonen authentifizieren sich im System über BundID mit der eID als Identifizierungsmittel, ergänzt um die European Digital Identity (EUDI)-Wallet. Für Organisationen erfolgt die Authentifizierung über das Organisationskonto („Mein Unternehmenskonto MUK“) und perspektivisch die European Business Wallet.

Phase I (2024-2025) lieferte Version 1.0 dieser Architektur und konsolidierte bestehende Anforderungen an das Gesamtsystem. Um die Zielarchitektur umzusetzen und für bestehende Systeme integrierbar zu machen, ist es erforderlich, komplexe Anforderungen wie Vollmachten, Adressbücher und Mehrnutzer:innenkommunikation für private Organisationen und öffentliche Stellen zu konkretisieren und auszuarbeiten. Dieses Dokument schreibt daher die Zielarchitektur aus Phase I fort, legt für bundesweit zentral bereitgestellte Komponenten ein Zielbild für Bebauung und Verantwortlichkeiten vor und konkretisiert die Umsetzung von Anforderungen sowohl an die Zielarchitektur als auch an die Systemgrenzen (föderale IT-Architektur sowie D-Stack). Das vorliegende Konzept beschreibt eine Zielarchitektur, also den mittelfristig anzustrebenden Zielzustand der Architektur von Postfach- und Kommunikationssystemen öffentlicher Stellen in Deutschland. Sie erhebt daher keinen Anspruch auf eine eigenständige Implementierbarkeit, sondern erfordert die Existenz von Umsystemen und vorbestehenden Infrastrukturen.

[1] vgl. Standards des Deutschland-Stack gemäß Beschluss des IT-Planungsrates, B-2026/03-IT

Die in diesem Dokument beschriebene Zielarchitektur ist die Grundlage für die in Phase II durchgeführten Planungen zur Transition wesentlicher Bestandslösungen sowie weiterer als Grundlage für die Umsetzung geschaffener Artefakte[2]. Die Entwicklung einer dedizierten Lösungs- und Softwarearchitektur je betroffenem Bestandspostfach ist Bestandteil der Programmphase III im Rahmen der Umsetzung der Transition. Daher werden hier nur lösungsarchitektonische Detailfragen von lösungsübergreifender Relevanz betrachtet. Lösungsspezifische Fragen werden gegebenenfalls umrissen und für die weitere Bearbeitung festgehalten. Die Hoheit über die Lösungsarchitekturen betroffener Systeme obliegt den jeweils zuständigen Stellen und wird im Rahmen der Programmphase III basierend auf den Vorgaben der Zielarchitektur sowie der in Phase II definierten Transitionsplanungen angepasst. Im Rahmen der technischen Validierung der ZaPuK im Vorhaben „Neo“ (Vorhaben „Pilotierung Matrix-basierter Kommunikationskanal für die G2C-Kommunikation“ des Föderalen IT-Architekturboards) wurden parallel zur Programmphase II Softwareartefakte und Lösungsarchitekturen entwickelt, die für die weitere Produktisierung von ZaPuK als Grundlagen genutzt werden können.

Dieses Dokument richtet sich vornehmlich an IT-Architekt:innen in Bund und Ländern sowie die produktverantwortlichen Architekt:innen bestehender und etwaiger zukünftiger Postfachlösungen, da hier die konkrete lösungsarchitektonische Ausgestaltung sowie die Bebauung der IT-Landschaft im Zielzustand im Vordergrund stehen. Für Entscheider:innen werden die übergeordneten Folgen und strategischen Handlungsempfehlungen in einem gesonderten Dokument (Management Summary) dargelegt.

Im weiteren Verlauf von Kapitel 1 wird zunächst auf die Methodik der Fortschreibung der Zielarchitektur hin zur vorliegenden Version 1.1 eingegangen. Kapitel 2 nimmt eine strategische Positionierung der ZaPuK vor, inklusive ihrer Wirkungsziele und einer Einordnung in D-Stack und Deutschland-Architektur. Im Kapitel 3 wird auf die Geschäftsarchitektur aus der vorangegangenen Version dieses Dokumentes verwiesen. In Kapitel 4 werden die Eckpunkte der Zielbebauung beschrieben, darunter Empfehlungen zu Rollen und Verantwortlichkeiten in der Realisierung zentral bereitgestellter Komponenten. Die IT-Architektur in Kapitel 5 beschreibt die angestrebte Architektur im engeren Sinne inklusive verschiedener Sichten zur technischen Ausgestaltung und einer Zusammenfassung der getroffenen Architekturent-

[2] insb. Rechtsgutachten, Konzeption zur Governance, Finanzierungskonzept

scheidungen. Kapitel 5 stellt das Kernstück und die wesentliche Erweiterung des Konzepts gegenüber der Version 1.0 dar.

Redaktioneller Hinweis: Die Fassung von Version 1.1 dieses Architekturkonzeptes als PDF dient insbesondere der Unterstützung der politischen Willensbildung in Bund und Ländern. Die Veröffentlichung aller relevanten Artefakte inklusive Konzepte, Architekturentscheidungen und Anforderungen, erfolgt unter kontrollierter Versionierung auf openCode.

1.1 Umfang, Geltungsbereich und Abgrenzung

Die Zielarchitektur bezieht sich auf Postfachsysteme und alle konzeptionell verwandten Kommunikationslösungen (z. B. Messenger-Dienste) zur bidirektionalen Abwicklung von anlassbezogenem elektronischem Schriftverkehr mit öffentlichen Stellen im Sinne einer meist natürlichsprachlichen Kommunikation, welche um etwaige Anhänge ergänzt werden kann. Dies geschieht sowohl asynchron als auch in Echtzeit. Diese Kommunikation erfolgt dabei mit Bezug zu je einem konkreten Anlass oder Anliegen zwischen beteiligten Privatpersonen und privaten Organisationen einerseits sowie zuständigen öffentlichen Stellen, beispielsweise Statusupdates, Rückfragen, Nachforderungen oder Ad-hoc-Nachrichtenaustausch im Zuge von Verwaltungs- oder Gerichtsverfahren. Die Kommunikation erfolgt mittels fachspezifischer IT-Lösungen (z. B. Fachverfahrensanwendungen, Unternehmensanwendungen) und Anwendungen in generischen Ausführungsumgebungen, wie Webbrowsern und Smartphones. Der Geltungsbereich und die Abgrenzung der ZaPuK bleiben gegenüber Version 1.0 dieses Dokuments in ihren Grundzügen unverändert.

Ein Kommunikationsszenario ist durch das Paar von Absender:innen und Empfänger:innen definiert, wobei Absender:innen vorn und die Empfänger:innen hinten genannt werden. Die Zielarchitektur wird für die folgenden Kommunikationsszenarien entworfen:

- C2G – Privatperson zu öffentlicher Stelle: Privatperson kann Konversation initiieren und auf Nachrichten antworten
- G2C – öffentliche Stelle zu Privatperson: Proaktive Verwaltungsleistung und Antwort auf Anträge und Nachrichten von Privatpersonen.
- B2G – private Organisation zu öffentlicher Stelle: Analog zu C2G
- G2B – öffentliche Stelle zu privater Organisation: Analog zu G2C
- G2G – zwischen öffentlichen Stellen

Das Kommunikationssystem fokussiert sich auf den Nachrichtenaustausch zwischen Postfächern, bei dem mindestens ein:e menschliche:r Postfachnutzer:in direkt Zugriff auf ein Post-

fach hat. Der Schwerpunkt der hier beschriebenen Architekturplanung liegt weiterhin auf Kommunikationsszenarien zwischen öffentlichen Stellen und Privatpersonen (G2C, C2G) sowie privaten Organisationen (G2B, B2G). Die Kommunikation zwischen öffentlichen Stellen (G2G) ist grundsätzlich abbildbar, dedizierte Anforderungen und Anwendungsfälle hierzu sollten aber zu einem späteren Zeitpunkt integriert werden, wenn auch hier eine Transition konkret geplant werden sollte.

Bestehende Infrastrukturen zur ausschließlichen Übermittlung strukturierter, für die automatisierte Verarbeitung intendierter Daten (M2M-Kommunikation) sind nicht Betrachtungsgegenstand. Automatisierter Datenaustausch weist jedoch ähnliche Anforderungen und Abläufe auf und könnte in zukünftigen Ausbaustufen höchstwahrscheinlich ebenfalls durch die in Kapitel 5 beschriebene IT-Architektur oder eine weiterentwickelte Fassung derselben einheitlich realisiert werden. Funktional übertragbar wären dabei Transport, Ende-zu-Ende-Verschlüsselung, Adressierung und Nachweise, nicht die fachlichen Datenformate. Entsprechende Ausführungen sind nicht Teil dieses Dokuments.

Mit Beschluss B-2026/03-IT[3] wurde die ZaPuK in das initiale Portfolio des D-Stacks aufgenommen. Sie bietet somit die architektonische Grundlage für dessen Basisdienst ‚Postfach' sowie die Ausgestaltung des Funktionsbausteins ‚*Postfach und Interaktion*' in der Deutschland-Architektur. Neu gegenüber der Vorfassung 1.0 wird in dieser Version der ZaPuK daher im Rahmen der verfügbaren Informationslage (Stand September 2026) konkreter auf die Integration sowie Abgrenzung in Querschnitts- und Basiskomponenten des *D-Stacks* insbesondere zu den durch die *Deutschland-Architektur* definierten Funktionsbausteinen *Authentifizierung* und *Datenaustausch* eingegangen.

1.2 Methodisches Vorgehen bei der Architekturentwicklung

Das methodische Vorgehen der Ent- und Weiterentwicklung der ZaPuK in den Phasen I und II folgt den Prinzipien einer TOGAF-basierten Architekturentwicklung (TOGAF-ADM). Bausteine der Architektur werden als Komponenten mit ihren Verantwortlichkeiten, Schnittstellen und Limitationen beschrieben. Auf eine separate Unterscheidung in Architecture Building Blocks (ABB) und Solution Building Blocks (SBB) wird in der IT-Architektur in Version 1.1 verzichtet, da die wesentlichen Technologieentscheidungen, unter anderem der Einsatz des Matrix-Standards als Kommunikationsschicht, bereits in Phase I getroffen und dokumentiert wurden (vgl. ADR-0011). Die aufbauende Beschreibung der ZaPuK auf lösungsarchitektonischer Abs-

[3] https://www.it-planungsrat.de/beschluss/b-2026-03-it

traktionsebene wurde durch einschlägige Stakeholder explizit als Grundlage der Transitionsplanungen gewünscht.

Architekturentscheidungen wurden in Form von Architecture Decision Records (ADR) vorbereitet und dokumentiert – eine in der Beschreibung von Lösungsarchitekturen verbreitete Art formeller und einheitlich strukturierter Textdokumente, in denen Architekturentscheidungen atomar und nachvollziehbar erörtert, dokumentiert und versioniert werden können. Diese ADRs stellen in der Informationssysteme-Architektur der Zielarchitektur die einzige Quelle der Wahrheit dar. Jeder ADR beschreibt dabei den Problemraum für ein Handlungsfeld oder einen Ausschnitt daraus, stellt verschiedene Lösungsoptionen gegenüber und wählt eine davon auf der Grundlage objektiv nachvollziehbarer Kriterien und Argumente aus. Dabei werden sowohl funktionale Kriterien (funktionale Eignung) als auch nichtfunktionale Kriterien (Zukunftssicherheit, Marktrelevanz, Einfachheit usw.) holistisch bewertet und abgewogen. Ziel dieses Vorgehens ist es, rationale Entscheidungen zu fördern und subjektive Einflüsse, z. B. persönliche Präferenzen der Beteiligten, einzuschränken (präskriptive Entscheidungstheorie). Durch die strukturierte Dokumentationsform von ADRs können Architekturentscheidungen nachvollziehbar gemacht und im Falle geänderter Rahmenbedingungen leichter überprüft und nachjustiert werden.

In regelmäßigen Arbeitsgruppensitzungen (FIT-AG) unter Schirmherrschaft des föderalen IT-Architekturboards (FIT-AB) mit Vertreter:innen von Bestandslösungen und Fachexpert:innen aus dem Architekturmanagement der Länder wurden zu den offenen Architekturfragen aus Phase I sowie zu den gemeinsam identifizierten weiteren Handlungsfeldern Bedarfe erhoben und in die Architekturarbeit integriert. Entwürfe einschlägiger Architekturentscheidungen auf der Abstraktionsebene einer Zielarchitektur wurden in zweiwöchentlichen Arbeitssitzungen gemeinsam erörtert und auf Grundlage des ergangenen Feedbacks verfeinert. Auf Basis dieses Inputs wurde eine Reihe neuer ADRs formuliert, die anschließend entsprechend ihres Reifegrades sowohl mit der FIT-AG als auch der Fachöffentlichkeit auf openCode in einem strukturierten Prozess konsultiert wurden. Dieses Vorgehen stellt eine frühzeitige und intensive Einbindung von Bedarfsträgern und Bestandssystemen bei der Weiterentwicklung der Architektur sicher.

Neben der Befassung der Architekt:innen und der Arbeitsgruppe mit atomaren Architekturfragen wurden zu verschiedenen Artefakten formelle Konsultationen durchgeführt. Initial wurde zwischen Januar und März 2026 eine öffentliche Konsultation auf openCode zu den Ergebnisartefakten von Phase I durchgeführt. Ein Entwurf des Architekturkonzepts in Version

1.1 wurde zudem im Sommer 2026 zur Kommentierung an wesentliche Bestandslösungen, die zuständigen Architekt:innen des D-Stacks sowie das föderale IT-Architekturboard verteilt. Eingegangenes Feedback wurde gesichtet und eingearbeitet.
Die Anforderungen an die Zielarchitektur wurden in Phase I aus den Dokumentationen der Bestandslösungen und Interviews mit Betreibern und Fachexpert:innen erhoben, mit Bund und Ländern qualitätsgesichert und auf openCode öffentlich konsultiert. Architekturrelevante Anforderungen sind in allen Phasen in die Ausgestaltung der ZaPuK eingeflossen (vgl. ADRs). Das im Neo-Vorhaben entwickelte zentrale Postfach-Frontend wurde durch dieses zudem in Nutzendentests verprobt.

2 Strategische Positionierung und Einordnung

Dieser Abschnitt beleuchtet das strategische Zielbild, das der Zielarchitektur zugrunde liegt, und geht auf die Wirkungsziele des Vorhabens ein.
Zu den Rahmenbedingungen der Architekturentwicklung wird auf die zu Phase I unveränderten Architekturprinzipien sowie die Einordnung in die D-Architektur eingegangen. Neu in Phase II ist die Einordnung in den durch D-Architektur und D-Stack vorgegebenen Gesamtrahmen.

2.1 Zielbild

Das Zielbild bleibt gegenüber Version 1.0 dieses Dokuments unverändert und beschreibt eine einheitliche föderale Kommunikationsinfrastruktur, über die Privatpersonen, Organisationen und öffentliche Stellen sicher und vertraulich kommunizieren. Basis sind offene Standards und eine durchgängige Ende-zu-Ende-Verschlüsselung. Die wichtigen Bestandteile wie Postfach-Backends können zentral oder dezentral betrieben sein.[4] Die langfristige Strategie verfolgt die Zusammenführung jeglicher anlassbezogenen Kommunikation mit dem Staat in der ZaPuK-Infrastruktur über alle Verwaltungsbereiche hinweg.

2.2 Architekturziele

Ausgehend von identifizierten Handlungsbedarfen im Status quo der föderalen IT-Landschaft (vgl. Beschluss B-2024/28-IT des IT-Planungsrates) soll die ZaPuK primär die in Tabelle 1 dargestellten Architekturziele realisieren.

Ziel	Implikationen für die Architektur
Hürden für den Anschluss abbauen	• Jede:r Nutzer:in muss sich über Fachlichkeiten und föderale Ebenen hinweg nur an eine Lösung anschließen • Nutzung offener, webbasierter Standards bei der Standardisierung der Schnittstellen • Unterstützung der Anbindung durch SDKs, insbesondere durch Erweiterung bestehender SDKs • Anbindung im Self-Service möglich

[4] Für Privatpersonen ist ausschließlich die Nutzung des zentral bereitgestellten Postfach-Backends vorgesehen; ein dezentraler Betrieb eigener Backends durch Privatpersonen ist ausgeschlossen

Wirtschaftlichen Betrieb durch Konsolidierung fördern	• Vermeidung mehrerer funktional identischer Lösungen durch Konsolidierung • Vermeidung proprietärer Schnittstellen und Protokolle • Nutzung eines einheitlichen Technologiestacks unter Nutzung von quell- und lizenzoffener Software • Gestaltung entlang einer föderal einheitlichen Zielarchitektur
Förderung von Ende-zu-Ende-Sicherheit	• Ende-zu-Ende-Verschlüsselung von Nachrichten und Anhängen • Kein Aufbrechen der Verschlüsselung • Einfache Verwendung durch die Nutzer:innen
Nutzer:innenerfahrung verbessern	• Nutzende benötigen für alle Kommunikationsszenarien nur einen Postfach-Zugang • Nutzer:innen werden einheitlich adressiert • Zeitgemäße Interaktionsmöglichkeiten ermöglichen, inklusive nativem Einsatz auf mobilen Endgeräten
Zukunftsfähige Weiterentwicklung auf dem Stand der Technik ermöglichen	• Interoperabilität mit anderen Bausteinen des D-Stacks sowie der EU (Wallets) ermöglichen • Redundante Lösungsbausteine vermeiden • Schnittstellen und Anforderungen an Umsysteme definieren • Offene Standards als Rückgrat der Architektur nutzen

Tabelle 1: Programmspezifische Architekturziele

2.3 Architekturprinzipien

Insbesondere folgende Architekturvorgaben wurden beim Treffen der Architekturentscheidungen zur Ausgestaltung der ZaPuK berücksichtigt:

- die *Föderale IT-Architekturrichtlinie* (Version: 1.9)
  - Verbindlichkeit: B-2025/17-IT[5] (26. März 2025)
  - Quelle: https://foederale-it-architekturrichtlinie.gov.de/
- der *Servicestandard* des IT-Planungsrates und DIN SPEC 66336:

[5] Beschluss 2025/17 - Föderale IT-Architekturrichtlinie | IT-Planungsrat

  - Verbindlichkeit: B-2025/24-IT (26. Juni 2025)
  - Quelle: https://servicestandard.gov.de/
- die Architekturprinzipien des D-Stacks bzw. der D-Architektur
  - Eckpunkte: API-First, Serviceorientierung und lose Kopplung, Wiederverwendbarkeit, DevSecOps only, Zero Trust, technologisch aktuell, Made in EU first, Prefer Buy over Make, Ende-zu-Ende-Digitalisierung, Managed Services only
  - Quelle: https://deutschland-stack.gov.de/gesamtbild/

Darüber hinaus wurden durch die verantwortlichen Architekt:innen zusätzlich die in Tabelle 2 dargestellten kontextspezifischen Architekturprinzipien[6] (KAP) entlang der Architekturziele der ZaPuK festgelegt:

Programmspezifische Architekturprinzipien
KAP-1 Zielerreichung über Bestandsschutz priorisieren: Bei der Gestaltung der Zielarchitektur ist der Zielerreichung ein höherer Stellenwert zuzuschreiben als dem Schutz der Bestandslösungen.
KAP-2 Migrationsaufwände geringhalten und Machbarkeit sicherstellen: Die Zielarchitektur soll eine Migration aus der bestehenden Architekturlandschaft mit einem realistischen Aufwand (Zeit, Kosten, Gesetzesanpassungen) ermöglichen .
KAP-3 Sicherheit priorisieren: Eine sichere Lösung ist zu priorisieren, auch wenn die Lösung dadurch weniger wirtschaftlich oder technisch komplexer ist.
KAP-4 Keine vollständige Kenntnis und Abdeckung jeder Anforderung bzw. eines jeden Anwendungsfalls der Bestandslösungen: Die Architekturen der Bestandslösungen verankern eine historisch gewachsene fachliche und technische Heterogenität und Komplexität. Anforderungen und Anwendungsfälle werden vor dem Hintergrund einer fachagnostischen, bundesweit einzusetzenden Basisinfrastruktur abstrahiert und bewertet. Etwaige in bestehenden Postfachlösungen umgesetzte fachspezifische Detailanforderungen ohne übergreifende Architekturrelevanz werden nicht aufgenommen und fließen nicht in die Lösungsgestaltung ein.
KAP-5 Abgegrenzter Baustein einer E2E-Verwaltungslösung: Die Zielarchitektur ist so zu gestalten, dass sie als ein abgegrenzter Bestandteil einer übergreifenden Ende-zu-Ende-Digitalisierungsinfrastruktur (beschrieben von der Deutschland-Architektur) eingesetzt werden

[6] In Version 1.0 noch ‚Projektspezifische Architekturprinzipien' (PSR)

kann.
KAP-6 Cloud-Native/-First Ansatz: Die Zielarchitektur soll auf einer modernen Cloudplattform betreibbar sein und nicht von einem Betrieb auf einem physisch lokalen Server ohne den Einsatz von Cloud-Technologien ausgehen. Nicht cloudfähige Software bietet nur begrenzte Möglichkeiten zur Abfederung von Lastspitzen und führt häufig zu einer ineffizienten Ressourcennutzung. Kompatibilität mit den Standards der DVC soll sichergestellt werden.
KAP-7 API-First: Die Zielarchitektur ist entsprechend dem Paradigma API-First so zu entwickeln, dass alle Funktionen vollständig über konsistente und dokumentierte Schnittstellen angeboten werden. Die Anbindung externer Systeme wird damit vereinfacht.

Tabelle 2: Programmspezifische Architekturprinzipien

2.4 Einordnung in das Ökosystem der Deutschland-Architektur sowie des D-Stacks

Die Zielarchitektur wurde mit Blick auf eine nahtlose Integration in die bestehende und künftige föderale IT-Architektur konzipiert. Bereits in Phase I wurde ihre Ausrichtung an der D-Architektur sichergestellt, die zugleich eine wesentliche Grundlage für die Entwicklung des D-Stacks als Digital Public Infrastructure (DPI) für Deutschland bildet.

Aufgrund der IT-Planungsratsbeschlüsse B-2026/03-IT sowie B-2026/18-IT ist die Zielarchitektur Bestandteil des initialen Portfolios der Basiskomponenten als Konzeptionierung des Bausteins „Postfach und Interaktion“ (siehe Abb. 1).

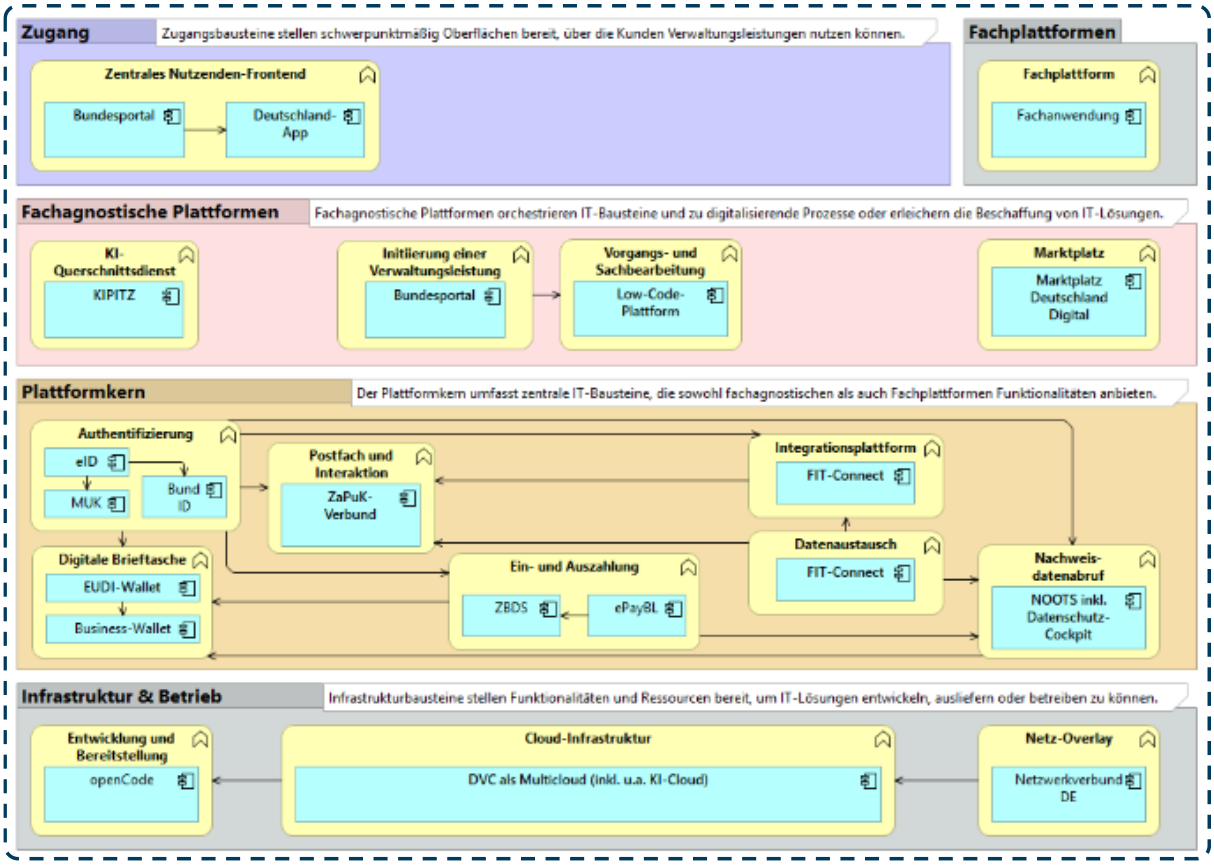

Abbildung 1: Zusammenspiel der Funktionsbausteine im D-Stack, Stand 18.9.2026 (wird fortwährend aktualisiert)

Die D-Stack-Integration greift eine wesentliche Erkenntnis aus Programmphase I auf: Für die Gewährleistung nationaler und europäischer Interoperabilität müssen Authentifizierung und Postfach voneinander entkoppelt werden (ADR-1110). Für Privatpersonen bedeutet dies, dass die Zielarchitektur sowohl die Authentifizierung und Adressierung über die BundID als auch perspektivisch direkt über die EUDI-Wallet ermöglichen muss (vgl. ADR-1105). Für Organisationen gilt dies analog für das Organisationskonto sowie künftig die European Business Wallet (EUBW). Darüber hinaus ist die perspektivische Anbindung an die Kommunikationsfunktionen der EUBW vorgesehen, um die europaweite Interoperabilität für die Übermittlung elektronischer Einschreiben (Qualified Electronic Registered Delivery Service, QERDS) zu realisieren. Das Postfach soll zudem Nachweisattribute (Electronic Attestations of Attributes, EAAs) an Wallet-Lösungen übermitteln können (ADR-1146, vgl. Abschnitt 5.4.8.2).

Entsprechend Beschluss B-2026/03-IT des IT-Planungsrats wurde für die Realisierung des Funktionsbausteins „Datenaustausch“ im initialen Portfolio des D-Stacks FIT-Connect als Produkt festgelegt. Die Anbindung eines zentralen ZaPuK-konformen Basisdienstes „Postfach“

im D-Stack mittels FIT-Connect ist möglich, da bestehende Komponenten zur Anbindung von FIT-Connect protokollagnostisch weiterentwickelt werden könnten bzw. wurden. Synergien ergeben sich aus der Nachnutzung bestehender Komponenten, gegebenenfalls auch als Teil einer zukünftig durch Ausgliederung aus FIT-Connect zu schaffenden föderalen Rollout- und Anbindungsinfrastruktur unter dem FITKO-Produktmanagement, insbesondere des Software Development Kit (SDK) zur Anbindung von Onlinedienstplattformen und Fachverfahren sowie des Self-Service-Portals (SSP) von FIT-Connect für die Administration der Anbindung. ZaPuK wiederum deckt viele Anforderungen des FIT-Connect-Datenaustauschs ab, sodass perspektivisch eine weitreichende Angleichung des eingesetzten Technologiestacks auf Basis des offenen Matrix-Standards denkbar ist.

Die Zielarchitektur ZaPuK wird perspektivisch die in Pilotierung befindliche *Föderale API-Autorisierungsinfrastruktur* (vgl. Beschluss B-2026/16-IT des IT-Planungsrates) als übergreifenden Sicherheits- und Autorisierungsbaustein zur Absicherung technischer Schnittstellen und föderaler Kommunikationsbeziehungen nutzen. Die Infrastruktur stellt föderal abgestimmte Mechanismen für die Registrierung von Organisationen und technischen Clients, die Authentifizierung von Systemen sowie die Autorisierung von API-Zugriffen bereit. ZaPuK integriert sich in diese Mechanismen und nutzt die dort definierten Sicherheitsstandards und Protokolle für den Zugriff auf interne und externe Schnittstellen.

Die Föderale API-Autorisierungsinfrastruktur ist dabei nicht als allgemeine Infrastruktur zur Identifikation oder Authentifizierung von Kommunikationsteilnehmer:innen (Privatpersonen wie Organisationen) vorgesehen. Die Aufgaben der Authentisierung sowie die Prüfung fachlicher Berechtigungen von Nutzenden verbleiben bei den Identitätslösungen der Postfach-Backends. Die Aufgabe der Föderalen API-Autorisierungsinfrastruktur besteht hingegen darin, technische Systeme, Organisationen und deren Zugriffsrechte innerhalb der föderalen IT-Landschaft zu verwalten.

Sie kann für die Registrierung, Zulassung und Verwaltung technischer Teilnehmer:innen genutzt werden. Auf Grundlage organisationsbezogener Attribute und Berechtigungen kann entschieden werden, welche Organisationen und von ihnen verantwortete Systeme die angebotenen Schnittstellen nutzen dürfen. Darüber hinaus stellt sie einheitliche Mechanismen für die Authentifizierung und Autorisierung technischer Kommunikationsbeziehungen bereit und unterstützt damit die vertrauenswürdige Zusammenarbeit zwischen Komponenten der Zielarchitektur sowie mit angebundenen Basisdiensten und weiteren externen Systemen.

2.5 Einordnung in das Ökosystem des Matrix-Standards

Entsprechend der bereits in Programmphase I getroffenen Architekturentscheidung ADR-0011 der ZaPuK wird die technische Kommunikation auf Grundlage von *Matrix* realisiert. Matrix ist ein offener Standard für sichere, Ende-zu-Ende-verschlüsselte, dezentrale, interoperable (Echtzeit-)Kommunikation. Der Matrix-Standard wird von der Matrix.org Foundation veröffentlicht und weiterentwickelt. Die Spezifikation steht unter einer offenen Lizenz (Apache 2.0 License). Matrix kann sowohl für die Realisierung von klassischen Postfächern als auch von Chat-Anwendungen eingesetzt werden, bietet zudem aufgrund der offenen Spezifikation und diverser Integrationen, aber auch eine flexible Basis für weitere Anwendungsfälle, insbesondere die Integration von (KI-)Chatbots sowie die Nutzung als sicheren Kommunikationslayer für maschinenlesbare M2M-Kommunikation auf Grundlage des gleichen technischen Protokolls. Zudem bietet Matrix mit MatrixRTC (Matrix Real Time Communication) ebenfalls einen standardisierten Interoperabilitätslayer für Audio-, Video- und Echtzeit-Datenkommunikation.
Rund um den Matrix-Standard hat sich ein großes Ökosystem aus einer Vielzahl an Unternehmen, Universitäten, öffentlichen und militärischen Einrichtungen sowie zivilgesellschaftlichen Organisationen gebildet. Es existieren zahlreiche Server- und Client-Implementierungen des Matrix-Standards. Neben quelloffenen und lizenzkostenfreien Lösungen (Free and Open Source Software, FOSS) stehen auch proprietäre Produkte mit professionellem Support zur Verfügung. Matrix wird überdies in Produkten wie Rocket.Chat zur Realisierung einer herstellerübergreifenden Chat-Interoperabilität oder auf den Plattformen Bluesky und Reddit zur Realisierung von Direktnachrichten eingesetzt.
Expertise zum Matrix-Standard besteht bereits in vielen Unternehmen wie beispielsweise IBM, Deutsche Telekom, Element, adesso SE, Bechtle AG, Dataport, BWI GmbH, gematik sowie die Krankenkassen in Deutschland, ZenDiS, adfinis AG, Materna Information & Communications SE, BearingPoint, Nordeck IT + Consulting, Famedly GmbH, fairkom, welche den Matrix-Standard in ihren Produkten und Projekten einsetzen - teils spezifisch angepasst auf die Anforderungen der öffentlichen Verwaltung, teils ausgerichtet auf die Anforderungen der Privatwirtschaft.
In Deutschland kommt Matrix bereits in einer Vielzahl an Projekten des Staates zum Einsatz, darunter im TI-Messenger (gematik) im gesamten deutschen Gesundheitssektor, im BundesMessenger & BwMessenger (BWI GmbH für die Bundeswehr), zur gegenseitigen digitalen Fallweitergabe zwischen ärztlichem Bereitschaftsdienst 116117 und den Leitstellen der 112 & in openDesk (ZenDiS) sowie als bundeseinheitlicher Standard für länderübergreifende Kom-

munikation in den 20 deutschen Polizeien im Rahmen des Programms P20. Matrix wird an über 50 Hochschulen zur Kommunikation genutzt und in drei Bundesländern für alle Schulen eingesetzt.

International wird in Projekten und Produkten in Frankreich (TChap), Belgien (BEAM), Luxemburg (LuxChat), den Niederlanden (MijnBureau), Schweden (SAFOS und Rocket.Chat) [Video, eSAM-Report], der Schweiz (Schweizer Post), Polen, Griechenland sowie in der EU-Kommission, der NATO, den Vereinten Nationen (UN) und zahlreichen europäischen und internationalen Militärs (darunter den Ukrainischen Streitkräften und der Bundeswehr) auf Matrix gesetzt. Das Protokoll ermöglicht eine Interoperabilität von Chat- und Kommunikationslösungen unter Wahrung der Ende-zu-Ende-Verschlüsselung, teils für hochkritische, hochsensible Anwendungsfälle.

In der Matrix-Foundation besteht überdies bereits eine Public Sector Working Group mit Teilnehmenden u. a. aus Frankreich, der Europäischen Kommission, Schweden, Deutschland, Luxemburg, den Niederlanden, Belgien, dem Vereinigten Königreich und Rumänien. Matrix ist kein deutscher Sonderweg, sondern ein europäisches Projekt.

Durch den Einsatz in der ZaPuK wird Matrix im Funktionsbaustein „Postfach und Interaktion“ sowie gegebenenfalls durch das Produkt FIT-Connect im Funktionsbaustein „Datenaustausch“ eine entscheidende Rolle im D-Stack spielen. Dem D-Stack fehlt aktuell ein solcher Kommunikationsstandard zur Realisierung von Nachrichtenübermittlungen, organisationsübergreifenden Chats und föderierter Echtzeitkommunikation (Video-/Audiotelefonie). Eine Aufnahme des Matrix-Standards in den D-Stack wird daher seitens des ZaPuK-Programms empfohlen.

3 Geschäftsarchitektur

Redaktioneller Hinweis: Die Geschäftsarchitektur der ZaPuK bleibt unverändert gegenüber Version 1.0 dieses Dokuments. Die Inhalte werden vor Einreichung zur 51. Sitzung des IT-Planungsrates übertragen.

Grundlegende geschäftsarchitektonische Abgrenzungen ergeben sich zudem aus dem Steckbrief des Funktionsbausteins „Postfach und Interaktion" der Deutschland-Architektur. Die ZaPuK gestaltet diesen inhaltlich aus (vgl. Beschluss B-2026/03-IT des IT-Planungsrates), der Steckbrief ist jedoch nicht Teil dieses Konzepts bzw. der Architekturartefakte der ZaPuK im engeren Sinne. Die Inhalte der ZaPuK fließen fortlaufend und iterativ in den Funktionsbausteinsteckbrief „Postfach und Interaktion" ein.

4 Zielbild für Entwicklung, Betrieb und Governance

Die IT-Architektur der ZaPuK (vgl. Kapitel 5) definiert abstrakt das Zusammenwirken einer Vielzahl von IT-Komponenten, die sowohl zentral (z. B. zentraler Postfach-Zugang) als auch dezentral betrieben werden (z. B. dezentral betriebene Postfach-Backends). Für die zentral bereitgestellten IT-Komponenten beschreibt Kapitel 4 die empfohlene Verteilung der Verantwortlichkeiten für Entwicklung, Betrieb und Steuerung im anzustrebenden Zielzustand. Im Zusammenwirken mit einschlägigen Umsystemen ist die Summe der zentral bereitgestellten IT-Komponenten der ZaPuK geeignet, aus Nutzendensicht den Basisdienst ‚Postfach' im Sinne des D-Stacks zu realisieren. Es wird empfohlen, die Zielarchitektur entlang dieses architektonischen Zielbildes (auch: Zielarchitekturplateau, Zielbebauungsplan) zeitnah in eine real existierende und produktiv nutzbare Kommunikationsinfrastruktur zu überführen. Die produktive Realisierung des in diesem Kapitel beschriebenen Zielzustandes wird in ZaPuK-Programmphase III („Transition & Migration") auf Basis der lösungsspezifischen Transitionsplanungen angestrebt.

Bei der Formulierung des Zielbilds betrachten wir die Kommunikationsinfrastruktur aus drei Dimensionen:

- **Entwicklung:** Wer verantwortet die Entwicklung, Weiterentwicklung und Wartung der konkreten technischen Lösungen? (Abschnitt 4.1)
- **Betrieb:** Wer verantwortet den Betrieb welcher entwickelten Lösungen? (Abschnitt 4.2)
- **Governance:** Wer regelt die Zuteilung der Verantwortlichkeiten für Entwicklung und Betrieb, setzt den technischen Rahmen und entscheidet über Streitfragen? (Abschnitt 4.3)

Da sowohl die strategischen als auch die operativen Governance-Strukturen des D-Stacks und der Deutschland-Architektur mit Stand September 2026 noch nicht übergreifend definiert sind, verstehen sich die jeweils betroffenen nachfolgenden Empfehlungen zu Entwicklung, Betrieb und Steuerung als vorläufige Empfehlungen auf Grundlage des Status quo der föderalen IT-Architektur (siehe Abb. 3).

Eine Abschätzung der finanziellen Aufwände für Entwicklung und Betrieb der jeweiligen Komponenten wird in diesem Dokument[7] nicht getroffen.

[7] Die finanzielle Betrachtung inkl. einer Abschätzung von Migrationskosten ist Teil eines separat vorgelegten Finanzierungskonzeptes.

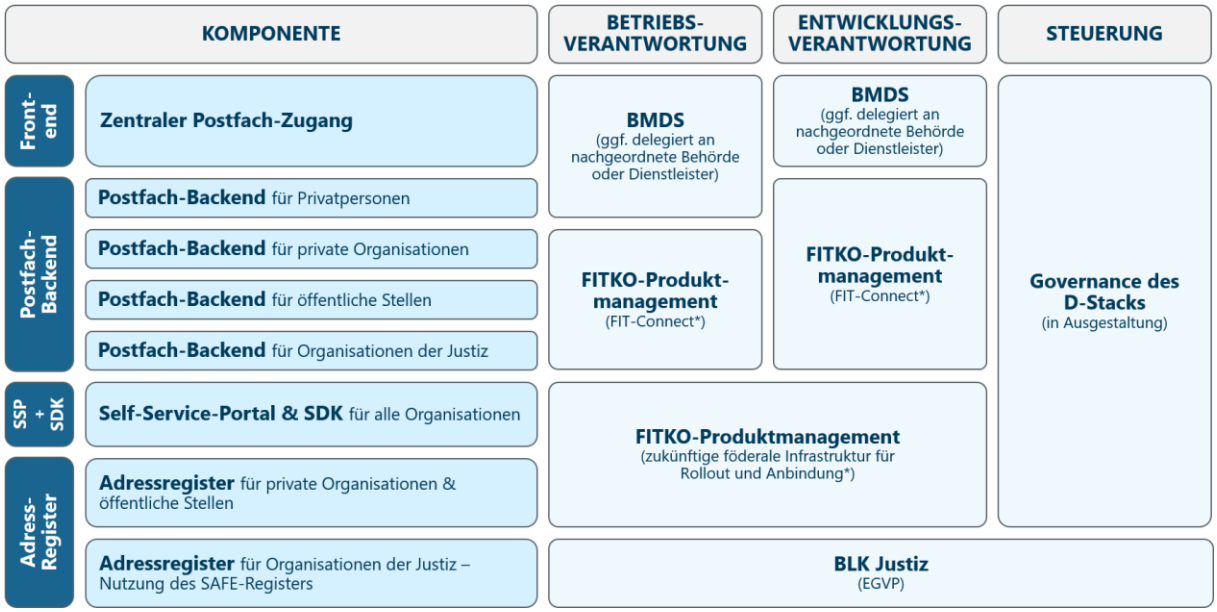

Abbildung 2: Empfohlene Verortung von Verantwortlichkeiten in Entwicklung, Betrieb und Steuerung zentraler IT-Komponenten der ZaPuK

**vorbehaltlich etwaiger Änderungen des FIT-Connect-Produktschnitts zur Schaffung einer föderalen Infrastruktur für Rollout und Anbindung auf Grundlage von SSPs und SDKs im Kontext des D-Stacks*

4.1 Zentrale Softwareentwicklung

Neben der initialen projekthaften Entwicklung müssen die Komponenten der Zielarchitektur dauerhaft in einer Produktstruktur weiterentwickelt und gewartet werden. Hierzu werden im Folgenden Verantwortlichkeiten definiert, um eine Produktverantwortung für die jeweiligen Komponenten sicherzustellen.

4.1.1 Backend-Komponenten

Das Backend der Kommunikationsinfrastruktur besteht aus den folgenden wesentlichen IT-Komponenten:

- **Postfach-Backend**: Ein auf einer Open-Source-Implementierung des Matrix-Standards basierendes Backend, bestehend aus Matrix-Homeserver, Datenbank und weiteren Microservices (z. B. für die Realisierung von Push-Notifications) sowie einer Administrationsoberfläche für die Pflege der Postfachadressen. Vorbehaltlich der Einhaltung der Vorgaben der ZaPuK inklusive der Anschlussbedingungen (ADR-1145), insbesondere der Querschnittlichkeit und fachlichen Agnostik der Kommunikationsinfrastruktur (ADR-0001), können fachliche Erweiterungen über die offenen Schnittstellen umgesetzt werden.

- **Self-Service-Portal**: Komponente für die Registrierung von Organisationen in Self-Service-Prozessen als Teil der Anbindung an die Infrastruktur.
- **Adressregister:** Zuordnung von Organisationsidentitäten zu den technischen Matrix-Adressen
- **Protokollkonverter**: Komponente für die sichere Anbindung dritter Kommunikationsinfrastrukturen. Im Gegensatz zu einer einfachen Bridge (deutsch „Brücke"), welche Nachrichten im Regelfall unverschlüsselt über Protokollgrenzen transportiert, realisiert der Protokollkonverter die Vermittlung von Nachrichten zwischen zwei Transportprotokollen (z. B. Matrix und OSCI) *ohne* Aufbrechen der Ende-zu-Ende-Verschlüsselung.
- **Software Development Kit**: Das SDK vereinfacht die Nutzung der öffentlichen APIs, z. B. durch Kapselung der Umsetzung der erforderlichen kryptographischen Funktionalitäten in einer Software-Bibliothek. Fachverfahren und Unternehmensanwendungen können so deutlich schneller und einfacher angebunden werden. Aber auch die zentral entwickelten Frontend-Komponenten sollen auf das SDK aufsetzen, um zentrale Funktionalitäten nur an einer Stelle implementieren zu müssen, was Komplexität und Wartungsaufwände reduziert.

Eine Bündelung von Entwicklung, Weiterentwicklung und Wartung dieser und evtl. weiterer ähnlich gelagerter Komponenten in genau einem Entwicklungsteam reduziert Kosten und Abstimmungsaufwände, beugt redundanten Entwicklungen vor und reduziert nachhaltig die Komplexität in der föderalen IT. Zudem wird hierdurch eine einheitliche Produktstrategie gefördert, von der alle für den Betrieb der Komponenten verantwortlichen Stellen gleichermaßen profitieren.

Für die Verortung des Entwicklungsteams kommen grundsätzlich drei Optionen infrage:

- Option A: Zentrale Entwicklung in den Produktstrukturen des bestehenden IT-Planungsrats-Produktes „FIT-Connect" **(Empfehlung)**
- Option B: Zentrale Entwicklung in neuem D-Stack-Produkt durch den Bund
- Option C: Zentrale Entwicklung in neuem IT-PLR-Produkt

Empfehlung:

- Option A: Empfohlen wird die Verortung der zentralen Softwareentwicklung für Backend-Komponenten in den Produktstrukturen des bestehenden IT-Planungsrats-Produktes „FIT-Connect".

Erwägungsgründe für diese Empfehlung:

- Durch die Nutzung etablierter technischer und organisatorischer Produktstrukturen (beispielsweise eingespieltes agiles Entwicklungsmodell, reifes operatives Anforderungsmanagement, vorhandene Entwicklungs-, Test- und Produktivumgebungen usw.) müssen keine neuen Strukturen geschaffen werden, um zentrale Backend-Komponenten bereitzustellen. Als Produkt des IT-Planungsrates verfügt FIT-Connect zudem über bewährte operative Managementstrukturen und eine belastbare Rechtsgrundlage für die Nutzung durch Länder und Kommunen. Es ist zu erwarten, dass dies die Vorlaufzeit zur Realisierung einer produktiven ZaPuK-konformen Lösung erheblich reduziert.
- Die Verortung im bestehenden Produkt FIT-Connect führt zu bedeutenden Synergieeffekten, da die Lösungsarchitektur des technischen Produktes FIT-Connect hinsichtlich seiner Kernfunktionalität als fachagnostischer föderaler Basisdienst für Antragsstellung bereits eine ähnliche funktionale Strukturierung zu IT-Komponenten der ZaPuK aufweist. So stellt das Produkt FIT-Connect bereits ein SSP sowie ein Software Development Kit (SDK) bereit, welche aufwandsarm entsprechend den Anforderungen der ZaPuK weiterentwickelt werden können. FIT-Connect plant zukünftig bereits ohnehin den Einsatz von Matrix-Servern im Produkt FIT-Connect. Übergreifend ist aufgrund der Lösungsarchitektur von FIT-Connect mit den geringstmöglichen technischen Transitionsaufwänden unter größtmöglicher Vermeidung neuer Komplexität in der föderalen IT-Architektur zu rechnen.
- Das Produkt FIT-Connect verfügt über ein bestehendes Anbindungsmanagement, welches perspektivisch generalisiert werden kann. Dieses kann als Grundlage für die Schaffung einer föderalen Rollout- und Anbindungsinfrastruktur auf Grundlage des FIT-Connect-SSPs und SDKs dienen. Für ZaPuK und FIT-Connect sowie ggf. weitere Basisdienste ergibt sich gegenüber Onlinediensten, Fachverfahren und Unternehmensanwendungen so das wirkmächtige Wertversprechen, sich für die Kommunikation im Verfahrenskontext, also sowohl Antragsstellung als auch Bescheidzustellung, Rückfragen oder Nachforderungen, nur einmalig technisch anbinden zu müssen.

4.1.2 Frontend: Zentraler Postfach-Zugang für Privatpersonen und Organisationen

Neben den Backend-Komponenten ist ein zentraler Postfach-Zugang im Sinne eines modernen Frontends für die Interaktion natürlicher und juristischer Personen mit öffentlichen Stellen und den Organisationen der Justiz essenziell für den Erfolg der Zielarchitektur. Der zentrale Postfach-Zugang soll modular entwickelt werden, sodass er eingebettet in bestehende Frontends der Verwaltung eingesetzt werden kann (z. B. im D-Stack-Baustein *Zentrales Nutzenden-Frontend* als Teil des Bundesportals oder perspektivisch in einer mobilen Deutschland-App sowie ggf. in weiteren Fachportalen). Hierzu sollte der Postfach-Zugang sowohl als

webbasierte Anwendung für Webbrowser als auch als mobile Anwendung für gängige mobile Betriebssysteme wie iOS, Android, LineageOS-basierte Systeme wie /e/OS und Linux-basierte Systeme wie postmarketOS bereitgestellt werden.
Bezüglich der Verortung der Entwicklungs-, Wartungs- und Weiterentwicklungsverantwortung kommen grundsätzlich drei Optionen infrage:

- Option A: Gemeinsame Entwicklung mit Backend- & Infrastruktur-Komponenten
- Option B: Zentrale Entwicklung entsprechend den Governance-Strukturen des D-Stacks und der Deutschland-Architektur **(Empfehlung)**
- Option C: Zentrale Entwicklung in neuem IT-PLR-Produkt

Empfehlung:

- Option B: Empfohlen wird, die Entwicklung des zentralen Postfach-Zugangs für Privatpersonen und Organisationen entsprechend den Governance-Strukturen des D-Stacks entlang der Funktionsbausteine der Deutschland-Architektur zu verorten. Das technische Produkt sollte mittelfristig, nach dem Abschluss der initialen projekthaften Umsetzung, im Deutschland-Architektur-/D-Stack-Funktionsbaustein *Zentrales Nutzenden-Frontend (Bundesportal, Deutschland-App)* verortet und in gemeinsamen Strukturen mit dem Funktionsbaustein *Postfach und Interaktion* gemanagt werden.

Erwägungsgründe für diese Empfehlung:

- Die Verortung in den Governance-Strukturen des D-Stacks entsprechend der Deutschland-Architektur stellt eine aufeinander abgestimmte Entwicklung der beiden Funktionsbausteine sicher und ermöglicht die Konzeption eines bausteinübergreifenden Service-Designs.
- Der Bund verantwortet gemäß Beschluss B-2026/03-IT des IT-Planungsrates bereits das Bundesportal als Lösung im Funktionsbaustein *Zentrales Nutzenden-Frontend* und darüber hinaus die Deutschland-App – beide sind prädestinierte Lösungen für die Verortung eines zentralen Postfach-Zugangs.
- Der Bund kann als Auftraggeber zentral steuernd für ein gutes bausteinübergreifendes Zusammenspiel der Produkte sorgen, insbesondere durch Aufbau gemeinsamer, dienstleister:innenübergreifender Teamstrukturen zur Entwicklung des Postfach-Zugangs mit Bundesportal und Deutschland-App.
- Der Bund hat mit dem DigitalService in den letzten Jahren eine sehr umfassende Unterstützungseinheit für Entwicklung und Service-Design aufgebaut und kann im In-

house-Verhältnis einfach auf diese Ressourcen zugreifen. Gleichzeitig kann durch das FITKO-Produktmanagement sowohl eine enge strategische Abstimmung mit den Backend-Komponenten als auch eine ausreichend modulare Entwicklung des Frontends für die Nachnutzung in weiteren Kontexten sichergestellt werden.

- Die Softwareartefakte (Web-App, iOS-App, Integration des Matrix-SDKs in das FIT-Connect-SDK) und Umsetzungsstrukturen des Vorhabens „Neo" stellen eine reife Grundlage für die initiale projekthafte Realisierung insbesondere des zentralen Postfach-Zugangs dar. Sie sollten aus der Pilotierung und technischen Validierung in Phase II übernommen und weiterentwickelt werden.

Die Sicherstellung einer modularen Entwicklung ist wichtig, um einen zu starken Fokus auf das zentrale Nutzenden-Frontend und dadurch bedingte konkurrierende Eigenentwicklungen durch Dritte, wie z. B. Fachportale, zu vermeiden und folglich einer zu starken Zersplitterung des Frontend-Ökosystems vorzubeugen.

Die operative Steuerung und Umsetzung im D-Stack, inklusive etwaiger Beauftragung Dritter, sind ergebnisoffen durch zuständige Stellen zu prüfen und festzulegen.[8]

4.1.3 Softwareentwicklung von Umsystemen und Lösungen Dritter

Neben den zuvor umrissenen und in Kapitel 5 ausgeführten IT-Komponenten, die Teil der Zielarchitektur sind, sind weitere Umsysteme erforderlich, die als technisch-funktionale Grundlage für die Zielarchitektur dienen. Hierzu zählen insbesondere Identitäts- und Authentifizierungslösungen wie die eID-Funktion des Personalausweises, die EUDI-Wallet, BundID, Mein Unternehmenskonto und perspektivisch die European Business Wallet sowie die Verwaltungs-PKI (V-PKI). Die Planung und Weiterentwicklung dieser Komponenten liegt außerhalb des Scopes der ZaPuK, ist jedoch ein zentraler Erfolgsfaktor für die Umsetzung.

Alternative Lösungen zum zentral entwickelten Front- bzw. Backend sind im Sinne eines modularen D-Stacks sowie eines schnellen Flächen-Rollouts z. B. als Integration in Unternehmensanwendungen explizit vorgesehen. Diese Lösungen müssen jedoch durch Dritte entwickelt werden. Die Entwicklungsverantwortung im Sinne dieses Dokuments endet mit der Bereitstellung von für die Entwicklung alternativer Lösungen geeigneter nachnutzbarer Bausteine.

[8] Empfehlungen zum Einsatz konkreter Dienstleister:innen sind nicht Betrachtungsgegenstand dieses Architekturkonzeptes.

4.1.4 Allgemeine Festlegungen zur Softwareentwicklung

Um das reibungslose Zusammenspiel der unterschiedlichen Komponenten und Betriebsinfrastrukturen zu gewährleisten, bestehen einige Anforderungen an den praktischen Softwareentwicklungsprozess, u. a.:

- **Offene Lizenzierung**: Softwareentwicklungsteams und technisch versierte Nutzer:innen der jeweiligen Komponenten (z. B. Fachverfahrenshersteller:innen, Dienstleister:innen der öffentlichen Verwaltung) profitieren vom gegenseitigen Erfahrungsaustausch. Komponenten sollen daher in Form von Quellcode- und Build-Artefakten gemäß Servicestandard[9] und Föderaler IT-Architekturrichtlinie[10] unter der freien *Open-Source-Lizenz für die Europäische Union* (EUPL) bereitgestellt werden. Die zu verwendende Lizenz wird mit der Umsetzung abschließend festgelegt. Somit stehen die Komponenten auch anderen europäischen Akteuren zur Nutzung bereit und der Erfahrungsaustausch auf EU-Ebene wird gefördert. Die entwickelten IT-Komponenten müssen im produktiven Betrieb vollständig unter freier Softwarelizenz ohne Nutzung von proprietären Drittkomponenten einsetzbar sein.
- **DevSecOps**: Um eine reibungslose Bereitstellung von Software-Artefakten zu ermöglichen, soll ein DevSecOps-Vorgehen etabliert werden. Dabei greifen Entwicklungstätigkeiten (Development), sichere Softwareentwicklungspraktiken (Security) und Betriebstätigkeiten (Operations) nahtlos ineinander. Ziel ist die Etablierung einer DevSecOps-Pipeline, welche eine Zusammenarbeit zwischen Entwicklungs- und Betriebsteams auch über Organisationsgrenzen hinweg ermöglicht. Parallel dazu sind die organisatorischen Prozesse umzusetzen. Dies geschieht u. a. durch den Einsatz von Continuous Integration und Continuous Delivery (CI/CD), analog zur bereits bestehenden Zusammenarbeit zwischen FIT-Connect und BundID bei Entwicklung und Betrieb des sog. ZBP-Adapters. Für die Umsetzung soll die DevSecOps-Plattform des D-Stacks evaluiert werden.
- **Offener Entwicklungsprozess**: Ein offener Entwicklungsprozess nach dem Vorbild des Open-Source-Vorgehensmodells schafft Möglichkeiten zur Meldung von Anforderungen, Fehlern sowie Verbesserungsvorschlägen in öffentlichen Issue-Trackern und erlaubt Einblicke der Community in den Entwicklungsprozess. Dieses Vorgehen schafft Vertrauen, Feedback-Schleifen und stärkt die Selbstwirksamkeit der verwaltungsinternen und -externen Community.

[9] https://servicestandard.gov.de/punkte/10-open-source-nutzen-und-code-teilen/
[10] https://foederale-it-architekturrichtlinie.gov.de/2_Architekturvorgaben/2_1_Allgemeine_Vorgaben/AV-07_Open_Source/

- **Nachnutzung:** Es werden primär vorhandene Software-Artefakte wie Open-Source-Implementierungen des Matrix-Standards eingesetzt und bedarfsorientiert weiterentwickelt. Die Neuentwicklung von ZaPuK-spezifischen Komponenten (wie z. B. der Raum-Management-Service und das Adressregister) erfolgt nur, wo solche nicht bereits als Ausgangsbasis existieren.
- **Beiträge zu Quellprojekten (Upstream Contributions)**: Alle Änderungen und Anpassungen, die an eingesetzten Fremd-Komponenten vorgenommen werden, werden als Patches dem jeweiligen Ursprungsprojekt unter dessen jeweiliger freier Softwarelizenz zur Verfügung gestellt. Dies unterstützt nicht nur die Nachhaltigkeit und Wartbarkeit der Lösung, sondern trägt auch zur Weiterentwicklung der Open-Source-Community bei und minimiert langfristige Abhängigkeiten durch eigene Modifikationen. Auch soll durch das Melden und Beheben von Fehlern (z. B. durch Code-Beiträge oder Änderungsvorschläge zu offenen Standards) sowie die Teilnahme an Diskussionen in fremden Open-Source-Projekten und offenen Standards (wie dem Matrix-Standard) zur Open-Source-Community beigetragen werden. Dies trägt zum Bestehen sowie zur kontinuierlichen Verbesserung und Erweiterung der Funktionalität von abhängigen Projekten bei.

Diese Punkte können u. a. durch Entwicklung auf der Plattform openCode umgesetzt werden.

4.2 Zentraler Betrieb

ZaPuK beschreibt sowohl zentral entwickelte und betriebene Komponenten als auch dezentral betriebene Komponenten (eigene Backends, eigene Zugänge). Dieser Abschnitt definiert die Verantwortlichkeiten für den Betrieb der zentral entwickelten IT-Komponenten der Kommunikationsinfrastruktur.

4.2.1 Entscheidungstreiber

Eine grundsätzliche Hürde für ein vertrauliches Kommunikationssystem sind Metadaten. Diese fallen entweder zwingend beim Betrieb an (z. B. IP-Adressen) oder können im Fall von unverschlüsselten Metadaten durch die betreibende Stelle grundsätzlich eingesehen werden. Durch Kenntnis solcher Metadaten kann z. B. ermittelt werden, wann wer mit wem kommuniziert. Selbst ohne Kenntnis der Nachrichteninhalte kann es sich hierbei um eine höchstsensible, schützenswerte Information handeln, z. B. wenn allein das Bekanntwerden einer Kommunikationsverbindung diskriminierungssensible Informationen offenlegt (z. B. Kommunikation einer Privatperson mit spezifischen Fachärzt:innen, Beratungsstellen, Strafverfolgungsbehörden etc.). Durch die Möglichkeit der massenhaften Korrelation sensibler Metadaten ergäben sich bei Kompromittierung zentraler Infrastrukturkomponenten zudem massive Sicherheits-

vorfälle – aufgrund der Menge und Sensibilität der Metadaten eines solchen Systems bis hin zu Risiken für die nationale Sicherheit.
Aus diesem und anderen Umständen ergeben sich die folgenden, teils zueinander im Konflikt stehenden Ziele, welche die nachfolgenden Empfehlungen maßgeblich beeinflussen:

- **Es sollten möglichst viele Kommunikationsteilnehmende den gleichen Homeserver haben**. Dadurch kann trotz Kenntnis der an einer Konversation beteiligten Homeserver schwieriger auf konkrete Teilnehmende geschlossen werden. Beispiel: Eine Kommunikation mit dem „Homeserver des Gesundheitswesens" ist ungleich weniger sensibel als eine Kommunikation mit dem „Homeserver der psychologischen Seelsorge".
- **Die Kommunikationsteilnehmenden eines Homeservers sollten möglichst gleichartig sein.** Dies reduziert die Komplexität bei der Administration der Homeserver und Teilnehmenden durch Ermöglichung einer Separierung einzelner Stakeholdergruppen (z. B. Organisationen der Justiz, private Unternehmen etc.). Maßnahmen, z. B. zur Informationssicherheit, können gezielt für die Bedarfe der Teilnehmenden des Homeservers sowie domänenspezifische fachliche Anforderungen vorgenommen werden.
- **Es sollte mehr als einen Homeserver mit unterschiedlichen Betreibenden geben.** Durch organisatorische Trennung der Betreibenden kann das Risiko verringert werden, dass ein Betreiber gleichzeitig Zugriff auf unverschlüsselte Kommunikations-Metadaten von sowohl Absender:in als auch Empfänger:in einer Kommunikation erlangt und daraus Schlüsse in Bezug auf deren Kommunikationsmuster ziehen kann (ADR-1114). Dies betrifft insbesondere die Kommunikation zwischen Stellen des Staates einerseits und privaten Akteuren andererseits.
- **Mehrere Homeserver sollten durch dieselbe Stelle betrieben werden.** Skaleneffekte und die Bündelung von Betriebskompetenz fördern einen qualitativ hochwertigen, sicheren und ökonomischen Betrieb. Zudem sorgen weniger Betreibende für geringere Komplexität beim Rollout technischer Änderungen und verringern die Angriffsfläche.

Die nachfolgenden Empfehlungen stellen einen bestmöglichen Kompromiss zwischen den sich gegenseitig beeinflussenden Zielen dar.

4.2.2 Überblick

Die folgende Grafik (siehe Abb. 4) gibt einen High-Level-Überblick über das Zusammenspiel der bundesweit zentral bereitgestellten IT-Komponenten der ZaPuK entsprechend der nach-

folgend empfohlenen Verortung von Betriebsverantwortung. In den weiteren Unterkapiteln werden Festlegungen zur Betriebsverantwortung dieser Komponenten näher beschrieben und begründet. Auch finden sich dort Erläuterungen zu Auswirkungen der getroffenen Empfehlungen.

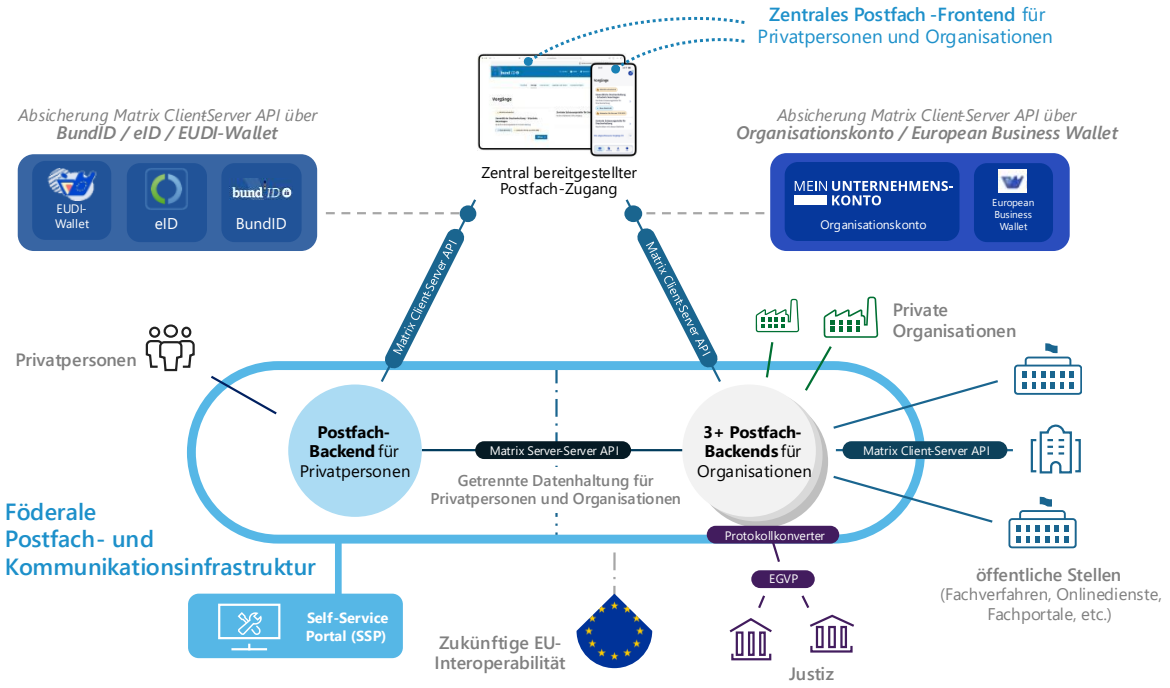

Abbildung 3: Zusammenspiel der Komponenten der Zielarchitektur

4.2.3 Backend-Komponenten

Im Folgenden werden die verschiedenen Betriebsverantwortlichkeiten für die bundesweit zentral bereitgestellten Backend-Komponenten dargestellt (siehe Tab. 3).

Die verschiedenen Postfach-Backends bilden einen einheitlichen föderierten Kommunikationsverbund. Sie sind technisch und architektonisch identisch, werden aus einer Hand entwickelt und binden Fachverfahren und Zugänge gleichartig an. Die Anbindung erfolgt dabei nur an ein einziges Postfach-Backend des Verbundes – eine gesonderte Anbindung der verschiedenen Backends je Zielgruppe ist explizit nicht notwendig. Die Kommunikation der Teilnehmenden-Gruppen untereinander erfolgt mittelbar über die Föderation der Matrix-Homeserver. Dies führt zu Einsparungen und Flexibilität durch eine leichte Erweiterbarkeit des Verbundes und die Standardisierung von Governance-Prozessen. Eine Erweiterung des Ver-

bundes um zusätzliche Postfach-Backends verursacht keinen weiteren Aufwand für bereits angebundene Kommunikationsparteien.

Komponente		Betriebsverantwortliche Stelle
Postfach-Backend Zentral entwickeltes Postfach-Backend wird in vier Instanzen nach Stakeholdergruppen separiert betrieben.	Postfach-Backend für Privatpersonen	BMDS (ggf. delegiert an nachgeordnete Behörde oder Dienstleister:innen)
	Postfach-Backend für private Organisationen	FITKO-Produktmanagement (FIT-Connect*)
	Postfach-Backend für öffentliche Stellen	FITKO-Produktmanagement (FIT-Connect*)
	Postfach-Backend für Organisationen der Justiz	FITKO-Produktmanagement (FIT-Connect*)
Self-Service-Portal	SSP für Organisationen	FITKO-Produktmanagement (ggf. zukünftige föderale Rollout- und Anbindungsinfrastruktur*)
Adressregister Wird nach Stakeholdergruppen separiert betrieben.	Adressregister für private Organisationen und öffentliche Stellen	FITKO-Produktmanagement (ggf. zukünftige föderale Rollout- und Anbindungsinfrastruktur*)
	Adressregister für Organisationen der Justiz unter Nutzung des SAFE-Registers	BLK Justiz (EGVP)

Tabelle 3: Backend-Komponenten **vorbehaltlich etwaiger Änderungen des FIT-Connect-Produktschnitts zur Schaffung einer föderalen Rollout- und Anbindungsinfrastruktur auf Grundlage von SSPs und SDKs*

4.2.3.1 Zentrales Postfach-Backend für Privatpersonen

Für Privatpersonen soll ein zentrales Backend bereitgestellt werden (ADR-1114). Hierbei handelt es sich um das Postfach-Backend gemäß Kapitel 5.2.2.1 (inkl. Matrix-Homeserver und anderen Teilen des Matrix-Backends) für natürliche Personen.
Die Absicherung der Schnittstellen des Postfach-Backends für Privatpersonen erfolgt per eID-, BundID- oder perspektivisch per EUDI-Wallet-Authentifizierung.

Empfehlung:

- Das Postfach-Backend für Privatpersonen soll durch das Bundesministerium für Digitales und Staatsmodernisierung (BMDS) betrieben werden (ggf. delegiert an nachgeordnete Behörde oder Dienstleister:innen).

Erwägungsgründe für diese Empfehlung:

- Privatpersonen können über einen einzigen Postfach-Zugang mit Fachbehörden aller Verwaltungsbereiche sowie den Organisationen der Justiz kommunizieren.
- Bei einer Privatperson lassen Informationen über die kontaktierten Konversationspartner:innen signifikante Rückschlüsse auf die Lebenssituation der Privatperson zu. Der Betrieb des Privatpersonen-Backends losgelöst vom restlichen Verbund ermöglicht eine organisatorische Separierung der anfallenden Metadaten auf mehrere Betriebsumgebungen. Die betriebsverantwortliche Stelle für das Privatpersonen-Backend ist bei entsprechender Metadaten-Separierung nicht in der Lage, Kenntnis davon zu erhalten, mit welcher Organisation eine Privatperson kommuniziert (sie erfährt nur, dass die jeweilige Privatperson zum Zeitpunkt X mit irgendeiner Organisation kommuniziert).
- Der Bund kommt seiner Bereitstellungs-Verantwortung für das Postfach des Bürgerkontos gemäß § 3 Abs. 1 OZG nach.
- Durch die organisatorische Trennung der Entwicklung von der Prüfung des Quellcodes durch die betreibende Stelle entsteht eine unabhängige Kontrollinstanz.

Konsequenzen dieser Empfehlung:

- Der Bund trägt die Verantwortung für die Prüfung des bereitgestellten Quellcodes der Backend-Komponenten vor dem Einspielen von Software-Updates.
- Fachverfahren, Onlinedienste und Fachportale (wie ELSTER oder service.justiz.de) übermitteln Nachrichten an das Postfach-Backend für Privatpersonen.
- Das zentrale Postfach-Backend für Privatpersonen ersetzt im Zuge der Transition das ZBP-Backend als primäres Bürgerpostfach. Damit ist keine Weiterentwicklung und insbesondere keine funktionale Erweiterung des aktuellen ZBP mehr erforderlich. Vorhandene Daten werden aus dem ZBP-Backend in das Postfach-Backend für Privatpersonen migriert.
- Für einen Übergangszeitraum sollte die API des ZBP weiter bestehen bleiben und für bereits angebundene Systeme eine Übermittlung von Nachrichten an das Matrix-basierte Backend ermöglichen („Legacy-Fassade").
- Das zentrale Postfach-Backend für Privatpersonen ersetzt in Kombination mit dem zentralen Matrix-Backend für Organisationen der Justiz zukünftig das MJP-Backend. Damit ist keine Weiterentwicklung und insbesondere keine funktionale Erweiterung des aktuellen MJP mehr erforderlich. Vorhandene Daten werden aus dem MJP-Backend in das Matrix-Backend für Privatpersonen migriert.

- Organisationen der Justiz sind über das Postfach-Backend für Justiz-Organisationen und den zugehörigen Protokollkonverter nach wie vor ohne Anpassungen an ihren Systemen in der Lage, Nachrichten an Privatpersonen zuzustellen.
- Die Ausstellung von Nachweisen in die EUDI-Wallet erfolgt über Abholscheine, die E2EE-verschlüsselt in das Postfach der Nutzenden zugestellt werden. Eine Aussteller-Komponente wird in der ZaPuK-Infrastruktur nicht eingeführt (ADR-1146, vgl. Abschnitt 5.4.8.2).

4.2.3.2 Zentrales Postfach-Backend für juristische Personen & Protokollkonverter

Der Betrieb des zentralen Postfach-Backends für juristische Personen, also für private Organisationen und öffentliche Stellen, umfasst alle Komponenten, die nach Kapitel 5.2.2 als Kerninfrastruktur für juristische Personen nötig sind. Hierzu zählen insbesondere je ein Homeserver für 1) private Organisationen, 2) öffentliche Stellen und 3) Organisationen der Justiz sowie der Protokollkonverter für die Anbindung des EGVP-Verbunds.

Für alle Organisationstypen erfolgt die Authentifizierung mit Hilfe des Organisationskontos gemäß § 2 Abs. 5 OZG (Mein Unternehmenskonto, MUK) und perspektivisch über die European Business Wallet. Für Postfach-Backends, Nachweisstellen und Siegel kommen PKI-Zertifikate zum Einsatz (vgl. Abschnitt 5.4.5.5). Übergangsweise könnte die Authentifizierung für Organisationen der Justiz mittels eines im SAFE-Verzeichnis hinterlegten Zertifikats erfolgen, sodass hier keine Registrierung eines Mein-Unternehmenskonto-Accounts erforderlich ist (zu klären im Rahmen der Transitionsgespräche).

Empfehlung:

- Die Backends für juristische Personen sollen im FITKO-Produktmanagement durch FIT-Connect betrieben werden.
- Die EGVP-Infrastruktur bleibt bestehen. Ein Protokollkonverter erlaubt die Kommunikation zwischen der Postfach- und Kommunikationsinfrastruktur und dem EGVP-Verbund unter Aufrechterhaltung der Ende-zu-Ende-Verschlüsselung.

Erwägungsgründe für diese Empfehlung:

- Organisationen können über ein einziges Postfach mit allen juristischen Personen und mit Privatpersonen gleichermaßen kommunizieren.
- Durch die Bündelung bei einer betreibenden Partei ist ein effizienterer und qualitativ hochwertigerer Betrieb möglich.
- Im Produkt FIT-Connect bestehen bereits organisatorische, technische und rechtliche Rahmenbedingungen, um öffentliche Stellen und private Organisationen an die FIT-

Connect-Infrastruktur anzubinden (z. B. SSP, Anschlussbedingungen, eine umfangreiche und viel gelobte technische und fachliche Dokumentation, Support-Strukturen für die angebundenen Stellen).

- Der Betrieb dreier Matrix-Homeserver als Teil des zentralen Postfach-Backends ermöglicht eine technische Segregation der Accounts für private Organisationen, öffentliche Stellen und Organisationen der Justiz, was eine Umsetzung und Durchsetzung von gruppenspezifischen Besonderheiten und Vorgaben erleichtert, z. B. den Betrieb des exklusiven Protokollkonverters für Justiz-Organisationen oder die Nutzung verschiedener PKI-Infrastrukturen für private Organisationen und öffentliche Stellen (Prinzip der Separation of Concerns).
- Risiken für die nationale Sicherheit sowie die Privatsphäre von Privatpersonen sind im Falle der Kompromittierung von Metadaten zur Kommunikation von juristischen Personen untereinander nicht in vergleichbarem Maße zu erwarten. Auf eine strikte Aufteilung der Betriebsverantwortung auf drei unabhängige Betreiber wird daher anders als bei der Trennung des Betriebs von Privatpersonen- und Organisations-Backends aufgrund der Vorteile eines gebündelten Betriebs verzichtet (ADR-1114).
- Reduktion der anzubindenden Systeme: Viele Fachbehörden sind bereits an FIT-Connect angebunden und müssen zum Versand bzw. Empfang von Anträgen auch zukünftig an FIT-Connect angebunden sein. Die Notwendigkeit eines zusätzlichen Anbindungswegs entfällt zukünftig.
- Einige Fachbehörden nutzen bereits jetzt die Möglichkeit, über die FIT-Connect-Infrastruktur Nachrichten an das Zentrale Bürger:innen-Postfach zu übermitteln (ZBP-Adapter).
- Aufgrund der Sonderrolle der Justiz im Rahmen der dreigliedrigen Gewaltenteilung besteht seitens des Programms ZaPuK keine Absicht, in die Entscheidungsprozesse der Justizverwaltung einzugreifen. Einer möglichen zukünftigen Entscheidung des E-Justice-Rates zur weiteren Verschmelzung der EGVP-Infrastruktur mit der Postfach- und Kommunikationsinfrastruktur des IT-Planungsrates soll daher nicht vorweggegriffen werden.

Konsequenzen:

- Unternehmen können über FIT-Connect zukünftig sowohl Anträge stellen als auch maschinenlesbar Antragsfolgekommunikation wahrnehmen. Damit können Unternehmen zukünftig mit einer einzigen Anbindung medienbruchfrei und vollständig maschinenlesbar über APIs mit der Verwaltung interagieren. Die Notwendigkeit der parallelen Nutzung von zwei Systemen (FIT-Connect und Unternehmenskonto-Postfach) entfällt.

- Die konkurrierende Koexistenz zwischen bidirektionaler Kommunikation über FIT-Connect und Zustellung von Antragsfolgekommunikation in das Postfach des Organisationskontos wird damit unter Berücksichtigung des bestehenden Rechtsrahmens aufgelöst.
- Eine Anbindung öffentlicher Stellen an mehrere Infrastrukturen wie bisher (MUK-Postfächer zur Kommunikation mit privaten Organisationen, BundID-Postfach zur Kommunikation mit Privatpersonen etc.) ist nicht mehr erforderlich.
- Das zentrale Postfach-Backend für private Organisationen und öffentliche Stellen ersetzt als erste Ausbaustufe der Transition die beiden Postfach-Backends des Mein Unternehmenskontos (Postfach 2.0 + OZG-Plus-Postfach) als primäres Organisations-Postfach. Damit sind keine Weiterentwicklung und insbesondere keine funktionale Erweiterung der Unternehmenskonto-Postfächer mehr erforderlich.
- Das zentrale Postfach-Backend für Organisationen der Justiz ersetzt in Kombination mit dem Protokollkonverter zukünftig das MJP-Backend. Damit ist keine Weiterentwicklung und insbesondere keine funktionale Erweiterung des aktuellen MJP mehr erforderlich.
- Prinzipiell wäre zukünftig auch eine Direktanbindung von Organisationen der Justiz an das Postfach-Backend für Justiz-Organisationen denkbar. Über eine solche Anbindung entscheiden die Organisationen und Governance-Strukturen der Justizverwaltung.
- Die hiermit einhergehende Überführung der Betriebsverantwortung für das Postfach des Organisationskontos nach § 2 Abs. 5 OZG erfordert die Anpassung der Verordnung nach § 3 Abs. 2 OZG.

4.2.3.3 Self-Service-Portal für Organisationen

Das zentrale SSP für Organisationen ermöglicht eine organisatorisch skalierfähige Anbindung einer Vielzahl von IT-Systemen an die Postfach- und Kommunikationsinfrastruktur. Der Betrieb des zentralen SSPs ermöglicht öffentlichen Stellen, privaten Organisationen und den Organisationen der Justiz eine einfache Registrierung des Zugriffs auf das zentrale Postfach-Backend für juristische Personen.

Empfehlung:

- Das zentrale SSP für Organisationen soll im FITKO-Produktmanagement betrieben werden – entweder als Teil des Produktes FIT-Connect oder, vorbehaltlich etwaiger Änderungen des FIT-Connect-Produktschnitts, als Teil einer zu schaffenden föderalen Rollout- und Anbindungsinfrastruktur auf Grundlage des FIT-Connect-SSPs und -SDKs.

Erwägungsgründe für diese Empfehlung:

- Im Zielbild betreibt FIT-Connect das zentrale Postfach-Backend für öffentliche Stellen, private Organisationen und Organisationen der Justiz. Ein gemeinsamer Betrieb des hierzu erforderlichen SSPs reduziert Abstimmungsaufwände hinsichtlich der Betriebskonfiguration dieser nur im engen Zusammenspiel arbeitenden Backend-Komponenten.
- FIT-Connect betreibt bereits ein SSP, welches von antragssendenden Systemen (Onlinedienste, IT-Systeme privater Organisationen) und antragsempfangenden Systemen (insbesondere Fachverfahren) bereits genutzt wird.

Konsequenzen

- Das zentrale SSP nutzt als Provider für Organisationsidentitäten das Organisationskonto nach § 2 OZG (Mein Unternehmenskonto) und perspektivisch die European Business Wallet.
- Das SSP für Organisationen stellt zusammen mit dem Postfach-Backend für juristische Personen eine Absicherung der APIs über die zukünftige föderale API-Autorisierungsinfrastruktur gemäß Beschluss B-2026/16-IT des IT-Planungsrates sicher.
- Die SSPs von BundID und Mein Unternehmenskonto bleiben zunächst bestehen, werden aber zukünftig nicht mehr von Onlinediensten und Fachverfahren für die Postfach-Kommunikation, sondern nur noch von Onlinediensten zur Authentifizierung von Privatpersonen bzw. privater Organisationen genutzt.

Ein Vorhaben zur vollständigen Zusammenführung der SSP in ein produktübergreifendes SSP, wie dies bereits im Produkt FIT-Connect als Teil der föderalen API-Autorisierungsinfrastruktur des IT-Planungsrates angedacht ist, wird seitens des ZaPuK-Programms grundsätzlich begrüßt, überschreitet aber den inhaltlichen Scope dieser Zielarchitektur. Diese Fragestellung muss im Rahmen einer ganzheitlichen Weiterentwicklung des D-Stacks adressiert werden. Das SSP der Zielarchitektur wird so entworfen, dass die Integration der Funktionalität in produktübergreifende Portale einfach möglich ist (ADR-1148).

4.2.3.4 Adressregister

Für die Zuordnung von Organisationsidentitäten zu den technischen Matrix-Adressen bedarf es eines oder mehrerer Adressregister.

Empfehlung:

- Ein Adressregister für private Organisationen und öffentliche Stellen soll im FITKO-Produktmanagement betrieben werden, entweder als Teil des Produkts FIT-Connect oder, vorbehaltlich etwaiger Änderungen des FIT-Connect-Produktschnitts, als Teil einer zu schaffenden föderalen Rollout- und Anbindungsinfrastruktur auf Grundlage des FIT-Connect-SSPs und -SDKs.
- Für Organisationen der Justiz wird das bestehende SAFE-Register nachgenutzt.
- Ein Adressregister für Privatpersonen wird nicht betrieben.

Erwägungsgründe für diese Empfehlung:

- Ein zentrales Adressregister für Privatpersonen birgt Risiken hinsichtlich einer staatlichen oder, im Falle einer Kompromittierung, nicht-staatlichen Profilbildung und ist in der aktuellen Rechtslage nicht umsetzbar. Umsetzungsoptionen zur Ermöglichung einer proaktiven Verwaltung, welche keinen Aufbau eines zentralen Adressregisters erfordern, werden im weiteren Programmverlauf eruiert. Dazu gehört die etwaige Aufnahme einer Postfachadresse in die Melderegister.
- Technisch gibt es keine relevanten Unterschiede zwischen einem Adressregister für private Organisationen und öffentliche Stellen. Ein einheitliches Register reduziert jedoch Betriebsaufwände.
- Technisch besteht eine enge Kopplung des Adressregisters für private Organisationen und öffentliche Stellen an das SSP, das neue Organisationen registriert. Da dieses bei FIT-Connect betrieben wird, sollte auch das Adressregister hier betrieben werden.
- Auch wenn sich die Anforderungen eines Adressregisters für Organisationen der Justiz nicht signifikant von denen des Adressregisters für private Organisationen und öffentliche Stellen unterscheiden, existiert mit dem SAFE-Verzeichnis bereits ein Adressregister für Organisationen der Justiz. Eine Zusammenführung dieses Verzeichnisses mit dem Adressregister für private Organisationen und öffentliche Stellen bietet keinen signifikanten Mehrwert, solange dessen Betrieb für den Erhalt der EGVP-Infrastruktur weiterhin parallel erforderlich ist.

4.2.4 Frontend: Zentraler Postfach-Zugang für Privatpersonen und Organisationen

Für Privatpersonen, private Organisationen, öffentliche Stellen und die Organisationen der Justiz soll an zentraler Stelle ein einheitlicher Postfach-Zugang geschaffen werden.

Empfehlung:

- Realisierung des zentralen Postfach-Zugangs für Privatpersonen und Organisationen im D-Stack durch Bundesportal und Deutschland-App (als Teil des Funktionsbausteins ‚Zentrales Nutzenden-Frontend' der Deutschland-Architektur; vgl. B-2026/03-IT) mit einheitlichem Look-and-Feel und übergreifendem Service-Design.

Erwägungsgründe für diese Empfehlung:

- Bundesportal und Deutschland-App realisieren gemäß Beschluss B-2026/03-IT des IT-Planungsrats den D-Stack-/D-Architektur-Funktionsbaustein „Zentrales Nutzenden-Frontend".

- Die Platzierung des Postfach-Zugangs in Bundesportal und Deutschland-App ermöglicht die Bündelung von Antragstellung und Antragsfolgekommunikation an einem Ort.
- Die Bündelung von Antragstellung und Antragsfolgekommunikation an einem Ort erleichtert durch ganzheitliches Service Design die Schaffung einer für die Nutzer:innen bestmöglichen User Experience (UX). Ein im Rahmen des D-Stack entwickeltes einheitliches Designsystem gibt das Look-and-Feel des Frontends vor.
- Auch in Fällen, in denen eine Antragstellung nicht im Bundesportal oder in der Deutschland-App erfolgt, trägt eine Auffindbarkeit jeglicher Kommunikation mit der Verwaltung an einem zentralen Ort, an dem auch über weitere Verwaltungsleistungen informiert wird, zu einer guten UX bei.
- Das Bundesportal bietet bereits jetzt Services sowohl für Privatpersonen als auch für private Organisationen.

Konsequenzen

- Das zentrale Postfach-Frontend für Privatpersonen und Organisationen ersetzt die bisherigen Postfach-Frontends in BundID, MJP und MUK. Damit ist keine parallele Weiterentwicklung dieser Frontends mehr erforderlich.
- BundID, MJP und MUK sollten nach Abschaltung der jeweiligen Postfach-UIs für einen Übergangszeitraum auf den zentralen Postfach-Client im Bundesportal verlinken.
- Zur besseren Auffindbarkeit (Discoverability) des zentralen Postfach-Zugangs sowie des Bundesportals empfiehlt sich im Rahmen der Weiterentwicklung des Bundesportals zum D-Stack-Baustein *Zentrales Nutzenden-Frontend* der Umzug der Domain verwaltung.bund.de auf eine Dachmarken-konforme gov.de-Domain.

4.3 Governance des ZaPuK-Kommunikationsverbunds

Die zentralen Komponenten eines ZaPuK-konformen Kommunikationsverbunds werden wie vorab beschrieben in mehreren IT-Produkten unter teils verteilter Entwicklungs- und Betriebsverantwortung umgesetzt. Darüber hinaus können Dritte am Kommunikationsverbund teilnehmen, z. B. durch Integration des Postfachs in Fachverfahren oder das Betreiben eines eigenen dezentralen Postfach-Backends. Eine übergeordnete Governance muss daher einen Rahmen setzen, in dem der Verbund ausgestaltet werden kann.

Empfehlung:

- Die strategische Steuerung des ZaPuK-Kommunikationsverbunds erfolgt innerhalb der Strukturen der zurzeit in Ausarbeitung befindlichen Governance des D-Stacks gemäß B-2026/18-IT und der Governance der Deutschland-Architektur gemäß B-

2026/17-IT. Es wird die Etablierung eines für alle Basisdienste des D-Stacks gültigen operativen Produktmanagementmodells empfohlen. In jedem Fall bzw. übergangsweise ist das operative Produktmanagement aller IT-Komponenten der ZaPuK methodisch kongruent auszugestalten und klare Entscheidungskompetenzen und Eskalationswege in diesem zu definieren.

Erwägungsgründe für diese Empfehlung:

- Die zentralen Komponenten werden im Kontext des D-Stacks umgesetzt, insbesondere im Baustein *Postfach und Interaktion*. Zur Sicherung eines erfolgreichen Zusammenspiels aller D-Stack-Bausteine und zur Vermeidung von Doppelstrukturen sollten für die Bausteine, die die Zielarchitektur betreffen, keine nebenläufigen Governance-Strukturen aufgebaut werden.

Aus dem ZaPuK-Programm heraus ergeben sich jedoch diverse Anforderungen an eine solche übergreifende Governance. Diese nachfolgenden Leistungen müssen durch die Governance-Struktur erbracht oder delegiert werden:

- Festlegung der Verantwortlichkeiten für Entwicklung und Betrieb auf Grundlage der jeweils gültigen Fassung des ZaPuK-Architekturkonzepts,
- Strategische Weiterentwicklung im Rahmen der Fortschreibung von Deutschland-Architektur sowie D-Stack (insbesondere in Bezug auf den Funktionsschnitt der Lösungen),
- Koordinierung der Weiterentwicklungsbedarfe zwischen relevanten Bedarfsträgern (insbesondere Teilnehmenden wie Ländern, Kommunen oder Interessensgemeinschaften, standardsetzenden Stellen wie der Matrix Foundation, potenziellen Partnern wie dem Deutschen Gesundheitswesen und der EU),
- Festlegung und Sicherstellung der Einhaltung von Standards, Richtlinien in Betriebsfragen, der Anschlussbedingungen, insbesondere unter Beachtung der besonderen Umstände einer föderierten Infrastruktur,
- Sicherstellung der rechtlichen und regulatorischen Compliance des Kommunikationsverbundes mit sich fortlaufend ändernden rechtlichen Rahmenbedingungen,
- Operative Koordinierung von Weiterentwicklung, Standards und Betrieb über die beteiligten Produkte hinweg,
- Definition von Eskalationspfaden bei Kompatibilitätskonflikten zwischen D-Stack-Bausteinen,
- Klärung der letztinstanzlichen Entscheidung von Streitfällen innerhalb des Kommunikationsverbunds, z. B. Teilnahme an geschlossener Föderation,

- Operative Prüfung, Sanktionierung und Eskalation bei Nichteinhaltung von Vorgaben der Zielarchitektur bzw. der geltenden Anschlussbedingungen durch Teilnehmer:innen des Kommunikationsverbundes, inkl. ggf. Ausschluss von Instanzen aus der geschlossenen Föderation,
- Sicherstellung eines hochverfügbaren und sicheren Betriebs des Kommunikationsverbunds,
- Umsetzung eines operativen, Baustein-übergreifenden Anbindungsmanagements (insbesondere Bereitstellung Dokumentation und Support zum Gesamtkommunikationsverbund),
- Einführung und nachhaltige Durchsetzung der allgemeinen Festlegungen zur Softwareentwicklung der ZaPuK, inkl. der Etablierung von DevSecOps-Pipelines, der Nutzung offener Lizenzen und der Etablierung eines offenen Zusammenarbeitsmodells (vgl. Abschnitt 4.1.4),
- Fortlaufende Dokumentation der Bebauung der Kommunikationsinfrastruktur in einschlägigen architektonischen Artefakten, ggf. als Teil der Dokumentation der Ist-Bebauung der Deutschland-Architektur.

Viele dieser Bedarfe bestehen analog in anderen D-Stack-Bausteinen, sodass eine Festlegung auf Ebene der D-Stack- bzw. Deutschland-Architektur-Governance erfolgen muss. Für die fortlaufende Wahrnehmung dieser Governance-Aufgaben müssen einschlägige operative Strukturen aufgebaut und langfristig unterhalten werden.

5 IT-Architektur

Die IT-Architektur beschreibt die technische Umsetzung der in der Geschäftsarchitektur beschriebenen Prozesse und Informationsobjekte (siehe Kapitel 3). Die zugrundeliegenden Architekturentscheidungen sind in Form von ADRs dokumentiert und für die Ausgestaltung der Zielarchitektur verbindlich. Die Verbindlichkeit der ADRs bezieht sich auf die im Kommunikationsverbund verwendeten Schnittstellen und Protokolle sowie die festgelegten Sicherheitsanforderungen. Die interne Architektur der jeweiligen Lösung, z. B. die Wahl der verwendeten Technologien, bleibt den für die Entwicklung zuständigen Stellen vorbehalten.
Das Kapitel 5 führt vom Allgemeinen zum Konkreten. Abschnitt 5.1 beschreibt das Architekturmodell und die Topologie. Abschnitt 5.2 stellt die Komponenten der Infrastruktur vor, Abschnitt 5.3 ordnet ihnen die Informationsobjekte aus der Geschäftsarchitektur zu. Abschnitt 5.4 fasst die Architekturentscheidungen zusammen, von Topologie, Postfächern und Verschlüsselung über Identität und Adressierung bis zu den Querschnittsthemen, die mehrere Komponenten betreffen. Abschnitt 5.5 zeigt, wie die Komponenten in den zentralen Anwendungsfällen zusammenwirken. Abschließend werden in Abschnitt 5.6 die von der Zielarchitektur unterstützten Betriebsmodelle für anzubindende Organisationen vorgestellt.

5.1 Überblick und Architekturmodell

Die Zielarchitektur ist als offene, föderierte Client-Server-Architektur entworfen, in der sowohl dezentral als auch zentral betriebene Komponenten enthalten sind (vgl. ADR-0002). Nachrichten werden in Postfach-Backends verwaltet und ausschließlich verschlüsselt gespeichert. Diese beschriebenen Bausteine bilden durch Föderation einen Kommunikationsverbund. Postfachzugänge ermöglichen Nutzenden den Zugriff auf ihre Postfächer. Neben dem zentral bereitgestellten Postfach-Frontend (im Folgenden Postfach-Zugang) können auch Fachverfahren und Unternehmensanwendungen über die offene API oder das SDK als Postfachzugänge angebunden werden (vgl. ADR-0003). Das Matrix-Protokoll bildet die einheitliche Schnittstelle im Verbund. Über die Client-Server-API greifen alle Postfachzugänge auf die Backends zu. Über die Server-Server-API föderieren die Postfach-Backends und stellen Nachrichten untereinander zu. Die auf dem Matrix-Protokoll basierende Zielarchitektur gibt die Ende-zu-Ende-Verschlüsselung für alle Nachrichten verbindlich vor (vgl. ADR-0011, ADR-0012). Die Endpunkte der Verschlüsselung sind Endgeräte oder Systeme im Machtbereich der Teilnehmenden (ADR-1100, ADR-1101).

Die Basis des Verbunds bilden Backend- und Frontendsysteme, die zentral bereitgestellt werden (vgl. ADR-0005, ADR-1114). Zudem können Organisationen eigene Backend-Systeme betreiben, wodurch sie die direkte Kontrolle über die Betriebsumgebung, Berechtigungen und Daten erhalten (vgl. ADR-0004). Am Verbund beteiligte Teilnehmer:innen müssen verpflichtende Anschlussbedingungen einhalten (vgl. ADR-1145). Die unterschiedlichen Betriebsmodelle für Organisationen mit und ohne eigene IT werden in Abschnitt 5.4.1 beschrieben (vgl. ADR-1103). Die Interoperabilität mit anderen Kommunikationssystemen wie z. B. OSCI wird über Protokollkonverter unter Beibehaltung der Ende-zu-Ende-Verschlüsselung realisiert (vgl. ADR-0010).

Das System wird nach Security-by-Design- sowie Privacy-by-Design-Prinzipien und basierend auf dem Zero-Trust-Prinzip entworfen. Die Kommunikationsparteien weisen ihre Identität gegenseitig im Ende-zu-Ende-verschlüsselten Kanal nach, wobei die Authentifizierung durch externe Identitätsprovider gewährleistet wird (vgl. Abschnitt 5.5). Bei bilateraler Kommunikation liegt der E2EE-Endpunkt im Endgerät (ADR-1100). Bei Mehrbenutzer:innen-Szenarien mit Funktionspostfächern (gemeinsamen Postfächern einer Organisation unter einer Funktionsadresse), Bearbeitungsgruppen und Bearbeitungsvertretungen kann ein zusätzlicher E2EE-Endpunkt auf einem Server im Machtbereich der Organisation liegen (ADR-1101). Die Prüfung von Anhängen auf Malware kann nach der Entschlüsselung sowohl in den Endgeräten als auch in Servern der Organisation erfolgen (vgl. ADR-1130).

Postfachzugänge können die Erzeugung von Abruf- und Lesebestätigungen ermöglichen (ADR-1118). Die beim Eingang im Postfach-Backend erzeugten Bereitstellungsbestätigungen sind verpflichtend umzusetzen (vgl. ADR-0018).

Um das Zusammenwirken der zentralen Komponenten zu illustrieren, werden nachfolgend drei beispielhafte Anwendungsfälle erläutert (siehe Abb. 5):

I. Ein Antrag einer Privatperson wird beschieden

Nach Anmeldung an einem Onlinedienst über den Identity-Provider BundID füllt die Privatperson einen Antrag aus und schickt ihn ab. Im Backend des Onlinedienstes wird dieser mittels FIT-Connect an die Behörde weitergereicht. Die Sachbearbeiter:innen der Behörde bearbeiten den eingegangenen Antrag in ihrem Fachverfahren. Im Antrag ist das Pseudonym der Privatperson als Bestandteil der Identität enthalten. Aus dem Pseudonym wird die Matrix-Adresse (MXID) der Privatperson abgeleitet und kann von der Behörde für die Rückantwort verwendet werden. Die zuständigen Sachbearbeiter:innen der Behörde erstellen nach der

Prüfung den Bescheid und übermitteln ihn über den in der Fachverfahrensanwendung enthaltenen Postfach-Zugang an die Adresse der Privatperson. Über die App, die den zentralen Postfach-Zugang realisiert, wird die Privatperson per Push-Benachrichtigung auf ihrem Mobilgerät über den Eingang einer Nachricht informiert. Sie öffnet den Postfach-Zugang, sieht eine Nachricht von der spezifischen Behörde, kann den Bescheid einsehen und lokal ablegen.

II. Eine Behörde schreibt ein Unternehmen an und bittet um Informationen

In einer Behörde gibt es ein spezifisches Anliegen an ein Unternehmen, für das noch kein Vorgang existiert. Eine Sachbearbeiter:in der zuständigen Gruppe sucht über den Postfach-Zugang im Adressregister des Verbunds eine zum Anliegen passende Postfachadresse eines Funktionspostfachs des Unternehmens (beispielsweise @brandschutz:unternehmen_xy.example.org). Die Einträge pflegt das Unternehmen selbst in der Administrationsoberfläche seines Postfach-Backends. Sie sind hier mit der Organisationsidentität verknüpft (ADR-1111, ADR-1148). Sie verfasst eine Nachricht mit dem konkreten Anliegen und übermittelt sie an das gewählte Postfach. Im Postfach-Zugang der Bearbeiter:innengruppe der Behörde wird dieser neue Vorgang sichtbar. Die Nachricht wird über das Postfach-Backend der Behörde in das Postfach-Backend des Unternehmens zugestellt. Das Postfach-Backend des Unternehmens quittiert den Eingang mit einer Bereitstellungsbestätigung. Ein:e Mitarbeiter:in der im Unternehmen zuständigen Gruppe greift über den zentralen Postfach-Zugang oder eine Unternehmensanwendung mit integriertem Postfach-Zugang auf das Funktionspostfach zu. Hier wurde durch das System ein neuer Vorgang angelegt. Die Mitarbeitenden verfassen die Antwort im Namen der Organisation, wobei der Identitätsnachweis die Organisationsidentität eindeutig zuordnet (ADR-1106, ADR-1107).

III. Ein Antrag eines Unternehmens wird beschieden

Zur Antragstellung meldet sich ein:e Mitarbeiter:in eines Unternehmens beim Onlinedienst mit dem Organisationskonto an. Die Einreichung des Antrags bei der Behörde ist wie im vorangegangenen Anwendungsfall über FIT-Connect umgesetzt. Im Antrag geben die Mitarbeitenden als Rückantwortadresse ein Funktionspostfach an. Dazu wählen die Mitarbeitenden aus der Liste der Funktionspostfachadressen des Unternehmens eine Postfachadresse aus (ADR-1104). Bevor die Behörde einen Bescheid an die angegebene Adresse übermittelt, prüft das Fachverfahren, ob die Adresse zum Unternehmen gehört, dessen Organisationsidentität im Antrag enthalten ist, und welchen Status der Eintrag im Adressregister hat (ADR-1111). Ein Versand an ein gesperrtes oder nicht dem Unternehmen zugehöriges Postfach wird verhin-

dert. Das anzuschreibende Funktionspostfach ist erst aktiv, wenn mindestens ein Mitglied der zugehörigen Gruppe existiert. Nachdem die Behörde den Bescheid an die angegebene Adresse übermittelt hat, wird ein Vorgangsraum erzeugt und die vom Unternehmen in der Administrationsoberfläche des Postfach-Backends für dieses Funktionspostfach konfigurierten Mitglieder werden in den Raum eingeladen (ADR-1102, ADR-1112). Analog zum vorangegangenen Anwendungsfall erhält die Behörde eine Bereitstellungsbestätigung (ADR-0018). Auf Seite des Unternehmens findet die Prüfung des in der Bescheid-Nachricht enthaltenen Identitätsnachweises statt (ADR-1106, ADR-1107). Die Umsetzung der kryptographischen Räume und die Rollen der technischen Nutzer sind in ADR-1109 festgelegt.

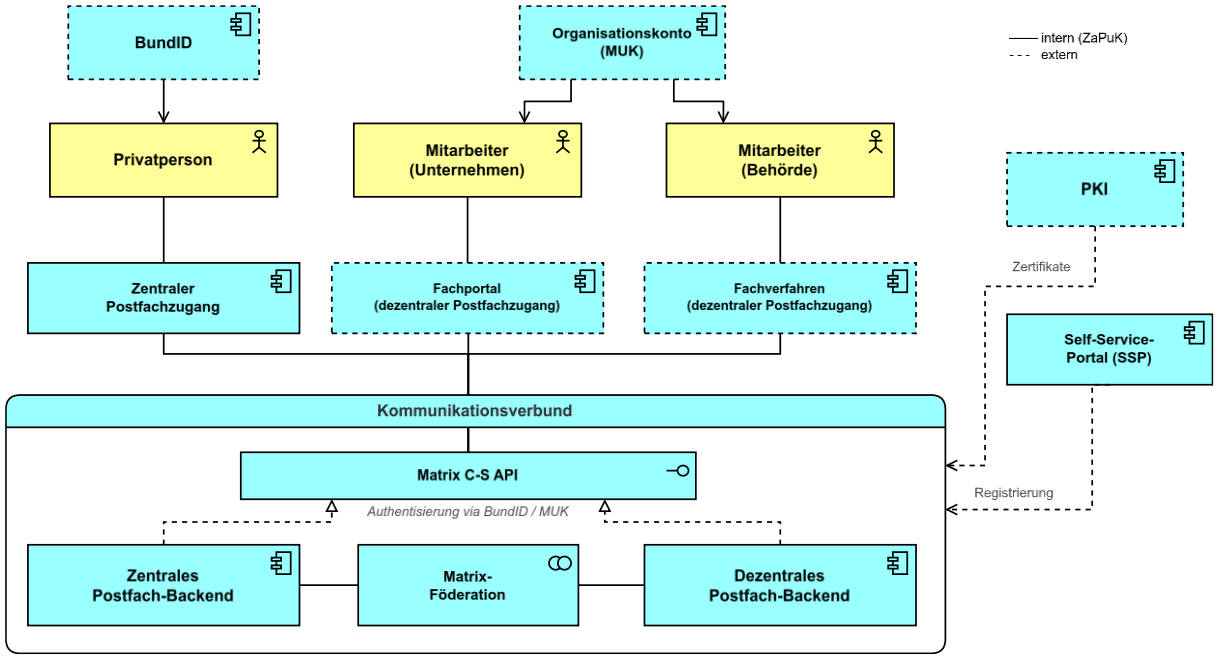

Abbildung 4: Applikationssicht des ZaPuK-Kommunikationsverbundes

5.2 Applikationssicht

In diesem Kapitel werden die Komponenten der Infrastruktur mit ihren Verantwortlichkeiten und Schnittstellen beschrieben (siehe Abb. 6).

In den in Abschnitt 5.1 beschriebenen Anwendungsfällen sind die Kernkomponenten der Zielarchitektur bereits in Teilen kurz genannt. Ein Postfach-Zugang ist die Anwendung (Client), mit der Nachrichten verfasst, versendet und erhalten werden. Die Nachrichten liegen verschlüsselt im Postfach-Backend, welches mit anderen Postfach-Backends den Verbund der Zielarchitektur bildet. Postfach-Backends können von Organisationen selbst betrieben wer-

den. Die Konfiguration der Gruppe der Nutzer:innen kann über organisationsinterne Berechtigungsverzeichnisse erfolgen (vgl. Abschnitt 5.6). Um Adressen von Organisationen zu ermitteln, werden diese im föderierten Adressregister registriert. Die das System nutzenden Personen authentifizieren sich über einen Identity-Provider. Mit über die Authentisierung erhaltenen Nachweisen, die Absender:innen im verschlüsselten Kanal übermitteln, können Empfänger:innen die Nachrichten zum Beispiel Organisationsidentitäten zuordnen. Adressen von Privatpersonen werden in keinem Adressregister gelistet. Diese leiten sich aus der Identität der Privatperson als Pseudonym ab.

Entsprechend ihrer Rolle in der Gesamtarchitektur sind die Komponenten der Zielarchitektur in drei Gruppen gegliedert. Infrastrukturnutzende Systeme greifen auf die Postfächer bzw. Nachrichten des Systems zu und bieten Nutzendenschnittstellen für die Kommunikation an. Die Kerninfrastruktur umfasst die für den Kommunikationsverbund notwendigen Komponenten für die Verarbeitung und den Versand von Nachrichten. Darüber hinaus gehören ihr querschnittliche Systeme für Governance und Administration an. Unterstützende externe Systeme sind nicht Bestandteil der Infrastruktur selbst, stellen aber für den Betrieb notwendige Dienste wie Identity-Provider zur Verfügung.

Jede Organisation entscheidet selbst, ob sie das zentrale Angebot nutzt oder den Betrieb eigenverantwortlich übernimmt (vgl. ADR-1103). Einige Komponenten werden ausschließlich zentral betrieben, andere können auch dezentral betrieben werden. Wie die Komponenten zusammenwirken, wird in Abschnitt 5.5 erläutert.

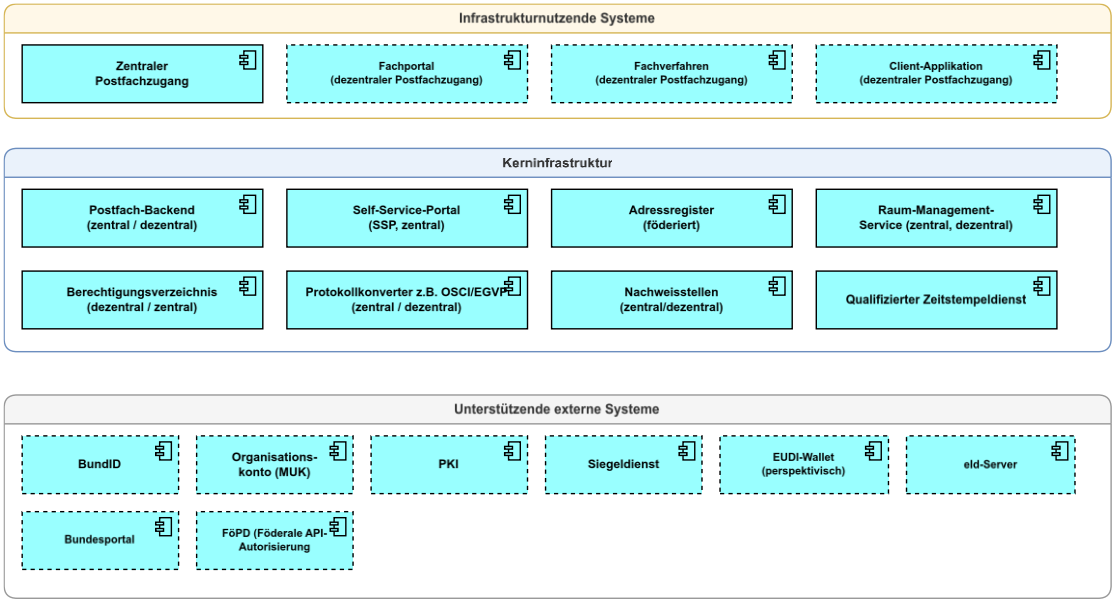

Abbildung 5: Infrastrukturnutzende und unterstützende externe Systeme

5.2.1 Infrastrukturnutzende Systeme

Infrastrukturnutzende Systeme sind alle Clients, über die Nutzer:innen auf Postfächer zugreifen. Die Infrastruktur unterscheidet zwischen dem zentral bereitgestellten Postfach-Zugang als Basisangebot und dezentralen Postfachzugängen. Dezentrale Postfachzugänge umfassen Fachportale, Fachverfahren, Unternehmensanwendungen und weitere Client-Applikationen. Alle Postfachzugänge greifen über die offene API auf die Infrastruktur zu, optional unter Verwendung des SDK (ADR-0003, ADR-0009) (siehe Tab. 4).

Komponente	Rolle	Bereitstellung	ADRs
Zentraler Postfach-Zugang	Frontend für alle Nutzendengruppen	zentral	0005
Fachportale (z.B. ELSTER)	Zugang im Kontext eines Verwaltungsbereichs	dezentral	0003, 1105
Fachverfahren und Unternehmensanwendungen	Anbindung über API/ SDK, interaktiv und automatisiert	dezentral	0003, 0009, 1119
Weitere Client-Applikationen	Mobile Apps, Desktop-Clients	dezentral	0003

Tabelle 4: Infrastrukturnutzende Systeme

5.2.1.1 Zentraler Postfach-Zugang

Die Matrix-Clients der Zielarchitektur, die den Zugriff auf die in den Postfach-Backends enthaltenen Postfächer ermöglichen, werden als Postfachzugänge bezeichnet. Sie ermöglichen den Zugriff nach Authentifizierung. Privatpersonen nutzen dafür die BundID mit der eID als Identifizierungsmittel (vgl. Abschnitt 5.4.5). Private Organisationen nutzen das Organisationskonto. Neben diesen Möglichkeiten wird auch eine Authentifizierung mittels eID-Server, EU-DI-Wallet und European Business Wallet entworfen (vgl. Abschnitt 5.2.3). Der zentrale Postfach-Zugang wird als Bestandteil der zentralen Infrastruktur bereitgestellt. Eine Besonderheit des zentralen Postfach-Zugangs für Privatpersonen ist, dass er mehrere bereichsspezifische Postfächer (Postfächer derselben Person in unterschiedlichen Verwaltungsbereichen) in einer gemeinsamen Ansicht zusammenführt (vgl. ADR-1105). Der Postfach-Zugang soll mindestens als webbasierter Client sowie als mobile Smartphone-App bereitstehen. Der Postfach-Zugang stellt Abholscheine für Nachweise dar und ermöglicht es, mittels der Wallet-App die Abholung des Nachweises zu initiieren (ADR-1146).

5.2.1.2 Fachportale

Fachportale sind dezentrale Postfachzugänge, die in einem bestimmten Verwaltungsbereich verwendet werden, z. B. das ELSTER-Fachportal für den steuerlichen Bereich, Justizportale im elektronischen Rechtsverkehr oder das Verwaltungsportal Bund. Die Authentisierung ist analog der Umsetzung im zentralen Postfach-Zugang entworfen. Der Unterschied liegt im Umfang des Zugriffs. Die Anmeldung erfolgt im jeweiligen Verwaltungsbereich und liefert nur die bereichsspezifische Adresse (MXID) des Nutzenden für diesen Bereich. Auf die Kommunikation der Nutzenden mit anderen Verwaltungsbereichen kann im Fachportal deshalb nicht zugegriffen werden (vgl. ADR-1105 zur bereichsspezifischen Adressierung). Die Anbindung erfolgt über das SDK oder die Matrix-Client-Server-API.

5.2.1.3 Fachverfahren und Unternehmensanwendungen

Fachverfahren und Unternehmensanwendungen sind dezentrale Postfachzugänge, die Nachrichten versenden und empfangen können. Für die Integration des Matrix-Clients in die Anwendungen kann das ZaPuK-SDK oder direkt die Matrix-Client-Server-API verwendet werden. Durch Teilnahme technischer Nutzer:innen (automatisierte Konten) an den Vorgangsräumen ist eine automatische Verarbeitung der Nachrichten möglich. Vorgangsräume sind abgeschlossene kryptografische Räume, in denen die Kommunikation eines Vorgangs enthalten ist (vgl. Abschnitt 5.4.3). Die Authentisierung erfolgt über die externen Identity-Provider oder andere Authentisierungsmittel wie eID oder EUDI-Wallet. Funktionen zur Aufbewahrung bzw. Veraktung sind Bestandteil der Fachanwendung.

5.2.1.4 Weitere Client-Applikationen

Durch die offenen Schnittstellen ermöglicht die Zielarchitektur unabhängig entwickelte und betriebene Client-Applikationen. Dazu können Webanwendungen, native Anwendungen oder mobile Applikationen gehören, die Drittanbieter entwickeln und vertreiben. Die Entwicklung wird durch das zentral entwickelte ZaPuK-SDK unterstützt, das Bibliotheken zur Implementierung der Schnittstellen enthält und diverse essenzielle Features bereits mitliefert. Eine Anbindung der Client-Server-API des Matrix-Protokolls ohne dieses SDK ist zwar aufwändig und nicht empfohlen, bleibt aber möglich. Nutzende erhalten so ein breites Angebot an Lösungen für den Zugang zu ihren Postfächern.

5.2.2 Kerninfrastruktur

Zur Kerninfrastruktur der Zielarchitektur gehören die Systeme, die den Verbund zur gemeinsamen Kommunikation technisch ermöglichen. Die bedeutendste Komponente ist das Post-

fach-Backend, das mit dem enthaltenen Matrix-Homeserver Nachrichten Ende-zu-Ende-verschlüsselt in Postfächern speichert und diese mit anderen Backends austauscht. Die Föderation dieser Postfach-Backends bildet den ZaPuK-Verbund, der die Adressierung gewährleistet und eine beweissichere Übermittlung der Nachrichten ermöglicht. Weitere Komponenten der Kerninfrastruktur ermöglichen die Umsetzung von Postfächern, die durch Gruppen genutzt werden (siehe Tab. 5).

Komponente	Aufgabe	Bereitstellung	ADRs
Postfach-Backend	Datenhaltung, Föderation, Adressverzeichnis, Postfachadministration, Quittierung, Benachrichtigung	zentral, dezentral optional	0004, 0007, 0011, 1103, 1104, 1105, 1114
Self-Service-Portal (SSP)	Registrierung, Onboarding, Anschlussbedingungen	zentral	0008, 1111, 1145, 1148
Adressregister	Zuordnung von Postfachadresse zu Organisationsidentitäten	logisch einheitlich, föderiert je Postfach-Backend	1111
Nachweisstellen	Erzeugung der Identitätsnachweise, zentrale Nachweisstelle und Org-IdP-Adapter	Instanz je zentralem Postfach-Backend oder dezentral (Org-IdP-Adapter)	1106, 1107, 1108
Raum-Management-Service (RMS)	Erzeugung und Steuerung von Vorgangsräumen, Durchsetzung von Bearbeitungsgruppen und Bearbeitungsvertretungen	zentral, dezentral	1101, 1102
Berechtigungsverzeichnis	Pflege von Postfachmitgliedschaften, Rollen und Bearbeitungsvertretungen für Funktionspostfächer	dezentral, alternativ zentral im Postfach-Backend	1102, 1112
Protokollkonverter	Interoperabilität mit Fremdsystemen auf E2EE-Schicht	zentral, dezentral	0010
Qualifizierter Zeitstempeldienst	Qualifizierte Zeitstempel für Bereitstellungsbestätigungen	zentral	0018, 1144

Tabelle 5: Überblick über Architekturentscheidungen je Komponente der Kerninfrastruktur

Die Zielarchitektur erlaubt entsprechend dem API-First-Ansatz, alle Funktionen vollständig über offene, gut dokumentierte Schnittstellen zu nutzen (ADR-0003).
Ergänzend wird ein SDK zentral bereitgestellt (ADR-0009). Das SDK kapselt insbesondere die Komplexität der Ende-zu-Ende-Verschlüsselung (Schlüsselmanagement, Schlüsselaustausch, Ver- und Entschlüsselung) und ermöglicht eine sichere Anbindung, ohne diese Funktionen selbst implementieren zu müssen. Das SDK ist nicht verpflichtend. Die API ist auch ohne SDK vollständig nutzbar.
Die API ermöglicht zudem die vollständig automatisierte Nutzung ohne interaktive Anmeldung. Fachverfahren und Unternehmensanwendungen authentisieren sich über Client Credentials und können Nachrichten automatisiert versenden, empfangen und verarbeiten. Die Autorisierung der Systemzugriffe auf Schnittstellen im Verbund (z. B. auf die Client-Server-APIs der Postfach-Backends) erfolgt über die föderale API-Autorisierungsinfrastruktur (vgl. Abschnitt 5.4.5.3).
Mittels des zentral bereitgestellten qualifizierten Zeitstempeldienstes werden im Verbund Bereitstellungsbestätigungen und weitere Nachweise mit qualifizierten Zeitstempeln versehen, die Zeitpunkte beweissicher angeben (ADR-0018, ADR-1144).

5.2.2.1 Postfach-Backend

Das Postfach-Backend speichert Nachrichten dauerhaft in Ende-zu-Ende-verschlüsselter Form, stellt die Föderation mit anderen Backends im Kommunikationsverbund sicher und erzeugt Bereitstellungsbestätigungen beim Nachrichteneingang. Es kommuniziert mit dem lokalen Adressregister-Dienst als Bestandteil eines föderierten Adressregisters und stellt dessen Abfrageschnittstelle bereit (vgl. Abschnitt 5.2.2.3, ADR-1111). Für die Pflege der Postfachadressen stellt es eine Administrationsoberfläche bereit. Es wird zentral bereitgestellt, kann aber optional von Organisationen dezentral im eigenen Machtbereich betrieben werden. Jedes Postfach-Backend besteht aus den in Abbildung 7 dargestellten Diensten, deren Beschreibungen Tabelle 6 zu entnehmen sind.

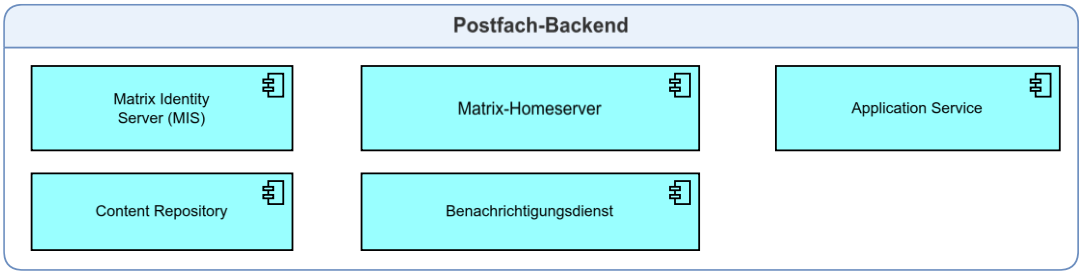

Abbildung 6: Dienstebündel zur Implementierung des Postfach-Backends

Dienst	Beschreibung	ADRs
Matrix-Homeserver	verwaltet Postfächer, speichert Nachrichten verschlüsselt, föderiert mit anderen Homeservern, bildet den Kommunikationsverbund	0006, 0011
Matrix-Identity-Service (MIS)	Schnittstelle des föderierten Adressregisters (vgl. Abschnitt 5.2.2.3), bildet Attribute wie Behördenkennzahl (BKZ) und X.509-Fingerprint auf Matrix-Adressen (MXIDs) ab	1104, 1105, 1111
Quittungsdienst (Application Service)	Erzeugt signierte Bereitstellungsbestätigungen und Löschquittungen, kein Zugriff auf Nachrichtenklartext	0018
Content Repository	Speichert Dateianhänge als verschlüsselte Blobs.	0011, 1120
Benachrichtigungsdienst	benachrichtigt bei neuen Nachrichten z. B. per E-Mail (SMTP) und Push (APNs/FCM), relevant für Bekanntgabefristen (§ 37 Abs. 2a SGB X, § 9 OZG).	0011

Tabelle 6: Bestandteile des Postfach-Backends

Bei souveränem Betrieb (ADR-1103) betreibt die Organisation alle genannten Dienste eigenverantwortlich. Eine Implementierung der wichtigen Komponenten wird zentral zur freien Verwendung angeboten. Durch Anschlussbedingungen wird der Rahmen für die Aufnahme der Komponenten in den Verbund vorgegeben, deren Einhaltung über die Registrierung im SSP verbindlich gemacht wird (ADR-0007, ADR-1145). Die Festlegung, wie die Anschlussbedingungen im Einzelnen durchgesetzt werden, erfolgt risikobasiert. Neben vertraglichen Zusicherungen und technischen Maßnahmen werden Auditierung und Prüfung durch die Governanceprozesse nur im notwendigen Fall durchgeführt. Ziel ist es, eine geringe Hürde für den Anschluss beizubehalten und dabei die Funktionalität und Sicherheit des Verbunds trotzdem zu gewährleisten.

5.2.2.2 Self-Service-Portal für Organisationen

Das SSP ist die zentrale Komponente für Anbindung, Onboarding und Verwaltung von Organisationen im Kommunikationsverbund (ADR-0008). Neben den Administrator:innen der Organisationen (Org-Admins) werden hier auch die dezentral betriebenen Komponenten registriert und verwaltet. Im Detail enthält es folgende Funktionen:

- Registrierung von Organisationen und ihrer ggf. dezentral betriebenen Backends im Kommunikationsverbund, einschließlich der Einholung der Zustimmung zu den Anschlussbedingungen (ADR-1103, ADR-1145). Zentrale Postfach-Backends werden ebenso wie dezentrale Backends über das SSP registriert.
- Postfach-Backends werden durch die Verbund-Governance in einem manuellen Freigabeschritt in die Föderationsliste aufgenommen. Alle anderen Schritte in den Prozessen zur Registrierung von Organisationen und Postfach-Backends werden automatisiert umgesetzt (ADR-1148).
- Registrierung öffentlicher Schlüssel (Zertifikate) der Postfach-Backends (ADR-0018).
- Konfiguration der Namen von Domains bzw. die Vergabe von Organisations-Präfixen bei Nachnutzung des zentralen Backends (ADR-1104). Die Postfachadressen selbst, also die Funktionspostfächer, legt die Organisation in der Administrationsoberfläche des zentralen Postfach-Backends an und pflegt sie dort (vgl. Abschnitt 5.2.2.1).
- Verwaltung von Zertifikaten der angebundenen Komponenten. Die API-Autorisierung (Client Credentials, Access Tokens, Policy Decisions) wird über die föderale API-Autorisierungsinfrastruktur umgesetzt, die mit dem SSP integriert ist (vgl. Abschnitt 5.4.5).
- Beim Betriebsmodell A (ADR-1103) wird die Zuordnung von Nutzenden zu Postfächern direkt in der Administrationsoberfläche des zentralen Postfach-Backends verwaltet (ADR-1112).
- Durch verbindlich definierte und dokumentierte Schnittstellen ist die Funktionalität des SSP leicht in andere Prozesse bzw. Portale integrierbar. Das Onboarding der Organisationen kann somit durch andere Prozesse wie zum Beispiel die digitale Unternehmensgründung angestoßen werden, wobei die Entwicklung medienbruchfreier Benutzerschnittstellen umsetzbar wird (ADR-1148).
- Die Registrierung kann in die Prozesse des Organisationskontos integriert werden, wobei Stammdaten aus der Identifizierung für die Vorbefüllung von Formularen verwendet werden können. Auch Onlinedienste können die Registrierung im Antragskontext integrieren, wenn eine digitale Rückantwort gewünscht ist und noch keine Adresse existiert (ADR-1148).

5.2.2.3 Adressregister

Das Adressregister ordnet organisationsbezogene Postfachadresse und Organisationsidentität eindeutig zu (ADR-1111). Es ist die im Verbund führende Quelle zur Ermittlung der korrekten Adressen bzw. der Prüfung, ob eine Adresse auch tatsächlich zu einer Organisation gehört.

Der Betrieb des Adressregisters erfolgt in jenem Postfach-Backend, dessen Domain den globalen Teil der im Register gelisteten Postfachadressen bildet. Das zentral betriebene Postfach-Backend enthält somit ein Adressregister ebenso wie die dezentral betriebenen Backends. Die Vergabe der Domains der Postfach-Backends und die Vergabe der Organisationspräfixe des zentralen Backends wird über das SSP gesteuert. Die einzelnen Postfachadressen pflegt die Organisation in der Administrationsoberfläche des Postfach-Backends. Die Betreiber dezentraler Postfach-Backends können den lokalen Teil der Adressen ihrer Postfächer frei wählen. Die Abfrage einer Adresse des Registers gibt der aufrufenden Person die Organisationszuordnung, den Status und das zuständige Backend (bzw. Domain) zurück. Eine Abfrage nach der Organisation ist ebenso möglich und erlaubt die Ermittlung der zugeordneten Postfachadressen. Technisch ist das Adressregister eine Implementierung der API Matrix-Identity-Service und föderiert mit den anderen Registern im Verbund (vgl. Abschnitt 5.2.2.1).

5.2.2.4 Nachweisstellen

Nachweisstellen erzeugen die Identitätsnachweise im ZaPuK-Verbund (ADR-1106, ADR-1107). Diese werden im verschlüsselten Nachrichtenkanal transportiert und bestätigen die fachliche Identität der Absender:innen. Die nachgewiesene Identität wird aus den Quellen BundID, Organisationskonto und der EUDI-Wallet bezogen. Folgende Nachweisstellen sind vorgesehen (ADR-1108):

- Zentrale Nachweisstelle, überführt die Assertions der IdP (BundID, Org-Konto) für Privatpersonen und Organisationen ohne eigenes IdM (Betriebsmodell A/B) in ZaPuK-konforme Identitätsnachweise (ADR-1107)
- Org-IdP-Adapter übersetzt die Nachweise eines organisationsinternen Identitätsmanagements (IdM) in ZaPuK-konforme Nachweise (ADR-1108)

In der verbundweiten Trust-Infrastruktur sind alle zugelassenen Nachweisstellen mit ihren Schlüsseln, Gültigkeitszeiträumen und der Statushistorie gelistet. Einträge werden zum Beispiel bei der Registrierung eines Org-IdP-Adapters durch den Org-Admin eines Unterneh-

mens im SSP initiiert. Die Einträge sind jeweils signiert und standardisiert abrufbar, etwa als Software Statement Assertions (ADR-1108).

5.2.2.5 Gruppenmitgliedschaften für Funktionspostfächer

Organisationen mit Funktionspostfächern benötigen Dienste, mit denen die Mitgliedschaften in Gruppen gesteuert werden. Diese Dienste, die in Tabelle 7 konkretisiert werden, werden im Machtbereich der Organisation betrieben (Betriebsmodell B und C) oder zentral bereitgestellt (Betriebsmodell A, vgl. ADR-1102, ADR-1103).

Dienst	Beschreibung	ADRs
Raum-Management-Service (RMS)	Erzeugt bei Anfragen an Funktionspostfächer automatisch Vorgangsräume, lädt zuständige Personen ein und setzt Bearbeitungsgruppen sowie Bearbeitungsvertretungen durch. Je nach Anforderung bzgl. Vertraulichkeit oder Vertretungsprozessen kann er ohne oder mit Teilnahme an E2EE konfiguriert werden. Der RMS kann organisationsintern betrieben werden oder es wird der RMS eines zentralen Postfach-Backends (ohne E2EE-Teilnahme) verwendet.	1101, 1102
Berechtigungsverzeichnis	Pflege von Postfachmitgliedschaften, Rollen und Bearbeitungsvertretungen für Funktionspostfächer. Liefert dem RMS die Berechtigungsinformationen. Zentral im Postfach-Backend (Betriebsmodell A) oder organisationsintern (ADR-1112).	1102, 1112

Tabelle 7: Gruppenmitgliedschaften für Funktionspostfächer

5.2.2.6 Protokollkonverter

Um externe Systeme, die andere Protokolle verwenden, an die Zielarchitektur anbinden zu können, wird ein Protokollkonverter verwendet. Protokollkonverter erlauben einen Transport über die Grenze der ZaPuK-Infrastruktur in das angebundene System unter Aufrechterhaltung der Ende-zu-Ende-Verschlüsselung. Dies wird durch Transformation des Kommunikationsprotokolls des externen Systems von und in Nachrichten gemäß dem Matrix-Protokolls ermöglicht, wobei die Verschlüsselungsschicht der jeweiligen Protokolle unangetastet bleibt. Die Nutzung eines Protokollkonverters erfordert die Unterstützung mindestens eines gemeinsamen Inhaltsdatenformats.

Im Rahmen der Transitionsbetrachtung des Mein-Justiz-Postfachs (MJP) wird diese Komponente für die Anbindung der EGVP/OSCI-Infrastruktur der Justiz verwendet. Dabei werden verschlüsselte OSCI-Container in Matrix-Nachrichten verpackt und zwischen dem Postfach-

Zugang und dem an den Protokollkonverter angebundenen OSCI-Intermediär ausgetauscht. Zusätzlich muss zwischen den Adressen der Zielarchitektur und des externen Systems übersetzt werden. Postfach-Zugänge müssen im Fall des MJP nun die Kryptografie von Matrix und des externen OSCI-Protokolls umsetzen sowie das im EGVP-Verbund genutzte Inhaltsdatenformat unterstützen, was entsprechende Komplexität mit sich bringt.
Eine alternative Umsetzung mittels einer Bridge, bei der Nachrichten des jeweiligen Systems bei der Vermittlung zunächst entschlüsselt werden, schließt die Zielarchitektur aufgrund des daraus resultierenden eklatanten Sicherheitsrisikos aus (ADR-0010).

5.2.3 Unterstützende externe Systeme

Unterstützende externe Systeme sind nicht Teil der Kommunikationsinfrastruktur, stellen aber Dienste bereit, die für den Betrieb notwendig sind. Sie werden nicht im Rahmen des Programms umgesetzt. Die Zielarchitektur definiert Schnittstellen zu diesen Systemen und formuliert gegebenenfalls Anforderungen an deren Weiterentwicklung (siehe Tab. 8). Besondere Bedeutung haben die externen Identitätsprovider. Ihre Identitätsnachweise werden über die Nachweisstellen (vgl. Abschnitt 5.2.2.4) in den ZaPuK-konformen Identitätsnachweis überführt (ADR-1106, ADR-1108).

Komponente	Rolle	Bereitstellung	ADRs
BundID	Identitätsprovider für Privatpersonen, bereichsspezifische Pseudonyme, die für die Adress-Ableitung verwendet werden	außerhalb des Programmumfangs	0014, 1105
Org-Konto	Identitätsprovider für Organisationen und Behörden	außerhalb des Programmumfangs	0015, 0016
PKI (V-PKI / ELSTER)	Zertifikate für Infrastruktur und Organisationen	außerhalb des Programmumfangs	1144
EUDI-Wallet	Perspektivisches Authentisierungsmittel für alle Nutzendengruppen, Abholung von Nachweisen über Abholscheine	außerhalb des Programmumfangs	0014, 0015, 0016, 1146
Wallet-Adapter / zentraler Issuer-Dienst (ZID)	Systeme für die Ausstellung der Nachweise in die EUDI-Wallet, betrieben durch Fachbehörden bzw. den Bund	außerhalb des Programmumfangs	1146
Siegeldienst	Qualifiziertes elektronisches Siegeln von Dokumenten vor Versand, zentraler Dienst des Bundes	außerhalb des Programmumfangs	0017

Malware-Scanner	Malware-Prüfung empfangener Nachrichten. Ort abhängig vom E2EE-Endpunkt und Betriebsmodell.	außerhalb des Programmumfangs	1130
Föderale API-Autorisierungsinfrastruktur (FöPD)	Autorisierung der System-zu-System-Zugriffe (Authorization Server, Client-Registrierung, Policy Decision Points)	außerhalb des Programmumfangs	

Tabelle 8: Unterstützende externe Systeme

5.3 Informationssicht

Tabelle 9 ordnet die Informationsobjekte der Zielarchitektur (siehe Version 1.0 dieses Konzepts) den Komponenten aus Abschnitt 5.2 zu und benennt ihre technische Repräsentation.

Informationsobjekt	Komponente	Techn. Repräsentation
Nachricht	Homeserver	Verschlüsseltes Matrix Room Event
Anhang	Content Repository	Verschlüsselte Datei, referenziert über URI
Vorgang	Homeserver, RMS	Matrix-Raum (Vorgangsraum) (ADR-1102)
Postfach	Homeserver	Matrix-Konto einer Matrix-User-ID (MXID) also einer Adresse zugeordnet (ADR-1102, ADR-1104)
Identitätsnachweis	Nachweisstelle, Client	Signiertes Token (SD-JWT VC), wird im Kommunikationskanal übermittelt (ADR-1106, ADR-1107)
Bereitstellungsbestätigung	Quittungsdienst	Signiertes Event über den Ciphertext-Eingang (ADR-0018)
Abrufbestätigung	Client	Verschlüsseltes Custom-Event (ADR-1118)
Lesebestätigung	Client	Verschlüsseltes Custom-Event (ADR-1118)
Berechtigung	Berechtigungsverzeichnis	Eintrag zu Postfachmitgliedschaft, Rolle und Bearbeitungsvertretung (ADR-1112)
Adresseintrag	Adressregister	Zuordnung von Postfachadresse, Organisationsidentität, Status und zuständigem Backend (ADR-1111)

Tabelle 9: Informationsobjekte

5.4 Architekturentscheidungen

ADR-ID	Phase	Titel des ADR
ADR-0000	I	Dokumentation von Architekturentscheidungen
ADR-0001	I	Querschnittlichkeit und Erweiterbarkeit der Infrastruktur
ADR-0002	I	Infrastrukturtopologie
ADR-0003	I	Bereitstellung von Postfach-Zugängen durch Dritte
ADR-0004	I	Bereitstellung von Postfach-Backends durch Dritte
ADR-0005	I	Anzahl und Zuschnitt der zentral bereitgestellten Postfach-Zugänge
ADR-0006	I	Anzahl und Zuschnitt der zentral bereitgestellten Postfach-Backends
ADR-0007	I	Implementierung von Postfach-Backends
ADR-0008	I	Einheitliche Anbindung über ein zentrales Self-Service-Portal
ADR-0009	I	SDKs zur vereinfachten Anbindung von Postfach-Zugängen
ADR-0010	I	Herstellung von Interoperabilität mit fremden Systemen außerhalb des Geltungsbereiches der Zielarchitektur
ADR-0011	I	Kommunikationsschicht
ADR-0012	I	Ende-zu-Ende-Verschlüsselungsschicht
ADR-0013	I	Authentizität in der Nachrichtenübermittlung
ADR-0014	I	Authentizität: Identität von Privatpersonen
ADR-0015	I	Authentizität: Identität öffentlicher Stellen
ADR-0016	I	Authentizität: Identität privater Organisationen
ADR-0017	II	Authentizität und Integrität von Inhalten

ADR-0018	II	Bereitstellungsbestätigung
ADR-1100	II	E2EE-Endpunkte bei bilateraler Kommunikation
ADR-1101	II	E2EE-Endpunkte bei der Kommunikation mit Funktionspostfächern
ADR-1102	II	Umsetzung von Funktionspostfächern und Vorgangsräumen
ADR-1103	II	Betriebsmodelle für Organisationen
ADR-1104	II	MXID-Struktur und Domain-Governance
ADR-1105	II	Pseudonyme Adressen von Privatpersonen
ADR-1106	II	Fachlicher Identitätsnachweis im Matrix-Nachrichtenkontext
ADR-1107	II	Nachweisformat des fachlichen Identitätsnachweises
ADR-1108	II	Nachweisstellen und Org-IdP-Adapter
ADR-1109	II	Raumtopologie bei Kommunikation mit Funktionspostfächern
ADR-1110	II	Entkopplung von Nutzerkonto und Postfach
ADR-1111	II	Auflösung und Lebenszyklus organisationsbezog. Postfachadressen
ADR-1112	II	Berechtigungsverzeichnis für Funktionspostfächer
ADR-1113	II	Externe Bevollmächtigung und gesetzliche Vertretung
ADR-1114	II	Getrennter Betrieb der zentralen Postfach-Backends nach Teilnehmenden-gruppen
ADR-1118	II	Abruf- und Lesebestätigungen
ADR-1119	II	Absendergesteuerte Zustelloptionen
ADR-1120	II	Beweissichere Übermittlung von Anhängen

ADR-1130	II	Malware-Prüfung unter E2EE
ADR-1135	II	Veraktung und Aufbewahrung von E2EE-Nachrichten
ADR-1144	II	PKI-Anforderungen
ADR-1145	II	Anschlussbedingungen und Föderationskontrolle
ADR-1146	II	Anbindung der EUDI-Wallet, Nachweisausstellung in die Wallet
ADR-1147	II	Schlüsselwiederherstellung für E2EE-Postfächer
ADR-1148	II	Onboarding im Self-Service-Portal

Tabelle 10: Übersicht ADRs auf Phase I und II

Die Architekturentscheidungen der Zielarchitektur sind als ADRs in einheitlichem Format dokumentiert (siehe Tab. 10). Im Folgenden werden zunächst die Entscheidungen zu den Kernfunktionen der Zielarchitektur behandelt. Des Weiteren werden Themen erläutert, die querschnittlich mehrere Komponenten betreffen. Für Details, die betrachteten Optionen und die vollständige Begründung wird auf die ADR-Dokumente verwiesen.

Im Zuge der Transitionsplanung werden neben den grundlegenden ADRs auch Transitions-ADRs (TADRs) formuliert. Diese entfalten nur für die jeweilige Stufe der Transitionsplanung auf dem jeweiligen Transitionsschritt Geltung.

5.4.1 Infrastrukturtopologie und Betriebsmodelle

Dieser Abschnitt beschreibt die zentralen Postfach-Backends je Teilnehmendengruppe (Privatpersonen, Behörden, private Organisationen, Justiz), die Betriebsmodelle für Organisationen (ADR-1103) und die dafür nötigen Komponenten wie Raum-Management-Service und Berechtigungsverzeichnis. Des Weiteren wird auf die unterschiedlichen Varianten des Anschlusses von Organisationen eingegangen.

Zentrale Postfach-Backends werden je Teilnehmendengruppe eigenständig bereitgestellt (ADR-1114). Jedes dieser Backends wird von einer dafür benannten Stelle betrieben, ist im Vertrauensverbund eindeutig adressierbar und nutzt die für die Teilnehmendengruppe maßgebliche Identitätsquelle gemäß ADR-0014 bis ADR-0016. Die Aufteilung in mehrere zentrale Backends entspricht den unterschiedlichen rechtlichen und betrieblichen Verantwortlichkei-

ten der Teilnehmendengruppen und vermeidet eine zentrale Bündelung aller Identitäten und Adressen an einer Stelle (ADR-1114). Organisationen, die mehreren Teilnehmendengruppen zugeordnet sind, können jeweils ein eigenes Postfach betreiben.
Privatpersonen nutzen ausschließlich das zentral bereitgestellte Postfach-Backend für Privatpersonen und betreiben keine eigenen Homeserver.
Organisationen haben die Wahl zwischen hinsichtlich der Souveränität bzw. Eigenverantwortung abgestuften Betriebsmodellen (ADR-1103, vgl. Abschnitt 5.6). Bei der **Minimalanbindung (Betriebsmodell A)** nutzt die Organisation ausschließlich die zentral bereitgestellten Dienste. Funktionspostfächer stehen über den RMS eines zentralen Postfach-Backends zur Verfügung, wobei neue Mitglieder nur mit Einschränkungen Zugriff auf alte Nachrichten erhalten (ADR-1102). Beim **Teilbetrieb (Betriebsmodell B)** betreibt die Organisation den Raum-Management-Service (RMS) und gegebenenfalls ein eigenes Berechtigungsverzeichnis, nutzt aber ein zentrales Postfach-Backend. Damit steht der volle Funktionsumfang der Funktionspostfächer zur Verfügung (vgl. Abschnitt 5.4.3). Beim **souveränen Betrieb (Betriebsmodell C)** betreibt sie das Postfach-Backend selbst und verfügt dann über eine eigene Adress-Domain.
Je nach Anforderung der Organisation hinsichtlich Datenhoheit oder ihren IT-Fähigkeiten stehen somit passende Betriebsmodelle zur Verfügung. Unabhängig vom gewählten Modell gelten die Anschlussbedingungen (ADR-1145), die Authentisierung gemäß ADR-0013 bis ADR-0016 sowie die Vorgaben zur E2EE-Terminierung (ADR-1100, ADR-1101). Details zum Entwurf der Modelle und zur Registrierung eigener Backends im SSP werden in den Abschnitten 5.6 und 5.2.2.2 beschrieben.

5.4.2 Postfächer und Postfachzugänge

Alle Kommunikationsteilnehmer:innen (Privatpersonen, Organisationen) verfügen über mindestens ein Postfach. Das Postfach ist mit der Identität der Teilnehmenden verknüpft und über eine eindeutige Postfachadresse (MXID) erreichbar, es ist kein Bestandteil eines Nutzerkontos (ADR-1110). Privatpersonen können mehrere bereichsspezifische MXIDs und damit mehrere Postfächer besitzen. Diese werden im zentralen Postfach-Zugang zu einer aggregierten Postfachsicht zusammengeführt (vgl. ADR-1105, Abschnitt 5.5.2.2). Alle Nachrichten liegen im Postfach-Backend in verschlüsselter Form vor und können über verschiedene Postfachzugänge (Matrix-Clients) abgerufen werden. Privatpersonen nutzen für den Zugriff immer Clients, die in ihrem Endgerät laufen. In Organisationen kann zusätzlich auf Postfächer auch

durch technische Nutzer im Server zugegriffen werden, wobei die E2EE damit nicht mehr strikt umgesetzt ist (vgl. Abschnitt 5.4.3).

Für den Zugriff auf Postfächer wird ein zentraler Postfach-Zugang als Webanwendung und mobile App für alle Nutzendengruppen bereitgestellt (ADR-0005). Der zentrale Postfach-Zugang steht Privatpersonen und Organisationen zur Verfügung und berücksichtigt dabei auch Personen in Doppelrollen (z. B. Kleinunternehmer, die zugleich als Privatperson auftreten).

Auch Dritte können eigene Postfachzugänge betreiben (ADR-0003), über die z. B. die Anbindung von Fachverfahren, Unternehmensanwendungen und weiteren Client-Applikationen an die Infrastruktur erfolgen kann. Die Authentisierung in den Postfachzugängen findet über externe Identity Provider statt, wobei das Postfach-Backend Nutzenden Zugriff auf seine Postfächer gewährt. Zur Zulassung von Software als Postfach-Zugang sind keine zentralen Zertifizierungsprozesse geplant (ADR-0003, ADR-1145). Nutzende können selbst zwischen den Softwareprodukten entscheiden.

Was ein Postfach-Zugang darüber hinaus umsetzen soll, etwa das Mindest-Übergabepaket für die Veraktung oder die Anzeige des Status der Nachweise, geben Spezifikationen vor, die das SDK umsetzt.

5.4.3 Funktionspostfächer und Vorgangsräume

Die Funktionspostfächer von Organisationen werden durch wechselnde Mitarbeitende bearbeitet. Zuständigkeiten und Vertretungsregelungen lassen sich konfigurieren und automatisch umsetzen (ADR-1102).

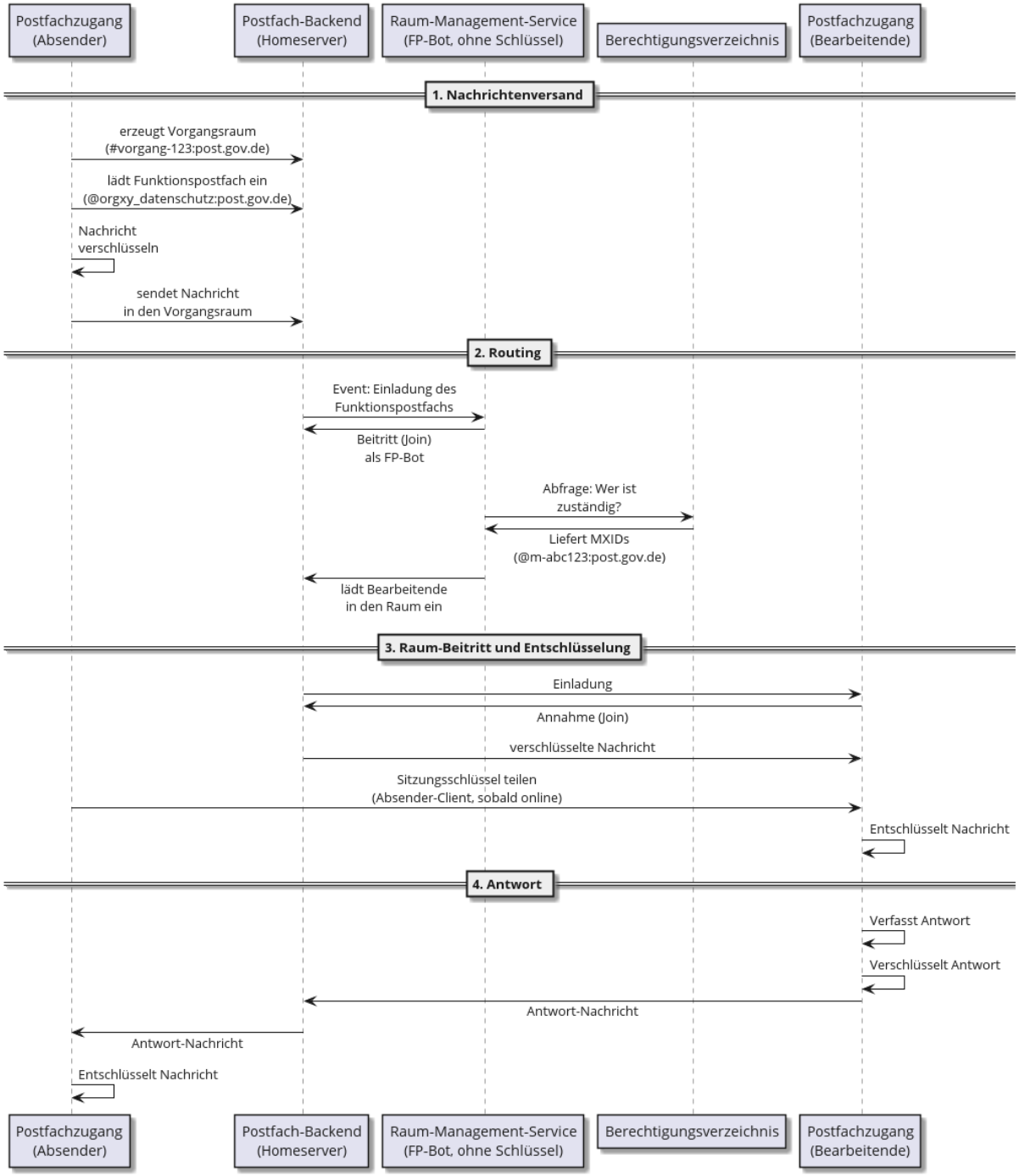

Abbildung 7: Übersicht Funktionspostfächer und Vorgangsräume

Jeder Vorgang wird in einem eigenen kryptografisch isolierten Raum (Vorgangsraum) bearbeitet (siehe Abb. 8). Ein Funktionspostfach wird durch einen technischen Nutzer (FP-Bot) betreut, der im Raum-Management-Service (RMS) betrieben wird. Der FP-Bot erzeugt die

Räume des zugehörigen Funktionspostfachs und hat im Raum Administratorrechte (ADR-1109). Geht eine Nachricht in einem Funktionspostfach ein, erzeugt der FP-Bot den organisationsinternen Vorgangsraum und lädt die zuständigen Mitarbeitenden auf Basis eines Berechtigungsverzeichnisses ein. Vertretungen werden durch die Einladung weiterer berechtigter Personen umgesetzt. Dies ist in allen Betriebsmodellen über den organisationseigenen RMS (Betriebsmodell B und C) oder über den RMS eines zentralen Postfach-Backends (Betriebsmodell A) automatisiert möglich. Zudem können Organisationen Gruppenräume manuell verwalten. Ebenso können auf der Seite der Absender:innen interne Vorgangsräume erzeugt und die Mitglieder der Gruppe der Absendenden hinzugefügt werden. Direkt in einem Raum kommunizieren dann nur die FP-Bots der beiden Organisationen und nicht die Mitarbeitenden der jeweils anderen Organisation.

Für die Kommunikation zwischen Funktionspostfächern hat eine Organisation je nach Schutzbedarf und Betriebsmodell unterschiedliche Möglichkeiten der Umsetzung (ADR-1109). Nachrichten an ein Funktionspostfach gelten mit dem Eingang im Empfänger:innen-Backend als bereitgestellt, dort wird die Bereitstellungsbestätigung erzeugt (ADR-0018).

Technische Nutzer:innen, die nicht auf den Klartext im Raum Zugriff haben, also keinen Zugriff auf die notwendigen Schlüssel besitzen, können trotzdem Teilnehmer:innen im Raum über die Application-Service-API verwalten. Die Entscheidung für oder gegen E2EE-Teilnahme im RMS, ist eine Abwägung zwischen Verfügbarkeit und Vertraulichkeit. Die Verfügbarkeit der Nachrichten durch automatischen Bearbeitungsvertretungen steht der Vertraulichkeit entgegen, da der Klartext nicht mehr nur in den Endgeräten der Teilnehmer:innen vorläge (vgl. ADR-1101, ADR-1102). Die folgenden Konfigurationen reichen von der vollen E2EE-Teilnahme des RMS über die rein administrative Verwaltung bis zur manuellen Raumverwaltung durch Administrator:innen.

Bei der **Möglichkeit mit weiterleitendem FP-Bot**, der Zugriff auf die E2EE-Schlüssel hat, entstehen je Vorgang drei Räume: ein organisationsinterner Raum auf Absender:innenseite (Bearbeiter:in samt Vertretungen und eigener FP-Bot), ein Raum zwischen den FP-Bots beider Organisationen und ein organisationsinterner Raum bei den Empfänger:innen. Die FP-Bots leiten die Nachrichten zwischen diesen Räumen weiter. Die Mitglieder einer Organisation sehen lediglich die Funktionspostfach-Adresse der Gegenseite, die Privatsphäre einzelner Mitarbeitender bleibt gewahrt. Vertretungen und neue Mitglieder erhalten über den internen Raum Zugriff auf sämtliche Nachrichten des Vorgangs. Da die Ende-zu-Ende-Verschlüsselung in den FP-Bots terminiert, setzt diese Möglichkeit das Betriebsmodell B oder C voraus, bei

dem die Organisation den RMS im eigenen Machtbereich betreibt. Kommuniziert eine Einzelperson mit einem Funktionspostfach, entfällt deren interner Raum. Sie befindet sich dann mit dem FP-Bot der Organisation in einem gemeinsamen Raum.

Bei einer **weiteren Möglichkeit, die die strikte Ende-zu-Ende-Verschlüsselung zwischen den Endgeräten aufrechterhält**, verwaltet der FP-Bot die Mitgliedschaften über die Application-Service-API, ohne Schlüssel zu besitzen. Die Mitglieder werden bereits bei Raumeröffnung eingeladen und verfügen damit über die Schlüssel der gesamten Kommunikation. Erst später hinzugefügte Teilnehmer:innen müssen die Schlüssel vergangener Nachrichten von bestehenden Mitgliedern explizit geteilt bekommen. Welche Vorgänge eine Person aktiv bearbeitet, wird über persönliche Bereiche (Matrix-Spaces) gesteuert. Diese Möglichkeit kann zentral betrieben werden und ist der Standard der Minimalanbindung (Betriebsmodell A, RMS im zentralen Postfach-Backend). Ein Zugriff des zentralen Betreibers auf die Klartexte der Nachrichten bleibt ausgeschlossen. Dagegen gibt es Einschränkungen bzgl. der Verfügbarkeit von Nachrichten, da nicht jederzeit ein neues Mitglied unverzüglich Zugriff auf die ältere Kommunikation hat und ggf. auf das Teilen der Schlüssel durch ein anderes Raummitglied warten muss.

Manuelle Raumverwaltung durch Administrator:innen: Der RMS erzeugt den Vorgangsraum initial und lädt die zuständigen Mitarbeitenden ein. Anschließend verlässt er den Raum. Die laufende Verwaltung (Einladen von Bearbeitungsvertretungen, Anpassen von Power-Levels) erfolgt durch menschliche Administrator:innen. Diese Konfiguration eignet sich insbesondere für Kommunikation mit hohem Schutzbedarf, bei der ein dauerhafter Zugriff des RMS auf den Raum nicht gewünscht ist.

Die MLS-Integration in Matrix ist noch nicht abgeschlossen. Je nach Ausgestaltung kann die heutige Trennung von unverschlüsselten State Events und verschlüsselten Message Events entfallen (vgl. ADR-1101, ADR-1102). Ein technischer Nutzer müsste dann MLS-Gruppenmitglied sein, um den Raum zu verwalten. Ob eine automatisierte Mitgliedschaftsverwaltung möglich bleibt, hängt von der konkreten Umsetzung in Matrix ab und ist derzeit nicht abschließend zu beurteilen. Die Auswirkungen auf die Betriebsmodelle sind vor einer Migration zu prüfen.

Die konkrete Umsetzung im Zusammenspiel der Komponenten wird in Abschnitt 5.5.5 beschrieben.

5.4.4 Kommunikations- und Verschlüsselungsschicht

Für die Zielarchitektur wurde Matrix als Kommunikationsprotokoll gewählt (ADR-0011). Die Ende-zu-Ende-Verschlüsselung erfolgt in Matrix aktuell über die auf dem Signal-Protokoll basierenden Verfahren Olm und Megolm. Als Alternative dazu wird derzeit die Umsetzung von MLS (Messaging Layer Security, RFC 9420) in Matrix vorangetrieben. Sobald diese Arbeiten abgeschlossen sind, ist eine Migration nach MLS vorgesehen (ADR-0012). Die Zielarchitektur ist entsprechend dem Entwurfsprinzip der Kryptoagilität so entworfen, dass eine spätere Migration möglich bleibt, ohne dass die Anwendungslogik grundsätzlich angepasst werden muss. MLS implementiert derzeit noch keine Post-Quantum-Kryptographie. Eine post-quantum-sichere Ausgestaltung des E2E-Verschlüsselungslayers der Zielarchitektur ist gegenüber dem Einsatz von MLS im Zweifel zu priorisieren. Ungeachtet dessen ist der Einsatz post-quantum-sicherer Transportverschlüsselung (TLS 1.3 mit post-quantum-sicherem Schlüsselaustausch) verbindlich vorzuschreiben. Durch die Verwendung des SDK, in dem die kryptographischen Operationen gekapselt sind, ist ein Wechsel des Verschlüsselungsprotokolls einfacher umsetzbar.

In einem System mit strikter Ende-zu-Ende-Verschlüsselung liegt der Klartext einer Nachricht ausschließlich in den Endpunkten der Kommunikationsteilnehmer:innen vor. Die dazwischenliegenden Systeme der Infrastruktur haben keinen Einblick in den Klartext.

Bei einer Kommunikation zwischen zwei Teilnehmer:innen ist eine strikte E2EE mit den gewählten Protokollen unproblematisch umsetzbar. Für die bilaterale Kommunikation legt die Zielarchitektur fest, dass die Terminierung der Verschlüsselung direkt im Endgerät stattfindet. Das private Schlüsselmaterial verlässt das Endgerät nicht (ADR-1100).

Bei einer Kommunikation zwischen Gruppen besteht die Herausforderung, dass die Mitglieder einer Gruppe wechseln können. Die Zielarchitektur erlaubt daher die Teilnahme technischer Nutzer:innen an der Kommunikation, die in Mehrbenutzer:innen-Szenarien (Funktionspostfächer, Vertretungen) die Mitgliedschaften in den Gruppen steuern können (ADR-1101, Option B). Diese technischen Nutzer:innen sowie die Steuerung der Mitgliedschaften in den kryptographischen Räumen werden in der Zielarchitektur durch den Raum-Management-Service (RMS) umgesetzt. Welche der in Abschnitt 5.4.3 beschriebenen Optionen umgesetzt werden, entscheidet die Organisation entsprechend des jeweiligen Schutzbedarfs.

Die Schlüsselwiederherstellung z. B. nach Geräteverlust soll mittels serverseitigem Key Backup (Secure Secret Storage and Sharing) ermöglicht werden. (s. Abschnitt 5.4.13)

5.4.5 Authentisierung und Autorisierung

Für die Authentisierung der Teilnehmer:innen sind unterschiedliche Ebenen zu unterscheiden (ADR-1106). Zunächst authentisieren sich Personen oder Systeme indem sie sich am Postfach-Zugang anmelden. Die Anmeldung erfolgt gegen den Authentisierungsdienst des jeweiligen Postfach-Backends ggf. unter Verwendung eines Identity-Providers (ADR-0014 bis ADR-0016, ADR-1110). Systeme authentisieren sich ohne interaktive Anmeldung über Client Credentials (vgl. Abschnitt 5.5.3).

In dem Identity-Provider BundID für Privatpersonen und dem Organisationskonto für juristische Personen dienen die eID bzw. das ELSTER-Organisationszertifikat als Identifizierungsmittel. Hinzu kommen die EUDI-Wallet und perspektivisch die European Business Wallet. Die Einbindung geplanter Identitätsdienste des D-Stacks (z. B. ein zentraler Identity Layer) bleibt möglich. Auch die Authentisierung der Privatpersonen mittels eID direkt bei einem eID-Server der Behörde sieht die Zielarchitektur als Option vor. Dabei liefert die eID das bereichsspezifische Pseudonym, aus dem die Postfachadresse abgeleitet wird. Dies benötigt einheitliche Pseudonyme in allen Authentifizierungsmöglichkeiten, die aus der eID abgeleitet werden (Zielbild Option 2C in ADR-1105).

Spezifische Schlüssel identifizieren das für die Kommunikation verwendete Gerät. Der Identitätsnachweis pro Nachricht belegt, in wessen fachlichem Namen gehandelt wird, etwa für eine Organisation bzw. ein Funktionspostfach. Eine erfolgreiche Anmeldung sagt nichts darüber aus, welches Gerät gesendet hat. Umgekehrt belegt ein verifiziertes Gerät noch keine fachliche Rolle.

Die folgenden Abschnitte gehen die Ebenen der Reihe nach durch und behandeln danach die Autorisierung, die Vertrauensniveaus und den PKI-Vertrauensanker.

5.4.5.1 Kryptografische Schlüsselidentität im E2EE-Kanal

Die Geräteschlüssel der Kommunikationsteilnehmer:innen sind mittels Matrix-Cross-Signing über den Master Signing Key (MSK) zu einer prüfbaren Schlüsselidentität verknüpft. Die Schlüsselidentität belegt nicht die fachliche Identität der Absender:innen, sondern lediglich die Identität des verwendeten Matrix-Accounts. Die fachliche Identität wird mit dem Identitätsnachweis über den Kanal belegt (vgl. Abschnitt 5.4.5.2). Für Anwendungsfälle mit erhöhten Sicherheitsanforderungen kann der Identitätsnachweis zusätzlich an die Geräte-Schlüsselidentität oder an einen Binding-Key gebunden werden (ADR-1106). Diese zusätzliche Schlüsselbindung schützt vor der Wiederverwendung eines Nachweises in fremden Gerä-

te- oder Senderkontexten. In den ADR-1107 und ADR-1108 ist die technische Umsetzung entworfen.

5.4.5.2 Identitätsnachweis pro Nachricht

Kommunikationsteilnehmer:innen können die jeweilige Anmeldung des Gegenübers in deren Postfächern nicht prüfen. Stattdessen belegen die Teilnehmer:innen ihre fachliche Identität einander mithilfe der mit den Nachrichten übermittelten Nachweise. Die empfangende Person kann den übermittelten Identitätsnachweis mit Hilfe der Trust-Struktur der Zielarchitektur überprüfen (ADR-1106, ADR-1107).

Nicht für alle Anwendungsfälle ist der Nachweis der Identität der Teilnehmer:innen notwendig. Die Fachverfahren können vorgeben, ob eine Authentifizierung der Kommunikationspartner vorgenommen werden muss.

Der Identitätsnachweis pro Nachricht wird in mehreren Schritten durch die empfangende Stelle geprüft. Zum einen muss geprüft werden, ob der Nachweis von einer zum Versandzeitpunkt in der Trust-Struktur zugelassenen und gültigen Nachweisstelle erzeugt wurde. Dann muss festgestellt werden, ob die Identität der sendenden Stelle für diesen Vorgang das notwendige Vertrauensniveau besitzt. Des Weiteren wird die technische Bindung geprüft, also die Zuordnung der Senderadresse zum Nachweis und, soweit gefordert, die Bindung an die Matrix-Schlüsselidentität. Dabei kann die Prüfung der Senderadresse bei Organisationsidentitäten gegen das Adressregister erfolgen. Bei Privatpersonen leitet sich die Adresse aus einem Attribut der Identität bzw. aus einem vom IdP erzeugten Pseudonym ab.

Die Prüfung des Identitätsnachweises muss sich auf die Gültigkeit zum Versandzeitpunkt beziehen, nicht auf den Prüfzeitpunkt. Deshalb muss die Trust-Infrastruktur historische Schlüssel und Statusverläufe der Nachweisstellen langfristig vorhalten und abrufbar machen.

5.4.5.3 Autorisierung der Postfach-Backends im Verbund

Die Voraussetzung zur Aufnahme in den Kommunikationsverbund ist die Bestätigung und Einhaltung der Anschlussbedingungen (ADR-1145). Postfach-Backends werden dazu über das SSP registriert und nach manueller Freigabe der zuständigen Stelle in den Vertrauensverbund aufgenommen (ADR-1148, vgl. Abschnitt 5.2.2.2). Darüber hinaus werden auch die öffentlichen Schlüssel der verwendeten Nachweisstellen registriert. Anwendungen, die Postfachzugänge umsetzen, werden nicht gesondert zugelassen. Sie erlauben einen Zugriff auf die Kommunikation nur, wenn Nutzende entsprechend im Postfach-Backend authentifiziert wurden (ADR-0003). Die Autorisierung der Systemzugriffe von Fachverfahren und Unterneh-

mensanwendungen auf die Postfach-Backends wird über die föderale API-Autorisierungsinfrastruktur umgesetzt (vgl. Abschnitt 5.5.3).
Ob eine bestimmte Aktion zulässig ist, ergibt sich aus der Raummitgliedschaft in einem Vorgangsraum und dem dort zugewiesenen Power-Level (vgl. Abschnitt 5.5.5). Ohne Mitgliedschaft besteht kein Zugriff. Die Steuerung der Mitgliedschaften in den Vorgangsräumen erfolgt über den RMS und das Berechtigungsverzeichnis (vgl. Abschnitt 5.2.2.5).

5.4.5.4 Vertrauensniveaus

Die Kommunikation kann auf unterschiedlichen eIDAS-Vertrauensniveaus (niedrig, substanziell, hoch) erfolgen (Anforderung SIC_VER_ÜBE_048). Das Niveau wird bei der Anmeldung auf Basis des eingesetzten Authentisierungsmittels festgelegt. Der Identitätsnachweis pro Nachricht enthält das Niveau als Claim. Empfänger:innen können somit nachvollziehen, auf welchem Niveau Absender:innen authentisiert wurden (SIC_ÜBE_ÜBE_008, ADR-1107). Sender:innen können für eine Nachricht ein Mindestniveau festlegen, das für das Lesen der Nachricht erforderlich ist (SIC_ÜBE_ÜBE_007). Die Umsetzung der Durchsetzung des Mindestniveaus kann über die Zustelloptionen und die Anmeldung der Empfänger:innen erfolgen (ADR-1119).

5.4.5.5 PKI-Vertrauensanker

In der Zielarchitektur werden diverse Nachweise erzeugt, die gegen die Trust-Infrastruktur prüfbar sind. Neben den Quittungen wie Bereitstellungsbestätigungen (ADR-0018) sind für das System vor allem die Identitätsnachweise der Kommunikationsteilnehmer:innen wichtig (ADR-1106). Das Siegelzertifikat für Bereitstellungsbestätigungen wird auf den Betreiber des Postfach-Backends als juristische Person ausgestellt und bei der Registrierung im SSP hinterlegt (ADR-1144, ADR-1148). Für private Organisationen kann die ELSTER-PKI entsprechend ertüchtigt werden. Im öffentlichen Bereich wäre nach einer Modernisierung die Nutzung der V-PKI denkbar.
Wichtige Anforderungen sind maschinenlesbare Organisationsattribute, die Möglichkeit zur automatisierten Zertifikatserneuerung (ACME) und eine Langzeitprüfbarkeit der Nachweise (ADR-1144).

5.4.6 Adressierung und Adressverzeichnis

In der Zielarchitektur wird zwischen technischen Absender:innen und den fachlichen Akteur:innen einer Nachricht unterschieden (siehe Abb. 9). Die technischen Absender:innen ent-

sprechen einem Postfach und haben eine Postfachadresse, unter der sie die Nachricht verschicken. Die Adresse ist pseudonym ausgestaltet und ist kein Nachweis der Identität.
Die fachliche Identität, in deren Namen die Nachricht versendet wird, ist bei Privatpersonen die Person selbst. Ihr aus der Identität abgeleitetes bereichsspezifisches Pseudonym findet sich in der Adresse. Bei Organisationen wird die Identität der Organisation mit der Identität der Mitarbeitenden verknüpft. Der fachliche Akteur ist dann in der Regel die Organisation bzw. eine über ein spezifisches Funktionspostfach verfügende Abteilung, wobei die Mitarbeitenden zwar innerhalb der Organisation identifizierbar bleiben, nach außen jedoch persönlich nicht in Erscheinung treten. Die handelnde Person bleibt dabei intern über das Berechtigungsverzeichnis (ADR-1112) und die Auditierung nachvollziehbar.
Jede Person und jede Organisation im Kommunikationsverbund verfügt über mindestens eine Matrix-User-ID (MXID) im Format *@[localpart]:[domain]*. Die Struktur der bei Matrix als Adressen verwendeten MXIDs und die Domain-Governance sind in ADR-1104 festgelegt.

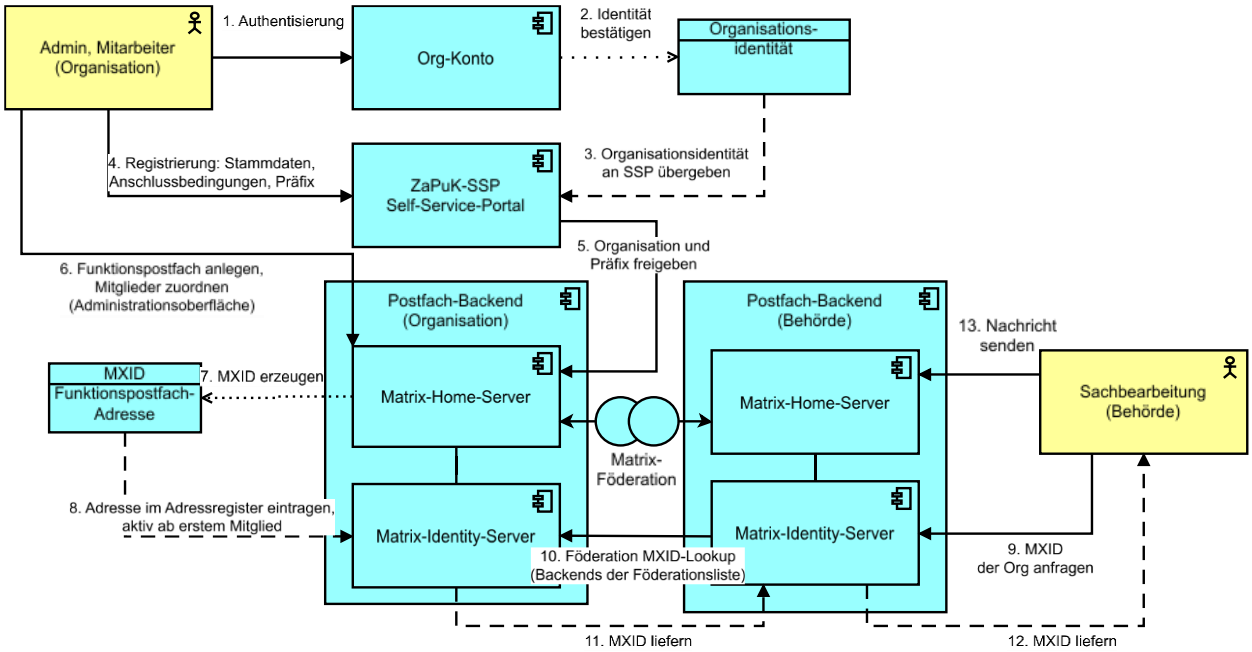

Abbildung 8: Adressierung von Organisationen

Organisationen registrieren ihre Domain im SSP. Ihre Funktionspostfächer pflegen sie in der Administrationsoberfläche des Postfach-Backends. Organisationen, die ein zentral betriebenes Postfach-Backend verwenden (Betriebsmodelle A und B, vgl. ADR-1103), erhalten Adressen auf der zentralen Domain (z. B. @orgxy_datenschutz:post.gov.de). Organisationen mit

eigenen Postfach-Backends nutzen eine eigene Domain (z. B. @datenschutz:org-xy.de), die natürlich auch im SSP hinterlegt ist.
Adressen von Organisationen und Berufsträgern (z. B. Steuerberater:innen) werden mit ihrer Organisationszuordnung im Adressregister gelistet. Sie können über den Matrix Identity Service (MIS) verbundweit abgefragt werden (ADR-1111). Eine lokale MIS-Instanz löst unbekannte Adressen über die übrigen Instanzen im Verbund auf. Bestehende Verzeichnisdienste (z. B. SAFE) können als Backend hinter dem MIS betrieben werden.
Adressen von Privatpersonen werden nicht im MIS gelistet. Ein globales Adressverzeichnis für Privatpersonen ist ausgeschlossen (ADR-1105). Die MXID wird stattdessen deterministisch aus einem bereichsspezifischen Pseudonym und der Domain des zentralen Postfach-Backends abgeleitet. Da die bereichsspezifische MXID nur im jeweiligen Verwaltungsbereich verwendet wird, wird eine Profilbildung durch Weitergabe an andere Stellen verhindert. Das Pseudonym wird vom Nutzerkonto (BundID) gebildet und im Rahmen der Authentifizierung bereitgestellt. Die EUDI-Wallet könnte das Pseudonym perspektivisch direkt bereitstellen. Die konkreten Abläufe der Adressregistrierung für Organisationen und der Antragsfolgekommunikation für Privatpersonen werden in Abschnitt 5.5 dargestellt.
Bei dem Entwurf wurde den Anforderungen an Datenschutz und Unlinkability entsprochen. Identitätsnachweise enthalten im Normalfall keine Klarnamen, Personalnummern oder sonstige personenbezogene Daten. Die persönliche Mitarbeiteridentität verlässt nicht die Organisation. Eine Wiedererkennung anhand technischer Merkmale über Vorgänge hinweg wird im Besonderen bei Privatpersonen vermieden. Für einen Vorgang notwendige Pflichtangaben werden natürlich übermittelt.

5.4.7 Interoperabilität

Die Kommunikationsinfrastruktur muss auch mit externen Systemen zusammenarbeiten können, die andere Protokolle als Matrix nutzen. ADR-0010 legt fest, wie diese Anbindung umzusetzen ist, ohne die Ende-zu-Ende-Verschlüsselung zu brechen.
Die Interoperabilität soll über sogenannte Protokollkonverter umgesetzt werden, wobei die Ende-zu-Ende-Verschlüsselung erhalten wird (vgl. Abschnitt 5.2.2.6). Bridges sollen dagegen nicht verwendet werden, da sie die E2E-Verschlüsselung brechen (ADR-0010).
Für die grenzüberschreitende Kommunikation innerhalb der EU setzt das eDelivery-Framework auf AS4 als Transportprotokoll. AS4 dient dem automatisierten Austausch von Dokumenten zwischen Servern. Dagegen setzt Matrix auf interaktive Echtzeitkommunikation zwischen Menschen. Die EU erprobt Matrix derzeit in Pilotprojekten für die verwaltungsinter-

ne Kommunikation. Ein AS4-Gateway als Protokollkonverter kann die Strecke zwischen Zustelldiensten überbrücken, sofern es ausschließlich verschlüsselte Daten transportiert (ADR-0010).

5.4.8 Verhältnis zu angrenzenden nationalen und EU-Vorhaben

Mehrere nationale und EU-Vorhaben, die sich selbst in dynamischer Entwicklung befinden, berühren Ziele und Anforderungen der Zielarchitektur. Um gemeinsame Bausteine nutzen zu können, ohne die Umsetzung von ZaPuK vom Fortschritt einzelner Projekte abhängig zu machen, sind entsprechende Schnittstellen bzw. Anschlusspunkte zu definieren. Dieses Kapitel nennt relevante Vorhaben mit ihrem Verhältnis zur Zielarchitektur und den jeweiligen Anschlusspunkte.

5.4.8.1 TI-Messenger der gematik

Fortgeschrittenes Matrix-basiertes Föderationssystem im Gesundheitswesen mit Anschluss von Funktionspostfächern.
Gemeinsamkeiten:

- Föderation (Registrierungsdienst + Föderationsliste), Funktionspostfächer (TI-M: Funktionsaccount), automatisierte Raumteilnehmer:innen (TI-M: Chatbot/Headless Client)
- Souveräner Betrieb (Modell C) also eigener Homeserver mit zentraler Registrierung, Registrierungsrolle übernimmt das SSP

Unterschiede des ZaPuK-Verbundes gegenüber TI-M:

- Identität: fachliche Identität per eID, EUDI-Wallet, Identity-Provider (Organisationskonto, BundID) statt Smartcard-PKI (SMC-B/HBA)
- zusätzliche rechtsverbindliche Bereitstellungsbeweise bzw. Empfangsquittungen (ADR-0018, ADR-1118, ADR-1120)
- bereichsspezifische Pseudonyme für Privatpersonen (ADR-1105)
- risikobasierter statt zertifizierungsbasierter Onboardingprozess (ADR-1145)

5.4.8.2 EUDI-Wallet

- Mit Beschluss B-2026/19-IT des IT-Planungsrates wurde ein Konzept zur Verwaltungsanbindung der EUDI-Wallet vorgelegt. Dieses Konzept unterscheidet drei Funktionen der EUDI-Wallet: die sichere Identifizierung, die Entgegennahme von Nachweisen aus der Wallet und die Ausstellung von Nachweisen in die Wallet. Die Zielarchitektur unterstützt die EUDI-Wallet als Authentisierungsmittel (vgl. Abschnitt 5.4.5).

- Eine elektronische Attributsbescheinigung (EAA) belegt einer Gegenstelle bestimmte Eigenschaften einer Identität. Die rechtssichere Bekanntgabe bzw. Bereitstellung von Bescheiden erfolgt dagegen über die ZaPuK-Postfächer. Für die Ausstellung von Nachweisen in die EUDI-Wallet darf eine Lösung die Ende-zu-Ende-Verschlüsselung nicht brechen und soll keine Aussteller-Komponente in der ZaPuK-Infrastruktur einführen (ADR-1146). Die im Fachverfahren vorliegenden Nachweisdaten werden zur Abholung bereitgestellt. Der Aussteller erzeugt im Rahmen des Antragsverfahrens einen Abholschein. Beim Abholschein handelt es sich um ein Credential Offer (OID4VCI Pre-Authorized Code) mit Einmal-Code in Form eines Links oder QR-Codes. Er wird zusammen mit dem Bescheid E2EE-verschlüsselt in das Postfach der Nutzenden zugestellt und kann im Postfach-Zugang verwendet werden, um mittels der Wallet-App die Abholung des Nachweises zu initiieren. Bei der Abholung über das Protokoll OID4VCI wird der Nachweis an die Wallet gebunden (Holder-Binding). Dazu ist eine Re-Identifizierung der Nutzenden durch den Aussteller notwendig. Der Abholschein ist technisch gesehen ein Verweis auf die öffentlichen Endpunkte der Aussteller. Im Zielzustand sind dies die Wallet-Adapter der Fachverfahren, für Registerdaten ggf. ein anderer Aussteller wie z. B. der zentrale Issuer-Dienst des Bundes (ZID). Die Siegelung der Nachweise erfolgt über einen QTSP, wobei nur Hashes und nicht der Klartext übermittelt werden.
- In der Transition wird die im Beschluss B-2026/19-IT für das ZBP geplante indirekte Anbindung der Nachweisausstellung berücksichtigt. Dabei übernimmt eine zentrale Stelle (ZBP, ZID) die Umwandlung der Formate und die Siegelung der Nachweise und erhält dazu Zugriff auf den Klartext der Nachweisdaten. Wobei eine Umsetzung mittels ZID bereits durch den Bund geplant ist. Der Parallelbetrieb der Legacy-APIs und der Wallet-Anbindung ist im Transitionsplan aufzunehmen. (ADR-1146)

Im Beschluss B-2026/19-IT des IT-Planungsrates enthält das EUDI-Wallet-Konzept einen Prüfauftrag an ZaPuK und den Bund, „inwieweit perspektivisch eine Zustellung von Bescheiden in das ZBP auch ohne vorherige Beantragung mit der BundID möglich gemacht werden kann", da bei direkter Anbindung der Wallet das Postfach-Handle der BundID-Identität fehlt.[11] In der Zielarchitektur ist ein solches Handle nicht erforderlich. Die Postfachadresse wird aus dem bereichsspezifischen Pseudonym abgeleitet, das die EUDI-Wallet bei der Antragstellung als Bestandteil der Identität übermittelt. Voraussetzung ist, dass Wallet und BundID für denselben Bereich dasselbe Pseudonym liefern. Dafür stellt die BundID die bereichsspezifischen

[11] Verwaltungsanbindung EUDI-Wallet, Konzept zum Zielbild (BMDS), 17.06.2026, Abschnitt 3.2, S. 22.

Pseudonyme als Verifiable Credentials in die EUDI-Wallet aus. Im Zielbild werden sie in allen Authentifizierungswegen aus der eID abgeleitet (ADR-1105, ADR-1146).

5.4.8.3 Weitere Vorhaben

Das Verhältnis zu untenstehenden Vorhaben ist Gegenstand der laufenden Programmarbeit und wird zu einem späteren Zeitpunkt konkreter beschrieben

- FIT-Connect: Empfohlener Betreiber zentraler Postfach-Backends für Organisationen, Entwickler:innen von Komponenten wie z. B. Backend und SDK (vgl. Abschnitt 4.1.1)
- FöPD (API-Autorisierung): Autorisierung von Systemzugriffen z. B. auf die Client-Server-API der Backends (vgl. Abschnitt 5.4.5.3)
- EUBW: Authentifizierung für Organisationen, ggf. Anschluss des Kommunikationsverbundes

5.4.9 Anschlussbedingungen und Föderationskontrolle

Voraussetzung für die Föderation im Verbund mit den anderen Backends ist eine Registrierung, wobei Anschlussbedingungen zugesichert werden (ADR-0004, ADR-0008). Aus den getroffenen Architekturentscheidungen leiten sich verbindliche Mindeststandards für an der Kommunikation teilnehmende Behörden und Organisationen ab (ADR-1145).

Für die Umsetzung der Anschlussbedingungen wird ein risikobasierter Ansatz verfolgt. Backends werden nicht einzeln zertifiziert oder auditiert. Stattdessen werden folgende Zusicherungsarten unterschieden:

- **strukturell:** durch Teilnehmendenkreis, Onboarding oder Architektur begrenzt. Eine Verletzung schadet überwiegend der eigenen Organisation.
- **technisch geprüft:** automatisch durchgesetzte oder geprüfte Bedingungen, wobei nicht der Betreiber bzw. die Organisation dies selbst prüfen. Stattdessen können die Kommunikationspartner und andere Stakeholder die Einhaltung der Bedingung entsprechend verifizieren. Dazu gehört die Identitätsprüfung beim Onboarding (ADR-0015, ADR-0016).
- **erkennbar:** die Nichteinhaltung einer Bedingung ist durch die Kommunikationspartner im Nachhinein nachweisbar, etwa über Signaturen, Quittungen oder Attestierungen.
- **vertraglich:** durch Selbstverpflichtung und Haftung im Anschlussvertrag, den die teilnehmende Organisation im SSP-Onboarding annimmt. Mit ihm übernimmt sie die Haftung für die in ihrem Machtbereich betriebenen Komponenten.

- **Konformitätsprüfung im Einzelfall:** Die Prüfung kann im Ausnahmefall oder stichprobenartig für wenige Bedingungen durchgeführt werden, um ein entsprechend hohes Risiko zu mitigieren. Diese Prüfungen sind bei Störungen oder Abnahmen anlassbezogen oder stichprobenartig möglich.

Aufnahme, Suspendierung und Ausschluss von Postfach-Backends in die Föderation werden über die Föderationsliste gesteuert (siehe Abb. 10). Die Beachtung der Föderationsliste selbst ist eine Anschlussbedingung. Jedes Backend föderiert ausschließlich mit dort gelisteten Backends. Die Durchsetzung beruht auf Gegenseitigkeit. Verstößt ein einzelnes Backend gegen diese Pflicht, verweigern die übrigen Backends dem nicht gelisteten Backend dennoch die Föderation. Der Verstoß schadet deshalb überwiegend dem nicht konformen Backend und seinen Postfächern.

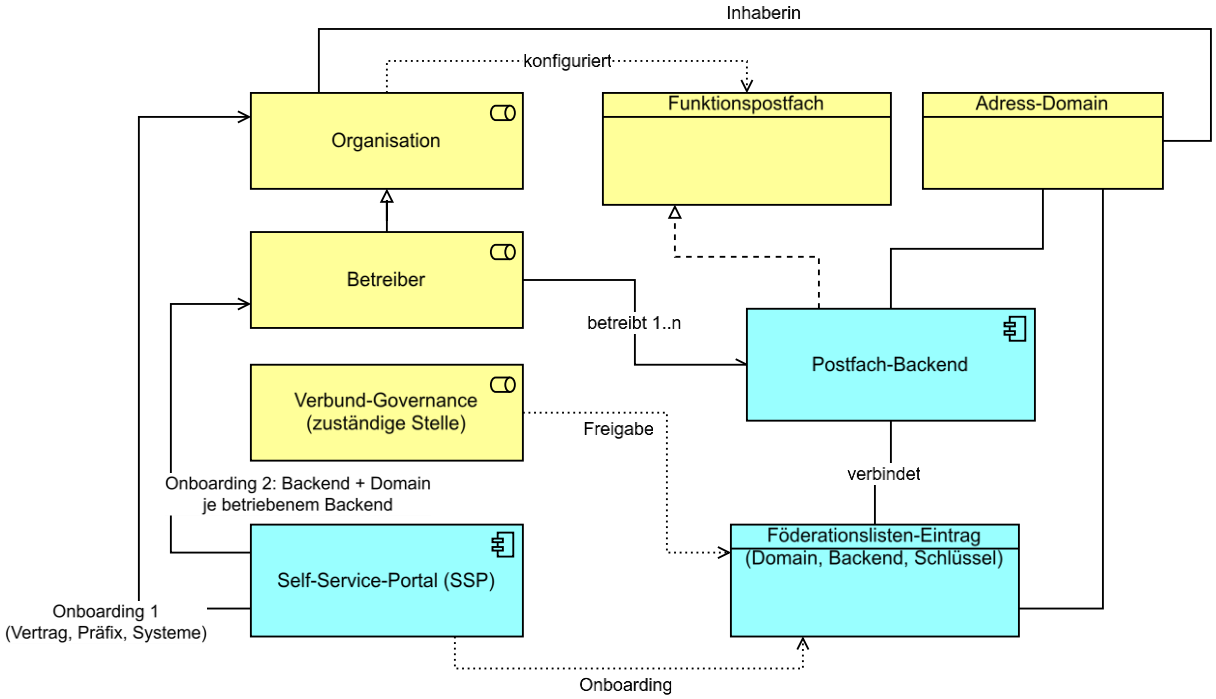

Abbildung 9: Rollen, Domains und Föderationsliste beim Onboarding im Self-Service-Portal

5.4.10 Malware-Prüfung unter Ende-zu-Ende-Verschlüsselung

Eine serverseitige Prüfung auf Schadinhalte ist ausgeschlossen, da das Medien-Repository nur Ciphertext enthält (Anforderung SIC_VER_ÜBE_032). Die Malware-Prüfung kann ausschließlich an E2EE-Endpunkten erfolgen. Die Infrastruktur stellt keinen zentralen Virenscanner bereit (ADR-1130). Die bei De-Mail umgesetzte Lösung, bei der für eine Prüfung Nachrichten dem Betreiber unverschlüsselt vorliegen, wird hier nicht gewählt.

Werden technische Nutzer:innen an Funktionspostfächern betrieben, die Zugriff auf den Klartext haben, kann am serverseitigen E2EE-Endpunkt eine Prüfung auf Malware vorgenommen werden. Ohne diese Möglichkeit des serverseitigen Zugriffs auf den Klartext, muss die Prüfung im Endgerät initiiert werden. Gestützt durch das ZaPuK-SDK kann ein organisationsinterner Scandienst angebunden werden. Wenn Organisationen die technischen Nutzer:innen aus Vertraulichkeitsgründen ohne E2EE-Teilnahme betreiben, verzichten sie gleichzeitig auf die serverseitige Malware-Prüfung. Sie müssen ebenso wie Privatpersonen die Prüfung auf dem Endgerät durch die dort installierte Endpoint Protection umsetzen.

5.4.11 Metadatenreduktion

Kommunikations-Metadaten, d.h. Informationen zu Kommunikationsbeziehungen und Zeitpunkten, weisen in vielen Fällen einen ähnlich hohen Schutzbedarf wie die eigentlichen Inhaltsdaten der Kommunikation auf (vgl. Abschnitt 4.2.1). Selbst ohne Kenntnis der Nachrichteninhalte können Metadaten höchstsensible, schützenswerte Information offenbaren, z. B. wenn allein das Bekanntwerden einer Kommunikationsverbindung diskriminierungssensible Informationen offenlegt. Als Beispiel sei hier die Kommunikation einer Privatperson mit einer spezifischen Fachärzt:in genannt, welche Rückschlüsse auf mögliche Erkrankungen offenbart. Auch lassen sich aus dem Wissen über das Stattfinden einer Kommunikation mit Fachbehörden Rückschlüsse auf die Lebenslagen einer Person ziehen. Nicht selten kann sich auf Grundlage dieser sensiblen Informationen eine Erpressbarkeit von Privatpersonen ergeben. Durch die Möglichkeit der massenhaften Korrelation sensibler Metadaten ergäben sich bei Kompromittierung zentraler Infrastrukturkomponenten damit massive Sicherheitsvorfälle. Aufgrund der Menge und Sensibilität der Metadaten eines solchen Systems reichen die Folgen möglicherweise bis hin zu Risiken für die nationale Sicherheit.

Grundlegendes Schutzziel der Zielarchitektur ist es daher, zu vermeiden, dass entsprechende Metadaten überhaupt erst anfallen, z. B. durch Einführung von Pseudonymen zur Adressierung (siehe Abschnitt 5.5.2) und durch verteilten Betrieb, welcher eine Separierung technisch notwendigerweise anfallender Metadaten auf mehrere Betriebsorganisationen ermöglicht (siehe Abschnitt 4.2). Bei der Umsetzung mit weiterleitendem FP-Bot sieht die Gegenseite zudem ausschließlich die Funktionspostfach-Adresse, Mitgliedschaften und Bearbeiter:innen bleiben nur organisationsintern erkennbar (ADR-1109, vgl. Abschnitt 5.4.3).

5.4.12 Nichtabstreitbarkeit und Abstreitbarkeit

Die Zielarchitektur vereint zwei scheinbar gegensätzliche Eigenschaften. Innerhalb des Kommunikationskanals gewährleistet das Verschlüsselungsprotokoll glaubwürdige Abstreitbarkeit (Anforderung SIC_AUT_ÜBE_014). Keine Kommunikationspartei kann einer dritten Partei beweisen, dass eine bestimmte Nachricht von einer bestimmten Person stammt. Dies schützt die Kommunikationsparteien vor Stigmatisierung und Diskriminierung im Fall einer Kompromittierung (ADR-0012, ADR-0013).

Da für eine rechtssichere Bekanntgabe von Verwaltungsakten eine Nichtabstreitbarkeit gegenüber Dritten aber erforderlich ist (Anforderung ANF_FUN_ZUS_044), wird diese nicht durch den verschlüsselten Kommunikationskanal gewährleistet. Stattdessen setzen die folgenden Konzepte außerhalb dieses Kanals die Anforderung entsprechend um, wobei die einzelne Funktionalität nicht bei jeder Nachricht genutzt werden muss (siehe Abb. 11):

- Die **Bereitstellungsbestätigung** (ADR-0018) belegt den Zugang einer Nachricht bei Empfänger:innen. Das empfangende Postfach-Backend erzeugt hierfür einen signierten Nachweis mit der Prüfsumme der verschlüsselten Nachricht, dem Zeitpunkt und weiteren Meta-Daten. Ein Zugriff auf den Klartext wird dafür nicht benötigt.
- Um Empfänger:innen die **Authentizität und Integrität des Dokumenteninhalts** zu belegen, werden die zu transportierenden Dateien vor dem Versand durch das absendende Fachverfahren mit einem qualifizierten elektronischen Siegel versehen (ADR-0017). Die Herkunft und die Unversehrtheit der Dokumente sind somit auch außerhalb des Systems gegenüber Dritten nachweisbar.
- Mit einer durch den Client (Postfach-Zugang) der Empfänger:innen erzeugten **Abrufbestätigung** kann belegt werden, dass eine Nachricht oder ein Anhang erfolgreich entschlüsselt wurde (ADR-1118). Eine ebenfalls optionale, durch die Empfänger:innen aktiv abgegebene Lesebestätigung dient als elektronisches Empfangsbekenntnis nach § 173 Abs. 3 ZPO. Eine qualifizierte elektronische Signatur ist hierfür keine notwendige Voraussetzung.

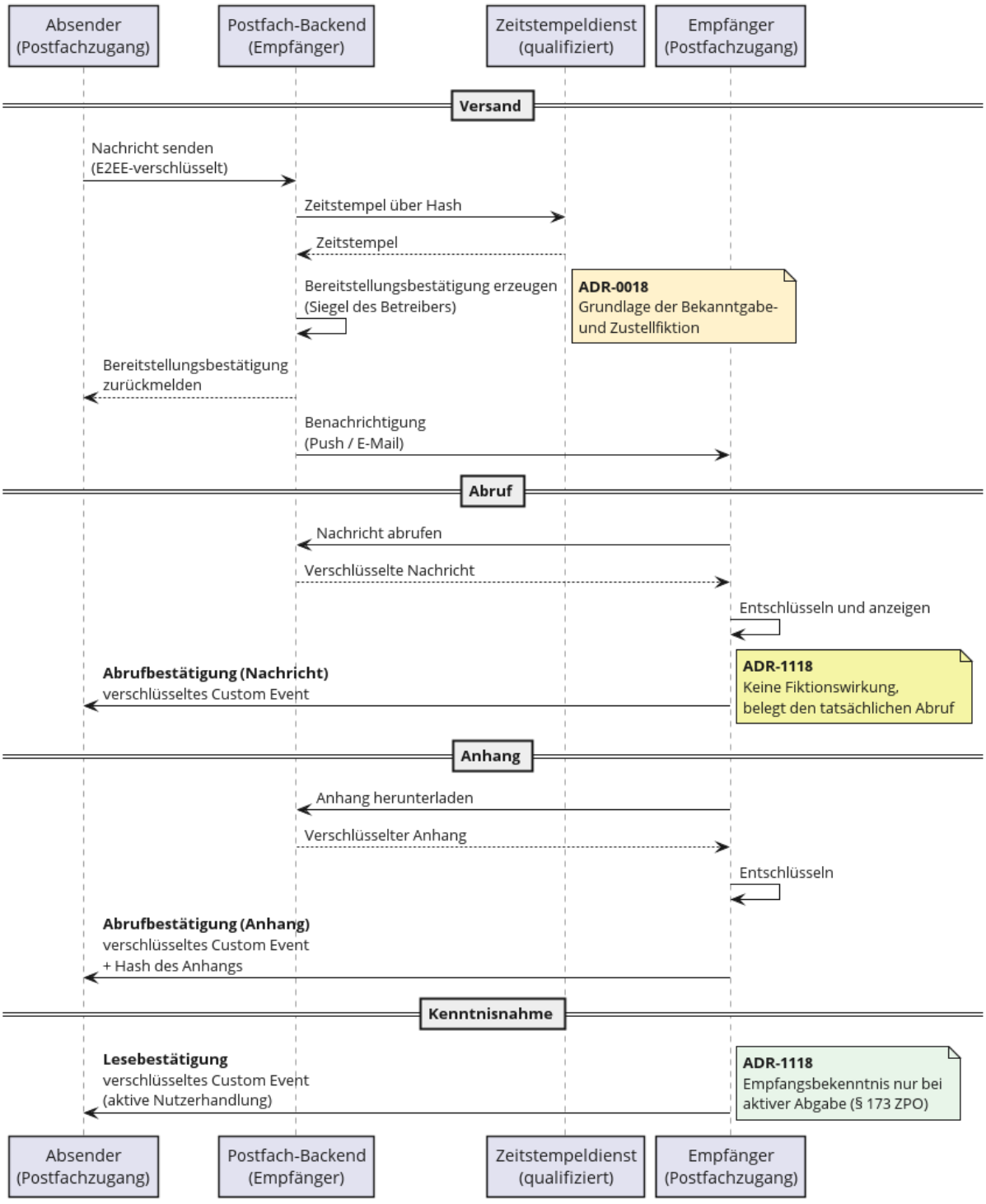

Abbildung 10: Sicherstellung der Nichtabstreitbarkeit zwischen Absender:in und Empfänger:in

Diese Funktionen wirken zusammen, ohne die Abstreitbarkeit im Kommunikationskanal zu beeinträchtigen. Die Kanalverschlüsselung schützt die Vertraulichkeit und bietet Abstreitbar-

keit gegenüber Dritten. Die Bestätigungen und Siegel stellen Nichtabstreitbarkeit dort her, wo sie rechtlich erforderlich ist.

5.4.13 Schlüsselwiederherstellung

Ohne Möglichkeit zur Wiederherstellung verlorener Schlüssel können Empfänger:innen trotz Bereitstellungsbestätigung den Erhalt einer Nachricht abstreiten (vgl. ADR-0018). Ein funktionierender Wiederherstellungsprozess ist deshalb insbesondere im Hinblick auf die beweissichere Bekanntgabe über den ZaPuK-Verbund notwendig. Dabei dürfen weder die Betreiber der Infrastruktur noch Dritte Zugang zu den Schlüsseln der Kommunikation erhalten (ADR-1147).

Nutzer:innen mit mehreren Geräten können die Schlüssel von einem Gerät zum anderen übertragen (Key Sharing zwischen per Cross-Signing verifizierten Geräten). Bei Verlust nur eines Gerätes wäre eine Wiederherstellung somit nicht erforderlich.

Bei Organisationen kann davon ausgegangen werden, dass Prozesse und Infrastruktur existieren, die den Verlust von Geräten bzw. Schlüsseln ausgleichen können. Sind mehrere Mitarbeitende Mitglied eines Raums, führt der Schlüsselverlust einer einzelnen Person nicht zum Verlust des Zugriffs, da die Schlüssel erneut geteilt werden können. Bei Nutzung des Raum-Management-Service können technische Nutzer:innen die Verfügbarkeit der Schlüssel gewährleisten (ADR-1101, ADR-1102).

Nutzer:innen privater Organisationen und Privatpersonen können sich nach einer Re-Authentisierung mit entsprechendem Vertrauensniveau an öffentliche Stellen wenden, um Zugriff auf Nachrichten wiederzuerlangen. Da dies ein langwieriger und aufwändiger Prozess wäre, wird mit serverseitigem Key Backup (Secure Secret Storage and Sharing) ein Verfahren angeboten, das eine Wiederherstellung der Schlüssel durch Nutzer:innen ohne Beteiligung Dritter ermöglicht. Dabei werden Schlüssel zunächst durch den Client der Nutzer:innen mit einem zufällig erzeugten Wiederherstellungsschlüssel (Recovery Key) verschlüsselt und anschließend im Postfach-Backend hinterlegt. Die Einrichtung erfolgt verpflichtend bei der Ersteinrichtung des Postfach-Zugangs. Der Wiederherstellungsschlüssel kann im Schlüsselbund des Betriebssystems, einem Passwort-Manager oder über einen Papierausdruck von den Nutzer:innen sicher verwahrt werden.

5.4.14 Archivierung unter Ende-zu-Ende-Verschlüsselung

Die langfristige Aufbewahrung von Nachrichten durch die Besitzer:innen der Daten erfolgt immer in deren Verantwortung (ADR-1135). Die Zielarchitektur unterstützt den Prozess der Archivierung und Veraktung, stellt aber keinen Aufbewahrungsdienst bereit. Das Postfach

hält Nachrichten vor, bis Nutzer:innen sie löschen oder eine durch den Betreiber konfigurierte Löschfrist greift.
Die Übernahme in das System zur Veraktung bzw. Archivierung findet im Endgerät oder über einen technischen Nutzer statt, der als E2EE-Teilnehmer am Vorgangsraum teilnimmt (vgl. ADR-1101, ADR-1102). Das für die Archivierung vom Postfach-Zugang bereitgestellte Exportpaket enthält die Nachrichten samt Quittungen, den Vorgangsbezug, die Identitätsnachweise, den Nachweis für die Bereitstellung, etwaige Abruf- und Lesebestätigungen sowie Siegel oder Signatur (ADR-1135).

5.5 Zusammenwirken der Komponenten

Die vorangehenden Abschnitte beschreiben die Komponenten und die zugrundeliegenden Architekturentscheidungen. Die folgenden Abschnitte zeigen, wie diese Komponenten in den zentralen Anwendungsfällen der Infrastruktur zusammenwirken.

5.5.1 Adressierung von Organisationen und Berufsträgern

Organisationen werden im Kommunikationsverbund über MXIDs adressiert. Die Adressierung umfasst zwei Schritte: die einmalige Registrierung einer Organisation im Verbund und die Auflösung und Prüfung von Adressen im laufenden Kommunikationsbetrieb.

5.5.1.1 Adressierung von Organisationen

Um an der Kommunikation teilnehmen zu können, muss sich eine Organisation im SSP registrieren und stimmt damit der Adressierbarkeit im Verbund zu (ADR-1111, ADR-1148). Dabei konfiguriert sie bei Nutzung eigener Postfach-Backends die zugehörige Domain (vgl. ADR-1104, Abschnitt 5.2.2.2). Die Namen ihrer Postfächer pflegt sie in der Administrationsoberfläche des Postfach-Backends (vgl. Abschnitt 5.2.2.1). Bei Verwendung des zentralen Postfach-Backends wird ein eindeutiges Präfix für die Organisation festgelegt. Die Postfachadresse ist somit ebenfalls eindeutig. Auf Basis der festgelegten Struktur der Adressen hat sie im zentralen Betrieb die Form `@[orgpräfix]_[funktion]:post.gov.de und` im souveränen Betrieb die Form `@[funktion]:[org-domain]` (ADR-1104).
Die fachlichen Attribute der Organisation werden mit den Postfachadressen (MXID) im Adressregister verknüpft. Das Adressregister implementiert die API Matrix-Identity-Service (MIS) und wird föderiert in den Postfach-Backends betrieben (ADR-1111). Organisationen mit bestehenden Verzeichnisdiensten (z. B. SAFE im Justizbereich) können diese hinter der lokalen MIS-Instanz betreiben.

5.5.1.2 Auflösung und Prüfung von Organisationsadressen

Um eine Nachricht an eine Organisation zu versenden, kann sie über das Adressverzeichnis ermittelt werden. Dazu führen Absender:innen eine Suchanfrage nach fachlichen Attributen der Organisation gegen die MIS-Instanz ihres Postfach-Backends aus. Für Einträge außerhalb der eigenen Domain leitet die lokale Instanz die Anfrage an andere MIS-Instanzen im Verbund weiter. Die Antwort enthält die MXID sowie Organisationszuordnung und Status des Eintrags.

Bei eingehenden Nachrichten können Empfänger:innen die Absender:innen-MXID über den MIS prüfen. Der Client der Empfänger:innen prüft, ob die Absender:innen-MXID in einem signierten Registereintrag der Organisation enthalten ist und welchen Status der Eintrag hat. Die MXID wird also nicht allein aufgrund ihres Namens bzw. der Domain einer Organisation zugeordnet, sondern erst nach erfolgreicher Prüfung des signierten Registereintrags. Diese Prüfung belegt nicht die fachliche Identität der einzelnen sendenden Person (vgl. Abschnitt 5.4.5.2).

Die Verlässlichkeit dieser Prüfung hängt von der Qualität des Registrierungsprozesses ab. Nur wenn der MIS-Eintrag bei der Registrierung korrekt erzeugt und vor unberechtigten Änderungen geschützt wurde, bildet er eine belastbare Grundlage für die Identitätsprüfung (ADR-1145).

5.5.1.3 Adressierung von Berufsträgern

Die Gruppe der Berufsträger (Steuerberater, Rechtsanwälte, Notare) authentifiziert sich als eine Teilmenge der natürlichen Personen über die BundID, eID oder EUDI-Wallet. Im Gegensatz zu Privatpersonen dürfen sie in den entsprechenden Registern (z.B. Kammern) mit ihren Matrix-Adressen gelistet werden. Für die berufliche Tätigkeit sollen diese Personen eigene Konten bzw. Adressen in der Zielarchitektur verwenden. Eine Registrierung ist auf Basis von Nachweisen möglich, die die Zugehörigkeit zu einer Kammer belegen. Perspektivisch ist das auch über Verifiable Credentials der EUDI-Wallet möglich.

5.5.2 Adressierung von Privatpersonen

Für Privatpersonen wird keine vorab registrierte Adresse verwendet. Die MXID wird dynamisch aus dem bereichsspezifischen Pseudonym des genutzten Nutzerkontos abgeleitet (vgl. Abschnitt **Error! Reference source not found.**). Das Pseudonym ist für jeden Benutzer innerhalb eines Verwaltungsbereichs eindeutig und stabil. Eine Person mit demselben Nutzerkonto erhält in der Kommunikation innerhalb desselben Verwaltungsbereichs immer dasselbe

Pseudonym also dieselbe MXID (ADR-1105). Privatpersonen werden nicht im MIS geführt (siehe Abb. 12).

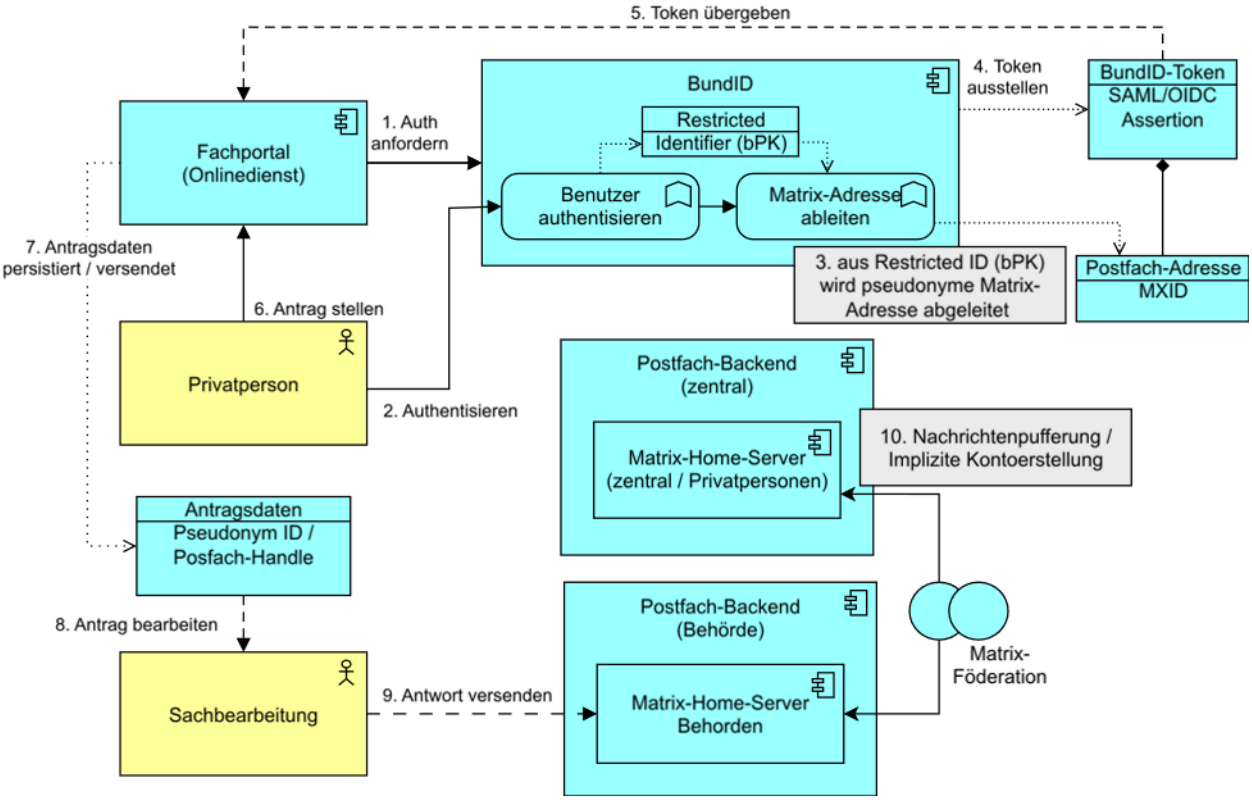

Abbildung 11: Adressierung von Privatpersonen

5.5.2.1 Adressierung von Privatpersonen im Antragskontext

Bei der Antragstellung über ein Fachportal oder einen Onlinedienst authentisiert sich eine Privatperson über die BundID mit der eID oder perspektivisch über die EUDI-Wallet. Das Nutzerkonto beziehungsweise die EUDI-Wallet erzeugt ein für den Nutzer stabiles und bereichsspezifisches Pseudonym, das den lokalen Teil der Postfachadresse (MXID) bildet. Das Pseudonym wird mit dem Antrag als Bestandteil des Identitätsnachweises übermittelt. Eine Antwort der Behörde ist somit ohne ein Adressregister möglich.

5.5.2.2 Zugriff auf Postfächer durch die Privatperson

Für den Zugriff auf die bereichsspezifischen Postfächer stehen zwei Wege zur Verfügung. Über ein Fachportal authentisiert sich die Privatperson im jeweiligen Verwaltungsbereich und hat dann ausschließlich auf die Kommunikation dieses Bereichs Zugriff.

Über den zentralen Postfach-Zugang kann sie dagegen auf die Nachrichten aller Bereiche zugreifen. Dafür liefert BundID nach erfolgreicher Authentifizierung die Liste aller bereichs-

spezifischen MXIDs, die dem Konto zugeordnet sind. Der Client führt die zugehörigen Bereichs-MXIDs in einer gemeinsamen Ansicht zusammen.

5.5.2.3 Proaktive Übermittlung durch Behörden

Wenn eine Behörde eine Nachricht an eine Privatperson übermitteln will, muss die bereichsspezifische pseudonyme Postfachadresse bereits im Fachverfahren vorliegen, z.B. aufgrund eines in der Vergangenheit durchgeführten Verwaltungsvorgangs (vgl. ADR-1105). Liegt diese noch nicht vor, muss die Person zunächst eine Authentisierung in einem Onlinedienst vornehmen, wobei das entsprechende Pseudonym als Bestandteil des Identitätsnachweises an die Behörde gelangt und dann dort eine Ableitung der Adresse möglich ist. Es bedarf also der Mitwirkung der Privatpersonen, bevor eine Behörde diese kontaktieren kann.
Die Aufnahme einer Postfachadresse für jede Privatperson in die Registerdaten des Meldewesens, gleichwertig zur Meldeanschrift, erscheint für die proaktive Übermittlung wünschenswert. Ob diese Adresse bereichsspezifisch definiert sein muss, ist gegen die Vorgaben zur pseudonymen Adressierung zu bewerten (ANF_FUN_ADR_024, ADR-1105). Die Umsetzbarkeit wird im weiteren Verlauf untersucht.

5.5.3 Automatisierte Nachrichteneinlieferung (M2M)

Fachverfahren und Unternehmensanwendungen können Nachrichten versenden, ohne dass eine interaktive Anmeldeprozedur durchgeführt werden muss. Das System authentisiert sich stattdessen über Client Credentials (OAuth 2.0 Client Credentials Flow) gegenüber dem Authorization Server der föderalen API-Autorisierungsinfrastruktur. Der Authorization Server prüft über den Policy Decision Point, ob das System berechtigt ist, in das adressierte Postfach einzuliefern. Die Nachricht wird anschließend Ende-zu-Ende-verschlüsselt an das Ziel-Postfach übermittelt. Die Identität des Systems wird bei der Übermittlung über X.509-Zertifikate (ggf. V-PKI, ELSTER-Organisationszertifikat) nachgewiesen. Für die Empfänger:innen soll es im Vorgangsraum als technische:r Nutzer:in erkennbar sein (vgl. ADR-1101, ADR-0003).

5.5.4 Beweissichere Übermittlung

Die beweissichere Übermittlung stützt sich auf mehrere Nachweise, die unterschiedliche Aspekte der Beweiskette abdecken (vgl. Abschnitt **Error! Reference source not found.**).
Die Zielarchitektur auf Basis der Matrix-Infrastruktur entwirft Lösungen zur gegenseitigen Authentifizierung der Kommunikationsteilnehmer:innen und für den Ende-zu-Ende-verschlüsselten Transport von Nachrichten bzw. Dokumenten. Falls die Prüfbarkeit der Au-

thentizität und Integrität des Inhalts fachlich notwendig ist, muss diese durch die Teilnehmer:innen über die Siegelung bzw. Signierung der übermittelten Dateien selbst gewährleistet werden. Dazu können zentrale Dienste und Trust-Infrastrukturen verwendet werden, die nicht im Rahmen von ZaPuK selbst umgesetzt sind (ADR-0017).

Den Zugang einer Nachricht oder eines Dokumentes zu einem bestimmten Zeitpunkt zu belegen, ist allerdings Kernanforderung an die ZaPuK-Architektur und im Rahmen des Transports zwischen den Teilnehmer:innen umzusetzen. Zu diesem Zweck erzeugen Postfach-Backends mit Hilfe des Quittungsdienstes (bzw. Application Service) Nachweise, die den Zugang zu einem bestimmten Zeitpunkt belegen. Diese Bereitstellungsbestätigungen enthalten eine Prüfsumme der verschlüsselten Nachricht mit einem Zeitpunkt und werden allen Teilnehmer:innen im Raum übermittelt. Zur Erzeugung ist ein Zugriff auf den Klartext nicht notwendig. Der belegte Eingangszeitpunkt, der Hash über den Ciphertext, die Referenz auf die Originalnachricht und der öffentliche Schlüssel des Empfänger:innen-Backends erlauben allen Teilnehmer:innen die Prüfung, ob die Nachricht entsprechend korrekt für die Empfänger:innen bereitgestellt wurde. (ADR-0018)

Im System übermittelte Dateien können sehr groß sein und werden nicht direkt als Matrix-Event übermittelt. Matrix setzt das Pull-Prinzip um, bei dem solche Anhänge verschlüsselt zunächst im Backend der Absender:innen abgelegt werden. Die Empfänger:innen erhalten lediglich einen Link in einer Nachricht, dessen Bereitstellung quittiert sein kann. Erst wenn Nutzende den Anhang über diesen Link laden möchten, wird er in das Postfach-Backend der Empfänger:innen repliziert. Dieses Prinzip, das in Räumen mit Teilnehmer:innen unterschiedlichster Backends sinnvoll ist, um unnötige Netzwerklast zu verhindern, stößt bzgl. der Verfügbarkeit an Grenzen. Ist das Backend der Absender:innen offline, können die Empfänger:innen die Datei nicht herunterladen, was dem Anspruch einer Belegbarkeit des Zugangs entgegensteht. Zur Lösung des Problems können Backends den proaktiven Pull von Anhängen aus dem Absender-Backend veranlassen (ADR-1120).

Bei den genannten Nachweisen zur Bereitstellung kann wegen der Ende-zu-Ende-Verschlüsselung lediglich die erfolgreiche Übermittlung verschlüsselter Daten belegt werden. Alle weiteren Prüfungen müssen über die Schlüssel in den einzelnen Vorgangsräumen vorgenommen werden. Dies ist möglich, aber aufwändig und ggf. ein nur schwer zu führender Beweis, ob eine Nachricht oder Datei bei den Empfänger:innen auch korrekt entschlüsselbar war. Für bestimmte Anwendungsfälle ist deshalb eine Abrufbestätigung sinnvoll, die der Client nach dem Abruf der Nachricht oder Datei und der erfolgreichen Entschlüsselung erzeugt.

Dieser Nachweis enthält eine Referenz auf die Originalnachricht und den Zeitpunkt, bei Anhängen zusätzlich den Hash des entschlüsselten Anhangs. Zusätzlich zu dieser automatischen Nachweiserzeugung ist das Einholen einer Lesebestätigung möglich, bei der die Empfänger:innen den Prozess aktiv initiieren. Grundsätzlich kann das clientseitige Erzeugen der Nachweise nicht erzwungen werden. Sie ersetzen somit die serverseitig erzeugten Bereitstellungsbestätigungen nicht. (ADR-1118)
Absender:innen können über ihren Client mittels der Anfrage von Zustelloptionen die Ausstellung der eben genannten Nachweise initiieren. Sie werden dann nur erzeugt, wenn das System (Postfach-Zugang, Postfach-Backend) der Gegenseite dies unterstützt und, im Falle der manuellen Lesebestätigung, die empfangende Person dies bewilligt. (ADR-1119).

5.5.5 Funktionspostfach und Vorgangsraum

Kontaktiert eine Person ein Funktionspostfach (z. B. *@orgxy_datenschutz:post.gov.de*), erzeugt der technische Nutzer des Funktionspostfachs (FP-Bot) automatisch einen kryptografisch isolierten Vorgangsraum (ADR-1102). Der FP-Bot wird im Raum-Management-Service (RMS) betrieben. Er ermittelt über das Berechtigungsverzeichnis die zuständigen Mitarbeitenden und lädt diese über deren Postfachadressen (MXIDs) in den Raum ein. Externe sehen immer ausschließlich ihren eigenen Vorgang.
Nutzen zwei miteinander kommunizierende Organisationen Funktionspostfächer, gibt es mehrere Möglichkeiten, die Vorgangsräume technisch umzusetzen (vgl. ADR-1109, Abschnitt **Error! Reference source not found.**).
Im Vorgangsraum gilt ein Rollenmodell auf Basis von Matrix Power-Levels (siehe Tab. 11).

Rolle	Berechtigung	Beispiel
Raum-Administrator:in	Raumverwaltung, Einladungen, Power-Level-Vergabe	Technische:r Nutzer:in (FP-Bot)
Moderator:in	Kann Vertretungen dem Raum hinzufügen	Administrator:innen
Bearbeiter:in	Lese- und Schreibrechte für Fallbearbeitung	Sachbearbeiter:innen
Lesende	Ausschließlich Leserechte	Aufsicht, Archivierungskomponente

Tabelle 11: Rollenmodell Matrix

Vertretungen werden durch Einladung zusätzlicher Personen in den bestehenden Vorgangsraum umgesetzt. Die Organisation wählt eine der beschriebenen Konfigurationen (vgl. Abschnitt **Error! Reference source not found.**). Die Abwägung richtet sich nach dem Schutzbedarf der Organisation (vgl. ADR-1101, ADR-1102).
Technische Nutzer:innen sind für die anderen Kommunikationsteilnehmer:innen als solche immer eindeutig gekennzeichnet. Administrative Änderungen an der Teilnehmer:innenschaft des Raums (Einladungen etc.) werden revisionssicher protokolliert. Dies gilt auch für die Moderation der FP-Bots (ADR-1109).

5.6 Zentrale vs. dezentrale Betriebsmodelle für Organisationen

Organisationen unterscheiden sich erheblich in ihren IT-Kapazitäten und in ihren Anforderungen an Souveränität und Datenhaltung. Ein kleines Unternehmen hat andere Anforderungen als ein Konzern mit eigener IT-Abteilung. Wie eine Organisation infrastrukturell an ZaPuK angebunden wird und wer welche Komponenten betreibt, hängt zudem davon ab, wo die Verschlüsselung terminiert: im Endgerät der Mitarbeitenden oder im administrativen Machtbereich der Organisation (vgl. -
In diesem Kapitel werden von der Zielarchitektur unterstützte Betriebsmodelle für anzubindende Organisationen vorgestellt. (ADR-1103)
Minimalanbindung (Betriebsmodell A): Die Organisation nutzt ausschließlich die zentral bereitgestellten Dienste und betreibt keinen eigenen RMS. Sie registriert sich mit ihrem Organisationskonto im SSP und legt ihre Funktionspostfächer in der Administrationsoberfläche des zentralen Postfach-Backends an. Das Initiieren der Vorgangsräume der Funktionspostfächer mit den initialen Teilnehmer:innen wird über den zentralen RMS ermöglicht. Bestehende Vorgangsräume werden über den zentralen RMS automatisiert oder von Nutzer:innen manuell verwaltet (vgl. Abschnitt **Error! Reference source not found.**). Die Matrix-Adressen enthalten die globale Domain des zentral betriebenen Postfach-Backends, eine organisationseigene Domain ist nicht vorgesehen. Der Aufwand für die IT der Organisation bleibt dadurch minimal (siehe Abb. 13).

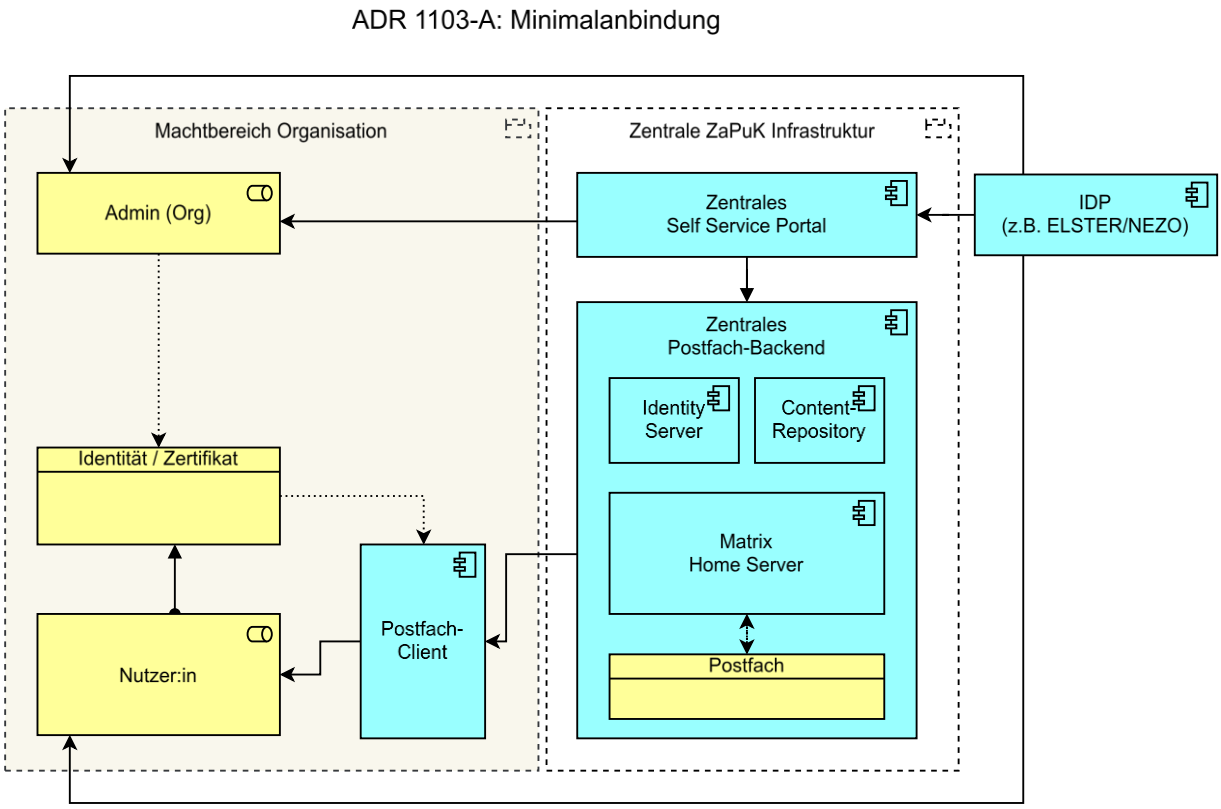

Abbildung 12: Minimalanbindung ohne eigene Serverkomponenten (Betriebsmodell A)

Teilbetrieb (Betriebsmodell B): Organisationen, die Funktionspostfächer mit vollem Funktionsumfang benötigen (z. B. serverseitige Archivierung, siehe auch Abschnitt **Error! Reference source not found.**), müssen den Raum-Management-Service selbst betreiben bzw. betreiben lassen (Auftragsverarbeitung), wobei das Berechtigungsverzeichnis organisationseigen betrieben oder zentral genutzt werden kann. Diese Infrastruktur nutzt das zentrale Postfach-Backend zum Transport und zur Ablage der Nachrichten bzw. Dateien. Der Aufwand der Organisation für Betrieb und Bereitstellung ist deutlich größer als im Betriebsmodell A. Die Matrix-Adressen enthalten die globale Domain des zentral betriebenen Postfach-Backends. Die Postfachzuordnung kann in der Administrationsoberfläche des zentralen Postfach-Backends verwaltet werden (geringster Aufwand) oder organisationsintern über ein eigenes Berechtigungsverzeichnis erfolgen (siehe Abb. 14).

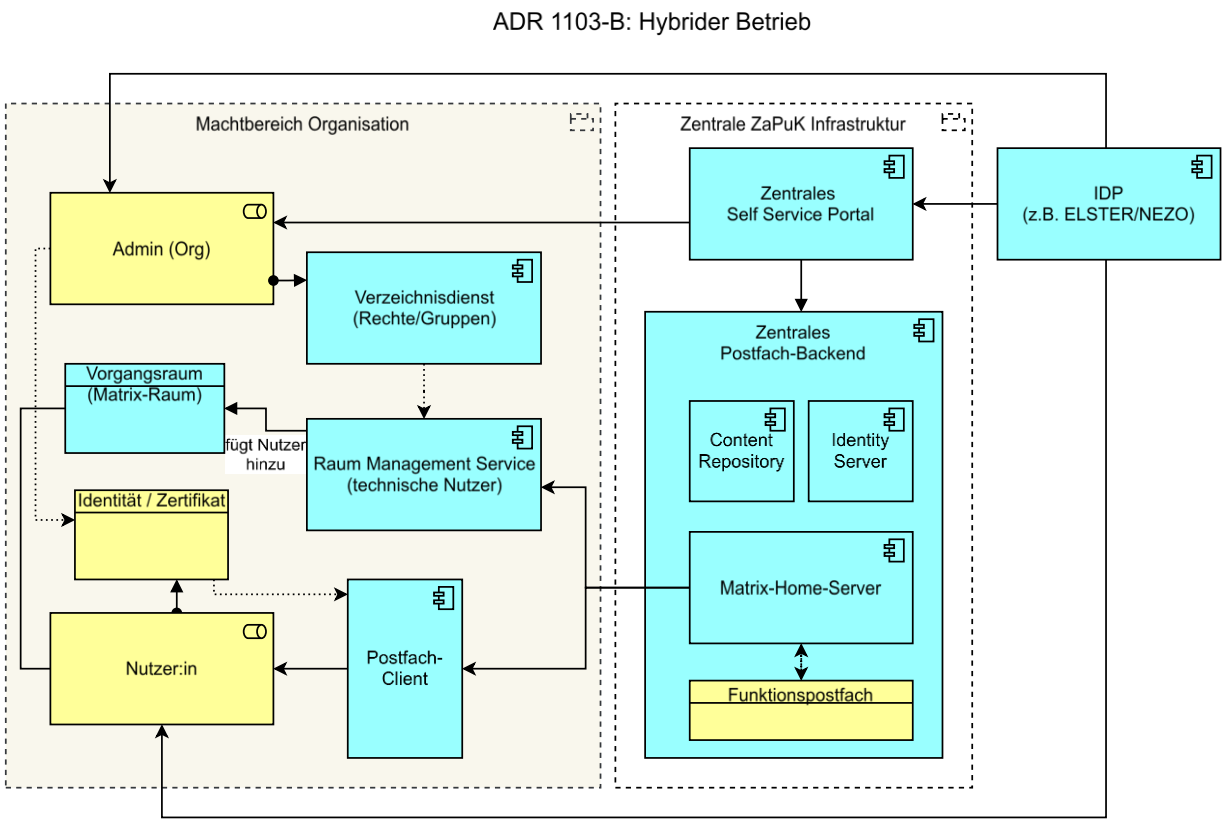

Abbildung 13: Teilbetrieb mit eigenen Serverkomponenten (Betriebsmodell B)

Souveräner Betrieb (Betriebsmodell C): Die Organisation betreibt die gesamte Infrastruktur eigenständig. Dies bietet maximale Unabhängigkeit bei im Vergleich mit den anderen Betriebsmodellen höchstem IT-Aufwand in Verantwortung der Organisation. Die Matrix-Adressen der Organisation verfügen über eine eigene Domain. Da die Organisation den Postfach-Backend-Server eigenständig betreibt, ist sie selbst für die Erzeugung und Signatur der Bereitstellungsbestätigungen verantwortlich (vgl. ADR-0018). Auch bei souveränem Betrieb ist der Einsatz von Funktionspostfächern und RMS optional. Eine Organisation kann dieses Betriebsmodell nutzen und ausschließlich mit Einzelchats und manuellen Gruppenräumen (ADR-1101, Option A) arbeiten. Der Betrieb des TI-Messengers der gematik ist mit diesem Betriebsmodell vergleichbar. Organisationen des Gesundheitswesens können eigene Homeserver betreiben und über einen zentralen Registrierungsdienst anmelden. In der Zielarchitektur übernimmt das SSP diese Funktion (vgl. ADR-0008). Ein kurzzeitiger Systemausfall wäre unproblematisch. Die sendende Seite wird eine Übermittlung in das dezentrale Backend der Empfänger:innen mehrfach neu versuchen (siehe Abb. 15).

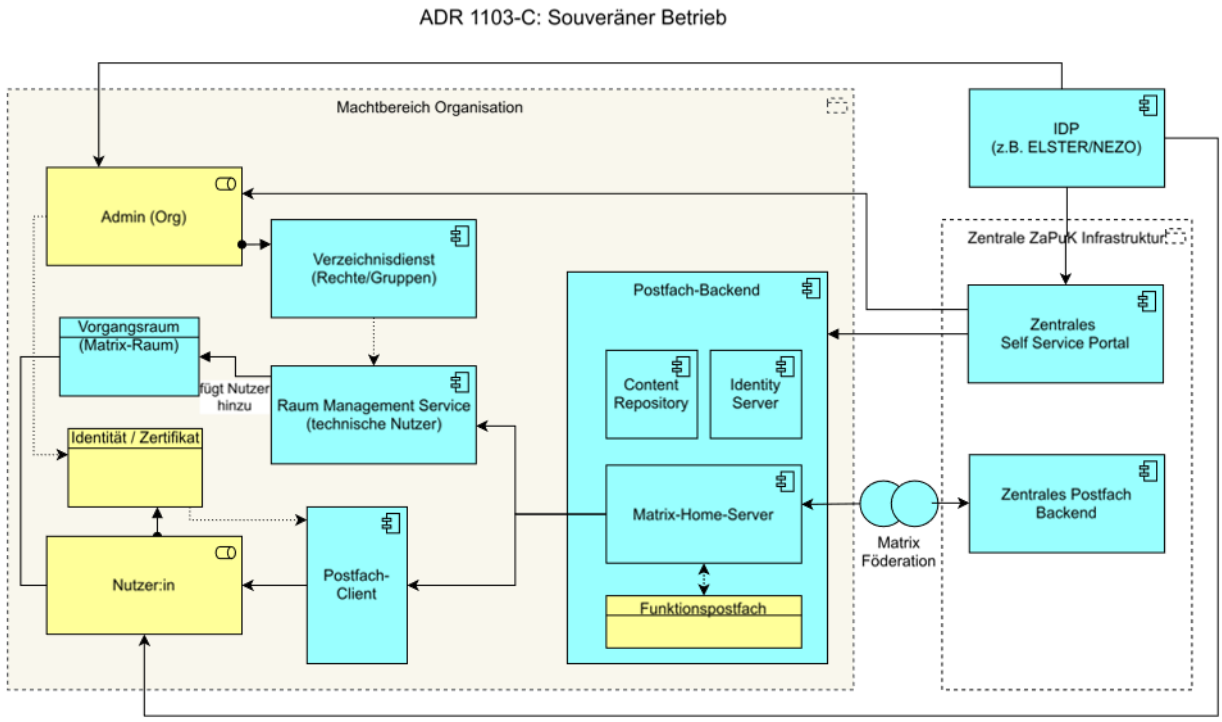

Abbildung 14: Souveräner Betrieb mit eigenem Postfach-Backend (Betriebsmodell C)

Zusammenfassung

Die Wahl des Betriebsmodells liegt bei der jeweiligen Organisation und richtet sich nach ihren IT-Kapazitäten und spezifischen Anforderungen.

Kleineren Organisationen wird mit der Minimalanbindung (Betriebsmodell A) eine vollständige Lösung angeboten. Sie erlaubt eine schnelle Teilnahme, ohne große Hürden bewältigen zu müssen. Funktionspostfächer werden unterstützt. Die Weitergabe der Schlüssel für vergangene Kommunikation übernehmen dabei aktive Raummitglieder. In kleinen Organisationen kann die den Raum administrierende Person die Schlüssel selbst weitergeben.

Größere Organisationen benötigen automatisierte Vertretungsregeln, die auch bei unerwarteten Ausfällen von Bearbeiter:innen und Neueinstellungen jederzeit und unverzüglich den Zugriff auf alle Nachrichten gewährleisten können. Dies kann durch den Betrieb eines organisationseigenen RMS gewährleistet werden, der die Schlüssel des Ende-zu-Ende-verschlüsselten Raums besitzt (Betriebsmodell B oder C). Die Nutzung des Systems mit uneingeschränktem Zugriff auf alte Nachrichten, serverseitiger Archivierung oder Malware-Prüfung kann auch zu einem späteren Zeitpunkt durch den Wechsel auf die Betriebsmodelle B oder C ermöglicht werden. Die Verschlüsselung terminiert im Endgerät, ein zusätzlicher serverseitiger Endpunkt

ist nur im Machtbereich der Organisation zulässig (ADR-1101, ADR-1102). Unabhängig vom gewählten Betriebsmodell sind die Anschlussbedingungen für Organisationen einzuhalten. Für den Betrieb von Postfach-Backends müssen die entsprechenden Anschlussbedingungen verbindlich zugesichert werden (ADR-1145).
Das System erlaubt allen Organisationen eine zu ihren Schutzzielen und weiteren Anforderungen passende Konfiguration ihrer Postfächer.

Glossar

Das diesem Dokument zugrundeliegende Glossar ist hier veröffentlicht: https://gitlab.opencode.de/it-planungsrat/fit-ab/zapuk/-/blob/main/Glossar.md

Abbildungsverzeichnis

Abbildung 1: Zusammenspiel der Funktionsbausteine im D-Stack, Stand 18.9.2026 (wird fortwährend aktualisiert) 15
Abbildung 2: Empfohlene Verortung von Verantwortlichkeiten in Entwicklung, Betrieb und Steuerung zentraler IT-Komponenten der ZaPuK **vorbehaltlich etwaiger Änderungen des FIT-Connect-Produktschnitts zur Schaffung einer föderalen Infrastruktur für Rollout und Anbindung auf Grundlage von SSPs und SDKs im Kontext des D-Stacks* 21
Abbildung 3: Zusammenspiel der Komponenten der Zielarchitektur 29
Abbildung 4: Applikationssicht des ZaPuK-Kommunikationsverbundes 44
Abbildung 5: Infrastrukturnutzende und unterstützende externe Systeme 45
Abbildung 6: Dienstebündel zur Implementierung des Postfach-Backends 50
Abbildung 7: Übersicht Funktionspostfächer und Vorgangsräume 61
Abbildung 8: Adressierung von Organisationen 68
Abbildung 9: Rollen, Domains und Föderationsliste beim Onboarding im Self-Service-Portal 73
Abbildung 10: Sicherstellung der Nichtabstreitbarkeit zwischen Absender:in und Empfänger:in 76
Abbildung 11: Adressierung von Privatpersonen 80
Abbildung 12: Minimalanbindung ohne eigene Serverkomponenten (Betriebsmodell A) 85
Abbildung 13: Teilbetrieb mit eigenen Serverkomponenten (Betriebsmodell B) 86
Abbildung 14: Souveräner Betrieb mit eigenem Postfach-Backend (Betriebsmodell C) 87

Tabellenverzeichnis

Tabelle 1: Programmspezifische Architekturziele 12
Tabelle 2: Programmspezifische Architekturprinzipien 14
Tabelle 3: Backend-Komponenten **vorbehaltlich etwaiger Änderungen des FIT-Connect-Produktschnitts zur Schaffung einer föderalen Rollout- und Anbindungsinfrastruktur auf Grundlage von SSPs und SDKs* 30
Tabelle 4: Infrastrukturnutzende Systeme 46
Tabelle 5: Überblick über Architekturentscheidungen je Komponente der Kerninfrastruktur 48
Tabelle 6: Bestandteile des Postfach-Backends 50
Tabelle 7: Gruppenmitgliedschaften für Funktionspostfächer 53
Tabelle 8: Unterstützende externe Systeme 55
Tabelle 9: Informationsobjekte 55
Tabelle 10: Übersicht ADRs auf Phase I und II 58
Tabelle 11: Rollenmodell Matrix 83

Abkürzungsverzeichnis

ACME	Automatic Certificate Management Environment
ADR	Architecture Decision Record
API	Application Programming Interface
APNs	Apple Push Notification Service
B2G	Business-to-Government
BKZ	Behördenkennzahl
BLK	Bund-Länder-Kommission
BMDS	Bundesministerium für Digitales und Staatsmodernisierung
C2G	Citizen-to-Government
CI/CD	Continuous Integration / Continuous Delivery
D-Stack	Deutschland-Stack
DPI	Digital Public Infrastructure
DVC	Deutsche Verwaltungscloud
E2EE	Ende-zu-Ende-Verschlüsselung
EAA	Electronic Attestation of Attributes
EGVP	Elektronisches Gerichts- und Verwaltungspostfach
eID	Elektronischer Identitätsnachweis
eIDAS	Electronic Identification, Authentication and Trust Services
ELSTER	Elektronische Steuererklärung
EUBW	European Business Wallet
EUDI	European Digital Identity
EUPL	European Union Public Licence
FCM	Firebase Cloud Messaging
FIT-AB	Föderales IT-Architekturboard
FIT-AG	Föderale IT-Arbeitsgruppe
FITKO	Föderale IT-Kooperation
FöPD	Föderale API-Autorisierungsinfrastruktur
FOSS	Free and Open Source Software
FP-Bot	Funktionspostfach-Bot
G2B	Government-to-Business
G2C	Government-to-Citizen
G2G	Government-to-Government

IdM	Identitätsmanagement
IdP	Identity-Provider
IT-PLR	IT-Planungsrat
JSON	JavaScript Object Notation
KI	Künstliche Intelligenz
KAP	Kontextspezifisches Architekturprinzip
M2M	Machine-to-Machine
MIS	Matrix Identity Service
MJP	Mein Justizpostfach
MLS	Messaging Layer Security
MUK	Mein Unternehmenskonto
MXID	Matrix User ID
OAuth	Open Authorization
OID4VCI	OpenID for Verifiable Credential Issuance
OSCI	Online Services Computer Interface
OZG	Onlinezugangsgesetz
PKI	Public Key Infrastructure
QERDS	Qualified Electronic Registered Delivery Service
QTSP	Qualified Trust Service Provider
REST	Representational State Transfer
RFC	Request for Comments
RMS	Raum-Management-Service
SAFE	Secure Access to Federated E-Justice/E-Government
SDK	Software Development Kit
SD-JWT VC	Selective Disclosure JSON Web Token Verifiable Credential
SGB X	Zehntes Buch Sozialgesetzbuch
SMTP	Simple Mail Transfer Protocol
SSP	Self-Service-Portal
TADR	Transition Architecture Decision Record
TI-M	TI-Messenger
TLS	Transport Layer Security
TOGAF	The Open Group Architecture Framework
TOGAF ADM	TOGAF Architecture Development Method

URI ..... Uniform Resource Identifier
UX ..... User Experience
V-PKI ..... Verwaltungs-Public-Key-Infrastruktur
VC ..... Verifiable Credential
ZaPuK ..... Zielarchitektur für Postfach- und Kommunikationslösungen
ZBP ..... Zentrales Bürgerpostfach
ZID ..... Zentraler Issuer-Dienst
ZPO ..... Zivilprozessordnung