Föderale Zielarchitektur für Postfach- und Kommunikationslösungen

Zukunftsweisende föderale Infrastruktur für die Kommunikation zwischen Privatpersonen, privaten Organisationen und öffentlichen Stellen

---

01 Anforderungs- und Bestandsanalyse

Version: 1.0

Stand: 13.05.2025

Titel	Dokumentart	Inhalt
Überblick und Handlungsempfehlung	Klammerdokument	Übergreifende Zusammenfassung des Vorhabens und Darstellung strategischer Implikationen
01_Anforderungserhebung und Bestandsanalyse	**Begleitdokument**	**Beschreibung des Vorgehens und der Erkenntnisse aus der Anforderungs- und Bestandsanalyse mit Auflistung der 151 konsolidierten Anforderungen**
02_Konzept Zielarchitektur	Begleitdokument	Darstellung der auf die Ziele des Vorhabens ausgerichtete Zielarchitektur zur Umsetzung der identifizierten Anforderungen
03_Glossar und Rahmenbedingungen	Begleitdokument	Übersicht über die zentralen Begriffe und Rahmenbedingungen

Nutzungsbedingungen

Inhaltsverzeichnis

Einleitung

Wesentliche Grundlage für den Entwurf einer föderalen Zielarchitektur für Postfach- und Kommunikationslösungen bildet die umfassende Kenntnis zu erfüllender Anforderungen sowie die Erkenntnisse, die aus bereits bestehenden Lösungen und Best-Practices abgeleitet werden können. Das vorliegende Dokument beschreibt das Vorgehen und die zentralen Erkenntnisse aus der Anforderungs- und Bestandsanalyse (Projektphase I).

Kapitel 1 beschreibt das methodische Vorgehen bei der Anforderungsanalyse. Die Analyse bestehender Lösungen bildete dabei eine wesentliche Quelle für die Ermittlung von Anforderungen. Darüber hinaus wurden hierbei auch Funktionsmerkmale sowie architektonische und technologische Grundlagen der Lösungen vergleichend dokumentiert, um diese Aspekte in der Konzeption der Zielarchitektur aufgreifen zu können.

Die Anforderungen werden führend in einem Anforderungskatalog vorgehalten und verwaltet. Ein aktueller Auszug der abgeleiteten konsolidierten Anforderungen an die Zielarchitektur ist in Kapitel 2 einsehbar.

Im abschließenden Kapitel 3 werden wesentliche Erkenntnisse aus der Anforderungs- und Bestandsanalyse dargestellt.

1 Methodisches Vorgehen

Die Anforderungen an die Zielarchitektur wurden in einem strukturierten multi-methodischen Analyseprozess zwischen Herbst 2024 und Frühjahr 2025 systematisch erhoben und konsolidiert. Ausgangspunkt für die strukturierte Erhebung von Anforderungen sowie die Ableitung relevanter Erkenntnisse für die Entwicklung der Zielarchitektur bildete

- die Bestandsanalyse bestehender Postfachlösungen und Best-Practices sowie
- die Analyse von Rahmenbedingungen.

Im weiteren Verlauf erfolgte

- die Durchführung von Workshops mit Fachexpert:innen sowie
- die Konsultation über openCode für eine breitere Öffentlichkeit.

Das Vorgehen orientierte sich an dem im Folgenden beschriebenen Phasenmodell.

1.1 Erhebung und Validierung von Anforderungen

Die Erhebung erfolgte anhand von Textanalysen anforderungsrelevanter Quellen sowie strukturierter Interviews. Ergänzend wurden weitere regulatorische, architektonische und strategische Rahmenbedingungen (Gesetze, Verordnungen, Architekturrichtlinien, die Föderale Digitalstrategie sowie relevante Technische Richtlinien des BSI) analysiert. Diese Quellen wurden bewertet, priorisiert und in die Anforderungsanalyse einbezogen.

Alle analysierten Quellen wurden in ein umfassendes Quellenverzeichnis aufgenommen, wobei die zugehörigen Dokumente in einer zentralen Projektablage hinterlegt wurden. Die zunächst unkonsolidiert erfassten ca. 900 Anforderungen (Stand: 04/2025) wurden thematisch strukturiert und rückverfolgbar zu den jeweiligen Quelldokumenten und den entsprechenden Textpassagen dokumentiert. Ergänzend wurden diese zunächst noch unkonsolidierten Anforderungen in Interviews und Workshops mit Fachexpert:innen validiert und erweitert.

In die Bestandsanalyse wurden wesentliche bestehende Postfach- und Kommunikationslösungen mit Relevanz für die föderale IT-Landschaft vertieft einbezogen.

Neben der Ableitung von **Anforderungen** für die Zielarchitektur wurden die Bestandslösungen auch hinsichtlich ihrer **Fähigkeiten** sowie ihren **architektonischen und technologischen Merkmalen** analysiert und dokumentiert.

Tabelle 1: Dokumentation der Ergebnisse aus der Bestandsanalyse

1.	Strukturierung und Dokumentation von Anforderung	➔ *Anforderungsliste (unkonsolidiert)*
2.	Strukturierung und Dokumentation von Fähigkeiten	➔ *Produktsteckbriefe*
3.	Erkenntnisgewinn über die jeweilige Architektur und Technologie	➔ *Produktsteckbriefe*

Aufgrund der zeitlichen Begrenzungen des Projektes lag der Fokus dabei insbesondere auf generalistischen Lösungen sowie solchen, die technologisch-architektonisch alternative Ansätze verfolgen. Spezifische Postfachlösungen einzelner Fachdomänen (z. B. Arbeit und Soziales oder Rentenversicherung) wurden hingegen nicht vertiefend betrachtet. Diese können jedoch im Rahmen der weiteren Arbeiten an einer gemeinsamen Zielarchitektur zukünftig berücksichtigt werden.

Die folgende Tabelle gibt einen Überblick über die analysierten Bestandslösungen:

Tabelle 2: Übersicht betrachteter deutscher Bestandslösungen

Bestandslösung	Zweck
Zentrales Bürgerpostfach (ZBP)	Das ZBP ist eine digitale Kommunikationsplattform, um zwischen öffentlichen Stellen und Privatpersonen eine sichere und effiziente Zustellung von Bescheiden und Nachrichten zu ermöglichen, wodurch der postalische Versand ersetzt werden kann. Das ZBP realisiert damit in erster Linie den digitalen Rückkanal nach digital in Anspruch genommenen OZG-Leistungen.
Postfach 2.0	Das Postfach 2.0 ist eine von zwei Postfachkomponenten von "Mein Unternehmenskonto" zur rechtsverbindlichen und digitalen Kommunikation zwischen öffentlichen Stellen und privaten Organisationen. Unterscheidungsmerkmal zum OZG-PLUS-Postfach ist die beschränkte Abbildbarkeit komplexerer Unternehmensstrukturen bei der Adressierung und Zugriffsberechtigung.
OZG-PLUS-Postfach	Das OZG-PLUS-Postfach ist eine alternative Postfachkomponente von "Mein Unternehmenskonto". Es wurde geschaffen, um eine einheitliche digitale *Ende-zu-Ende-verschlüsselte* (E2EE) Kommunikation zwischen öffentlichen Stellen und privaten Organisationen gemäß OZG zu gewährleisten. Dabei unterstützt es komplexere Unternehmensstrukturen durch eigenverwaltete Funktionspostfächer und Vertretungsregelungen.

Bestandslösung	Zweck
De-Mail	De-Mail bietet eine sichere, vertrauliche und nachweisbare elektronische Kommunikationsinfrastruktur für einen verbindlichen Rechts- und Geschäftsverkehr zwischen öffentlichen Stellen, Privatpersonen und privaten Organisationen.
TI-Messenger	Die TI-Messenger Infrastruktur erlaubt die sichere, vertrauliche und datenschutzkonforme Echtzeitkommunikation zwischen verschiedenen Akteuren im Gesundheitswesen und in Zukunft auch für Krankenversicherte.
Elektronisches Gerichts- und Verwaltungspostfach (EGVP)	Der elektronische Rechtsverkehr (ERV) ermöglicht die elektronische Kommunikation mit Gerichten und Behörden unter Wahrung der Rechtssicherheit. Es können Schriftsätze, Dokumente sowie maschinenlesbare strukturierte Daten im XJustiz-Format rechtswirksam an alle teilnehmenden Gerichte und Behörden übermittelt werden. Ursprüngliches Ziel ist es, den Beteiligten an gerichtlichen Verfahren die Abgabe verbindlicher Erklärungen gegenüber den Gerichten und Justizbehörden in elektronischer Form zu ermöglichen. Mittlerweile finden aber auch weitere Kommunikationsszenarien bis hin zu Registerabfragen statt. EGVP bildet die grundlegende Transportinfrastruktur. Für die Nutzung der Infrastruktur ist je Domäne individuelle ERV-Sende- und Empfangssoftware (ERV-SES) erforderlich, die sich an diese Infrastruktur anbinden muss und die für den jeweiligen Nutzerkreis eigene Zugangswege für IT-Systeme oder Benutzeroberflächen schafft. Beispiele sind beA, beN, beSt, beBPo.
Besondere elektronische Bürger- und Organisationspostfach (eBO) / Mein Justizpostfach (MJP)	Mit dem eBO können Privatpersonen und private Organisationen elektronische Dokumente sicher und zuverlässig mit der Justiz über die EGVP-Transportinfrastruktur austauschen. Diese ERV-SES-Lösung bietet allerdings ausschließlich einen Postfach- und Schnittstellenzugang. Anwender benötigen spezifische Clients für den Zugriff. Seit dem 12. Oktober 2023 steht für Privatpersonen zusätzlich das kostenlos nutzbare Mein Justizpostfach (MJP) als Browseranwendung zur Verfügung zur Kommunikation mit der Justiz sowie mit Behörden, Anwält:innen, Notar:innen und Steuerberater:innen. Als ERV-SES erfordern beide Lösungen die EGVP-Transportinfrastruktur.
BwMessenger / BundesMessenger	Der BundesMessenger ist ein quelloffener Messenger für die öffentliche Verwaltung. Er ist die Weiterentwicklung des BwMessengers, der eigens für die Bundeswehr entwickelt wurde. Das Ziel ist eine moderne und sichere Zusammenarbeitsplattform für die Verwaltung in Deutschland zu schaffen, die sich den Bedürfnissen und Vorgaben der Verwaltung anpasst (primärer Use-Case ist die verwaltungsinterne Kommunikation zwischen Behördenmitarbeitenden).

Ein zentraler Bestandteil im Anforderungsmanagement war die Einbindung der relevanten Stakeholder. Durch strukturiertes Stakeholdermanagement wurden die Beteiligten identifiziert, um die aktive Einbindung aller relevanten Fachexpert:innen in die Untersuchung der betrachteten Bestandslösungen sicherzustellen. In Workshops und Interviews wurden technologische und fachliche Anforderungen konkretisiert und wichtige Perspektiven zu den bestehenden Lösungen aufgenommen. Die Ergebnisse dieser Zusammenarbeit schufen damit eine fundierte Grundlage für die Entwicklung der Zielarchitektur.

Parallel zur Anforderungserhebung anhand der Erkenntnisse der Bestandssysteme erfolgte durch das Projektteam eine Ableitung von insbesondere übergreifenden Anforderungen auf Grundlage von Erfahrungswissen aus der Disziplin des *Föderalen IT-Architekturmanagements (FIT-AM)*.

1.2 Thematische Strukturierung

Zur Unterstützung einer vergleichenden und strukturierten Analyse erfolgte eine induktive Zerlegung des Lösungsraumes in thematische Kategorien und Unterkategorien. Das resultierende **Kategorienschema** war strukturgebend sowohl für die Methodik (bspw. Interviewleitfaden, Stakeholderworkshop), als auch für die Ergebnisartefakte. Ergänzt wurden die thematischen Kategorien um Kategorien für **Qualitätsanforderungen**, die sich an der Struktur des Standards ISO/IEC 25010[1] orientieren.

[1] ISO/IEC 25010:2023 - Systems and software engineering — Systems and software Quality Requirements and Evaluation (SQuaRE) — Product quality model

Abbildung 1: Thematische Struktur der Anforderungsliste und Produktsteckbriefe

In der folgenden Tabelle werden die Kategorien knapp erläutert. Es ist zu beachten, dass dort getätigte Aussagen nicht zwingend einer Anforderung an die Zielarchitektur entsprechen müssen, sondern beschreibende Eigenschaften von Bestandslösungen darstellen.

Tabelle 3: Erläuterung der Kategorien

Kategorie	Beschreibung
Use Case	Die Kategorie **Use Case** beschreibt geschäftliche Anwendungsfälle, die von Postfach- und Kommunikationslösungen zu unterstützen sind, die beteiligten Teilnehmer:innen sowie administrative Prozesse, die zur Steuerung und Verwaltung notwendig sind.
Nachrichten	Die Kategorie **Nachrichten** umfasst Merkmale und Funktionen wie den Versand von Anhängen (z. B. Bescheide, Nachweise) mit bestimmten Größen- und Formatvorgaben. Zudem können Nachrichten in unterschiedlichen Textformaten gestaltet werden und mit fachlichen Metadaten wie Fallbezügen oder Identifikatoren angereichert werden. Durch die Einbindung in Vorgänge lassen sich Nachrichten in Prozesse oder Workflows integrieren, etwa für Widersprüche.
Identifikation	Die Mechanismen zur Verifizierung und Authentisierung von Nutzer:innen im System werden in der Kategorie **Identifikation** behandelt. Dazu gehören Identity Provider, die Identitäten bestätigen. Zudem spielen Authentisierungsmittel wie beispielsweise eID oder ELSTER-Zertifikate eine Rolle. Die Kommunikation und Sicherstellung der Identitäten erfolgt über Authentifizierungs- und Autorisierungsprotokolle.

Kategorie	Beschreibung
Adressierung	In der Kategorie **Adressierung** wird beschrieben, wie Empfänger:innen adressiert werden. Dabei kann die Adressierung zum Beispiel initiativ aus einem Adressbuch, aus Übermittlung eines Antrags oder als Antwort erfolgen. Darüber hinaus sollen Regelungen zur Stellvertretung möglich sein, die temporär oder dauerhaft vergeben werden können. Ein weiteres Merkmal ist die Nutzung von Funktionspostfächern, die mehreren berechtigten Personen gemeinsamen Zugriff auf Nachrichten ermöglichen. Die Kommunikation mit mehreren Beteiligten wird ebenfalls betrachtet.
Transport	**Transport** bezeichnet den Prozess der Auswahl des Pfades für die Übertragung von Nachrichten oder Datenpaketen von einer Absender:in zu einer Empfänger:in über ein Netzwerk. Dabei umfasst das Routing die Auswahl des Übertragungspfads. Gegebenenfalls sind beim Transport die Einhaltung von Complianceregeln sicher zu stellen.
Speicherung	Die Kategorie **Speicherung** beschreibt die Fähigkeiten zur Speicherung und Löschung von Nachrichten auf Ebene der Infrastruktur. An dieser Stelle werden keine Anforderungen an die Speicherung auf Clients beschrieben.
Zustellung	In der Kategorie **Zustellung** werden Mechanismen behandelt, die sicherstellen, dass Nachrichten zuverlässig, nachvollziehbar und rechtssicher zugestellt werden. Die Nachvollziehbarkeit gewährleistet eine lückenlose Dokumentation des Zustellprozesses, während Nichtabstreitbarkeit sicherstellt, dass der Versand und Empfang von Nachrichten nicht geleugnet werden können. Bestätigungen quittieren den Versand und die Abholung von Nachrichten. Die Zustellgarantie stellt sicher, dass Nachrichten nicht verloren gehen, während die Zustellfiktion festlegt, unter welchen Bedingungen eine Nachricht als zugestellt gilt. Durch rechtssicheren Schriftformersatz werden gesetzliche Anforderungen erfüllt, z. B. bei Fristen oder Widersprüchen. Schließlich sorgt eine Eingangsbenachrichtigung dafür, dass Empfänger:innen über neue Nachrichten auf alternativem Weg informiert werden.
Postfachzugang	Die Kategorie **Postfachzugang** beinhaltet Anforderungen und Funktionen der nutzendenseitigen Zugänge zur Infrastruktur insbesondere aus Perspektive der Privatpersonen. Anforderungen an Clients mit graphischen Bedienoberflächen wurden allerdings nicht strukturiert und explizit erfasst, sondern nur im Zuge der Quellenanalyse mit dokumentiert. Für die aktuelle Phase der Arbeit an einer Zielarchitektur mit Fokus auf einer interoperablen Infrastruktur wurde die Detail-Konzeption von Clients zunächst ausgeklammert. Diese Konzeption wird im Falle der Umsetzung des Projektes mit der Erstellung der Lösungsarchitektur adressiert. Dabei gilt es dann, die Zugänge zur Infrastruktur aus Nutzer:innenperspektive zu gestalten. Aus Sicht der Privatpersonen muss der Zugang zum Postfach in den Kontext der allgemeinen Interaktionsmöglichkeiten mit öffentlichen Stellen gestellt werden, wie zum Beispiel der Antragstellung, der Verwaltung von Authentisierungsmitteln, Vollmachten und Dokumenten oder der Integration in Wallets.
Architektur	Die Kategorie **Architektur** differenziert sich in die Beschreibung von Client- und Server-Bausteinen. Unter Administration werden Systeme zur Verwaltung von Benutzer:innen, Berechtigungen und Systemkomponenten geführt. Die Governance

Kategorie	Beschreibung
	legt Richtlinien und Verantwortlichkeiten zur Steuerung fest. Die Unterkategorie Betrieb umfasst alle Aktivitäten und Prozesse, die notwendig sind, um eine Lösung zuverlässig und effizient auszuführen und zu administrieren. Die Unterkategorien dienen in erster Linie der strukturierten Beschreibung in den Produktsteckbriefen. Anforderungen zur Kategorie Architektur wurden nur begrenzt erfasst, da diese über andere Wege dokumentiert werden (Architekturprinzipien, Architekturrichtlinien).
Anbindung	Die Kategorie **Anbindung** beschreibt die Möglichkeiten und Anforderungen für die Integration durch externe Systeme. Über Schnittstellen erfolgt die Kommunikation zwischen Komponenten. *Software Development Kits* (*SDKs*) erleichtern die Entwicklung und Anbindung von Anwendungen, während die API-Dokumentation sicherstellt, dass Schnittstellen nachvollziehbar und standardkonform für Menschen und Maschinen lesbar beschrieben sind.
Sicherheit	Die Kategorie **Sicherheit** beschreibt Maßnahmen zum Schutz von Nachrichten und Daten vor unbefugtem Zugriff, Manipulation und Malware. Der Schutzbedarf ist abhängig von der Vertraulichkeit von Daten. Das zu realisierende Vertrauensniveau erfordert ein diesem angemessenes Sicherheitsniveau, insbesondere hinschlich des Grads des Vertrauens in die Identität einer Person oder eines Systems. Die Authentizität und Integrität einer Nachricht werden durch Siegel oder Signaturen gewährleistet, um die Echtheit und Unversehrtheit der Daten sicherzustellen. Eine PKI dient zur Verwaltung und Verifikation von Schlüsseln. Für den sicheren Transport kommt eine Ende-zu-Ende-Verschlüsselung zum Einsatz. Zudem wird durch Nachrichtenverschlüsselung sichergestellt, dass gespeicherte Nachrichten nur für autorisierte Personen zugänglich sind.

1.3 Anforderungskonsolidierung

Die ca. 900 identifizierten Einzelanforderungen wurden in einem Konsolidierungsprozess zusammengeführt und mündeten in einem Entwurf einer **konsolidierten Anforderungsliste**[2] mit ungefähr 150 Anforderungen. Hierzu wurden verschiedene Faktoren holistisch abgewogen, insbesondere deren Architekturrelevanz und das jeweilige Abstraktionsniveau. Im Rahmen des Prozesses erfolgte somit zunächst eine Bewertung des Abstraktionsgrades und der Relevanz der Anforderungen. Detailanforderungen ohne Relevanz für die übergreifende Zielarchitektur wurden für eine spätere Betrachtung im Rahmen der Realisierung konkreter Lösungsarchitekturen ausgegrenzt. Technologiebezogene sowie lösungsspezifische, nicht generalisierbare Anforderungen wurden ausgegrenzt oder verworfen. Darüber hinaus wurden redundante Anforderungen aus unterschiedlichen Quellen zusammengefasst.

[2] Konsolidierte-Anforderungen · IT-Planungsrat / Föderales IT-Architekturboard / Zielarchitektur Postfach- und Kommunikationslösungen

Ein weiterer Schwerpunkt des Konsolidierungsprozesses lag auf der begrifflichen Schärfung und Vereinheitlichung. Dazu wurde ein **Glossar**[3] erstellt, welches zentrale Begriffe definiert und so die durchgängige Verwendung einer kohärenten Terminologie sicherstellt.

Durch ein System methodengetriebener Verweise in einem zentralen Anforderungsregister wurde die **Rückverfolgbarkeit** aller Anforderungen sichergestellt, sodass die Herkunft jeder konsolidierten Anforderung zurückführbar auf eine oder mehrere nicht-konsolidierte Ursprungsanforderungen ist und bis auf die entsprechende Textpassage ihrer ursprünglichen Quelle nachvollzogen werden kann (siehe Abbildung 2).

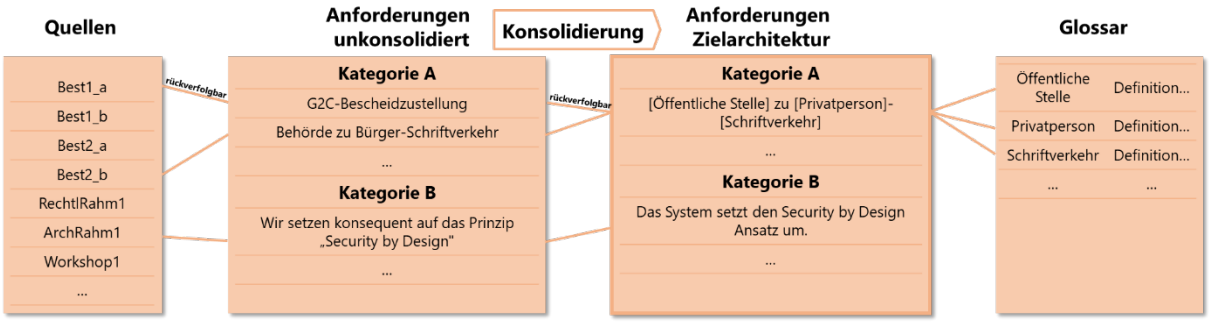

Abbildung 2: Ableitung und Konsolidierung von Anforderungen aus Quellen

1.4 Qualitätssicherung

Aufgrund der hohen Relevanz der konsolidierten Anforderungsliste erfolgten im Verlauf des Projektes bereits verschiedene Maßnahmen zur Qualitätssicherung. Neben einer kontinuierlichen **internen Qualitätssicherung** im Projektteam wurde die konsolidierte Anforderungsliste den Verantwortlichen der Bestandslösungen, den Mitgliedern der Arbeitsgruppe des Föderalen IT-Architekturboards sowie weiteren Fachexpert:innen **zur Kommentierung bereitgestellt**. In einem **Anforderungsworkshop** am 27. Januar 2025 erfolgte mit ca. 30 Stakeholdern aus Bund und Ländern unter Einbeziehung der Betreiber:innen aller Bestandslösungen ein intensiver Diskurs über die erste Fassung der konsolidierten Anforderungsliste. Nach Einarbeitung der Ergebnisse aus dem Workshop wurde diese Liste mit Stand v0.6 zur breiteren Konsultation auf der Plattform openCode veröffentlicht.

[3] Glossar · IT-Planungsrat / Föderales IT-Architekturboard / Zielarchitektur Postfach- und Kommunikationslösungen

2 Konsolidierte Anforderungsliste der Zielarchitektur

Der aktuelle Stand der konsolidierten Anforderungsliste[4] und eine detaillierte Beschreibung des methodischen Vorgehens zur Anforderungsanalyse findet sich auf der Plattform open-Code.

Eine Version v 0.6 zum Berichtszeitpunkt (Stand 04/2025) findet sich in der Anlage zu diesem Dokument.

[4] Konsolidierte-Anforderungen · IT-Planungsrat / Föderales IT-Architekturboard / Zielarchitektur Postfach- und Kommunikations-lösungen

3 Wesentliche analytische Erkenntnisse

Über die konsolidierte Anforderungsliste hinausgehende wesentliche Erkenntnisse aus der Anforderungs- und Bestandsanalyse werden im Folgenden zusammenfassend dargestellt.

Alle Lösungen setzen überwiegend identische Fähigkeiten um: Alle Lösungen bieten ähnliche grundlegende Funktionsmerkmale zum Austausch von elektronischem Schriftverkehr. Dies bedeutet, dass in der Postfachlandschaft aktuell zahlreiche funktional ähnliche Lösungen parallel entwickelt und betrieben werden.

Vergleichbare Fähigkeiten sind heterogen umgesetzt und strukturell verankert: Ähnlich geartete Fähigkeiten werden in bestehenden Postfach- und Kommunikationslösungen unterschiedlich umgesetzt. Sie unterscheiden sich insbesondere aufgrund der heterogenen und historisch gewachsenen technischen, juristischen und organisatorisch-strukturellen Lagen innerhalb der und zwischen den verschiedenen Bereichen des staatlichen Handelns.

Exemplarisch konnten folgende Arten und Quellen der Heterogenität identifiziert werden:

- **Rechtliche Rahmenbedingungen wirken auf die Systemgestaltung ein**: Die aktuelle Postfachlandschaft ist historisch gewachsen. Grundlegend und existenzbegründend sind in der Regel Rechtsvorschriften, die teils kleinteilig und inkrementell Fähigkeiten vorgeben.[5] Darüber hinaus schreiben Rechtsvorschriften teilweise auch architektonische Rahmenbedingungen oder konkrete technische Standards vor (Beispiel: Verwendung von OSCI im ERV). Eine über alle staatlichen Institutionen reichende Gesamtstrategie ist ohne Anpassung der aktuellen Rechtsgrundlagen vermutlich nicht abbildbar.
  Als konkretes Beispiel sei hier die Umsetzung von Fähigkeiten für die Erfüllung von Anforderungen der Nichtabstreitbarkeit zu nennen. Die Beweiskraft der Umsetzungsansätze ist dabei unterschiedlich weitreichend. Dies ist auch darin begründet, dass heterogene Regelungen definiert sind, beziehungsweise Freiheitsgrade in Rechtsgrundlagen Interpretationen für die Umsetzung erlauben. Die Heterogenität der Rechtsgrundlagen erschwert damit auch Ansätze für ein gemeinsame Zielarchitektur. Digitaltauglichkeitsprüfungen von Gesetzesentwürfen sollten hier zukünftig für eine Harmonisierung sorgen.
- **Governance- und Organisationsstrukturen sind heterogen**: Bestehende Lösungen werden teils im Rahmen entkoppelter Strukturen finanziert, gesteuert, technisch und planerisch weiterentwickelt und betrieben.

[5] vgl. Impulse für eine kohärente Digitalverfahrensgesetzgebung – NEGZ · Kompetenznetzwerk Digitale Verwaltung

- **Nutzer:innen-Orientierung ist kontextuell beschränkt**: Meist betrachtet jede Bestandslösung Nutzer:innen isoliert im Kontext ihrer jeweiligen fachlichen Perspektive. Dem Umstand, dass dieselbe natürliche Person oder Organisation in unterschiedlichen Situationen in unterschiedlichen fachlichen Rollen auftritt (z. B. als Antragsteller:in, Kläger:in, Patient:in, Mitarbeiter:in, ...) wird nur selten Rechnung getragen.
- **Lösungen sind architektonisch und technologisch unterschiedlich ausgestaltet**: Die historisch und planerisch entkoppelte Genese der bestehenden Lösungen führte zu Technologie- und Architekturentscheidungen, die zum jeweiligen Entwicklungszeitpunkt ggf. den gegebenen Anforderungen und dem Stand der Technik entsprachen, in der heutigen Gesamtschau der IT-Landschaft aber zu Komplexität führen. Beispiele sind dezentrale vs. zentrale Architekturen, Identitäten, die Umsetzung der Verschlüsselung oder die Schnittstellentechnologien.
  - Dezentrale vs. zentrale Architektur: Bei den analysierten Kommunikationslösungen waren sowohl zentrale als auch zunehmend dezentrale föderierte Architekturen anzutreffen. Diese Dimension erstreckt sich dabei über verschiedene architektonische Bereiche, wie Betriebsverantwortung, Datenhaltung etc.
  - Dezentrale vs. zentrale Identitäten: Auch in Bezug auf die Einbindung von Identity Providern unterscheiden sich die Ansätze. Während zum Beispiel im Gesundheitssektor ein föderiertes sektorales Identitätsmanagement für Versicherte anzutreffen ist, finden sich bei anderen Lösungen zentralisierte Ansätze für Nutzergruppen.
  - Verschlüsselungsansatz: Es existiert eine Vielzahl von Verschlüsselungsansätzen, die an verschiedenen Stellen im Einsatz sind. Die untersuchten Matrix-basierten Kommunikationslösungen (TI-Messenger, BundesMessenger) verwenden die im Standard übliche Ende-zu-Ende-Verschlüsselung mit kurzlebigen Schlüsseln (Double Ratchet Algorithms), die in Zukunft auch durch den neuen Standard Messaging Layer Security (MLS) umgesetzt werden kann. Andere Lösungen dagegen verwenden langlebige Schlüssel, manchmal auch unter Aufbrechen der Verschlüsselung (z. B. zur Umschlüsselung) oder unter Verwendung von Proxy Reencryption, um eine Entschlüsselung durch mehrere Teilnehmende zu ermöglichen. Lösungen sehen Ende-zu-Ende-Verschlüsselung optional oder verpflichtend vor. Einige Systeme setzen keine Ende-zu-Ende-Verschlüsselung um und nutzen stattdessen separate Verschlüsselungen für jede Punkt-zu-Punkt-Verbindung sowie Verschlüsselung zur Speicherung von Daten.

- Schnittstellendesign und -technologie: Sowohl an den Versand- und Empfangsschnittstellen für den Transport als auch für die Authentifizierung kommen vielfältige Paradigmen, Kommunikationsprotokolle, Spezifikationen und Datenformate zur Anwendung. So werden an der Versand- und Empfangsschnittstelle unter anderem individuelle SOAP oder REST Services mit individuell definierten Datenserialisierungen in JSON oder XML verwendet. Mit XTA/OSCI oder der Matrix-Client-Server-API kommen auch standardisierte Schnittstellen- und Datenformate zur Anwendung. Auch der umgekehrte Weg ist anzutreffen, indem der Standard SMTP verwendet und angepasst wurde, sodass er in Teilen inkompatibel mit anderen, den Ursprungsstandard verwendenden, Lösungen wird. Die Verwendung bestimmter Protokolle wird teils in Rechtsgrundlagen festgelegt (Beispiel EGVP = OSCI). Die Vielfalt in der Ausprägung der Schnittstellen erschwert die Interoperabilität und stellt anbindende Akteure vor deutlich erhöhte Integrationsaufwände.
- Abbildung von Fähigkeiten in unterschiedlichen Architekturbausteinen: Fähigkeiten sind unterschiedlichen Architekturbausteinen zugeschlagen. Die Fähigkeit, Nachrichten dauerhaft zu speichern wird teils in der zentralen Transportinfrastruktur und über dessen Transportprotokoll realisiert. Andere Ansätze lagern diese Fähigkeit aus der Transportinfrastruktur aus und nutzen diese nur als temporären Zwischenspeicher bis zur Abholung und sorgen mit eigenen Postfachverwaltungskomponenten (teils wieder Client-Server-Architekturen) für eine dauerhafte Speicherung und Verwaltung ausgehender und eingehender Nachrichten (Beispiel EGVP/OSCI mit ERV-Sende- und Empfangskomponenten). Die Architekturentscheidung zur Verteilung von Fähigkeiten auf bestimmte Architekturbausteine hat somit auch Auswirkungen auf die Wahl der nutzbaren Interoperabilitätsstandards oder umgekehrt, die Wahl eines Interoperabilitätsstandards erfordert geeignet geschnittene Architekturbausteine.

Unterschiede liegen in konkreten Funktionalitäten: Neben zahlreichen gleich oder ähnlich gearteten Fähigkeiten, die heterogen umgesetzt sind, setzen einzelne untersuchte Lösungen auch individuelle Fähigkeiten um. Im Folgenden sollen einige beispielhaft hervorgehoben werden, da diese im Zuge einer Arbeit an einer gemeinsamen Zielarchitektur erörtert und berücksichtigt werden müssen:

- Funktionspostfach: Das OZG-PLUS-Postfach verfügt über das Funktionspostfach mit konfigurierbarer Zugriffsmöglichkeit für mehrere Personen. Eine berechtigte Rolle in der Organisation übernimmt die Verwaltung und Zugriffssteuerung.
- Adressierung / Adressbücher: Unterschiedliche Ansätze werden auch im Kontext von Adressierung und Adressbüchern verfolgt. So sind in bestimmten Lösungen keine zentralen Adressbücher vorgesehen und nötig, da zum Beispiel im Kontext OZG die Zieladresse für eine Bescheidzustellung über die Antragstellung an eine Behörde übermittelt wird und in diesem Zuge auch die Einwilligung zum elektronischen Empfang erfolgt. Bei diesem speziellen Anwendungsfall muss also weder eine Behörde durch den Antragsteller adressiert werden noch muss eine Behörde eine Adresse ermitteln, da diese bereits mit dem Antrag mitgeliefert wird. Allerdings sind damit keine initiativen oder proaktiven Anwendungsfälle möglich (keine initiative Kontaktaufnahme von Privatpersonen oder Behörden). Im Kontext des elektronischen Rechtsverkehrs hingegen existiert der SAFE-Verzeichnisdienst, der bei Nutzung des MJP durch Privatpersonen die Speicherung von Kontaktdaten und öffentlichem Zertifikat zwingend vorsieht und für öffentliche Stellen auffindbar macht. Privatpersonen werden hier automatisch mit der Anlage des Postfachs aufgenommen. Ein föderiertes Adressbuch für Privatpersonen mit zentraler Suchkomponente existiert auch bei De-Mail, hier erfolgt die Aufnahme allerdings als Opt-In.
- Zustellregeln: Zustellregeln stellen sicher, dass Nachrichten technisch und rechtlich zugestellt werden dürfen. Die Regeln und die Ansätze zur Realisierung dieser Regel sind in den Bestandslösungen heterogen umgesetzt.

Unzureichende Adressierung zukünftiger Herausforderungen: Die Föderale Digitalstrategie benennt die Herausforderungen und Rahmenbedingungen einer zukunftsweisenden digitalen Infrastruktur (Entwicklung und Eingliederung in eine Deutschland-Architektur, konzeptionelle Berücksichtigung von Security- und Privacy-by-Design, Zero-Trust-Ansatz, Resilienz, Cloud-Fähigkeit, Interoperabilität mit EU-Lösungen etc.). Dies bekräftigt die Notwendigkeit ambitionierter strategisch-architektonischer Planung durch eine gemeinsame Zielarchitektur.

Die aktuellen, teils über einen langen Zeitraum gewachsenen, Bestandslösungen sind zum jeweiligen Zeitpunkt der Konzeption mit dem Stand der Technik und den dort gültigen Rahmenbedingungen entstanden. Diese in der föderalen Digitalstrategie genannten Herausforderungen waren daher meist keine zentralen Gestaltungsziele und werden unter den Bestandslösungen daher noch nicht holistisch adressiert.

Für den Kontext der Zielarchitektur besonders relevant ist dabei der Aspekt Sicherheit. Mit den Ansätzen Zero-Trust, Security-by-Design und Privacy-by-Design geht die Notwendigkeit von E2E-Verschlüsselung und Kryptoagilität einher, um auf zukünftigen Angriffsvektoren, insbesondere hinsichtlich einer Post-Quantum-Sicherheit, reagieren zu können. Skalierbarkeit und Resilienz der Infrastruktur sowie die ebenenübergreifende Vernetzung sollen die Grundlage schaffen, um auch in Krisenfällen handlungsfähig zu bleiben. Eine Betreibbarkeit der Infrastruktur in einer Cloud zahlt ebenfalls darauf ein. Hinzu kommen zukünftig Anforderungen an die Interoperabilität mit EU-Infrastrukturen und Lösungen.

Diese und darüberhinausgehende Weiterentwicklungsbedarfe bekräftigen die Notwendigkeit der zentralen strategisch-architektonischen Planung der vorliegenden Zielarchitektur.

Glossar

Ein aktuelles Glossar findet sich auf der Plattform openCode.[6]

[6] Glossar · IT-Planungsrat / Föderales IT-Architekturboard / Zielarchitektur Postfach- und Kommunikationslösungen

Abbildungsverzeichnis

Tabellenverzeichnis

Abkürzungsverzeichnis

AfoID	Anforderungsidentifikationsnummer
AO	Abgabenordnung
API	Application Programming Interface
BDSG	Bundesdatenschutzgesetz
beA	besonderes elektronisches Anwaltspostfach
beBPo	besonderes elektronisches Behördenpostfach
beN	besonderes elektronisches Notarpostfach
beSt	besonderes elektronisches Steuerberaterpostfach
BITV	Barrierefreie-Informationstechnik-Verordnung
BSI	Bundesamt für Sicherheit in der Informationstechnik
C2C	Consumer-to-Consumer / Citizen-to-Citizen
DDOS	Distributed Denial-of-Service
DSGVO	Datenschutz-Grundverordnung
DVC	Deutsche Verwaltungscloud
E2E	Ende-zu-Ende
E2EE	End-to-End-Encryption
eBO	elektronisches Bürger- und Organisationspostfach
EGVP	Elektronisches Gerichts- und Verwaltungspostfach
eID	Elektronische Identität
eIDAS	electronic Identification, Authentication and Trust Services
ELSTER	Elektronische Steuererklärung
ERV	Elektronischer Rechtsverkehr
FIT-AM	Föderales IT-Architekturmanagement
JSON	Javascript Object Notation
KI	Künstliche Intelligenz
MJP	Mein Justizpostfach
MLS	Messaging Layer Security
NdB	Netze des Bundes
OSCI	Online Services Computer Interface
OZG	Onlinezugangsgesetz
PCS	Post-Compromise Security
PET	Privacy-Enhancing Technologies
PFS	Perfect Forward Secrecy
PKI	Public Key Infrastructure
QR	Quick Response
REST	Representational State Transfer

SAFE	Secure Access to Federated E-Justice/E-Government
SDK	Software Development Kit, Software Development Kit
SES	Sende- und Empfangssoftware
SMTP	Simple Mail Transfer Protocol
SOAP	Simple Object Access Protocol
TI	Telematikinfrastruktur
TR	Technische Richtlinie
VN	Verbindungsnetz
VwVfG	Verwaltungsverfahrensgesetz
VwZG	Verwaltungszustellungsgesetz
XML	Extensible Markup Language
XTA	XML Transport Adapter
ZBP	Zentrales Bürgerpostfach

A Konsolidierte Anforderungsliste

A.1 Einleitung

Nachfolgende Anlage enthält die konsolidierte Liste der Anforderungen an die föderale Zielarchitektur Postfach- und Kommunikationslösungen in der v 0.6 (Stand 04/2025), die in der Anforderungs- und Bestandsanalyse gewonnen wurden. Aus ursprünglich ca. 900 identifizierten Einzelanforderungen sind in einem Konsolidierungsprozess die hier aufgeführten 151 Anforderungen entstanden. Methodische Erläuterungen zu sowie wesentliche analytische Erkenntnisse aus diesem Prozess sind in diesem Dokument unter Kapitel 1 - Methodisches Vorgehen dargestellt.

Die Anforderungen werden auf Basis der Rückmeldungen aus einem öffentlichen Konsultationsprozess iterativ fortgeschrieben. Die stets aktuelle Fassung der im Rahmen des Projektes erhobenen konsolidierten Anforderungen finden sich auf der openCode-Plattform.[7]

[7] Konsolidierte-Anforderungen · IT-Planungsrat / Föderales IT-Architekturboard / Zielarchitektur Postfach- und Kommunikationslösungen

A.2 Konsolidierte Anforderungsliste Version 0.6 (Stand 04/2025)

Tabelle 4: Anforderungen der Kategorie "Übergreifend"

Kategorie	Unterkategorie	AfoID	Beschreibung
Übergreifend		ANF_FUN_ÜBE_002	[Das System] soll vollständig E2E digitalisierte Verwaltungsprozesse unterstützen.
		BED_BEN_ÜBE_008	[Das System] erlaubt eine einfache und intuitive Bedienung, um auch unregelmäßigen und nicht-IT-affinen [Nutzer:innen] eine Verwendung zu ermöglichen.
		BED_BEN_ÜBE_002	[Das System] ermöglicht eine medienbruchfreie Kommunikation.
		BED_AKZ_ÜBE_001	[Das System] ist sehr einfach nutzbar, um eine hohe Akzeptanz zu erfahren.
		BED_BAR_ÜBE_003	[Das System] ermöglicht eine barrierefreie Kommunikation.
		BED_BAR_ÜBE_007	[Das System] erfüllt die Anforderungen an die Barrierefreiheit gemäß der Barrierefreie-Informationstechnik-Verordnung (BITV 2.0).
		RAH_ÜBE_144	[Das System] ermöglicht [Privatpersonen] und [privaten Organisationen] über einen einzigen Zugang eine Kommunikation über alle Bereiche der [öffentlichen Stellen] hinweg (Allgemeine Innere Verwaltung; Schulwesen; Wissenschaft; Forschung und Kultur; Gesundheit; Sport und Erholung; Sozialwesen; Steuerverwaltung; Wirtschaftsförderung; Gesundheitswesen; Justizverwaltung; usw.).
		RAH_ÜBE_143	[Das System] ermöglicht den verschiedenen Staatsgewalten (Judikative, Exekutive, Legislative) die unabhängige Wahrnehmung ihrer verfassungsmäßigen Rolle.
		RAH_VOR_006	[Das System] erfüllt die Anforderungen des Servicestandards für die digitale Verwaltung (DIN SPEC 66336 – Qualitätsanforderungen für Onlineservices und -portale der öffentlichen Verwaltung).

Kategorie	Unterkategorie	AfoID	Beschreibung
		POR_AUS_HER_002	Die Bestandteile [des Systems] sind unter einer offenen Software-Lizenz lizenziert.
		WAR_MOD_ÜBE_001	[Das System] ist bezüglich seiner Komponenten/Dienste modular aufgebaut und lose gekoppelt.

Tabelle 5: Anforderungen der Kategorie "Use Case"

Kategorie	Unterkategorie	AfoID	Beschreibung
Use Case	**Use Case**	ANF_FUN_USE_036	[Öffentliche Stellen] können [elektronischen Schriftverkehr] in Form von [Nachrichten] mit [Nutzer:innen] und untereinander austauschen.
		ANF_FUN_USE_001	[Nutzer:innen] können mit am [Portalverbund] angeschlossenen [öffentlichen Stellen] vorgangsbezogen kommunizieren. (i.S.v. § 2 Abs. 7 OZG)
		ANF_FUN_USE_060	[Das System] ermöglicht es [Online-Diensten] und [Fachverfahren] [Nachrichten] in das [Postfach] einer [Privatperson] und/oder einer [privaten Organisation] zuzustellen.
		ANF_FUN_USE_037	[Nutzer:innen] können [Nachrichten] und deren [Anhänge] empfangen und einsehen.
		ANF_FUN_USE_066	[Das System] ermöglicht die rechtsverbindliche und vertrauliche Übermittlung von [Nachrichten] und [Anhängen].
		ANF_FUN_USE_055	[Das System] ermöglicht eine [Echtzeitkommunikation] zwischen zwei [Nutzer:innen].
		ANF_FUN_USE_063	[Das System] ermöglicht [öffentlichen Stellen] das Versenden von [Bescheiden] an [Privatpersonen], [private Organisationen] oder [öffentliche Stellen].
		ANF_FUN_USE_062	[Das System] ermöglicht [Nutzer:innen] den Empfang von [Bescheiden].
		ANF_FUN_USE_064	[Das System] ermöglicht das Beantworten von [Nachrichten].
		ANF_FUN_USE_069	[Das System] unterstützt eine bidirektionale Kommunikation, ggf. eingeschränkt durch die [Absender:in] auf unidirektional.
		ANF_FUN_USE_070	[Das System] ermöglicht der [Nutzer:in] das Anlegen, Bearbeiten und Löschen von [Nachrichten] und [Anhängen] im Posteingang.

Kategorie	Unterkategorie	AfoID	Beschreibung
		ANF_FUN_USE_071	[Das System] ermöglicht der [Nutzer:in] das Anlegen, Löschen, Sperren und die Wiederherstellung des eigenen [Postfachs].
		ANF_FUN_USE_072	[Das System] ermöglicht die Nutzung von [Funktionspostfächern].
		ANF_FUN_USE_077	[Das System] kann in einer zukünftigen Ausbaustufe zu einem eIDAS-konformen Dienst für die [Zustellung] [elektronischer Einschreiben] weiterentwickelt werden.
	Administration	ANF_FUN_USE_059	[Org-Admins] können Systemmeldungen an [Nutzer:innen] senden.
		ANF_FUN_USE_080	[Öffentliche Stellen] und [private Organisationen] können über eine Self-Service-Funktionalität eine Übersicht ihrer [Postfächer] einsehen.
	Teilnehmer:innen	ANF_FUN_USE_026	[Das System] kann von [Privatpersonen], [privaten Organisationen] und [öffentlichen Stellen] genutzt werden [= Nutzer:innen].
		ANF_FUN_USE_048	[Nachrichten] können auch mit Hilfe von [Drittanwendung] an [Nutzer:innen] übermittelt und von diesen empfangen werden.
		ANF_FUN_USE_075	[Das System] ermöglicht die Nutzung durch vertretungsberechtigte natürliche Personen.
		ANF_FUN_USE_074	[Das System] unterscheidet in den Rollen [Postfachmitglieder] und [Org-Admins] im Kontext [Funktionspostfach].
		ANF_FUN_USE_087	[Das System] ermöglicht die Nutzung durch vertretungsberechtigte juristische Personen.

Tabelle 6: Anforderungen der Kategorie "Nachricht"

Kategorie	Unterkategorie	AfoID	Beschreibung
Nachricht	**Übergreifend**	LEI_KAP_ÜBE_014	[Das System] ist aus technischer Sicht in der Lage, beliebig große [Nachrichten] und [Anhänge] zu versenden.
		ANF_FUN_NAC_183	Die [Nachricht] soll [Strukturierte Daten] übertragen können, um eine Maschinenlesbarkeit zu ermöglichen.
		ANF_FUN_NAC_185	[Das System] ermöglicht eine bidirektionale Kommunikation, die die [öffentliche Stelle] durch Einstellung zulassen/untersagen kann.
	Anhänge	ANF_FUN_NAC_118	[Nachrichten] können elektronische Dokumente als [Anhänge] enthalten.
		ANF_FUN_NAC_189	[Das System] unterstützt beliebige Dateiformate für [Anhänge], per Konfiguration können jedoch Restriktionen vorgenommen werden (Allowlist, z. B. per Mime-Type-Filter. Beispiele: PDF, CSV, XML, JSON, PNG, TXT, ICS, ICAL).
		ANF_FUN_NAC_195	Die Art einer übermittelten [Nachricht] (z. B. [Bescheid], formlose Rückfrage, etc.) kann in maschinenlesbarer Form annotiert werden, um eine optimierte Darstellung in Clients zu ermöglichen (z. B. Übersicht aller erhaltenen [Bescheide]).
	Textformat	ANF_FUN_NAC_119	[Nachrichtentext] kann fett, kursiv und unterstrichen, als Überschriften und Aufzählungen formatiert werden.
		ANF_FUN_NAC_120	[Nachrichtentext] kann Tabellen enthalten.
		ANF_FUN_NAC_191	[Nachrichtentext] kann Links enthalten, um z. B. auf [Onlinedienste] oder Widerspruchsdienste verweisen zu können.
		ANF_FUN_NAC_121	[Nachrichten] können Medien enthalten (z. B. QR-Codes, Logos).

Kategorie	Unterkategorie	AfoID	Beschreibung
		ANF_FUN_NAC_202	[Nachrichtentext] kann Emojis enthalten.
	Fachliche Metadaten	ANF_FUN_NAC_124	[Nachrichten] können mit beliebigen, elektronisch auswertbaren [fachlichen Metadaten] versehen werden.
		ANF_FUN_NAC_122	[Nachrichten] können mit einem Verfahrensreferenz (Aktenzeichen) versehen werden.
		ANF_FUN_NAC_123	[Nachrichten] können mit einer Antragsreferenz versehen werden (Antrags-ID), um antragsbezogene Kommunikation zu ermöglichen.
		ANF_FUN_NAC_193	In [Nachrichten] hinterlegte [Referenzen] und Metadaten liegen in strukturierter Form vor und sind maschinell auslesbar.
		ANF_FUN_NAC_186	Als [Fachliche Metadaten] der [Nachricht] kann der [Status der Nachricht] geführt werden, sichtbar oder abfragbar für die [Empfänger:in] und ggf. die [Absender:in].
		ANF_FUN_NAC_187	[Das System] ermöglicht die Übermittlung von (teil-)strukturierten Statusinformationen zu einem Verwaltungsverfahren ([Status der Antragsbearbeitung] sowie [Status der Antragsbearbeitung Informationen]), welche sichtbar oder abfragbar für die [Empfänger:in] und ggf. die [Absender:in] sind.
	Einbindung in Vorgänge	ANF_FUN_NAC_125	[Nachrichten] können von der [Absender:in] mit vordefinierten Antwortoptionen versehen werden, die der [Empfänger:in] beim Lesen der [Nachricht] angeboten werden.

Tabelle 7: Anforderungen der Kategorie "Identifikation"

Kategorie	Unterkategorie	AfoID	Beschreibung
Identifikation	**Übergreifend**	ANF_FUN_IDE_001	Die Rolle einer [Absender:in] ([öffentliche Stelle], [private Organisation], [Privatperson], etc.) muss an einer [Nachricht] erkennbar sein.
		ANF_FUN_IDE_047	[Das System] stellt der [Empfänger:in] einer [Nachricht] die Information bereit, ob diese von einer natürlichen Person (z.B. einer Sachbearbeitung) oder automatisiert (z. B. [Fachverfahren], KI Chatbot) verfasst wurde.
		ANF_FUN_IDE_056	[Das System] verfügt über eine Anbindung zu einem externen Identifikations- und Authentifizierungssystem.
	Identity Provider	ANF_FUN_IDE_023	Zur [Identifikation] von [Privatpersonen] werden mindestens die in § 3 OZG genannten [Identifizierungsmittel] unterstützt. Die [Identifikation] muss mindestens über das Bürgerkonto gemäß § 3 OZG ([Bund-ID] / [DeutschlandID]) erfolgen können.
		ANF_FUN_IDE_024	Zur [Identifikation] von [privaten Organisationen] werden mindestens die in § 3 OZG genannten [Identifizierungsmittel] unterstützt. Die [Identifikation] muss mindestens über das einheitliche Organisationskonto gemäß § 3 OZG erfolgen können.
		ANF_FUN_IDE_025	Die [Identifikation] über [EUDI-Wallet] mit starker kryptografischer Bindung muss perspektivisch möglich sein, sofern die organisatorischen und technischen Voraussetzungen hierzu geschaffen sind (vgl. eIDAS-Credential mit Anonymous Credentials, Zero Knowledge Proofs, Deniability, selbstverwaltete kryptografische Identität).
		ANF_FUN_IDE_050	Zur [Identifikation] von [öffentlichen Stellen] werden mindestens die in § 3 OZG genannten [Identifizierungsmittel] unterstützt. Die [Identifikation] muss mindestens über das einheitliche Organisationskonto gemäß § 3 OZG erfolgen können.
	Authentisierungsmittel	ANF_FUN_IDE_034	[Das System] sollte in der Lage sein, zukünftig ggf. auch weitere vom BSI festgelegte [Authentisierungsmittel] zu unterstützen, wenn der initiale [Nachweis] der [Identität] natürlicher Personen maximal auf Vertrauensniveau "substantiell" erbracht wurde. (vgl. § 12 Abs. 5 OZG)

Kategorie	Unterkategorie	AfoID	Beschreibung
		ANF_FUN_IDE_044	[Das System] unterstützt die Integration bestehender europäischer Identitätslösungen ([Identitäten] nach eIDAS 1.0).
	Authentifizierungs- und Autorisierungsprotokolle	ANF_FUN_IDE_027	[Das System] verwendet offene Standardprotokolle zur [Authentifizierung] und [Autorisierung] der [Nutzer:innen].

Tabelle 8: Anforderungen der Kategorie "Adressierung"

Kategorie	Unterkategorie	AfoID	Beschreibung
Adressierung	**Adressierungsansatz**	ANF_FUN_ADR_065	[Öffentliche Stellen] können zur Adressierung [private Organisationen] (bzw. deren jeweilige Organisationseinheiten) aus einem [Adressbuch] auswählen.
		ANF_FUN_ADR_059	[Öffentliche Stellen] können zur Adressierung andere [öffentliche Stellen] (bzw. deren jeweilige Organisationseinheiten) aus einem [Adressbuch] auswählen.
		ANF_FUN_ADR_060	In einer zukünftigen Ausbaustufe können [Privatpersonen] Servicecenter (z. B. 115) aus einem Verzeichnis auswählen und leichtgewichtig per Chat über [das System] kontaktieren.
		ANF_FUN_ADR_020	[Öffentliche Stellen] können [Nachrichten] an eine [Privatperson] übermitteln, sofern diese zuvor durch Inanspruchnahme einer elektronischen Verwaltungsleistung (vgl. § 9 Abs. 1 S. 2 OZG) oder Einwilligung einen Identifier für ihr [Postfach] an die [öffentliche Stelle] übermittelt hat.
		ANF_FUN_ADR_021	[Nutzer:innen] können Nachrichten initiativ an [Nutzer:innen] übermitteln. (i. S. v. "Neue Nachricht"-Button)
		ANF_FUN_ADR_024	[Das System] nutzt keine global eindeutigen Identifikatoren, die sich direkt oder indirekt auf [natürliche Personen] beziehen.
		ANF_FUN_ADR_039	[Privatpersonen] können nur nach vorheriger Einwilligung über [das System] kontaktiert werden; ein Widerruf der Einwilligung ist jederzeit möglich.
		ANF_FUN_ADR_058	[Öffentliche Stellen] können festlegen, ob Antworten auf gesendete [Nachrichten] möglich sind oder nicht.
		ANF_FUN_ADR_061	[Private Organisationen] und [öffentliche Stellen] können nach vorheriger Registrierung ohne erforderliche Einwilligung über [das System] kontaktiert werden.

Kategorie	Unterkategorie	AfoID	Beschreibung
		ANF_FUN_ADR_085	Das System ermöglicht eine pseudonyme Nutzung durch [Privatpersonen] mit eingeschränkten Funktionalitäten (abhängig vom Vertrauensniveau).
	Funktionspostfach	ANF_FUN_ADR_026	[Nachrichten], die an [öffentliche Stellen] und [private Organisationen] versendet wurden, können von ein oder mehreren natürlichen Personen in der Rolle [Postfachmitglied] anhand von vorher durch [Org-Admins] definierten Zugriffsberechtigungen auf das jeweilige [Postfach] eingesehen werden ("[Funktionspostfach]-Funktionalität").
		ANF_FUN_ADR_062	[Org-Admins] [Öffentlicher Stellen] und [private Organisationen] können einzelnen natürlichen Personen Zugriff auf [Postfächer] erteilen und auch wieder entziehen.
		ANF_FUN_ADR_063	Bei Erteilung von Zugriffen auf [Postfächer] von [öffentlichen Stellen] und [privaten Organisationen] ist die gesamte Kommunikationshistorie für die neu berechtigten [Nutzer:innen] einsehbar.
		ANF_FUN_ADR_071	[Org-Admins] können Zugriffe auf [Postfächer] bei Bedarf auf Basis einer gruppenbasierten Rechteverwaltung managen (z. B. Zuweisung einer Berechtigung an eine zuvor definierte Gruppe von Personen).
		ANF_FUN_ADR_070	Von [Org-Admins] durchgeführte administrative Änderungen werden revisionssicher protokolliert.
	Stellvertretung	ANF_FUN_ADR_025	[Das System] muss Vertretungsregelungen und Vollmachten unterstützen.

Tabelle 9: Anforderungen der Kategorie "Transport"

Kategorie	Unterkategorie	AfoID	Beschreibung
Transport	**Übergreifend**	ANF_FUN_TRA_006	[Das System] muss von [Nutzer:innen] über das Internet und aus Behördennetzen (insb. NdB,VN) ohne unsachgemäße Schwächung von Sicherheitsmaßnahmen erreichbar sein.
	Routing	ANF_FUN_TRA_017	Das System transportiert [Nachrichten] über das Internet.
	Durchgesetzte Complianceregeln	ANF_FUN_TRA_007	[Das System] erlaubt/unterbindet den Versand von [Nachrichten] anhand von konfigurierbaren, rollenbasierten Rechten, z. B. Unterbindung der C2C-Kommunikation.

Tabelle 10: Anforderungen der Kategorie "Speicherung"

Kategorie	Unterkategorie	AfoID	Beschreibung
Speicherung	**Speicherdauer**	ANF_FUN_SPE_031	[Das System] speichert [Nachrichten] zuverlässig und dauerhaft, sofern [Nutzer:innen] keine Löschung der Daten angestoßen haben oder Löscherfordernisse gemäß gesetzlicher Löschfristen bestehen.
		ANF_FUN_SPE_012	[Das System] unterstützt [öffentliche Stellen] bei der Umsetzung von gesetzlichen Löschfristen oder anderen gesetzlichen Löscherfordernissen (bspw. Zeugenschutzprogramme, Rechte gemäß DSGVO) durch eine Funktionalität zur automatischen und/oder manuellen Löschung.
	Speicherung von Nachrichten	ANF_FUN_SPE_038	[Das System] ermöglicht das Speichern ein- und ausgehender [Nachrichten].
		ANF_FUN_SPE_042	[Das System] ermöglicht das Speichern eines Entwurfs einer [Nachricht].

Tabelle 11: Anforderungen der Kategorie "Zustellung"

Kategorie	Unterkategorie	AfoID	Beschreibung
Zustellung	**Übergreifend**	ANF_FUN_ZUS_044	[Das System] unterstützt sowohl die rechtssichere Zustellung/Bekanntgabe von [Verwaltungsakten] oder [Entscheidungen(juristisch)] (z. B. unter Verwendung von [qualifizierten elektronischen Signaturen]/[qualifizierten elektronischen Siegeln]/Zeitstempeln), als auch Kommunikation ohne solche Anforderungen hinsichtlich der Beweisbarkeit der erfolgten Übermittlung und [Authentizität] gegenüber Dritten.
	Empfangsbenachrichtigung	ANF_FUN_ZUS_026	Die [Empfänger:in] einer [Nachricht] kann sich über dritte Wege ([Eingangsbenachrichtigung Empfänger:in]) informieren lassen, wenn eine neue [Nachricht] in ihrem [Postfach] eingegangen ist (E-Mail oder mobiler Push-Notification (App-basiert)).
	Nichtabstreitbarkeit	ANF_FUN_ZUS_020	[Das System] protokolliert den (rechtlich relevanten) Zeitpunkt der Übermittlung einer [Nachricht] und macht diesen den [Absender:innen] und den [Empfänger:innen] bekannt.
		SIC_NAC_NIC_004	[Das System] ermöglicht bei Bedarf eine rechtssichere und zuverlässige Zustellung von [Nachrichten] an [öffentliche Stellen], die von keinem Kommunikationspartner abgestritten werden kann.
	(Lese-)Bestätigungen	ANF_FUN_ZUS_022	[Das System] übermittelt [Absender:in] und [Empfänger:in] automatisch eine [Bereitstellungsbestätigung] im Falle eines erfolgreichen Versands einer [Nachricht] an eine [Empfänger:in].
		ANF_FUN_ZUS_046	[Das System] übermittelt [Absender:in] und [Empfänger:in] eine [Abrufbestätigung] im Falle eines erfolgreichen Abrufs einer [Nachricht] aus dem [Postfach] durch die [Empfänger:in].
	Zustellfiktion	ANF_FUN_ZUS_024	[Das System] erfüllt die gesetzlich definierten Anforderungen zur rechtsicheren Realisierung einer [Bekanntgabe-] bzw. [Zustellfiktion] bei der elektronischen Übermittlung von [Verwaltungsakten]. (vgl. § 122 AO, § 5 VwZG, § 9 OZG, § 41 VwVfG)

Kategorie	Unterkategorie	AfoID	Beschreibung
	Zustellgarantie	ANF_FUN_ZUS_023	[Das System] stellt sicher, dass [Nachrichten] auch bei gescheiterten Übermittlungsversuchen nicht verloren gehen.

Tabelle 12: Anforderungen der Kategorie "Sicherheit"

Kategorie	Unterkategorie	AfoID	Beschreibung
Sicherheit	**Übergreifend**	SIC_ÜBE_ÜBE_015	[Das System] setzt den Security by Design Ansatz um.
		SIC_ÜBE_ÜBE_018	[Das System] setzt den Zero Trust Ansatz um.
		SIC_AUT_ÜBE_014	Die [Integrität] und Ende-zu-Ende-Authentizität der übermittelten [Nachrichten] wird auf kryptographischer Ebene unter Wahrung glaubwürdiger Abstreitbarkeit (plausible deniability) realisiert, um im Falle von Kompromittierungen keine Echtheit einzelner übermittelter Informationen belegen zu können und so Individuen vor Stigmatisierung und Diskriminierung zu schützen.
		SIC_VER_ÜBE_058	[Das System] unterstützt eine Wiederherstellung des Zugangs nach Geräteverlust oder Verlust von Authentisierungsfaktoren (Passwörtern).
	Schutzbedarf	SIC_ÜBE_ÜBE_005	Die technische Realisierung [des Systems] berücksichtigt mindestens die Anforderungen des BSI-Grundschutz auf dem Schutzbedarf "hoch".
	Vertrauensniveau	SIC_ÜBE_ÜBE_006	[Nutzer:innen] können bis zum Vertrauensniveau "hoch" (gemäß BSI TR-03107-1) authentifiziert werden.
		SIC_ÜBE_ÜBE_007	[Das System] erlaubt Zugriff auf [Nachrichten] durch die [Empfänger:in] nur, wenn die [Empfänger:in] mit dem von der [Absender:in] für diese [Nachricht] definierten Vertrauensniveau authentifiziert wurde.
		SIC_ÜBE_ÜBE_008	Die [Empfänger:in] einer [Nachricht] kann nachvollziehen, auf welchem Vertrauensniveau die [Absender:in] authentifiziert wurde.
		SIC_VER_ÜBE_048	Nachrichtenkommunikation kann auf unterschiedlichen Vertrauensniveaus erfolgen wofür entsprechend zugelassene [Authentisierungsmittel] zu verwenden sind.

Kategorie	Unterkategorie	AfoID	Beschreibung
	Authentizität	SIC_AUT_ÜBE_007	[Das System] stellt die Authentizität einer [Nachricht] auf dem Vertrauensniveau sicher, auf dem die [Absender:in] authentifiziert wurde.
		SIC_AUT_ÜBE_008	[Nutzer:innen] können beim Senden einer [Nachricht] die [Empfänger:in] und beim Empfangen einer [Nachricht] die [Absender:in] klar, menschenlesbar und eindeutig identifizieren.
		SIC_AUT_ÜBE_013	[Das System] ermöglicht die [qualifizierte elektronische Signatur] oder [qualifiziertes elektronisches Siegeln] von [Nachrichten].
	Integrität	SIC_INT_ÜBE_003	[Das System] stellt die [Integrität] der übermittelten [Nachrichten] sicher.
	Verschlüsselung bei Übermittlung	SIC_VER_ÜBE_026	[Das System] stellt eine Ende-zu-Ende-Verschlüsselung der übermittelten [Nachrichten] (inklusive [Anhängen] und [Vertraulichen Metadaten]) sicher.
		SIC_VER_ÜBE_029	Das eingesetzte Verschlüsselungsverfahren unterstützt moderne kryptographische Eigenschaften wie Perfect Forward Secrecy (PFS), Post-Compromise Security (PCS, auch: Future Secrecy) und Plausible Deniability.
		SIC_VER_ÜBE_032	Die Verschlüsselung übermittelter und gespeicherter [Nachrichten] kann weder von der Betreiberin [des Systems], noch von Dritten gebrochen, umgangen oder entschlüsselt werden.
		SIC_VER_ÜBE_055	[Das System] verwendet – zusätzlich zur Inhaltsdatenverschlüsselung (E2EE) – flächendeckende Transportverschlüsselung.
	Nachrichtenverschlüsselung	SIC_VER_ÜBE_027	[Nachrichten] werden ausschließlich in verschlüsselter Form gespeichert.
		SIC_VER_ÜBE_028	Das für die E2E-Verschlüsselung genutzte private Schlüsselmaterial darf nur der [Absender:in] bzw. der [Empfänger:in] zugänglich sein (kein Zugriff durch Dritte Parteien).

Kategorie	Unterkategorie	AfoID	Beschreibung
		SIC_VER_ÜBE_031	[Das System] setzt Crypto-Agilität um, um beim Bekanntwerden von Schwächen in eingesetzten Verschlüsselungsverfahren auf neue [Verfahren] wechseln zu können und um in der Zukunft Post-Quantum-Kryptographie zu realisieren.
		SIC_VER_ÜBE_051	Alle Metadaten, die nicht zwingend für die korrekte Zustellung einer [Nachricht] erforderlich sind, werden vermieden, als Teil der übermittelten [Nachricht] als [vertrauliche Metadaten] verschlüsselt oder durch Privatsphäre-schützende Technologien (Privacy-Enhancing Technologies, PET) verschleiert.
	Malware Prüfung	SIC_ÜBE_MAL_005	[Das System] unterstützt die [Nutzer:innen] bei der Realisierung einer Prüfung von [Nachrichten] auf Schadinhalte nach dem Empfang von [Nachrichten] (z. B. durch Unterstützung in SDKs).
	Vertraulichkeit	SIC_VER_ÜBE_056	Um eine rechtswirksame Zustellung zu gewährleisten und die Vertraulichkeit bei der Zustellung zu wahren, dürfen [Nachrichten] nur die richtige [Empfänger:in] erreichen.
	Nachweisbarkeit	SIC_NAC_NAC_005	Von [Org-Admins] durchgeführte Änderungen werden revisionssicher protokolliert.
	Datenschutz	DAT_ÜBE_ÜBE_021	[Das System] setzt den Privacy by Design Ansatz um.
		ZUV_WIE_ÜBE_003	Es wird gewährleistet, dass eingesetzte IT-Systeme im Störungsfall wiederhergestellt werden können (Wiederherstellbarkeit). (§ 64 Abs. 3 Nr. 9 BDSG)
		SIC_ÜBE_ÜBE_017	[Das System] stellt sicher, dass sensible Informationen, wie z. B. Namen und Inhalte einer [Nachricht] nicht in für Dritte zugänglicher Form (unverschlüsselt) über Push Server (von Google und Apple) übertragen werden.
		DAT_ÜBE_ÜBE_020	[Das System] unterstützt [Privatpersonen] bei der aufwandsarmen und zeitnahen Realisierung von Auskunftsbegehren durch technische Maßnahmen. (Art. 15 DSGVO)
		DAT_ÜBE_ÜBE_022	[Das System] implementiert angemessene technische und organisatorische Maßnahmen zum Schutz personenbezogener Daten. (Art. 31 Abs. 1 DSGVO)

Tabelle 13: Anforderungen der Kategorie "Anbindung"

Kategorie	Unterkategorie	AfoID	Beschreibung
Anbindung	**Übergreifend**	ANF_ARC_ANB_019	Für alle Bausteine der Gesamtinfrastruktur steht mindestens eine unter freier Softwarelizenz lizenzierte Referenzimplementierung bereit, die nach hohen Sicherheits-, Usability- und Barrierefreiheits-Standards entwickelt wurden.
	Schnittstellen	ANF_ARC_ANB_006	Die Funktionalitäten [des Systems] stehen den [Nutzer:innen] ohne Funktionseinschränkungen über Schnittstellen zur Verfügung (Umsetzung des API-First Ansatz).
		ANF_ARC_ANB_008	Die Anbindung an [das System] muss so einfach sein, dass eine große Zahl an [Nutzer:innen] aufwandsarm an [das System] angebunden werden kann.
		ANF_ARC_ANB_007	Alle Schnittstellen [des Systems] basieren auf offenen Standards.
		ANF_ARC_ANB_021	Alle Schnittstellen [des Systems] sind ohne die Notwendigkeit des Einsatzes von proprietären Komponenten ansprechbar.
	API-Dokumentation	ANF_ARC_ANB_009	Alle Schnittstellen [des Systems] sind strukturiert, vollständig und öffentlich einsehbar dokumentiert.
	Software Development Kit	ANF_ARC_ANB_018	[Das System] unterstützt die einfache Anbindung durch Bereitstellung von Software Development Kits (SDKs).

Tabelle 14: Anforderungen der Kategorie "Architektur"

Kategorie	Unterkategorie	AfoID	Beschreibung
Architektur	**Übergreifend**	ANF_ARC_ARC_048	Zur Evaluierung und Erfolgsmessung stellt [das System] anonymisierte Daten zu erfolgten Anbindungen, Anzahl der Nutzenden, Anzahl der übermittelten [Nachrichten], Anzahl und Größe von [Anhängen], etc. als Open Data über das Verwaltungsdatenportal GovData bereit.
		ANF_ARC_ARC_050	Das Management von kryptografischen Schlüsseln ist für [Nutzer:innen] einfach.
		BED_ABS_ÜBE_003	[Das System] gibt im Fehlerfall zuverlässig verständliche und aussagekräftige Fehlermeldungen aus.
		KOM_INT_STA_003	[Das System] unterstützt den Zeichensatz gem. DIN 91379 vollständig.
		LEI_ZEI_ÜBE_002	Das Antwortverhalten [des Systems] ermöglicht eine Echtzeit-Kommunikation (vergleichbar mit den Reaktionszeiten privater oder nicht-kommerzieller Messenger-Dienste).
		RAH_ÜBE_007	[Das System] soll ohne Bindung an einen Mobilfunkvertrag nutzbar sein, d. h. eine Telefonnummer ist zur Registrierung und Nutzung [des Systems] nicht nötig.
		ZUV_VER_ÜBE_002	[Das System] ist auf Hochverfügbarkeit (99,9XX %) ausgelegt.
		ZUV_ÜBE_RES_002	[Das System] muss organisatorisch und technisch resilient ausgelegt sein, um auch in Krisenfällen einen Nachrichtenaustausch sicherstellen zu können.
		LEI_KAP_ÜBE_012	[Das System] muss skalierbar sein und sich dynamisch an Lasten anpassen (Skalierbarkeit & Elastizität).
		ZUV_VER_ÜBE_006	[Das System] verfügt über ein robustes Backend, das auch im Internet DDOS Angriffen standhält.

Kategorie	Unterkategorie	AfoID	Beschreibung
	Client-Bausteine	ANF_ARC_ARC_016	[Privatpersonen] können [das System] einfach und komfortabel per mobiler App oder über einen responsiven webbasierten Zugang nutzen.
		ANF_ARC_ARC_051	Der Zugriff auf [Nachrichten] kann über mehrere Geräte erfolgen, welche dieselbe Sicht auf die Kommunikationsinhalte bieten.
	Administration	LEI_KAP_ÜBE_011	[Das System] ist in der Lage, die maximale Größe von [Nachrichten] und [Anhängen] per Konfigurationsoption einzuschränken.
	Betrieb	ANF_ARC_ARC_018	[Das System] ist geeignet, um in der Deutschen Verwaltungscloud (DVC) betrieben zu werden.

Tabelle 15: Anforderungen der Kategorie "Postfachzugang für Bürger:innen"

Kategorie	Unterkategorie	AfoID	Beschreibung
Postfachzugang für Bürger:innen	**Übergreifend**	ANF_FUN_CLB_032	[Das System] macht eingehende und ausgehende [Nachrichten] im [Postfach] kenntlich.
		ANF_FUN_CLB_031	[Das System] macht neu empfangene und nicht gelesene [Nachrichten] im [Postfach] kenntlich.
		ANF_FUN_CLB_013	[Nutzer:innen] müssen die Möglichkeit besitzen, [Nachrichten] [im System] zu strukturieren und zu ordnen.
		ANF_FUN_CLB_029	[Das System] ermöglicht die manuelle sowie automatisierte Sortierung und Filterung von [Nachrichten] in bestimmte Kategorien/Ordnern, welche individuell durch die [Nutzer:in] definiert werden können.
		ANF_FUN_CLB_033	[Das System] ermöglicht die Sortierung von [Nachrichten] nach verschiedenen Merkmalen (z. B. Betreff, Absendezeitpunkt, [Absender:in], [Anhänge], Vorgang).
		ANF_FUN_CLB_030	[Das System] ermöglicht das Durchsuchen von [Nachrichten] innerhalb des [Postfachs].
		ANF_FUN_CLB_012	[Das System] muss in verschiedenen Sprachen, mindestens jedoch in Deutsch und Englisch, nutzbar sein.
		ANF_FUN_CLB_026	[Das System] unterstützt die lokale Speicherung, das Herunterladen und den Export von [Nachrichten] und [Anhängen] (vgl. Art. 15 DSGVO).
		ANF_FUN_CLB_034	[Nutzer:innen] können Login-Versuche auf [das System] überprüfen und sich aus anderen Sitzungen aus der Ferne abmelden.
		ANF_FUN_CLB_011	[Nutzer:innen] müssen sich aus [dem System] ausloggen können.