Neukonzeption und Neuentwicklung OSiP – NEOSiP

Anforderungserhebung und Architekturkonzeption

Konzept

Version: 01.00

Titel	Dokumentenart	Inhalt
Konzept	Klammerdokument	Übergreifende Zusammenfassung des Vorhabens.
01 Executive Summary	Begleitdokument	Zusammenfassung der Problemstellung, Zielsetzung und der vorgeschlagenen Lösung.
02 Anforderungsliste	Begleitdokument	Detaillierte Beschreibung der für die Neuentwicklung aufgenommenen Anforderungen und deren Quellen.
03 Architekturentscheidungen	Begleitdokument	Detaillierte Abwägung aller signifikanten Architekturentscheidungen.
04 Glossar	Begleitdokument	Übersicht über die zentralen Begriffe.

Nutzungsbedingungen

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

Kontaktinformationen

Produktmanagement (osip@fitko.de)

- David Brodesser (david.brodesser@fitko.de)
- Dr. Daniel Biedermann (daniel.biedermann@fitko.de)

Architekturmanagement

- Dr. George-Petru Ciordas-Hertel (george.ciordas@fitko.de)

Inhaltsverzeichnis

1 Einleitung

Dieses Konzeptpapier wird auf Grundlage des Beschlusses 2025/20 des IT-Planungsrats zur Neukonzeption, Neuentwicklung und zum Rollout der Online-Sicherheitsprüfung (OSiP) vorgelegt. Der IT-Planungsrat hat die Föderale IT-Kooperation (FITKO) beauftragt, unter Einbeziehung relevanter Fachbehörden und Erkenntnisstellen eine übergreifende Architektur für OSiP zu erarbeiten. Maßgebliche Leitlinien sind die im Beschluss benannten Ziele: Eine medienbruchfreie und Ende-zu-Ende-verschlüsselte Lösung zu entwickeln, die die Prinzipien Secure- und Data-Protection-by-Design berücksichtigt und einen Zero-Trust-Ansatz verfolgt. Außerdem die Komplexität des Betriebs zu reduzieren, die Robustheit, Effizienz und Skalierbarkeit des Produkts zu steigern sowie die Homogenisierung von Schnittstellen für die unmittelbare Anbindung, Authentifizierung und Adressierung von Fachverfahren und Behördensystemen zu erreichen.

Das Dokument erfasst die Ergebnisse der Projektphase „Anforderungserhebung und Architekturkonzeption" und legt das konzeptionelle Zielbild der Architektur einschließlich zentraler Architekturentscheidungen sowie die konsolidierten Anforderungen vor. Diese Inhalte bilden die fachlich-architektonischen Leitplanken, auf deren Basis die Umsetzung erfolgen soll. Detaillierte Planungen zu Umsetzung, Transition, Migration und Rollout werden in folgenden Projektphasen erarbeitet.

Folgend werden der Projektkontext, das Vorgehen für die abgeschlossene Projektphase, die Ergebnisse der Anforderungserhebung und Bestandsanalyse, sowie relevante Architekturentscheidungen und die Zielarchitektur aufgezeigt.

1.1 Projektkontext

Die OSiP ist ein Produkt des IT-Planungsrats zur digitalen Durchführung von ZSÜ in sicherheitskritischen Bereichen wie zum Beispiel Luft- und Hafensicherheit, Waffenrecht, Einbürgerung oder Aufenthaltsrecht. Diese Überprüfungen sind gesetzlich vorgeschrieben und erfordern die Zusammenarbeit zahlreicher Akteure wie Antragstellende (Bürger:innen, Unternehmen), Genehmigungsbehörden (GB), EKS und Registern.

OSiP wurde ursprünglich als Anwendung des IT-Planungsrats eingeführt[1] und mit dem 1. Januar 2022 als Produkt in das Portfolio der FITKO überführt. Die Übernahme durch die FITKO erfolgte, um den Betrieb und die Weiterentwicklung zentral zu steuern und die föderale Nutzung zu erleichtern. Perspektivisch soll OSiP in allen Bundesländern zum Einsatz kommen. Die strategische Bedeutung des Produkts für die öffentliche Sicherheit ist hoch, da es die

[1] vgl. Beschluss 2017/12 - Online-Sicherheitsüberprüfung (OSiP) als Anwendung des IT-Planungsrats | IT-Planungsrat

rechtskonforme und manipulationssichere Durchführung gesetzlich vorgeschriebener ZSÜ gewährleistet, den föderalen Datenaustausch zwischen Behörden und EKS absichert und damit unmittelbar zur Prävention sicherheitsrelevanter Risiken beiträgt. Vor allem im Kontext geopolitischer Entwicklungen und einer volatilen Sicherheitslage in Deutschland wird es in Zukunft noch wichtiger sein, Sicherheitsüberprüfungen schnell, sicher und effizient abwickeln zu können.

1.2 Begründung der Neukonzeption

Im Jahr 2024 wurde OSiP einer umfassenden Prüfung unterzogen, einschließlich eines Architektur-Reviews und begleitender Sicherheitsanalysen. Die Ergebnisse wurden in der 45. Sitzung des IT-Planungsrats (13.11.2024, Berlin) vorgestellt und zeigen, dass die bestehende Architektur die aktuellen und künftigen Anforderungen an Sicherheit, Skalierbarkeit, Wartbarkeit und Betrieb nicht erfüllt.[2]
Die Analyse zeigte drei zentrale Problemfelder auf:

- **Technische Schulden:** Veraltete Bibliotheken, fehlende, großflächige Refactorings und komplexe Prozess- sowie Schnittstellenflüsse mit Mischbetrieb alter und neuer Schnittstellengenerationen.
- **Sicherheitsarchitektur und Betrieb:** Wiederholte, kritische Findings in Security-Audits, fehlende Betriebs-, IT-Sicherheits- und Datenschutzkonzepte sowie hohe Risiken aufgrund einer veralteten Sicherheitsarchitektur und hohe Zusatzaufwände bei Lastspitzen (z. B. UEFA EURO 2024).
- **Föderaler Nutzungskontext:** Unvollständige Umsetzung von Vorgaben (z. B. Multibundeslandfähigkeit, Standardanbindung) bei gleichzeitig wachsendem Bedarf an zentral bereitgestellten Instanzen.

Diese Befunde zeigen deutlich, dass eine inkrementelle Weiterentwicklung weder wirtschaftlich noch sicherheitstechnisch vertretbar ist.

1.3 Vision, strategische Ziele und Leitprinzipien

Die Vision beschreibt die langfristige Ausrichtung des Produkts. Die strategischen Ziele konkretisieren die Erwartungen an das neue System und die Leitprinzipien geben verbindliche Vorgaben für die Umsetzung, welche in der Konzeptionsphase bereits berücksichtigt werden müssen.

[2] vgl. IT-Planungsrat | Steckbrief TOP 22; Beschluss 2024/52 – Neukonzeption OSiP

Vision

Das Produkt verfolgt die Vision einer zukunftsfähigen, sicheren und skalierbaren ZSÜ, die eine medienbruchfreie und rechtskonforme Abwicklung im föderalen Kontext ermöglicht. Diese Vision ist in den Beschlüssen des IT-Planungsrats verankert und dient als Orientierung für alle weiteren konzeptionellen und technischen Entscheidungen.[3]

Strategische Ziele

Die strategischen Ziele wurden aufgrund der Beschlusslage des IT-Planungsrats festgelegt[4] und orientieren sich an standardisierten Qualitätsmerkmalen[5]. Die Ziele sind gemäß ihrer Priorität aufgeführt:

- **Sicherheit:** Sehr hohe Sicherheitsstandards aufgrund min. hohem Schutzbedarf. Umsetzung u.a. durch Zero-Trust-Ansatz, Secure-by-Design, Data Protection-by-Design und Ende-zu-Ende-Verschlüsselung (E2EE) entlang aller relevanten Prozessketten.
- **Funktionale Eignung:** Korrekte und konsistente Abdeckung aller Anwendungsfälle der Zuverlässigkeits- und Sicherheitsprüfung. Umsetzung u.a. durch homogenisierte Schnittstellen, einheitliche Prozesse und konsistente Datenmodelle zur Abbildung einer medienbruchfreien Lösung.
- **Zuverlässigkeit:** Hohe Robustheit des Systems, um die Kontinuität der abgebildeten sicherheitskritischen Prozesse dauerhaft und kontinuierlich zu gewährleisten.
- **Wartbarkeit:** Niedrige Komplexität der Betriebs- und IT-Architektur, um u.a. schnelle Anpassungen aufgrund von Gesetzesänderungen und simple Weiterentwicklungen aufgrund von neue AWBs zu ermöglichen.
- **Leistungseffizienz:** Skalierbare und responsive IT-Architektur, um die wachsende Nutzung im föderalen Kontext zuverlässig unterstützen zu können. Umsetzung durch u.a. eine einheitliche und unmittelbare Anbindung von Fachverfahren und Behördensystemen.

1.4 Rahmenbedingungen

Die Rahmenbedingungen werden primär durch den Einsatz im behördenübergreifenden Informationsaustausch und die damit verbundenen strengen rechtlichen Vorgaben bestimmt.

---

[3] vgl. Beschluss 2025/20 - Neukonzeption OSiP | IT-Planungsrat
[4] vgl. Beschluss 2025/20 - Neukonzeption OSiP | IT-Planungsrat; IT-Planungsrat | Steckbrief TOP 22
[5] ISO/IEC 25010

Die vollständigen Quellen für die rechtlichen und technischen Rahmenbedingungen sowie die spezifisch daraus extrahierten Anforderungen sind im Begleitdokument 2 „Anforderungsliste“ aufgeführt.

Es gilt insbesondere die Einhaltung der DSGVO sowie die Datenschutzgesetze der Länder. Gemäß der FITKO-Leitlinie erfolgt die Umsetzung des Weiteren nach IT-Grundschutz (Standards 200-1 bis 200-3). Perspektivisch wird zudem eine Eignung zur Verarbeitung von Verschlusssachen (VS) gemäß Verschlusssachenanweisung (VSA) angestrebt. Nach dem IT-NetzG ist der Anschluss an das Verbindungsnetz von Bund und Ländern verpflichtend. Die Zielarchitektur muss dementsprechend technisch und organisatorisch so konzipiert sein, dass alle Komponenten in dieser Kommunikationsinfrastruktur betrieben werden können und die Sicherheitsvorgaben des Bundes erfüllen.

2 Vorgehensweise und Methodik

2.1 Bestandsanalyse und Stakeholderbeteiligung

Als zentraler Bestandteil der Vorgehensweise und Methodik wurden sowohl die systematische Bestandsanalyse als auch die umfassende Stakeholderbeteiligung eng miteinander verzahnt. Das Vorgehen folgte dem Grundsatz, das bestehende OSiP-System sowie seine fachlichen, technischen und organisatorischen Rahmenbedingungen ganzheitlich zu verstehen, bevor darauf aufbauend Anforderungen erhoben und ein Zielbild für NEOSiP entwickelt wurden.

2.1.1 Bestandsanalyse

Die technische Bestandsaufnahme basierte auf einer Analyse von Handbüchern, Netzplänen, Schnittstellendokumenten und dem IT-Service-Katalog. Zur Validierung der Schichtenmodelle und Kommunikationswege wurden Expert:inneninterviews durchgeführt. Dies ermöglichte die Rekonstruktion der Systemstruktur sowie die Identifikation von Abhängigkeiten und Datenflüssen in ersten Architekturdiagrammen. Zusätzlich wurde das Backlog des Bestandssystems gesichtet und Anforderungen aus diesem, in Absprache mit dem Produktmanagement, übernommen.

Das fachliche Verständnis wurde durch die Auswertung von Prozessdokumentationen, Use-Cases und Mockups erarbeitet. Um die bestehende Nutzerführung und Navigationslogik realitätsnah zu erfassen, ergänzte eine systembasierte Analyse der Oberflächen (inkl. Systemdemonstrationen) die theoretische Sichtung.

Expert:innenaustausch

Um die Einblicke aus dem vorherigen Schritt zu validieren und zu ergänzen, fanden Interviews zum Austausch mit ausgewählten Expert:innen und Wissensträger:innen statt. Dies umfasste den Austausch mit Ansprechpartner:innen, die langjährige Erfahrung im Produktmanagement

des Bestandssystem OSiP haben, sowie Personen die Verantwortung im Kontext Betrieb und Support tragen. Alle erhobenen Informationen wurden in einer zentralen Projektablage dokumentiert und können damit auch in zukünftigen Projektphasen als Referenzen herangezogen werden.

Auf Basis der in der Bestandsanalyse erhobenen Informationen wurden gezielt Fragestellungen für die Interviews und das Konzept für die Fachworkshops zur anschließenden Anforderungserhebung abgeleitet.

2.1.2 Stakeholderbeteiligung

Die Stakeholderbeteiligung war zentral für die Anforderungserhebung und Architekturkonzeption von NEOSiP. Über eine strukturierte Abfrage wurden bundesweit 58 Personen und 39 Funktionsadressen kontaktiert, um aktuelle Bedarfe sowie zukünftige Nutzungsperspektiven (auch von Nicht-OSiP-Nutzern) zu erfassen. Die methodische Umsetzung erfolgte durch Interviews, Workshops und Fragebögen, deren Ergebnisse kontinuierlich an den Lenkungsausschuss und das Produktboard gespiegelt wurden.

Genehmigungsbehörden (GB)

Als fachliche Hauptakteure wurden Behörden aus 10 Bundesländern sowie Bundesstellen einbezogen (16 Interviews, 6 Workshops). Die Beteiligung deckte fast alle Anwendungsbereiche (u. a. Luftsicherheit, Waffenrecht, ZSÜ) ab; lediglich für den Bereich Aufenthalt konnten keine Teilnehmer gewonnen werden.

Erkenntnisstellen (EKS)

LKAs aus 9 Bundesländern sowie BKA, ZKA und BAMAD lieferten Input zu Schnittstellen und Sicherheit. Aufgrund des sicherheitssensiblen Kontexts waren Auskünfte teils eingeschränkt (7 Interviews, 1 Workshop, 3 Fragebögen); eine Nachverifizierung wird empfohlen (Handlungsbedarf 5.14).

Fachverfahrenshersteller

Vier Hersteller (Condition, nextgov iT, HZD, cib Software) wurden primär über Interviews eingebunden, um ein gemeinsames Verständnis für Schnittstellen und Best Practices zu entwickeln.

Expert:innen & Produktboard

Gezielte Interviews (u. a. mit BITBW, IT.NRW) vertieften komplexe Querschnittsthemen wie Betrieb, Support und Administration. Ergänzend steuerten Mitglieder des Produktboards aus 9 Bundesländern strategische Anforderungen bei.

2.2 Erhebung von Anforderungen

Quellen der Anforderungen

Die Anforderungen für NEOSiP wurden auf Grundlage eines multi-methodischen Vorgehens erhoben, um unterschiedliche Perspektiven systematisch zu erfassen und eine belastbare Grundlage für die Architekturentwicklung zu schaffen. Die Erhebung stützte sich auf eine Kombination aus Dokumentenanalysen regulatorischer Vorgaben und IT-architektonischer Rahmenbedingungen, der Analyse des Bestandssystems, bestehender Tickets sowie der Ableitung aus Expert:innenwissen zentraler Projektstakeholder. Ein weiteres Kernelement der Anforderungserhebung waren Interviews mit GB, EKS, Fachverfahrenshersteller:innen und Mitglieder des Produktboards sowie Fachworkshops mit GB und EKS. Darüber hinaus floss Expert:innenwissen aus dem Projektteam in die Erhebung ein.

2.2.1 Erhebung funktionaler Anforderungen

Durchführung der Erhebung

Die Durchführung der funktionalen Anforderungserhebung erfolgte in drei Formaten wie Tabelle 1 verdeutlicht.

Tabelle 1: Vergleichstabelle der Erhebungsformate Expert:innengespräche, Interviews und Workshops mit Kurzbeschreibung des jeweiligen Zwecks zur Erhebung funktionaler Anforderungen.

Format	Erläuterung
Expert:innengespräche	Expert:innengespräche wurden teilstrukturiert geführt und fokussierten sich auf identifizierte Barrieren, Herausforderungen und gegebenenfalls (ggf.) ergänzende Stakeholder, deren Ansprache als hilfreich erachtet wurde.
Interviews	Interviews basierten auf strukturierten Leitfäden zur Erhebung von Anforderungen sowie zur Bewertung und Verbesserung bestehender Komponenten.
Workshops	Workshops konzentrierten sich auf funktionale Anforderungen entlang der Prozessschritte „Antragserfassung & Prüfung“ sowie „Erkenntnisermittlung & Rückmeldung“. Hierbei kamen Methoden wie Prozessskizzen, Pain Point Mapping, User Story Mapping und das Kreativsegment „Wünsch dir was“ zum Einsatz.

Dokumentation der Erhebung

Die Anforderungserhebung wurde systematisch dokumentiert, um eine transparente und nachvollziehbare Ableitung der Ergebnisse sicherzustellen. Für jedes Interview und jeden Workshop wurden aufeinander aufbauende Dokumente erstellt, die eine methodisch konsistente Auswertung ermöglichten.

Als erster Schritt erfolgte die vollständige Transkription des Gesprächs oder des Workshops. Anschließend wurde das Transkript bereinigt und verbleibende Aussagen wurden thematisch gegliedert und nach Sprecher strukturiert, um eine klare inhaltliche Zuordnung zu gewährleisten. Für Interviews wurde zusätzlich eine offene Codierung des bereinigten Transkripts durchgeführt.

Ableitung von Anforderungen und User Stories

Auf Grundlage der Transkripte wurden konkrete Anforderungen sowie ergänzende User Stories abgeleitet.

Konsolidierung der Anforderungen

Die erhobenen Anforderungen wurden in einem strukturierten Prozess konsolidiert und qualitätsgesichert, indem Redundanzen entfernt und funktional ähnliche Inhalte zusammengeführt wurden. Divergenzen wurden markiert und gezielten Entscheidungsprozessen zugeführt, während Experten aus IT-Sicherheit, Architektur und User Experience die Liste validierten.

Das Projektteam verfeinerte die Anforderungen fortlaufend, wobei die Nachvollziehbarkeit der Quellen sichergestellt wurde. Kritische oder widersprüchliche Punkte wurden iterativ erörtert: Operative Entscheidungen wurden direkt dokumentiert und umgesetzt, während strategische Entscheidungsbedarfe zur Klärung an den Lenkungsausschuss eskaliert wurden, dem zudem die kontinuierliche Kommentierung der Liste offenstand.

Die grafische Darstellung in Abbildung 1 macht den Prozess bei der Konsolidierung der Anforderungsliste deutlich.

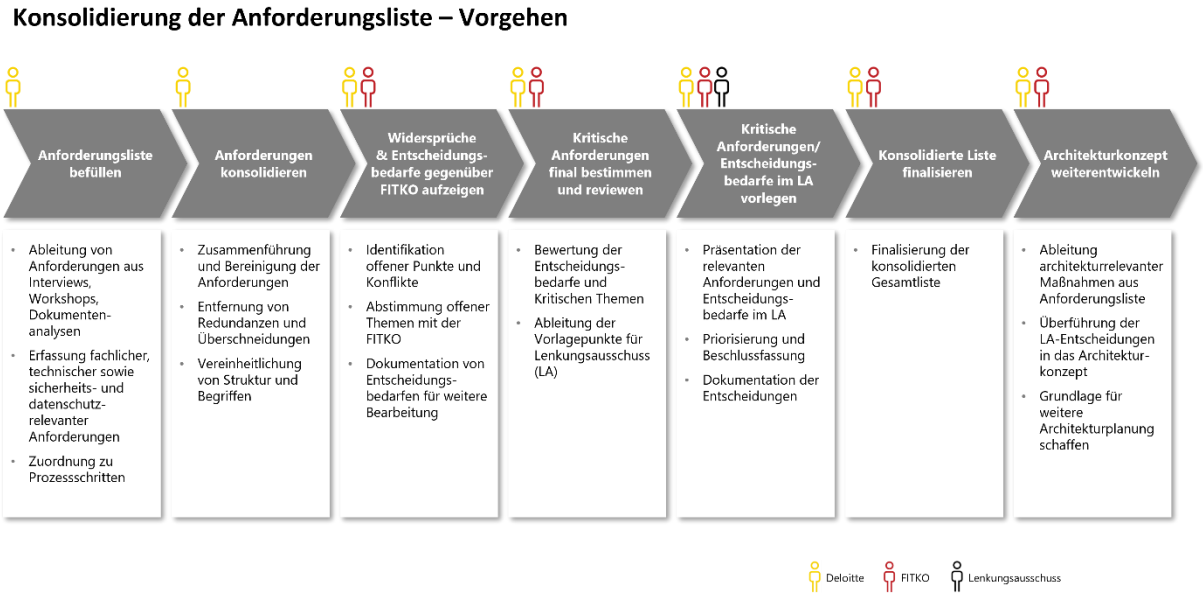


Abbildung 1: Prozessgrafik, die die Schritte zur Konsolidierung, Qualitätssicherung und Entscheidungsvorbereitung der erhobenen Anforderungen zeigt

2.2.2 Erhebung nicht-funktionaler Anforderungen

Die Ermittlung der nicht-funktionalen Anforderungen (NFA) basierte auf einem multidimensionalen Ansatz: Interviews mit Fachverfahrenshersteller:innen, Betreibern, EKS und dem FITKO-Informationssicherheitsbeauftragten lieferten zentrale Erkenntnisse zu Architektur, IT-Sicherheit und Datenschutz. Ergänzend wurden öffentliche Standards und Best Practices analysiert, um externe Vorgaben für NEOSiP abzuleiten.

Der Konsolidierungsprozess erfolgte systematisch durch Erfassung, Kategorisierung und Bereinigung von Redundanzen. Divergierende Anforderungen wurden markiert und im Projektteam oder durch Feedback des Lenkungsausschusses geklärt. Alle resultierenden Anpassungen flossen in die finale Liste ein. Das vollständige Quellenverzeichnis (inkl. Geheimschutz gemäß Kapitel 3.2.3.3) ist im Begleitdokument „**Anforderungsliste**“ im Bereich „Quellen“ hinterlegt.

2.3 Architekturentwicklung

Auf Basis der konsolidierten Anforderungen wurde eine robuste und anpassungsfähige Zielarchitektur entwickelt, die den aktuellen Kenntnisstand in einem dynamischen, föderalen Umfeld widerspiegelt. Die Modellierung erfolgte standardkonform in der Notation ArchiMate, um eine verständliche und einheitliche Darstellung sicherzustellen.

Der iterative Entwicklungsprozess ermöglichte eine kontinuierliche Schärfung von Entwürfen und Annahmen. Auf Geschäftsebene wurden die FITKO-Ziele und die OSiP-Wertschöpfungskette definiert. Daraus resultierte eine funktionale Prozessdarstellung, deren Kern der Nachrichtentransportprozess bildet (siehe Kapitel 3.3.4). Aus diesem Prozess wurde die logische Applikationsarchitektur mit ihren Services, Bausteinen und Schnittstellen sowie die zugehörige Informationsarchitektur abgeleitet.

Identifizierte Handlungsfelder auf Ebene der Informationssysteme wurden strukturiert aufbereitet (siehe Kapitel 5). Noch offene Architekturentscheidungen sind markiert und werden im weiteren Projektverlauf priorisiert adressiert oder in Folgeversionen der Zielarchitektur ergänzt.

2.4 Architekturentscheidungen

Architekturentscheidungen sind für die strukturelle Ausgestaltung, Interoperabilität und Sicherheit des Gesamtsystems im föderalen Kontext zentral. Sie wurden dort initiiert, wo Anforderungen, Bestandsanalysen oder Zielkonflikte über allgemeine Prinzipien hinausgehende Festlegungen erforderten.

Die Vorbereitung und Dokumentation erfolgt mittels Architecture Decision Records (ADRs). Jeder ADR beschreibt einen spezifischen Problemraum, stellt realistische Lösungsoptionen gegenüber und bewertet diese systematisch anhand funktionaler und nicht-funktionaler Kriterien (z. B. Wartbarkeit, Zukunftsfähigkeit). Ziel ist eine rationale, von persönlichen Präferenzen unabhängige Herleitung.

Die Anforderungslisten, ADRs, das Zielbild der Architektur und herangezogene Quellen sind auf der Plattform OpenCode in der Projektgruppe der FITKO für eine öffentliche Konsultation bereitgestellt[6].

[6] vgl. https://gitlab.opencode.de/fitko/osip/neukonzeption-osip

3 Ergebnisse der Untersuchung

3.1 Technische Bestandsanalyse

Die technische Bestandsanalyse beschreibt die wesentlichen fachlichen und technischen Eigenschaften des aktuellen Systems, die für die Zielarchitektur relevant sind. Die Betrachtung erfolgt auf einer hohen Abstraktionsebene und konzentriert sich auf Aspekte, welche die Anforderungen, Architekturentscheidungen und Gestaltungsprinzipien maßgeblich beeinflussen. Damit bildet die Analyse den verbindenden Kontext zwischen der Ist-Situation und der künftigen Zielarchitektur.

3.1.1 Überblick und Systemeinordnung

Das Bestandssystem fungiert als zentrale, vermittelnde Infrastruktur für den Austausch von Anträgen und Erkenntnissen zwischen Genehmigungsbehörden (GB) und Erkenntnisstellen (EKS). Es stellt die technische Basis für den Nachrichtentransport und das adressatengerechte Routing bereit.

Der Betrieb des Bestandssystems erfolgt föderal. Jedes Bundesland verantwortet einen eigenen OSiP-Kern als zentrale Datendrehscheibe für die jeweils angebundenen Akteure. Während Fachverfahren der GB und EKS an diese Kerne koppeln, nutzen Länder ohne eigenes Fachverfahren optional eine bereitgestellte OSiP-Fachanwendung in Eigenregie.

Diese verteilte Struktur ermöglicht zwar den Austausch zwischen technisch unabhängigen Partnern, prägt jedoch maßgeblich die Rahmenbedingungen für Wartung, Harmonisierung und Weiterentwicklung. Die föderale Betriebsarchitektur sowie die Systeminteraktionen sind in Abbildung 2 visualisiert.

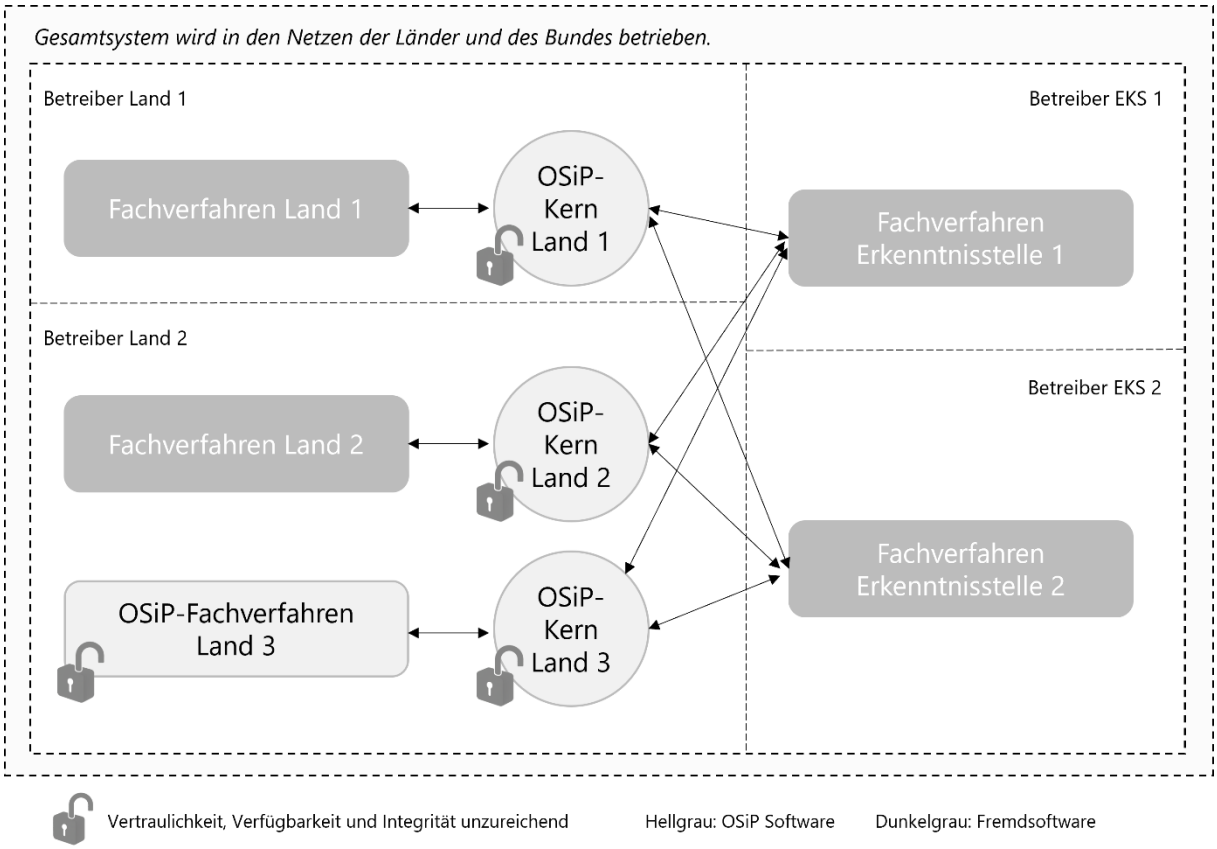


Abbildung 2: Übersicht des föderalen Betriebs mit landesspezifischen OSiP-Kernen als Vermittlungsinstanzen und den angebundenen Fachverfahren (aus Bestandsdokumentation)

3.1.2 Architekturstil und Systemaufbau

Der architektonische Aufbau des Bestandssystems ist eine über mehrere Jahre gewachsene Entwicklung und weist eine entsprechend heterogene Struktur auf. Zentraler Bestandteil des Bestandssystems ist der OSiP-Kern, der den Nachrichtenaustausch zwischen den angebundenen Fachverfahren organisiert und als zentrale Vermittlungsinstanz fungiert. Neben der Weiterleitung von Daten übernimmt der OSiP-Kern eine Vielzahl zusätzlicher Aufgaben, unter anderem im Bereich der Verwaltung von Metadaten sowie der Abbildung zustandsabhängiger Verarbeitungslogiken. Diese Bündelung unterschiedlicher Verantwortlichkeiten führt zu einer hohen funktionalen Dichte innerhalb der zentralen Komponente. Ergänzend zum OSiP-Kern existieren mehrere eigenständige Systemkomponenten, die jeweils spezifische Aufgaben im Gesamtprozess übernehmen. Dazu zählen unter anderem ein Fachverfahren für GB, EKS und antragstellende Organisationen sowie weitere unterstützende Komponenten für Administration, Integration und Sonderanbindungen. Beispiele hierfür sind eigenständige Clients zur Antragserfassung und -bearbeitung, spezielle Adapter zur Anbindung externer Dienste sowie Hilfskomponenten zur Administration des OSiP-Kerns. Diese Komponenten sind historisch entstanden und in

unterschiedlichem Maße miteinander gekoppelt. Die Anbindung weiterer Systeme erfolgt teilweise direkt an die jeweiligen Client-Anwendungen, etwa zur Unterstützung nachgelagerter fachlicher oder organisatorischer Prozesse. Dadurch entsteht eine zusätzliche Kopplung zwischen einzelnen Komponenten, die über den eigentlichen Nachrichtenaustausch hinausgeht. Insgesamt ergibt sich ein Systemaufbau, der aus einer Kombination zentraler Kernkomponenten und zahlreicher spezialisierter Zusatzkomponenten besteht, deren Zusammenspiel maßgeblich durch historische Entwicklungsentscheidungen geprägt ist. Zur Veranschaulichung des beschriebenen Aufbaus wird an dieser Stelle ein vereinfachtes Architekturdiagramm des Bestandssystems in Abbildung 3 herangezogen. Dies stellt die wesentlichen Komponenten und deren Zusammenwirken auf einer hohen Abstraktionsebene dar.

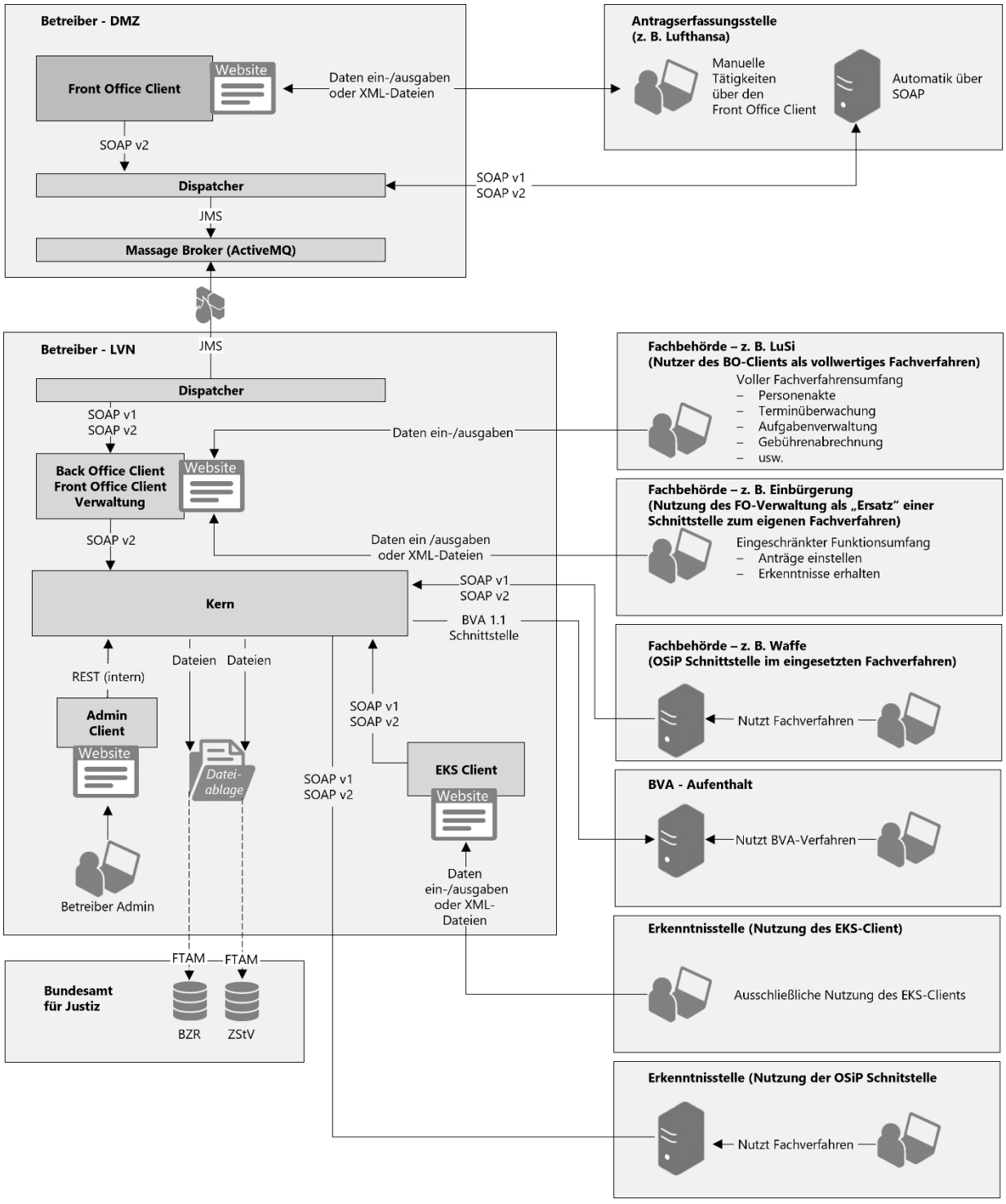


Abbildung 3: Diagramm der zentralen Systemkomponenten des Bestandssystems und ihrer Kommunikationsbeziehungen auf hoher Abstraktionsebene (aus Bestandsdokumentation)

3.1.3 Kommunikations- und Integrationsprinzipien

Die Kommunikations- und Integrationsprinzipien des Bestandssystems sind durch die föderale Struktur und den dezentralen Betrieb der OSiP-Kerne geprägt. Da jedes Bundesland einen eigenen OSiP-Kern betreibt, müssen externe Fachverfahren, insbesondere jene der EKS, technisch an mehrere OSiP-Instanzen angebunden werden. Die Verantwortung für die Anbindung sowie für die korrekte Adressierung der jeweils zuständigen OSiP-Kerne liegt dabei bei den angebundenen Systemen selbst.

Die Integrationslogik ist stark system- und fallbezogen ausgeprägt. Anbindungen werden je Fachverfahren und je EKS auf unterschiedliche Weise umgesetzt, wodurch eine Vielzahl unterschiedlicher Schnittstellenvarianten entstanden ist. Eine einheitliche, abstrahierte Integrationsschicht ist im Bestand nur eingeschränkt vorhanden. Dies führt zu einer hohen Komplexität in der Pflege und Weiterentwicklung der Schnittstellenlandschaft.

Im Kommunikationsverhalten des Bestandssystems kommen sowohl asynchrone als auch synchrone Interaktionsmuster zum Einsatz. Der OSiP-Kern selbst arbeitet überwiegend asynchron. Eingehende Daten werden dort abgelegt und von den empfangenden Systemen aktiv abgerufen. Dieses Prinzip ermöglicht eine zeitliche Entkopplung der beteiligten Systeme und reduziert die Abhängigkeit von deren gleichzeitiger Verfügbarkeit.

Daneben existieren jedoch auch synchrone Kommunikationsbeziehungen zwischen einzelnen Komponenten, etwa zwischen Client-Anwendungen für die Antragserfassung und -bearbeitung. Diese synchronen Kopplungen erhöhen die gegenseitigen Abhängigkeiten der beteiligten Systeme und wirken sich negativ auf Verfügbarkeit, Fehlertoleranz und Skalierbarkeit aus.

Insgesamt ergibt sich eine Integrationslandschaft mit vielfältigen, unterschiedlichen Schnittstellen und Kommunikationsbeziehungen, deren Absicherung und Harmonisierung nicht einheitlich umgesetzt ist. Eine detaillierte Betrachtung der vorhandenen Schnittstellen und deren Eigenschaften erfolgt im nachfolgenden Kapitel zur Schnittstellenanalyse.

3.1.4 Schnittstellen

Ziel dieses Kapitels ist es, die wesentlichen architektonischen Eigenschaften der bestehenden Schnittstellen als Grundlage für die Ableitung der Zielarchitektur herauszuarbeiten. Eine vollständige technische Dokumentation einzelner Schnittstellen ist ausdrücklich nicht Gegenstand dieser Betrachtung.

Die Schnittstellenlandschaft des Bestandssystems ist durch zahlreiche Anbindungen zwischen den zentralen Komponenten geprägt (veranschaulicht in Abbildung 4 und 5):

- Front-Office-Client (FO-Client): Antragserfassung durch externe Parteien.
- Back-Office-Client (BO-Client): Antragserfassung, -prüfung sowie Erkenntnisabfrage.
- OSiP-Kern: Zentrale, vermittelnde Instanz.
- EKS-Client: Anbindung externer Fachverfahren (EKS).

Die Kommunikation erfolgt primär zwischen den Clients und dem OSiP-Kern sowie zwischen dem OSiP-Kern und den externen EKS-Fachverfahren.

Protokolle und Formate

Im Bestand dominieren SOAP-basierte Schnittstellen in diversen Versionen, punktuell ergänzt durch andere Protokolle. Die fehlende Standardisierung erhöht den Integrations- und Wartungsaufwand.

Der Datenaustausch basiert überwiegend auf XML. Es kommen jedoch unterschiedliche, oft systemspezifische Strukturen zum Einsatz, was die Interoperabilität und Wiederverwendbarkeit einschränkt.

Sicherheit und Zugriffskontrolle

Die Absicherung erfolgt größtenteils über Transportverschlüsselung, wird jedoch nicht in allen Kommunikationsbeziehungen einheitlich angewendet. Eine konsistente Absicherung auf Nachrichtenebene fehlt im Bestand weitgehend. Die Zugriffskontrolle ist meist direkt an die beteiligten Systeme gekoppelt und nicht als übergreifendes Konzept umgesetzt – dies zeigt sich besonders bei dateibasierten Schnittstellen.

Auffällig ist, dass bei OSiP teilweise mehrere Schnittstellenversionen parallel betrieben werden, abhängig von der jeweiligen Client- oder Kernversion. Ergänzt wird dies durch stark zweckgebundene, kaum übertragbare Adapter- und Sonderlösungen. Diese Historie erschwert die koordinierte Weiterentwicklung der Systeme erheblich.

Zusammenfassend ist die Schnittstellenlandschaft des Bestandssystems als komplex, heterogen und historisch gewachsen einzuordnen. Die Vielfalt an Protokollen, Datenformaten, Sicherheitsausprägungen und Varianten stellt eine zentrale architektonische Rahmenbedingung dar und ist bei der Konzeption der Zielarchitektur ausdrücklich zu berücksichtigen. Die hier dargestellten Eigenschaften bilden eine wesentliche Grundlage für die Beschreibung der Zielarchitektur und der dort getroffenen Architekturentscheidungen. Das Ergebnis der Bestandsanalyse der Schnittstellen wird in Tabelle 2 dargestellt.

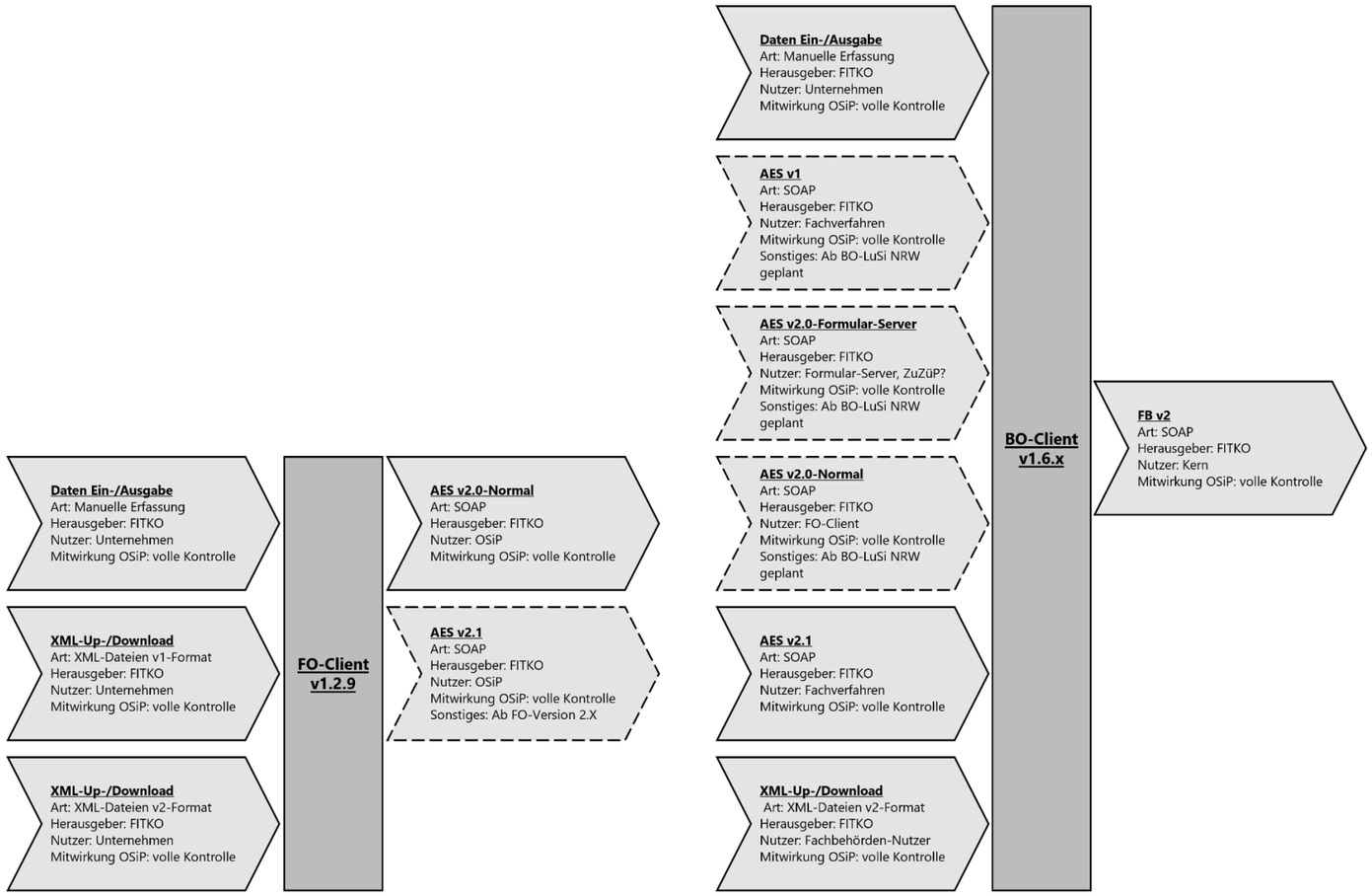


Abbildung 4: Erste Teilansicht der Schnittstellenlandschaft zwischen FO-Client, BO-Client, OSiP-Kern und EKS-Client aus der Bestandsdokumentation

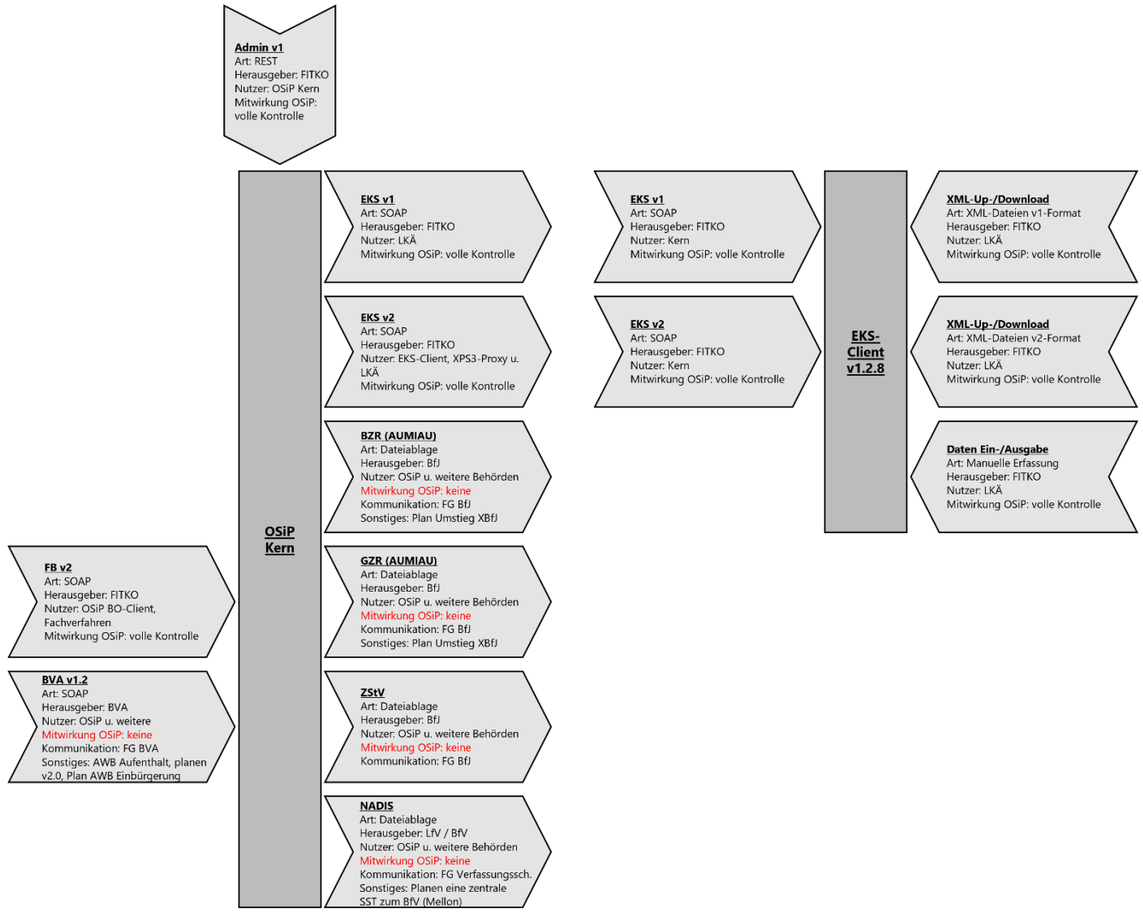


Abbildung 5: Zweite Teilansicht der Schnittstellenlandschaft zwischen FO-Client, BO-Client, OSiP-Kern und EKS-Client aus der Bestandsdokumentation

Tabelle 2: Übersichtstabelle zu Schnittstellen des Bestandssystems mit Beteiligten Systemen, Zweck, Schnittstellenart, Richtung, Protokoll, Datenformat, Frequenz, Sicherheitsmaßnahmen, Abhängigkeiten, Kopplungsgrad, Risiken, Quellen und Status

Kürzel	Name der Schnitt-stelle	Beteiligte Systeme	Fachlicher Zweck	Art der Schnitt-stelle	Datenfluss-Richtung	Protokoll	Daten-format	Aufruf-Frequenz	Sicherheits-maßnah-men	Abhängig-keiten	Kopplungs-grad	Risiken/ Schwach-stellen	Bemerkung	Bearbei-tungsstatus
Eindeutige Kennung der Schnittstelle	Klarer Name	Quell- und Zielsystem	Wofür wird die Schnittstelle genutzt? (z. B. Antrags-über-mittlung)	Push/Pull, synchron/a-synchron, API, Datei-transfer, Messaging etc.	Eingehend, ausgehend oder bi-direktional	z. B. HTTPS, SOAP, REST, SFTP, AUMIAU, Active-MQ	z. B. XML, JSON, CSV, proprietär, XÖV-Standard	z.B. Periodisch (täglich/ sekündlich)	z. B. TLS-Verschlüssel-ung, Zertifikats-authentifizier ung, API-Schlüssel, keine Sicherung	Welche anderen Schnitt-stellen oder Prozesse hängen davon ab?	Lose/eng gekoppelt	z. B. proprietär, unver-schlüsselt, hoher Wartungs-aufwand, Single Point of Failure.		Status der Erfassung
Erkenntnisstellen														
XPS3	XPS3-Server-API	System A: NEOSiP Transport-infrastruktur - XPS3-Adapter System B: XPS3-Server	Anfragen-über-mittlung Erkenntnis-austausch	Bei beiden Systemen handelt es sich um passive Systeme. Daher wird ein aktiver Adapter (Bezeich-nung XPS3-Proxy) benötigt	A <-> B	SOAP / REST (nicht RESTful, sondern "aufgesetzt" auf SOAP)	XML (XPolizei nach XÖV-Standard aber nicht öffentlich)	Voraus-sichtlich > 1 Mrd. bidirektio-nale Aufrufe / Monat	Technischer Nutzer, dessen Zugangs-daten im Header der SOAP Nachricht SOAP Nachricht ent-sprechend WS-I Basic Security Profile 1.1	NEOSiP-Standard-schnittstelle	Hohe Kopplung, da Daten transfor-miert werden müssen	Unver-schlüsselt, Außerhalb des eigenen Einfluss-bereichs	Unzureichende Schnittstelle nspezifikation	Fertig
NADIS	Nachrichten-dienstliches-Informations system	System A: OSIP-Kern System B: EKS (Bundesamt für Verfassungs-schutz (BfV) und Landesamt für Verfassungs-schutz (LfV)	Anfragen-über-mittlung Erkenntnis-austausch	Dateiablage	A <-> B	Dateiablage	.csv .xml (an LfV)	Unbekannt	Unbekannt	Unbekannt	Hoch	Unbekannt	Fehlende Dokumenta-tionen	Fertig
BZR (AUMIAU)		System A: OSIP-Kern System B: EKS (Bundes-zentral-register)	Anfragen-über-mittlung Erkenntnis-austausch	Dateiablage	A <-> B	Dateiablage	XML	Unbekannt	Unbekannt	Unbekannt	Hoch	Unbekannt	Fehlende Dokumenta-tionen	Fertig

ZStV	Zentrales Staats-anwalt-schaftliches Verfahrens-register	System A: OSIP-Kern System B: EKS (Zentrales staatsanwalts chaftliches Verfahrens-register)	Anfragen-über-mittlung Erkenntnis-austausch	Dateiablage	A <-> B	Dateiablage	XML	Unbekannt	Unbekannt	Unbekannt	Hoch	Unbekannt	Fehlende Dokumenta-tionen	Fertig
GZR (AUMIAU)	Gewerbe-zentral-register	System A: OSIP-Kern System B: EKS (Gewerbe-zentral-register)	Anfragen-über-mittlung Erkenntnis-austausch	Dateiablage	A <-> B	Dateiablage	XML	Unbekannt	Unbekannt	Unbekannt	Hoch	Unbekannt	Fehlende Dokumenta-tionen	Fertig
XBFJ		System A: OSIP-Kern System B: EKS (Bundesamt für Justiz)	Anfragen-über-mittlung Erkenntnis-austausch	Unbekannt	A <-> B	Unbekannt	Unbekannt	Unbekannt	Unbekannt	Unbekannt	Unbekannt	Unbekannt	Fehlende Dokumenta-tionen	Fertig
ZDI	Zentrale Daten-austausch Infrastruktur	System A: System B: Register-stellen des Bundes-amtes für Justiz	Anfragen-über-mittlung Erkenntnis-austausch	Unbekannt	A <-> B	Unbekannt	Unbekannt	Unbekannt	Unbekannt	Unbekannt	Unbekannt	Unbekannt	Fehlende Dokumenta-tionen	Fertig
Mellon	Unbekannt	System A: OSIP-Kern System B: EKS (Ver-fassungs-schutz)	Unbekannt	Unbekannt	Unbekannt	Unbekannt	Unbekannt	Unbekannt	Unbekannt	Unbekannt	Unbekannt	Unbekannt	Sollte perspekt-ivisch NADIS ersetzen und daher unterstützt werden. Fehlende Dokumenta-tionen	Fertig
SFTP	SFTP	System A: OSIP-Kern System B: EKS (Ver-fassungs-schutz)	Anfragen-über-mittlung Erkenntnis-austausch	sFTP-Gateway	A <-> B	Unbekannt	Unbekannt	Unbekannt	Unbekannt	Unbekannt	Unbekannt	Unbekannt	Fehlende Dokumenta-tionen	Fertig

Erkenntnis Up-/Download	Erkenntnis Up-/Download	System A: EKS-Client System B: Anwender Erkenntnis-stelle	Dateiablage	Dateiablage	A <-> B	Dateiablage	Unbekannt	Unbekannt	Benutzer-authori-sierung	keine	Unbekannt	Unbekannt		Fertig
EKS-V1	Erkenntnis-stelle v1	System A: OSIP Kern System B: EKS	Anfragen-über-mittlung Erkenntnis-austausch	Push, synchron, API	A <-> B	SOAP	XML v1	Unbekannt	Passwort wird im Header Base64 encodiert übermittelt	Anfragen-über-mittlung Erkenntnis-über-mittlung	Hoch	Unbekannt	Fehlende Dokumenta-tionen	Fertig
EKS-V2	Erkenntnis-stelle v2	System A: OSIP Kern System B: EKS-Client	Anfragen-über-mittlung Erkenntnis-austausch	Push, synchron, API	A <-> B	SOAP	XML v2	Unbekannt	Passwort wird im Header Base64 encodiert übermittelt	Anfragen-über-mittlung Erkenntnis-über-mittlung	Hoch	Unbekannt	Fehlende Dokumenta-tionen	Fertig
Antrag Up-/Download	Antrag Up-/Download	System A: EKS-Client System B: Anwender Erkenntnis-stelle	Dateiablage	Dateiablage	A <-> B	Dateiablage	XML v1 & v2	Unbekannt	Passwort wird im Header Base64 encodiert übermittelt	Anfragen-über-mittlung Erkenntnis-über-mittlung	Hoch	Unbekannt	Fehlende Dokumenta-tionen	Fertig
Genehmigungsbehörden														
FB-V2	Fach-behörde V2	System A: OSIP Kern System B: BO-Client	Unbekannt	Unbekannt	Unbekannt	Unbekannt	Unbekannt	Unbekannt	Unbekannt	Unbekannt	Unbekannt	Unbekannt	Fehlende Dokumenta-tionen	Fertig
Antragserfassungsstelle (AES)														
AES-V2.1	Antrags-erfassungs-stelle V2.1	System A: BO-Client System B: FO-Client	Antrags-über-mittlung über Netzgrenze an GB Nur Luft-sicherheit und Anlass-bezogene Überprüfung	Push, synchron, API	B -> A	SOAP	XML v2.1	Unbekannt	Passwort wird im Header Base64 encodiert übermittelt	Antragserfas sung	Hoch	Unbekannt		Fertig

AES-V2 normal	Antrags-erfassungs-stelle V2	System A: BO-Client System B: FO-Client	Antrags-über-mittlung über Netzgrenze an GB	Push, synchron, API	B -> A	SOAP	XML v2	Unbekannt	Passwort wird im Header Base64 encodiert übermittelt	Antrags-erfassung	Hoch	Unbekannt		Fertig
AES-V2 Formular-Server	Antrags-erfassungs-stelle V2 Formular-Server	System A: BO-Client System B: FO-Client	Antrags-über-mittlung über Netzgrenze an GB	Push, synchron, API	B -> A	SOAP	XML v2	Unbekannt	Passwort wird im Header Base64 encodiert übermittelt	Antrags-erfassung	Hoch	Unbekannt		Fertig
AES-V1	Antrags-erfassungs-stelle V1	System A: BO-Client System B: FO-Client (nur Lufthansa)	Antrags-über-mittlung über Netzgrenze an GB	Push, synchron, API	B -> A	SOAP	XML v1	Unbekannt	Passwort wird im Header Base64 encodiert übermittelt	Antrags-erfassung	Hoch	Unbekannt		Fertig
Antrag Up-/Download	Antrag Up-/Download	System A: FO-Client System B: Anwender Antrags-stellung	Upload & Download von Anträgen	Dateiablage	A <-> B	Dateiablage	XML	Unbekannt	Benutzer-authori-sierung	Antrags-erfassung	Hoch	Unbekannt	Fehlende Dokumenta-tionen	Fehlende Dokumenta-tionen
Antrag Up-/Download	Antrag Up-/Download	System A: FO-Client System B: Anwender Antrags-stellung	Upload & Download von Anträgen	Dateiablage	A <-> B	Dateiablage	XML v1 & v2	Unbekannt	Unbekannt	Antrags-erfassung	Hoch	Unbekannt	Fehlende Dokumenta-tionen	Fehlende Dokumenta-tionen
Interne Schnittstelle														
Admin v1	Admini-strations-schnittstelle	System A: Admin-Client System B: OSIP-Kern	Administrati on des Kerns	Push, synchron, API	A <-> B	REST	JSON	Unbekannt	Cookie mit bearer-token, Login über Keycloak und Generieren des entsprechen-den Tokens	Keine	Gering	Unbekannt	Fehlende Dokumenta-tionen	Fertig
Nicht zugeordnet														
Druckstraße	Druckstraße	System A: BO-Client System B: Druckstraße	Briefversand von Zu-/Absagen	Dateiablage	A->B	Daten-ablage	PDF	Unbekannt	Interne Schnitt-stelle, keine	keine	gering	keine	Fehlende Dokumenta-tionen	Fehlende Dokumenta-tionen

									Absicher-ung					
BVA v1.2	Bundes-verwaltungs-amt	System A: OSiP Kern System B: BVA	Abholen von Anfragen (Ausländer-behörde)	SOAP, in Zukunft REST bei Schlüssel-katalogen	A -> B	SOAP / REST	XML	Unbekannt	Unbekannt	Keine	Hoch	Unbekannt	Fehlende Dokumenta-tionen	Fehlende Dokumenta-tionen

3.1.5 Mengengerüste

Zur Bewertung der Übertragbarkeit in Hinblick auf die Skalierbarkeit, Leistungseffizienz und Zuverlässigkeit der Zielarchitektur ist eine belastbare Einordnung der im Bestandssystem verarbeiteten Mengen erforderlich. Dieses Kapitel fasst die wesentlichen Mengengerüste des Bestandssystems zusammen und stellt diese in Bezug zu den organisatorischen und technischen Rahmenbedingungen. Betrachtet werden sowohl durchschnittliche Lasten als auch beobachtete Spitzenbelastungen. Nordrhein-Westfalen dient dabei aufgrund der hohen Fallzahlen im Betrachtungszeitraum als repräsentativer Referenzfall.

Vorgangsmengen und zeitliche Verteilung

Im Bestandssystem OSiP wurden im Jahr 2024 bundesweit rund 1,9 Millionen Sicherheitsüberprüfungen durchgeführt. Davon standen 173.495 Vorgänge im Zusammenhang mit der Fußball-Europameisterschaft. Auch im Jahr 2025 bewegt sich die Gesamtzahl der durchgeführten Sicherheitsüberprüfungen mit erneut rund 1,9 Millionen Vorgängen auf einem vergleichbaren Niveau, ohne dass es eine vergleichbare Großveranstaltung wie 2024 gab. Parallel dazu stieg die Anzahl der angeschlossenen Fachbehörden von 1.007 im Jahr 2024 auf 1.024 im Jahr 2025.

Die Auswertung der Produktivdaten aus Nordrhein-Westfalen aus dem Zeitraum Juli 2024 bis Juni 2025 verdeutlicht die Spannbreite zwischen durchschnittlicher Last und temporären Spitzen. Während im Dezember 2024 nur 27.068 Erstanträge eingingen, wurden in der Spitze der verfügbaren Daten im Mai 2025 94.871 Erstanträge gestellt. Der Durchschnitt pro Monat liegt bei 41.900 Erstanträgen. Folgeanträge werden in Nordrhein-Westfalen im Durchschnitt mit rund 13.400 Vorgängen pro Monat bearbeitet, wobei auch hier saisonale Schwankungen und ereignisbedingte Ausschläge erkennbar sind.

Diese Verteilungen machen deutlich, dass die Architektur nicht allein auf mittlere Durchschnittswerte ausgelegt werden darf. Insbesondere ereignisgetriebene Spitzen, wie sie im Kontext von Großveranstaltungen auftreten, stellen erhöhte Anforderungen an Durchsatz, Entkopplung und Fehlertoleranz der beteiligten Systeme.

Datenvolumina je Landesinstanz

Neben den reinen Vorgangszahlen sind die gespeicherten Datenvolumina ein zentraler Indikator für die Belastung der Systemlandschaft. Für die Datenbanken der Landesinstanzen zeigen sich deutliche Unterschiede zwischen den betrachteten Bundesländern. In Nordrhein-Westfalen wurde der verfügbare Datenbankspeicher von 300 GB im Jahr 2023 auf 490 GB im Jahr 2025 erhöht. Dieses Wachstum korreliert mit der hohen Anzahl an Vorgängen sowie mit der langfristigen Vorhaltung fachlicher und technischer Metadaten.

In Hessen und Brandenburg fanden hingegen keine Anpassungen des Speicherplatzes der Datenbanken statt. Die Unterschiede verdeutlichen die stark variierenden Belastungen der Landesinstanzen und unterstreichen die Notwendigkeit einer Architektur, die sowohl kleine als auch sehr große Installationen wirtschaftlich und stabil unterstützt.

Vielfalt angebundener Fachverfahren

Ein weiterer mengenrelevanter Aspekt ist die Anzahl unterschiedlicher, externer Fachverfahren, die an die jeweiligen Landesinstanzen angebunden sind. In Nordrhein-Westfalen sind derzeit sechs unterschiedliche Fachverfahren verschiedener Hersteller angebunden. Hessen nutzt fünf unterschiedliche externe Fachverfahren, während in Brandenburg lediglich ein externes Fachverfahren angebunden ist.

Diese Unterschiede haben unmittelbare Auswirkungen auf Integrationsaufwand, Schnittstellenvielfalt und Betriebsaufwand. Insbesondere in Ländern mit hoher Herstellerdichte.

Einordnung für die Zielarchitektur

Die dargestellten Mengengerüste zeigen, dass die Zielarchitektur sowohl hohe Dauerlasten als auch kurzfristige Lastspitzen zuverlässig verarbeiten können muss. Gleichzeitig ist eine erhebliche Heterogenität zwischen den Landesinstanzen zu berücksichtigen, sowohl hinsichtlich der Vorgangszahlen als auch der angebundenen Fachverfahren und Datenvolumina. Die Zielarchitektur muss daher skalierbar, elastisch und entkoppelt ausgelegt sein, ohne sich ausschließlich an einem einzelnen Landesprofil zu orientieren. Nordrhein-Westfalen dient in diesem Kontext als Belastungsreferenz, stellt jedoch nicht den alleinigen Maßstab für die Ausgestaltung der Architektur dar.

3.2 Listen funktionaler und nicht-funktionaler Anforderungen

3.2.1 Erläuterungen und Aufbau der Anforderungslisten

Die wesentlichen Erkenntnisse aus der Anforderungserhebung werden anhand der zwei Dimensionen der funktionalen und nicht-funktionalen Anforderungen abgebildet. Die funktionalen Anforderungen beschreiben dabei konkrete Funktionen und Prozessschritte, die das System ausführen soll. Nicht-funktionale Anforderungen hingegen definieren Qualitätsmerkmale und Rahmenbedingungen wie Sicherheit, Performance, Skalierbarkeit oder Compliance, die die Umsetzung und den Betrieb des Systems betreffen. Diese Unterscheidung ermöglicht eine klare Trennung zwischen „Was soll das System tun?“ und „Wie soll das System arbeiten?“

Die konsolidierten sind im Begleitdokument „Anforderungsliste“ dokumentiert. Das Dokument umfasst die in Tabelle 3 aufgezeigten Bereiche.

Tabelle 3: Strukturübersicht des Begleitdokument „Anforderungsliste“ mit Bereichen für funktionale, nicht-funktionale und Geheimschutz-Anforderungen samt Glossar und Quellen

Bereich	Erläuterung
Tabelle der funktionalen Anforderungen	Enthält alle funktionalen Anforderungen und Anforderungen an Nutzer:innenfreundlichkeit einschließlich Barrierefreiheit und Nutzerführung.
Tabelle der nicht-funktionalen Anforderungen	Dokumentiert Anforderungen zu IT-Sicherheit, Datenschutz, Architektur und weiteren übergreifenden Themen.
Tabelle der Anforderungen zu Geheimschutz	Dokumentiert Anforderungen, die zu berücksichtigen sind, wenn Verschlusssachen handzuhaben sind.
Glossar	Definiert feststehende Begriffe, die in den Anforderungen verwendet werden.
Erläuterung der Kategorien	Beschreibt Wertebereiche zu Kategorien und Subkategorien.
Quellen	Verweist auf die Herkunft der Anforderungen aus Interviews, Workshops, Standards, Gesetzen und Richtlinien.

3.2.2 Wesentliche Erkenntnisse funktionaler Anforderungen

3.2.2.1 Prozessschritte der Online-Sicherheitsprüfung

Das Ergebnis der funktionalen Anforderungserhebung ist die Abbildung der grundlegenden Prozessschritte, deren Abwicklung seitens der befragten Stakeholder im Rahmen der Online-Sicherheitsüberprüfung gesehen werden, sowie eine Anforderungsliste, die Details zu gemeldeten, funktionalen Bedarfen innerhalb der Prozessschritte beinhaltet. Ziel war es, ein Bild der Anforderungen unabhängig von den zugrundeliegenden, technischen Komponenten zu erhalten. Abbildung 6 zeigt die Prozessschritte und die Stakeholder, denen sie zugeordnet sind, auf.

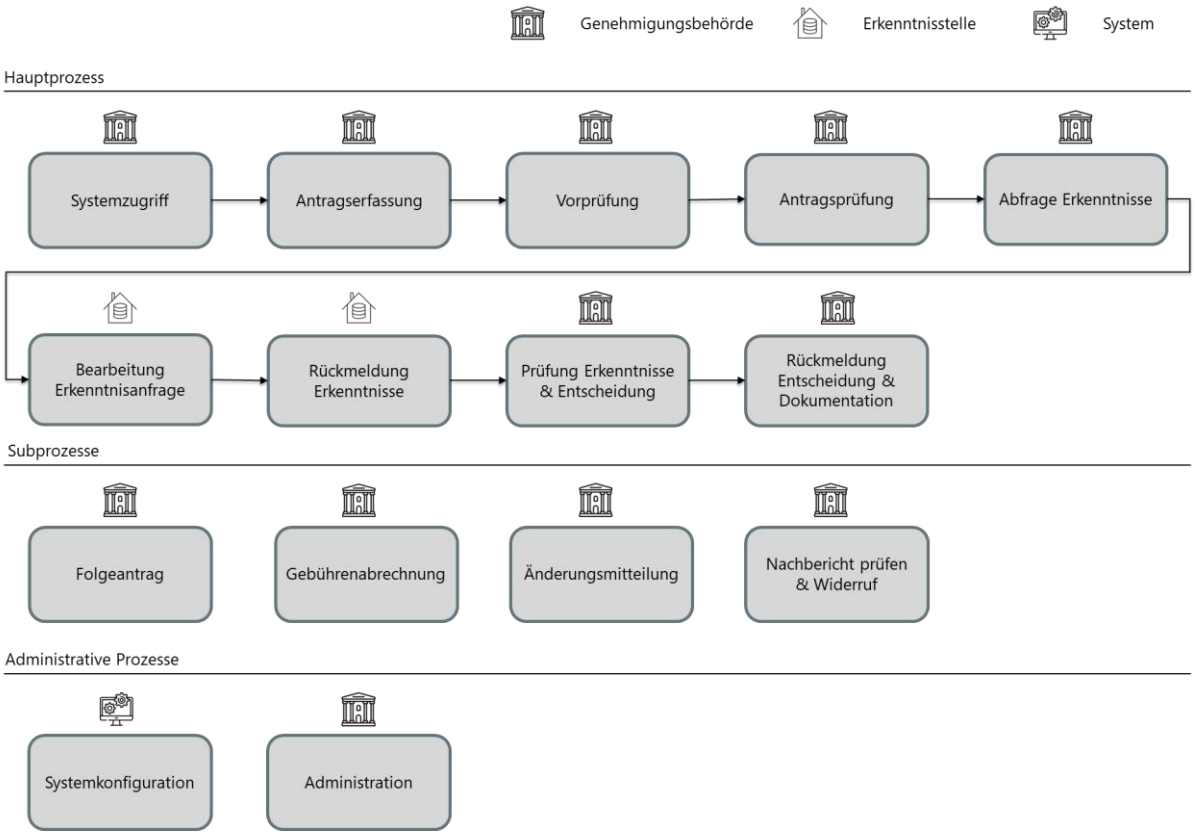


Abbildung 6: Grafische Darstellung der Hauptprozessschritte der Online-Sicherheitsüberprüfung mit Stakeholder-Zuordnung entlang des Verfahrens.

Der Hauptprozess umfasst dabei die grundlegenden Schritte der Online-Sicherheitsüberprüfung und ist in Tabelle 4 aufgeführt.

Tabelle 4: Liste der Hauptschritte (z. B. Systemzugriff, Antragserfassung, Vorprüfung, Antragsprüfung, Erkenntnisabfrage, Entscheidung, Dokumentation) mit Kurzbeschreibung je Schritt

Prozessschritt	Erläuterung
Systemzugriff	Authentifizierung und Autorisierung von Nutzern, um den Zugang zu den Funktionen des Systems zu ermöglichen.[7]
Antragserfassung	Erfassung und Speicherung der Antragsdaten im System, einschließlich aller erforderlichen Nachweise und Angaben.

[7] Insbesondere aus Sicht des Geheimschutzes gilt es den Grundsatz „Kenntnis nur, wenn nötig" einzuhalten, wozu sowohl in der Verschlusssachenanweisung als auch im BSI IT-Grundschutz detaillierte Vorgaben gemacht werden.

Vorprüfung	Erste fachliche und formale Prüfung eines Antrags auf Vollständigkeit und Plausibilität.
Antragsprüfung	Fachliche Bewertung des Antrags durch die zuständige Behörde, einschließlich Prüfung der Voraussetzungen und Rechtsgrundlagen.
Abfrage Erkenntnisse	Automatisierte oder manuelle Anfrage an EKS zur Ermittlung sicherheitsrelevanter Informationen.
Bearbeitung Erkenntnisanfrage	Verarbeitung und Beantwortung der eingegangenen Erkenntnisanfragen durch die EKS.
Rückmeldung Erkenntnisse[8]	Übermittlung der Ergebnisse der Erkenntnisprüfung an die anfragende Behörde.
Prüfung Erkenntnisse & Entscheidung[9]	Zusammenführung und Bewertung aller Erkenntnisse zur Ableitung einer Entscheidung über den Antrag.
Rückmeldung Entscheidung & Dokumentation	Mitteilung der Entscheidung an Antragstellende und Dokumentation im System für Nachvollziehbarkeit.

Die Subprozesse bilden ergänzende Schritte ab, die zusätzlich zum Hauptprozess erfolgen können, folgend in Tabelle 5 abgebildet.

Tabelle 5: Ergänzende OSiP-Subprozessschritte (Folgeantrag, Gebührenabrechnung, Änderungsmitteilung, Nachbericht/Widerruf) mit jeweiliger Erläuterung.

Prozessschritt	Erläuterung
Folgeantrag	Initiierung und Bewertung eines weiteren Antrags für denselben Antragsstellenden i. d. R. nach Ablauf der Gültigkeit des initialen Antrags.
Gebührenabrechnung	Berechnung und Erhebung von Gebühren für die Durchführung des Verfahrens gemäß den geltenden Vorschriften.
Änderungsmitteilung	Verarbeitung von Mitteilungen über Änderungen relevanter Daten oder Informationen, die eine Anpassung des Verfahrens erfordern.
Nachbericht prüfen & Widerruf	Prüfung von Nachberichten und ggf. Einleitung eines Widerrufs der erteilten Genehmigung.

[8] In diesem Prozessschritt besteht die Möglichkeit, das VS gehandhabt werden. Daher müssen insbesondere hier Anforderungen des Geheimschutzes berücksichtigt werden, um den Grundsatz „Kenntnis nur, wenn nötig" einzuhalten, siehe Kapitel 3.2.3.3:
[9] In diesem Prozessschritt besteht die Möglichkeit, das VS gehandhabt werden. Daher müssen insbesondere hier Anforderungen des Geheimschutzes berücksichtigt werden, um den Grundsatz „Kenntnis nur, wenn nötig" einzuhalten, siehe Kapitel 3.2.3.3.

Administrative Prozesse adressieren die Systemkonfiguration auf der Ebene einer übergeordneten Systemadministration sowie die konkrete Verwaltung von Einstellungen auf Ebene der Genehmigungsbehörde. Tabelle 6 zeigt diese auf.

Tabelle 6: Administrative OSiP-Prozessschritte mit Systemkonfiguration und Administration

Prozessschritt	Erläuterung
Systemkonfiguration	Einrichtung und Anpassung der technischen und fachlichen Parameter des Systems.
Administration	Verwaltung des Systems, einschließlich Benutzer- und Rollenmanagement und Konfiguration von Behördenspezifika.

Die funktionale Anforderungsliste ist im Begleitdokument „Anforderungsliste" einzusehen. Dabei werden Anforderungen klar den jeweiligen Prozessschritten zugeordnet. Eine visuelle Zusammenführung der übergeordneten Prozessschritte und der darunterliegenden Anforderungen wird im Rahmen des Kapitels zu den Geschäftsprozessen bereitgestellt (siehe Kapitel 3.3.4).

3.2.2.2 Kernaspekte der Anforderungsliste

In der Gesamtbetrachtung der Anforderungen wurden von den Stakeholdern insbesondere die nachfolgenden Aspekte als wesentlich hervorgehoben:

Medienbruchfreie Abbildung des Prozesses der Online-Sicherheitsprüfung

Im Rahmen der Interviews und Workshops mit den beteiligten Stakeholdern wurde aufgezeigt, dass es aktuell sehr unterschiedliche Wege gibt, wie die ZSÜ operativ durchgeführt wird. Dies reicht im Rahmen der Antragserfassung von Emails und Excel-Listen, die zwischen GB und EKS ausgetauscht werden, über eigene Fachverfahren bei den GB, deren Output manuell im Rahmen von XML- oder Exceldateien wieder in OSiP überführt werden, bis hin zu Schnittstellenanbindungen, die eine Übernahme in OSiP digital ermöglichen. Gleichzeitig wurde die Herausforderung dargestellt, dass die Abfrage der Erkenntnisse bei den EKS oftmals auf verschiedenen Kommunikationswegen erfolgen muss, da bisher nicht alle EKS an OSiP angebunden sind. Durch die diversen und mit Medienbrüchen besetzten Varianten der ZSÜ-Abwicklung besteht oftmals auch keine Transparenz darüber, in welchem Bearbeitungsstand sich ein Antrag befindet.

Daraus resultierte der Wunsch nach einer medienbruchfreien Abbildung des Prozesses der OSiP. Das bedeutet laut den befragten Stakeholdern, dass eine Aufnahme von Anträgen über

technische Schnittstellen in NEOSiP gegeben sein soll. Gleichzeitig soll die direkte Eingabe von Anträgen durch Sachbearbeiter:innen, sowie deren Einspeisung über das Hochladen von Dateien ermöglicht werden. Dieser Schritt der Antragserfassung und alle folgenden Prozessschritte der OSiP sollen integriert durch einen übergreifenden digitalen Workflow abgebildet werden. Dieser soll über technische Komponenten hinweg ein Verständnis schaffen, in welchem Bearbeitungsstand sich ein Antrag befindet. Jeder Schritt dieses digitalen Ablaufes soll im Sinne der Nachvollziehbarkeit protokolliert, sowie ggf. bei Übergabe zwischen Systemkomponenten quittiert werden. Im Rahmen der Abfrage von Erkenntnissen, war es wesentlich für die befragten GB, dass in Zukunft alle gesetzlich vorgeschriebenen EKS über NEOSiP angefragt werden können, um eine vollständige Datenbasis zur Prüfung der Anträge an einem Ort sicherzustellen und somit einen Wechsel zu anderen Kommunikationswegen zu vermeiden.

Standardisiertes Template zur Datenübertragung durch Datenstandard

Im Sinne eines medienbruchfreien Prozesses, besteht die Anforderung nach einem Datenstandard, der eine nahtlose Kommunikation mit angrenzenden Systemen ermöglicht. Im Rahmen des Datenstandards sollen Vorgaben zur Übertragung der gesetzlich vorgegebenen Informationen festgelegt werden. Perspektivisch könnte in diesem Kontext in Zukunft auch die Übermittlung biometrischer Daten (z.B. Fingerabdrücke, Fotos) Berücksichtigung finden.

Eine Validierung gegen diesen Standard vor Versand der Anfragen an EKS ist gewünscht.

Berücksichtigung unterschiedlicher Anwendungsfälle

Neben dem Wunsch nach einem klaren, medienbruchfreien Prozess zur ZSÜ, spiegelt die aufgezeigte Arbeitsrealität den Bedarf nach einer Flexibilisierung wider, um unterschiedliche Anwendungsfälle zu berücksichtigen.

Diese ergeben sich aus der Abbildung der unterschiedlichen AWB. Die AWB unterliegen verschiedenen Bundes- oder Landesgesetzen, welche spezifische Vorgaben zu erfassenden Daten machen, sodass der Wunsch im Sinne der Nachnutzung besteht, diese Unterschiede in der Antragserfassung zu berücksichtigen.

Zusätzlich gibt es Unterschiede in den Prozessschritten, die in den AWB Teil der ZSÜ sind. So gilt es im Bereich der Luftsicherheit z. B. die sogenannte Fortgeltungsfiktion zu berücksichtigen, während in anderen AWB Anhörungsverfahren ein Schritt hin zur ZSÜ sind und optimalerweise Teil des digitalen Workflows wären.

Das Ausmaß der Berücksichtigung AWB-spezifischer Unterschiede wird im Rahmen der Umsetzungsphase auf Basis der NEOSiP-Produktstrategie und der Zusammenarbeit mit den operativen Arbeitsgruppen weiter eingegrenzt.

Automatisierung

Um eine Vielzahl an Anträgen zur ZSÜ effizient abwickeln zu können, besteht der Wunsch, dort wo sinnvoll und möglich, Prozessschritte zu automatisieren, um Sachbearbeiter:innen in den GB zu entlasten. Aus diesem Wunsch heraus soll NEOSiP eine logikbasierte Erkenntnisabfrage auf Basis konfigurierbarer Kriterien (z. B. Wohnort, Staatsangehörigkeit, Beschäftigungsart) ermöglichen. So kann – wenn gewollt – eine automatisierte Abfrage der relevanten EKS nach Aufnahme des Antrages erfolgen. Der Großteil der Erkenntnisanfragen verläuft ohne Rückmeldung von Erkenntnissen, sodass auch an dieser Stelle das Potential besteht, Erkenntnisrückmeldungen ohne Ergebnis automatisiert weiterzuverarbeiten und Entscheidungen an Antragstellende und Fachbehörden, ohne erneuten Eingriff von Sachbearbeiter:innen, der GB gegenüber zu kommunizieren. Wichtig ist an dieser Stelle, dass diese Funktionalitäten bei Berücksichtigung optional sein müssen, da im Fall vorliegender Erkenntnisse und bei manchen AWB generell, eine Prüfung durch Sachbearbeiter:innen erfolgen muss. Ebenso soll eine automatisierte Wiedervorlage an die zuständigen Sachbearbeiter:innen der GB ausgelöst werden, sobald Nachberichte seitens der EKS eingehen.

Unterstützende Mechanismen für Sachbearbeiter:innen der GB

Vorgänge, die nicht automatisiert werden können, um Sachbearbeiter:innen zu entlasten, sollen möglichst so gestaltet werden, dass Sachbearbeiter:innen in ihrer Arbeit effizient unterstützt werden. Dies umfasst u.a. Mechanismen, die bei der Vorprüfung die Vollständigkeit und Plausibilität von Antragsdaten sicherstellen, bevor diese in die weitere Bearbeitung überführt werden. Als Beispiele können die Validierung der Angaben und hochgeladenen Nachweise, einschließlich der Kontrolle verpflichtender Dokumente, dienen. Das System soll die Steuerung von Nachforderungen bei fehlenden oder unvollständigen Angaben unterstützen und Erinnerungen unter Berücksichtigung definierter Fristen ermöglichen. Funktionen zur Dublettenprüfung im Rahmen der Verwaltung von Erst- und Folgeanträgen sollen Teil von NEOSiP sein. Zur Entscheidungsunterstützung sollen eine Notiz- und Markierungsfunktion zur Dokumentation prüfungsrelevanter Informationen sowie regelbasierte Checklisten für Entscheidungen und eine Verknüpfung von Anträgen bei Alias-Personalien oder abweichenden Geburtsdaten ermöglicht werden. Auf organisatorischer

Ebene soll eine sinnvolle Zuteilung der Antragsbearbeitung durch Sachbearbeiter:innen der GB auf Basis konfigurierbarer Logiken (z. B. Zufallsprinzip, Wohnsitz der Antragstellenden,

erfassende Person in der Behörde) sowie eine Übertragung und Anerkennung von ZSÜ AWB- und bundeslandübergreifend unterstützt werden, um Mehrfachprüfungen zu vermeiden, sofern eine entsprechende gesetzliche Grundlage dazu gegeben ist.

Arbeitsansichten

Wiederholte Anforderungen für den gesamten Prozess bezogen sich auf Arbeitsübersichten mit Such-, Filter-, Paging- und Exportoptionen für die Sachbearbeiter:innen der GB. Im Sinne einer konsistenten Nutzerführung soll abhängig des Kontextes, in dem sich Sachbearbeiter:innen gerade befinden, Übersichten mit Schwerpunkten auf erfassten Anträgen, versandten und offenen Erkenntnisabfragen, rückgemeldeten Erkenntnissen und offenen oder ausstehenden Entscheidungen zur Verfügung stehen. Diese Übersichten sollten Metadaten, Statusinformationen und ggf. Fristen abbilden. Ausgehend von diesen Übersichten soll eine intuitive Nutzerführung hin zu Detailansichten oder den nächsten, auszuführenden Aktionen durch Sachbearbeiter:innen möglich sein.

Transparenz durch Statistiken und Dashboards

Im Rahmen der Befragung der Stakeholder wurde an unterschiedlichen Stellen im Prozess der OSiP und auf unterschiedlichen Ebenen der Wunsch nach Transparenz durch Statistiken und Dashboards geäußert.

Im Rahmen der Systemkonfiguration besteht der Wunsch nach Dashboards auf Mandantenebene, welche nutzungsrelevante, technische Kennzahlen, wie z. B. Durchlaufzeiten, aufzeigen. Aus Sicht der GB sind individualisierbare Statistiken direkt verknüpft mit dem Antragsprozess selbst wünschenswert. Diese könnten u.a. Informationen wie die Anzahl bearbeiteter Anträge, Erkenntnisquoten, Genehmigungsquoten, Gebühren oder die Anzahl von Nachberichten beinhalten.

Kontrollierte Nutzung des Systems

Dies betrifft die Prozessschritte Systemkonfiguration sowie Systemzugriff und Administration. Im Rahmen der funktionalen Anforderungserhebung wurde der Bedarf nach einer sicheren und

kontrollierten Nutzung des Systems durch berechtigte Personen festgehalten.[10] Er umfasst auf Ebene der Systemkonfiguration die Verwaltung von Mandanten, sowie im Sinne der Administration die Verwaltung von Nutzer:innen-/Administrator:innenkonten und die Authentifizierung und Autorisierung der Zugriffe für Nutzende der GB.

3.2.2.3 Anforderungen außerhalb der NEOSiP-Produktstrategie

In der Sondersitzung des Lenkungsausschusses im Dezember 2025 wurden wesentliche Festlegungen zum Umfang und zur funktionalen Ausrichtung von NEOSiP getroffen, der Einfluss auf den Anforderungskatalog hatten. Im Ergebnis konnten einige Anforderungen im Projektkontext nicht weiter berücksichtigt werden:

Überprüfung der Zustimmung von Antragstellenden zur ZSÜ und ggf. damit einhergehende Identitätsprüfung

- **Beschreibung:** Im Rahmen der Anforderungserhebung wurde die Anforderung benannt, dass die Zustimmung der Antragstellenden für eine Antragstellung vorliegen muss. Darauf basierend stellte sich im Projektkontext die Frage, inwiefern diese Zustimmung seitens des Systems geprüft und darauf basierend, inwiefern auch eine Identitätsprüfung dieser Antragstellenden für das System berücksichtigt werden müsste.
- **Argumentation:** Es existieren bereits funktionierende Prozesse seitens der GB, in denen Antragstellende identifiziert und - wo gesetzlich vorgesehen – die Zustimmung zur ZSÜ eingeholt wird.
- **Entscheidung:** Die Verantwortlichkeit für diesen Schritt wird weiterhin in den GB gesehen, sodass eine derartige Prüfung nicht im System abgebildet werden sollte.

Übertragung von Kerndaten über Dokumente im Rahmen der Online-Sicherheitsprüfung

- **Beschreibung**: Im Rahmen der Anforderungserhebung wurden unterschiedliche Bedarfe aufgedeckt, wie eine Übertragung von Informationen – von GB an EKS und umgekehrt - für das System wünschenswert ist. Z. B. wurde seitens des Verfassungsschutzes aufgezeigt, dass eine Übermittlung von Erkenntnissen vorrangig per PDF-Dateien erfolgen könnte.

[10] Insbesondere aus Sicht des Geheimschutzes gilt es den Grundsatz „Kenntnis nur, wenn nötig" einzuhalten, wozu in der Verschlusssachenanweisung als auch im BSI IT-Grundschutz detaillierte Vorgaben gemacht werden.

- **Argumentation:** Um eine standardisierte Übertragung von Informationen über unterschiedliche, technische Komponenten hinweg zu ermöglichen, müssen Daten einheitlich maschinell verarbeitbar sein. Dies kann mit einem Datenstandard mit verbesserter Interoperabilität im Vergleich zur Übertragung von Dokumenten erreicht werden. Zudem würden viele funktionale Anforderungen wie bspw. Suchen nicht hinreichend erfüllt werden können.
- **Entscheidung:** Eine Übertragung von Kerndaten ist über einen Datenstandard abzubilden. Eine Übertragung der Kerndaten in beliebigen anderen Formaten (z. B. PDF) entfällt. Dies schließt die Übertragung von Dokumenten innerhalb des Datenstandards, die im Rahmen der Verfahren anhängig sind, wie beispielsweise Nachweise, nicht aus.

Integration einer Aktenablage oder Anbindung der e-Akte

- **Beschreibung**: Im Rahmen der Anforderungserhebung wurde der Bedarf gemeldet, dass das System optimalerweise selbst eine Aktenablage (inkl. Aktenmanagement) bereitstellt oder dies über die Anbindung der e-Akte ermöglicht.
- **Argumentation**: Als strategisches Produktziel für den Funktionsumfang wurde festgelegt, dass das System sich stark auf die Kernfunktionen fokussieren soll, welche notwendig sind, um die Online-Sicherheitsüberprüfung durchzuführen. Zusätzlich ist eine Anbindung der e-Akte voraussichtlich nicht trivial, da hier Unterschiede in der Handhabung je Bundesland bestehen.
- **Entscheidung**: Eine Aktenablage im System oder die Anbindung der e-Akte wird nicht als Kernfunktion betrachtet.

Integration von alternativen Kommunikationswegen zur Erkenntnisabfrage

- **Beschreibung:** Im Rahmen der Anforderungserhebung wurde der Bedarf gemeldet, dass das System weitere Kommunikationskanäle explizit einbinden soll, sodass auch veraltete technische Anbindung von EKS ermöglicht werden. So bspw. über das Behördenpostfach, eine E-Mail oder gar ein e-Fax, Erkenntnisse abgefragt werden können.
- **Argumentation:** Ziel ist es, eine moderne und insb. sichere Datenübertragung zu implementieren. Des Weiteren soll sich der Umfang des Systems klar auf Kernfunktionen fokussieren, um ein schlankes, generisches und wartungsarmes Gesamtsystem bereitzustellen.

- **Entscheidung:** Erkenntnisse werden über eine einheitliche, hoch abgesicherte technische Schnittstellenanbindung abgefragt.

Bereitstellung einer Funktion zur Gebührenabrechnung

- **Beschreibung:** Im Rahmen der Anforderungserhebung wurde der Bedarf einer Funktion zur optionalen Berechnung, Abrechnung und Dokumentation von Gebühren gemeldet.
- **Argumentation:** Da auch andere Verfahren – abseits von OSiP – den Bedarf einer Gebührenabrechnung in der Vergangenheit zeigten, wird es als sinnhafter erachtet, dass die zentrale Umsetzung einer derartigen Komponente außerhalb des Systems erfolgt, sodass eine Anbindung erfolgen kann.
- **Entscheidung:** Es wird keine Gebührenabrechnung als originäre Funktionalität geben.

Der Umfang der funktionalen Anforderungen kann im weiteren Projektverlauf, vor allem im Rahmen der Umsetzungsphase, auf Basis einer sich stetig weiterentwickelnden Produktstrategie noch Änderungen unterliegen.

3.2.2.4 Zukunftsvisionen

Die Kategorie Zukunftsvisionen beschreibt Erweiterungen, die in der vorliegenden Konzeption noch nicht berücksichtigt werden können. Abhängig von der Entwicklung der Produktstrategie könnten sie in folgenden Phasen der Weiterentwicklung des Produktes Berücksichtigung finden.
Die genannten Anforderungen umfassen dabei Folgendes:

- Eine Web-Vorbefragung mit Upload-Checklisten, um Unterlagen strukturiert zusammenzustellen, ohne einen vollständigen Online-Antrag ausfüllen zu müssen.
- Ein Nachreichungs-Modul, über das fehlende Nachweise oder Informationen durch die GB eingefordert und durch AES hochgeladen werden können.
- Die Nutzung eines eindeutigen Identifikationsmerkmals (z.B. Steuer-ID) könnte in Zukunft zum einen die Identifikation der zu prüfenden Personen über den gesamten Prozess erleichtern und zum anderen dazu dienen, mit nur wenigen Nutzendeninformationen, alle weiteren relevanten Informationen und Nachweise über Register zu beziehen.
- Für die Antragsprüfung könnte eine Registeranbindung mit täglichem Abgleich zur Validierung und Dublettenprüfung geplant werden (z. B. mit Bewacherregister).

- Weitere prozessuale Schritte, wie die Planung und Dokumentation von Präsenzterminen für Sprach- und Echtheitsprüfungen könnten digital abgebildet und ergänzt werden.
- Entscheidungen könnten in Zukunft durch KI-basierte Prüfmechanismen ergänzt und unterstützt werden, um komplexe Bewertungen automatisiert vorzubereiten.
- Für die Bescheiderstellung ist die Integration von Quick Response (QR) -Verifikation und Revocationslogik eine mögliche Weiterentwicklungsstufe. Die QR-Verfikation würde in diesem Fall dazu dienen, dass ein QR-Code fälschungssicher gestaltet wird und dieser QR-Code im Rahmen einer Revocationslogik als ungültig erklärt werden kann, wenn die positive Bescheidung der ZSÜ zurückgenommen werden würde.
- Die digitale Unterstützung umfangreicher Sicherheitsüberprüfungen nach dem Ü1–Ü3-Modell könnte eine zukünftige Erweiterung der inhaltlichen Bandbreite von NEOSiP darstellen.

3.2.3 Wesentliche Erkenntnisse nicht-funktionaler Anforderungen

Die Erkenntnisse der nicht-funktionalen Anforderungen werden im Folgenden für die Bereiche Architektur, IT-Sicherheit, Geheimschutz sowie Compliance und Datenschutz dargestellt. Insgesamt wurden 272 nicht-funktionale Anforderungen aufgenommen, welche im Detail dem Begleitdokument „Anforderungsliste" zu entnehmen sind. In diesem Begleitdokument ist im Bereich „Quellen" einsehbar, welche Stakeholderbefragungen, Gesetze, Richtlinien und Standards zur Ableitung der Anforderungen gesichtet und geprüft wurden.

3.2.3.1 Architektur

Wesentliche Aspekte der ausgearbeiteten Anforderungen, die im Rahmen der Architekturentscheidungen und der Architekturkonzeption Berücksichtigung gefunden haben, sind Folgende:

IT-Governance: Im Rahmen der IT-Governance sollen verbindliche Architekturleitplanken festgelegt, sowie das Architekturkonzept und die Architekturentscheidungen kontinuierlich dokumentiert werden.

Systemgrenzen: Die Architektur muss klare Schnittstellen zwischen den beteiligten Akteuren definieren, um eine saubere Trennung der Verantwortlichkeiten zu gewährleisten. Zentral ist dabei die Entkopplung der Transportinfrastruktur (TI) und der fachlichen Anwendungen. Ergänzend dazu besteht die Anforderung, ein zentrales Fachverfahren als Standardlösung für GB bereitzustellen, die über keine eigenen Systeme zur Anbindung verfügen.

Architekturprinzipien: Zentrale Prinzipien, wie der durchgängige Zero-Trust-Ansatz[11] (siehe Kapitel 3.2.4 und 4.5.4), dem API-First-Konzept und einem modularen Aufbau zur Sicherstellung von Wartbarkeit und Erweiterbarkeit sollen mit Blick auf die Entwicklung einer Zielarchitektur eingehalten werden.

Schnittstellen und Interoperabilität: Im Rahmen der Architekturkonzeption soll berücksichtigt werden, dass alle Funktionen über standardisierte, dokumentierte Schnittstellen (APIs) bereitgestellt werden, wodurch Interoperabilität, Wiederverwendbarkeit, eine einfache Integration in andere Systeme und damit eine weitreichende Nachnutzung gewährleistet sind. Ein modularer Aufbau soll die flexible Anpassung und Erweiterbarkeit der Architektur sicherstellen, ohne die Stabilität des Gesamtsystems zu gefährden. Alle Schnittstellen sollen auf offenen, aktuellen Standards und Protokollen zum Datenaustausch basieren und dokumentiert sein. Um eine reibungslose Kommunikation zwischen technischen Komponenten zu ermöglichen, soll ein eigener Datenstandard entwickelt und evtl. als XÖV-Standard publiziert werden, was in der Handlungsempfehlung in Kapitel 6.1 näher ausgeführt wird. Das System soll durch technische Unterstützungsmechanismen wie bspw. Software Development Kits (SDKs) im Datenaustausch maschinenlesbare Schemas erzwingen, sowie deren Validierung unterstützen. SDKs sind vorkonfigurierte Entwickler:innenpakete, die Bibliotheken, Schnittstellen und Beispielcode enthalten und die Anbindung an die System-APIs des NEOSiP-Systems für EKS und GB vereinfacht. Fehlerzustände im Rahmen der Validierung sollen innerhalb des automatisierten Informationsaustauschs zwischen Maschinen strukturiert überwacht und gemeldet werden. SDKs sollen in gängigen Programmiersprachen bereitgestellt werden.

Multimandantenfähigkeit: Die Architektur muss Mandantenfähigkeit sicherstellen, um Bund, Länder- und Kommunalorganisationen auf der einen Seite mit klarer Datentrennung zu unterstützen und gleichzeitig ein übergreifendes Reporting zu ermöglichen. Dabei soll das System zwischen mandantenabhängigen und mandantenübergreifenden Daten und Objekten unterscheiden. Der Begriff „Mandant" muss dabei eindeutig festgelegt werden (siehe Kapitel 3.2.3.4). Wünschenswert seitens der Anforderungsstellenden ist, dass der Betrieb eines Fachverfahrens im Grunde zentral erfolgt, dennoch soll ein dezentraler Betrieb für einzelne Länder technisch unterstützt werden. Der Support durch den zentralen Betreiber beschränkt sich hier lediglich auf die Nachnutzung des bereitgestellten Fachverfahrens.

[11] Ggf. sind bei der Umsetzung im Detail Anforderungen aus dem Geheimschutz zu den jeweiligen Themenbereichen zu berücksichtigen.

Skalierbarkeit & Hochverfügbarkeit: Anforderungen in diesem Bereich sollen sicherstellen, dass das System auch unter hoher Last zuverlässig und sicher betrieben werden kann und verfügbar ist, sodass die Kontinuität sicherheitskritischer Prozesse und eine stabile Systemperformance gewährleistet werden. Das System soll auch bei wachsender Mandantenzahl verfügbar und wartbar bleiben.

Systembetrieb & Administration: Im Rahmen des Systembetriebs und der Administration sollen kritische Operationen durch Sicherungsmechanismen für die Authentifizierung[12], Löschung und Wiederherstellung von Daten sowie eine feingranulare Zugriffskontrolle abgesichert werden. Zur Unterstützung des Betriebs sollten aussagekräftige Fehlermeldungen vorgesehen werden, die keine sensiblen Informationen preisgeben und eine schnelle Fehleranalyse ermöglichen.

Entwicklung & Qualitätssicherung: Der Bereich Entwicklung & Qualitätssicherung definiert zentrale Grundsätze für eine sichere, standardisierte und zukunftsfähige Softwareentwicklung. Eigenentwickelter Code soll – soweit möglich – als Open Source zur öffentlichen Begutachtung und Nachnutzung bereitgestellt werden.

Für das Deployment sollen automatisierte Continues Integration/Continues Delivery (CI/CD)-Pipelines vorgesehen werden, die eine klare Trennung von Entwicklungs-, Test-, Staging- und Produktionsumgebungen sicherstellen.

Usability & Barrierefreiheit: Der Bereich Usability & Barrierefreiheit stellt sicher, dass die Systemnutzung für alle Zielgruppen intuitiv, zugänglich und normenkonform erfolgt. Frontends sollen vorrangig als desktopoptimierte Nutzer:innenoberflächen konzipiert werden, erlauben durch responsives Design jedoch die Nutzung für unterschiedliche Endgeräte[13]. Die Gestaltung folgt einem klaren, leicht erlernbaren Interaktionskonzept und erfüllt die Anforderungen der Web Content Accessibility Guidelines (WCAG 2.1 AA) sowie nationaler Barrierefreiheitsnormen.

Datenmigration: Anforderungen des Bereichs Datenmigration stellen sicher, dass der Übergang von Altsystemen zur neuen Lösung effizient, sicher und ohne Datenverlust erfolgt. Das System soll eine automatisierte, skalierbare und fehlerfreie Migration sämtlicher relevanter

[12] Auch bekannt als Zwei-Faktor-Authentisierung (2FA) oder Mehrfaktorauthentisierung (MFA) und eine der wesentlichen Anforderungen des Geheimschutzes, siehe auch Kapitel 3.2.3.3.
[13] Responsives Verhalten kann in der Umsetzungsphase nur in dem Ausmaß berücksichtigt werden, das bei möglicher Umsetzung von Geheimschutzanforderungen möglich ist.

Datenbestände ermöglichen und die Einhaltung fachlicher und technischer Erfordernisse gewährleisten.

Governance Koordination & Produktmanagement: Anforderungen im Bereich Governance, Koordination & Produktmanagement stellen die zentrale, strategische Steuerung, die transparente Zusammenarbeit und die nachhaltige Begleitung der Weiterentwicklung und des Betriebs des Systems sicher. Der Fokus soll dabei auf transparenter Information und kontinuierliche Einbeziehung aller relevanten Stakeholder für die weitere Konzeptions-, Umsetzungs-, Test-, Rollout- und Betriebsphase liegen. Ziel soll es sein, standardisierte, nachvollziehbare Prozesse zu etablieren und zu dokumentieren.

Routing & Transport: Anforderungen im Bereich Routing & Transport betreffen die regelkonforme, manipulationssichere Adressierung und Zustellung von Anfragen. In diesem Rahmen sollen Routing-Regeln festgelegt und über einen festgelegten Prozess gepflegt werden. Der Transport von Daten soll diesen zentral hinterlegten Regeln zwingend folgen. Die Protokollierung von Änderungen an Routing-Regeln soll Nachvollziehbarkeit, Auditierbarkeit und revisionssichere Governance gewährleisten.

3.2.3.2 IT-Sicherheit

Aufgrund der Kritikalität der im System verarbeiteten Informationen ist die IT-Sicherheit ein wichtiger Schlüsselfaktor für die Funktionsfähigkeit und Verlässlichkeit des Gesamtsystems.

Für die künftig im System verarbeiteten Informationen wird mindestens ein hoher Schutzbedarf angenommen. Diese Annahme stützt sich auf die Einschätzung des Informationssicherheitsbeauftragten der FITKO und lässt sich aus der Informationssicherheitsleitlinie der FITKO ableiten. Inhaltlich basiert sie insbesondere auf der geplanten Art, dem vorgesehenen Umfang und dem Einsatzzweck der Datenverarbeitung bzw. Nutzung der Informationen. Diese Schutzbedarfsannahme bildet die Grundlage für die nachfolgend dargestellten Anforderungen.

Zur Umsetzung des IT-Grundschutzes auf Basis von ISO/IEC 27001 ist für das NEOSIP-System ein IT-Sicherheitskonzept mit risikobasierten Sicherheitsmaßnahmen zu erstellen. Das Sicherheitskonzept beinhaltet eine Definition des Informationsverbunds, eine Strukturanalyse,

eine Schutzbedarfsfeststellung, eine Modellierung, einen IT-Grundschutz-Check, eine Risikoanalyse und einen Umsetzungsplan[14].

Bei externer Vergabe des Betriebs hat der IT-Dienstleister die hohen Anforderungen während der gesamten Vertragslaufzeit zu erfüllen. Der IT-Dienstleister hat ein gültiges ISO-27001-Zertifikat auf Basis von IT-Grundschutz vorzulegen und während der gesamten Vertragslaufzeit aufrechtzuerhalten. Der Zertifikatsgeltungsbereich umfasst den VN-TNA-Anschluss (Anbindung an das Verbindungsnetz des Bundes) und dient als Nachweis der technischen und organisatorischen Maßnahmen gem. Art. 32 DSGVO. Ist der IT-Dienstleister direkt an das Verbindungsnetz angeschlossen, hat er die dafür geltenden sicherheitstechnischen Vorgaben zu erfüllen. Das Rechenzentrum bzw. der für das NEOSiP-System genutzte Bereich ist als hochsichere Zone auszuweisen und innerhalb dieser Zone zu betreiben. Dies gilt mindestens für die NEOSiP-TI, da über sie der Datenaustausch zwischen Bund und Ländern erfolgt.

Dabei werden weitere Sicherheitsanforderungen von GB und EKS berücksichtigt. Dies betrifft insbesondere den Fall einer vorgesehenen Verarbeitung von Verschlusssachen. In diesem Fall sind die Vorgaben zum Geheimschutz maßgeblich - siehe hierzu Kapitel 3.2.3.3 Geheimschutz.

Um Anforderungen an den Datenschutz auch technisch umzusetzen, unterstützt das System die sichere Speicherung von Informationen (z.B. personenbezogene Daten, Protokolldaten und Metadaten). Dies erfolgt unter Einhaltung der gesetzlichen sowie ergänzend fachlich festgelegten Mindest- und Höchstaufbewahrungsfristen. Näheres ist in Kapitel 3.2.3.4 beschrieben.

Kern des Systems ist der abgesicherte Informationsaustausch zwischen GB, EKS und weiteren Stellen über verschlüsselte Kommunikationskanäle[15]. Damit ist das System mandantenfähig und stellt eine strikte Datenisolation sicher:

Um bei der Übertragung neben Vertraulichkeit, auch die Authentizität und Integrität sicherzustellen, wird „Authenticated Encryption" genutzt. Insgesamt werden ausschließlich starke und öffentlich geprüfte Algorithmen verwendet[16]. Das Schlüsselmanagement umfasst

[14] Hinsichtlich VS sind bei der Umsetzung des IT-Grundschutzes auch die dortigen Vorgaben zum Geheimschutz (im Prozess-Baustein CON.11.1) zu berücksichtigen sowie die der VSA und ggf. weiterer Anforderungsdokumente, siehe Kapitel 3.2.3.3.
[15] Hinsichtlich der Verschlüsselung ist sich an der BSI TR-02102 „Kryptographische Verfahren: Empfehlungen und Schlüssellängen" zu orientieren.
[16] Um VS angemessen zu schützen, sind nur kryptografische Verfahren erlaubt, die den Anforderungen der Technischen Richtlinie des BSI (BSI TR-02102) genügen und somit freigegeben sind.

den gesamten Lebenszyklus von Generierung, Rotation, Widerruf und Löschung und wird zentral in einem Krypto-Kataster dokumentiert.

Das System verfügt über ein Identitäts- und Berechtigungsmanagement, das an die Geschäftsprozesse, Organisationsstrukturen und den hohen Schutzbedarf angepasst ist. Der Grundsatz „Kenntnis nur, wenn nötig" ist hierbei maßgeblich. Das System setzt diese Anforderungen durch ein föderiertes Identitätsmanagement (Federated IAM) um, dass die dezentrale Nutzerverwaltung der beteiligten Behörden anbindet und respektiert. Die Authentifizierung (Identitätsfeststellung) erfolgt im Hoheitsbereich der entsendenden Behörde.

Dabei muss die Funktionstrennung sicherstellen, dass kein Nutzer:innenkonto mehrere Rollen erhält und kritische Aufgaben nicht durch Einzelkonten ausgeführt werden können. Die Rechte werden immer nach dem Prinzip der minimalen Rechte vergeben, sodass Konten nur genau über die Rechte verfügen, die sie zur Ausübung der vorgesehenen Tätigkeiten benötigen. Auch Administrationsaufgaben sind rollenbasiert vergeben und Administrationskonten verfügen über keine übergreifenden Berechtigungen. Dabei erfolgen kritische Tätigkeiten nach dem Vier-Augen-Prinzip. Zur Gewährleistung der Nachvollziehbarkeit sind alle Nutzer:innenkennungen eindeutig einem Mandanten oder Administrator:innen zugeordnet und durch Mehr-Faktor-Authentisierung geschützt. Dagegen authentifizieren sich Maschinen und APIs zertifikatsbasiert.

Das Netz des Systems ist an das Verbindungsnetz des Bundes oder ein gleichwertig gesichertes Netz angebunden und in verschiedene Segmente eingeteilt (siehe Kapitel 1.4). Die Netzarchitektur umfasst interne Netze, eine demilitarisierte Zone und -Anbindungen an externe Netze.

Alle sicherheits- und systemrelevanten Ereignisse müssen chronologisch und manipulationssicher protokolliert werden. Protokolldaten werden unveränderbar, vollständig signiert und verschlüsselt an eine zentrale Stelle zur Speicherung übermittelt. Die Grundsätze der Zweckbindung und Datenminimierung sowie der Beschäftigtendatenschutz werden eingehalten.

Das System wird kontinuierlich überwacht, um Sicherheitsereignisse und Systemzustände zentral zu detektieren. Zentrale Monitoring- und Logging-Funktionen ermöglichen eine effiziente Überwachung und die Bereitstellung von Performance-Kennzahlen. Das System speichert regelmäßig Konfigurationsdaten, Antragsentwürfe und Systemzustände als Backups. Alle Backups sind verschlüsselt, mandantengetrennt und revisionssicher.

Vor der Produktivsetzung des Systems erfolgen umfassende Sicherheitsprüfungen, bei denen ggf. identifizierte Schwachstellen vollständig behoben werden.

3.2.3.3 Geheimschutz

Bei möglicher Verarbeitung sicherheitsrelevanter Informationen[17] im Rahmen von Sicherheitsüberprüfungen ergibt sich die Notwendigkeit, Geheimschutzanforderungen – soweit einschlägig – einzubeziehen. Die Sicherheitsüberprüfungen können zumindest teilweise Erkenntnisse beinhalten, die als VS eingestuft sind, sodass neben den Anforderungen des Datenschutzes (DSGVO) und der Informationssicherheit (z. B. aus ISO 27001 bzw. IT-Grundschutz) auch die des Geheimschutzes berücksichtigt werden müssen. Die Einstufung dieser VS wird dabei voraussichtlich den Grad VS-NfD nicht übersteigen. Somit muss NEOSiP prinzipiell sicherstellen, dass es die vertrauliche Handhabung von VS (vorrangig hinsichtlich der Übertragung zwischen den beteiligten Stellen) technisch ermöglicht.[18] Dazu ist stets der Grundsatz „Kenntnis nur, wenn nötig" einzuhalten.

Die allgemeinen Anforderungen des Geheimschutzes werden neben dem Prozessbaustein CON.11.1 des IT-Grundschutzes vor allem durch die Verschlusssachenanweisung (VSA) und deren Anlagen – für VS-NfD insbesondere Anlage V („VS-NfD-Merkblatt") – geregelt. Da es sich bei NEOSiP um eine digitale Verarbeitung im Rahmen einer Webanwendung handelt, sind vor allem die hier gemachten Vorgaben zur VS-IT zu berücksichtigen. Zudem sind Technische Richtlinien (TR) des BSI hierfür einschlägig, beispielsweise hinsichtlich kryptografischer Verfahren: BSI TR-02102. Zusätzlich zu den TR des BSI gibt es weitere spezifische Dokumente wie z. B. VS-Anforderungsprofile, die u. a. konkrete Anforderungen an IT-Produkte/-Systeme stellen. Da das NEOSiP-System selbst ein IT-Fachverfahren ist bzw. teilweise auf andere IT-Fachverfahren zurückgreift, sind zumindest einige Anforderungsprofile einschlägig.

Das Anforderungsprofil „E-Mail und Dateiaustauschverschlüsselung" (BSI-VS-AP-0014) wird für NEOSiP nicht herangezogen, dass es die SaaS-spezifische Ausprägung von NEOSiP nicht abbildet:

„Bei der E-Mail- und Dateiaustauschverschlüsselung handelt es sich unter Umständen um zwei verschiedene Anwendungsfälle: E-Mail-Verschlüsselung einerseits und Dateiaustausch-Verschlüsselung andererseits. […] Die klassische E-Mail-Verschlüsselung erfolgt von Client zu Client (E2EE). Bei der Client-basierten E-Mail-Verschlüsselung verschlüsselt und signiert das

[17] Handlungsbedarf zu Festlegung in Kapitel **Fehler! Verweisquelle konnte nicht gefunden werden.** adressiert.
[18] Sollten weitere Aspekte, wie z.B. die Speicherung (Aufbewahrung) von VS, hinzukommen, so sind ggf. weitere Maßnahmen zu treffen, um zusätzliche Anforderungen aus dem Geheimschutz zu erfüllen.

entsprechende Produkt auf dem Client-Rechner des Absenders die E-Mail vor dem Versenden. […] Auch die Dateiaustausch-Verschlüsselung ist ein auf dem Client-Rechner installiertes Softwareprodukt, mit der es möglich ist, einzelne Dateien oder gesamte Ordner zu verschlüsseln und mit einem Integritäts- und Authentizitätsschutz zu versehen. Derartig verschlüsselte und geschützte Dateien können dann bspw. als Anhang einer unverschlüsselten E-Mail oder über einen Daten-Server ohne weitere Sicherheitsvorkehrungen versendet bzw. ausgetauscht werden."

Stattdessen wird das VS-Anforderungsprofil „Sicherer Messenger und Videokonferenzsysteme" (BSI-VS-AP-0024) herangezogen:

„Ein Sicherer Messenger und Videokonferenzsysteme (SM/VC) ist ein Produkttyp, der für den sicheren Austausch von als VS-NfD klassifizierten Daten zwischen Nutzer:innengeräten wie Smartphones oder PCs verwendet wird. Der Hauptunterschied zwischen dem Produkttyp SM/VC und anderen sicheren Diensten zur Kommunikation, zum Beispiel Email- oder Dateiverschlüsselung, ist, dass es nicht die zugrundeliegende Hardwaretechnologie der Endgeräte ist, sondern im SM/VC eine integrierte Infrastruktur zum Nutzer:inmanagement existiert, die es Nutzer:innen erlaubt die Authentizität anderer Nutzer:innen zu verifizieren. Um dies zu erreichen, bietet der SM/VC eine E2EE zwischen den Nutzer:innengeräten, die auch als Endgeräte bezeichnet werden."

Da das NEOSiP-System weder ein typischer Messenger noch ein Videokonferenzsystem ist, ist das Anforderungsprofil „Sicherer Messenger und Videokonferenzsysteme" (VS-AP-0024) nur teilweise anwendbar, sodass manche Anforderungen nicht beachtet werden oder im Zweifel nur sinngemäß verfahren wird.

Darüber hinaus ist unter Umständen das Anforderungsprofil „Digitales Labelling" (BSI-VS-AP-0023) relevant. Es stellt Vorgaben zur Kennzeichnung elektronischer VS (siehe auch VSA, Anlage V, Nr. 4) bei Verwendung eines digitalen Labellings auf. Da die sicherheitsrelevanten Informationen in Form von Erkenntnissen durch die entsprechenden Erkenntnisbehörden mit ihren jeweiligen Fachverfahren bereitgestellt werden (siehe Kapitel 3.1.2.1) erfolgt auch die Einstufung als VS durch diese. Somit sind die Erkenntnisbehörden in der Verantwortung, die VS ordnungsgemäß zu kennzeichnen, bevor diese durch NEOSiP übertragen werden. Je nach Art und Weise der Kennzeichnung, sollte NEOSiP jedoch in der Lage sein, das digitale Labelling gemäß BSI-VS-AP-0023 technisch zu unterstützen, wenn dies seitens der Erkenntnisbehörden verwendet wird.

Weitere Anforderungsprofile, die relevant sind, aber voraussichtlich durch bereits freigegebene IT-Produkte abgedeckt und somit nicht selbst entwickelt werden müssen, sind „Key-

Management-Software“ (BSI-VS-AP-0027), „Hardware-Sicherheitsmodule“ (BSI-VS-AP-0002) oder auch „Hardware-Sicherheitsanker“ (BSI-VS-AP-0022). Entsprechende IT-Produkte wären zu beschaffen und in NEOSiP zu integrieren, wo erforderlich und technisch möglich. Sie werden vor allem hinsichtlich der Verschlüsselung und der Authentisierung/Authentifizierung eingesetzt. Sofern weitere Produkte wie bspw. Firewalls (siehe auch BSI-VS-AP-0018) eingesetzt werden sollen, ist ähnlich zu verfahren. Entsprechend freigegebene Produkte sind in der BSI-Schrift 7164 „Liste der zugelassenen IT-Sicherheitsprodukte und -systeme“ zu finden.

Da es sich bei NEOSiP um ein IT-System in Form eines SaaS-Modells handelt (siehe Kapitel 3.1.2.2), werden vorwiegend technische Maßnahmen umgesetzt, wodurch das Prinzip der mehrschichtigen Sicherheit nur bedingt umgesetzt werden kann, um den Grundsatz „Kenntnis nur, wenn nötig“ einzuhalten. NEOSiP stellt daher primär sicher, dass während der Übertragung der Zugriff auf VS nur für befugte Personen möglich ist. Ist jedoch unter Umständen ein Zugriff auf VS durch Personen erforderlich, die ansonsten nicht mit der Bearbeitung von VS betraut sind, sind diese Personen z. B. entsprechend zu verpflichten bzw. zu belehren. Dabei handelt es sich um eine organisatorisch-personelle Maßnahme, die durch NEOSiP nicht selbst erbracht werden kann. Dies ist grundsätzlich auch in anderen Fällen denkbar, bspw. hinsichtlich der Sicherheitsmaßnahmen bei Endgeräten oder Servern. Für organisatorische und personelle oder auch bauliche Geheimschutzmaßnahmen gemäß VSA und IT-Grundschutz sind somit letztlich beteiligte Dritte (wie Betreiber, Erkenntnisstellen, Genehmigungsbehörden, Nutzer etc.) verantwortlich, da diese eben nicht gänzlich von der NEOSiP-IT-Architektur berücksichtigt werden können und somit außerhalb der Verantwortung von NEOSiP liegen.

Daher gelten für beteiligte Dritte z. B. folgende Anschlussbedingungen:

- Die eingesetzten Endgeräte erfüllen die Anforderungsprofile „Sichere Mobile Lösung“ (BSI-VS-AP-0003) und „Sicherer VS-Arbeitsplatz“ (BSI-VS-AP-0007).
- Die verwendeten Webbrowser richten sich nach dem Mindeststandard des BSI zu Webbrowsern.
- Ggf. Erfüllung von System-Bausteinen aus „INF: Infrastruktur“ des IT-Grundschutzes etwa bei eingesetzten Rechenzentren/Servern.

Diese Verantwortung von Dritten muss deshalb seitens des Projektmanagements in den Vertragsunterlagen, u.a. in den Ausschreibungsunterlagen anhand von Anschlussbedingungen etc., sowie der Kommunikation und Kooperation mit diesen berücksichtigt werden.

3.2.3.4 Compliance & Datenschutz

Im System sind im Sinne der Compliance die einschlägigen fachgesetzlichen Anforderungen zur Sicherheitsprüfungen (Bund/ Länder) einschließlich behördenspezifischer/ länderspezifischer Ausprägungen durch geeignete technische Funktionen zu berücksichtigen.

Datenschutz ist ein wesentlicher Erfolgsfaktor für die Akzeptanz des Systems, da umfangreich personenbezogene Daten, darunter auch sensible Angaben zu Personen verarbeitet und gespeichert werden. Maßgeblich hierbei sind die Anforderungen der DSGVO. Das System hat die Einhaltung der DSGVO von Beginn an durchgängig nach den Prinzipien Datenschutz durch Technikgestaltung (*Data Protection by Design)* und Datenschutz durch datenschutzfreundliche Voreinstellungen (*Data Protection by Default)* sicherzustellen - von der Datenverarbeitung bis zur Kommunikation zwischen den Systemkomponenten. Die Umsetzung dieser Prinzipien erfolgt insbesondere anhand der Datenschutzgrundsätze Zweckbindung, Datenminimierung und Speicherbegrenzung.

Das System stellt sicher, dass personenbezogene Daten ausschließlich für die jeweils festgelegten Verarbeitungszwecke verarbeitet und auf das notwenige Maß beschränkt werden. Die Verarbeitungszwecke werden gemäß den einschlägigen Fachgesetzen festlegt. Die technische Umsetzung erfolgt insbesondere durch datenschutzfreundliche Voreinstellungen und restriktive Gestaltung der Eingabefelder. Sensible Funktionen oder erweiterte Datenzugriffe sind im System standardmäßig deaktiviert und werden erst nach ausdrücklicher Freigabe aktiviert.

Pflichtfelder sind technisch auf die für die jeweilige Sicherheitsüberprüfung erforderlichen, personenbezogenen Daten beschränkt. Weitergehende Angaben bleiben optional oder technisch ausgeschlossen. Personenbezogene Daten werden in Formularen nicht automatisch vorbefüllt, sondern nur nach aktiver bzw. manueller Nutzer:innenaktion eingetragen.[19]

Das System erlaubt Such- und Auswahlfunktionen ausschließlich auf Basis vordefinierter, rechtlich zulässiger Kriterien basieren. Freies und ungezieltes Suchen sind ausgeschlossen. Ebenso erfolgt die Datenübermittlung ausschließlich anhand vordefinierter und zulässiger Parameter, wodurch datenschutzkonforme Datenflüsse auch über Systemgrenzen hinweg sichergestellt werden.

[19] Zulässig sind lediglich Adressvorschläge aus einem Geo-/ Adressdienst nach Nutzer:inneneingabe (z. B. ab drei Zeichen), wobei die Adresse erst nach expliziter Auswahl in das Feld übernommen wird.

Der Grundsatz der Speicherbegrenzung wird durch ein Löschkonzept abgebildet, dessen Löschregelungen systemseitig durch entsprechende Löschroutinen umgesetzt werden.

In Log-, Diagnose- oder sonstigen technischen Protokolldaten können personenbeziehbare Metadaten enthalten sein (z. B. Benutzerkennung, Rolle der Sachbearbeitung, Client-Adresse, Gerätekennung). Personenbezogene Daten aus den jeweiligen Fachverfahren (Antragsdaten) sind hiervon nicht umfasst. Die technische Protokollierung personenbeziehbarer Metadaten dient ausschließlich technischen oder sicherheitsrelevanten Zwecken. Der Umfang ist auf das notwendige Minimum beschränkt. Zudem werden für diese protokollierten Metadaten systemseitig Löschfristen definiert und technisch umgesetzt. Die Löschung erfolgt automatisiert nach Ablauf der jeweils festgelegten Aufbewahrungsdauer. Die Definition der Aufbewahrungszeiten bzw. Löschfristen orientiert sich an den zugrunde liegenden, rechtlichen und betrieblichen Erfordernissen. Dabei wird zwischen technischen System- und Sicherheitsprotokollen sowie revisionsrelevanten Protokollen unterschieden. Erstere erfassen insbesondere betriebs- und sicherheitsrelevante Ereignisse sowie Nutzer:innenaktivitäten und Zugriffe, um den ordnungsgemäßen Systembetrieb sicherzustellen und unberechtigte Zugriffe erkennen zu können. Letztere dokumentieren dagegen vor allem administrative Tätigkeiten, Änderungen an Berechtigungen und Systemeinstellungen und dienen der Nachvollziehbarkeit sowie der Erfüllung von Compliance-Anforderungen.

Das System stellt sicher, dass die durch die Sachbearbeiter:in festgelegte Schutzbedürftigkeit einer Information technisch mitgeführt und eindeutig gekennzeichnet wird. Dadurch bleibt die Schutzstufe im gesamten Prozess der Übermittlung von personenbezogenen Daten erhalten und wird bei der Weitergabe an EKS und GB verlässlich ausgewiesen. Darüber hinaus ermöglicht das System die Korrektur bzw. Berichtigung von personenbezogenen Daten, ohne die Integrität oder Nachvollziehbarkeit des ursprünglichen Datenbestands zu beinträchtigen. Änderungen dürften ausschließlich von hierzu berechtigten Rollen vorgenommen werden. Die Vergabe und Kontrolle dieser Berechtigungen erfolgt über das zentrale Zugriffs- und Berechtigungsmanagement, um unbefugte Änderungen oder Manipulationen wirksam zu verhindern.

Sofern die Voraussetzungen nach Art. 35 DSGVO erfüllt sind, ist für die mit dem System verbundenen Datenverarbeitung eine Datenschutz-Folgenabschätzung (DSFA) durchzuführen. Im Rahmen der DSFA werden Datenschutzrisiken, die sich aus der Verarbeitung von besonders sensiblen Daten im jeweiligen Verfahren ergeben können, systematisch ermittelt und bewertet. Daraus werden geeignete technische und organisatorische Maßnahmen abgeleitet.

Das System ist so ausgelegt, dass die für die DSFA erforderlichen Informationen strukturiert, nachvollziehbar und schnell abrufbar sind.

Das System unterstützt die Umsetzung der Betroffenenrechte nach DSGVO (Art. 12 bis 22) durch technische Funktionen zur Anzeige, Änderung, Einschränkung, Löschung und zum Export von Datensätzen im Rahmen der E2EE. Die fachliche und rechtliche Umsetzung von Betroffenenanfragen, einschließlich Prüfung, Entscheidung und Dokumentation, obliegt den jeweils zuständigen GB. Kennzeichnungen von Erkenntnissen, die durch die EKS vorgenommen werden, werden systemseitig abgebildet und bei Auskunft, Export und Protokollierung berücksichtigt.

3.2.4 Zero Trust

Im Rahmen der Untersuchung wird das Sicherheitsparadigma Zero Trust als zentrales Leitprinzip für die Ausgestaltung der NEOSiP-Zielarchitektur betrachtet. Zero Trust stellt einen bewussten Gegenentwurf zu klassischen, perimeterbasierten Sicherheitsmodellen dar, bei denen von der Vertrauenswürdigkeit innerhalb des eigenen Netzes ausgegangen wird. Diese implizite Annahme wird im Rahmen des Zero-Trust-Modells in Frage gestellt und erweist sich somit insbesondere im föderalen, organisationsübergreifenden Kontext von NEOSiP als tragfähig, da eine Vielzahl unterschiedlicher Akteure, Netze und Betriebsverantwortlichkeiten eingebunden ist.

Das BSI beschreibt ein Integrationsmodell, das Zero Trust nicht als einzelne technische Maßnahme, sondern als ganzheitliches Architekturprinzip versteht[20]. Das Modell gliedert sich in die Säulen Identität, Gerät, Netz, Anwendung und Daten, und hebt „Detektion und Reaktion" explizit als querschnittlichen Bestandteil hervor, der die ersten 4 Säulen durchzieht.

Aus dem Zero-Trust-Ansatz ergeben sich grundlegende Annahmen, die für NEOSiP als verbindlich betrachtet werden. Zentrales Prinzip ist der Verzicht auf implizites Vertrauen, vor allem über Netzgrenzen, Systemzugehörigkeiten oder organisatorischen Kontexte hinaus. Jeder Zugriff auf Funktionen oder Daten muss unabhängig vom Ursprungsnetz geprüft werden. Identität, Autorisierung und Datenzugriff sind dabei strikt voneinander zu trennen. Vertrauensentscheidungen erfolgen kontextabhängig und sind zeitlich begrenzt, dauerhafte oder pauschale Vertrauensannahmen sind somit zu vermeiden.

[20] vgl. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeLeitlinien/Zero-Trust/Zero-Trust_04072023.pdf?__blob=publicationFile&v=4

Hieraus lassen sich zentrale Anforderungen an die Zielarchitektur ableiten. Sämtliche Nutzer:innen und Systeme müssen jederzeit eindeutig identifizierbar sein. Für jede sicherheitsrelevante Aktion sind Authentifizierung und Autorisierung erforderlich. Die Architektur muss so gestaltet sein, dass Vertrauensdomänen möglichst klein gehalten und laterale Bewegungen innerhalb des Systems minimiert werden. Das Least-Privilege-Prinzip ist konsequent umzusetzen, sodass Akteure ausschließlich die für ihre jeweilige Aufgabe notwendigen Rechte erhalten.

Ein wesentlicher Bestandteil des Zero-Trust-Modells ist die klare Trennung zwischen Entscheidungs- und Durchsetzungsebene. Entscheidungen darüber, ob ein Zugriff zulässig ist, werden an definierten Policy Decision Points getroffen, während deren technische Durchsetzung durch Policy Enforcement Points erfolgt. Diese Trennung ermöglicht eine konsistente, nachvollziehbare und zentral steuerbare Zugriffskontrolle, die auf verschiedenen Ebenen der Architektur technisch wirksam ist.

Darüber hinaus betont das BSI die Bedeutung von Detektion und Reaktion für den Betrieb von Zero-Trust-Architekturen. Sicherheitsrelevante Ereignisse müssen kontinuierlich überwacht werden, um Veränderungen im Risikoprofil frühzeitig zu erkennen. Die Ergebnisse dieser Detektion sind in laufende Autorisierungsentscheidungen einzubeziehen. Gleichzeitig müssen technische Reaktionsmechanismen umgesetzt werden, um Zugriffe einzuschränken oder zu unterbinden und damit Sicherheitsentscheidungen wirksam durchzusetzen.

Für den weiteren Architekturentwurf des NEOSiP-Systems bedeutet dies, dass Zero Trust als durchgängiges Prinzip zu verstehen ist, dass sich in allen Sichten der Architektur widerspiegeln muss. Die in diesem Kapitel beschriebenen Grundannahmen bilden die konzeptionelle Grundlage für die Bausteinsicht, die Laufzeitsicht sowie die Querschnittskonzepte der Zielarchitektur. Konkrete Umsetzungsentscheidungen und deren technische Ausprägung werden in den nachfolgenden Kapiteln hergeleitet und erläutert.

3.3 Geschäftsarchitektur

3.3.1 Geschäftsziele

Im Rahmen des Projektkontexts wurden die Geschäftsziele der FITKO für NEOSiP spezifiziert. NEOSiP soll eine vollständig digitale ZSÜ ermöglichen, mit dem Ziel, die Kontrolle für den Zugang zu sicherheitsrelevanten Bereichen digital abzuwickeln. Die ZSÜ-Prozesse sollen mit NEOSiP robust, effizient, sicher, auditierbar und fehlerfrei durchführbar sein. Es soll eine Ablösung papiergebundener Teilprozesse durch ein digitalisiertes Ende-zu-Ende-Verfahren entstehen.

Ein zentrales Ziel ist, dass in Zukunft ein gehärtetes System vorliegt, bei dem eine Minimierung der Angriffsfläche nach aktuellem Stand der Technik erreicht wird. Zukünftige Sicherheitsaudits sollen ohne Feststellung kritischer Sicherheitslücken im Release-Status verlaufen.

Gleichzeitig soll der Betrieb durch eine skalierbare und erweiterbare Architektur, sowie durch eine Homogenisierung der Schnittstellen vereinfacht werden, um neue AWB mit geringerem technischem Aufwand als im Bestandssystem zu integrieren. Das Ziel sind nachweislich geringere Kosten für Beauftragung und Betrieb pro Nutzer im Vergleich zum Altsystem bei gleichzeitiger Sicherstellung strikter Datenschutzkonformität.

Entscheidend für den Erfolg von NEOSiP ist, dass noch nicht angebundene Länder und der Bund in Zukunft deutlich schneller und einfacher an NEOSiP angebunden werden können. Mit der Neukonzeption soll die Dauer für die Beauftragung, sowie die Kosten für Entwicklung und Betrieb für die Nutzer:innen günstiger werden als im Bestandssystem. Eine signifikante Verkürzung der Durchlaufzeiten vom Erstkontakt bis zur operativen Anbindung im Vergleich zum aktuellen Standardprozess soll erreicht werden.

3.3.2 Wertschöpfungsketten

Die nachfolgende Wertschöpfungskette beschreibt die fachliche Abfolge der Wertschöpfungsschritte, durch die im Verfahren NEOSiP aus einem eingehenden Antrag eine behördliche Entscheidung in Form eines Bescheids entsteht. Sie stellt die wertstiftende Ansicht auf das Produkt dar und fokussiert auf das fachliche Ergebnis für externe Verfahrensbeteiligte.

Die Wertschöpfungsschritte sind bewusst unabhängig von organisatorischen Zuständigkeiten, konkreten Prozessmodellen und technischen Umsetzungsentscheidungen formuliert. Ergänzend zur grafischen Darstellung in Abbildung 7 werden die einzelnen Schritte kurz in Tabelle 7 erläutert, um ein einheitliches fachliches Verständnis sicherzustellen und eine belastbare Grundlage für die Ableitung von Fähigkeiten, Prozessen und Architekturentscheidungen zu schaffen.

Abbildung 7: Übersicht der Wertschöpfungskette vom Antrag bis zum Bescheid

Tabelle 7: Tabellarische Beschreibung der Wertschöpfungsschritte (Antragserfassung, Antragsprüfung, Erkenntnisabfrage, Erkenntnisbewertung, Bescheiderlass) mit Zweck je Schritt

Wertschöpfungsschritt	Erläuterung
Antragserfassung	Fachliche Entgegennahme und strukturierte Erfassung eines eingegangenen Antrags als Startpunkt des Verwaltungsverfahrens.
Antragsprüfung	Fachliche und formale Prüfung des Antrags auf Vollständigkeit, Zulässigkeit und Plausibilität als Voraussetzung für die weitere Verarbeitung.
Erkenntnisabfrage	Fachliche Anforderung und Entgegennahme sicherheitsrelevanter Erkenntnisse von zuständigen EKS zur Unterstützung der Entscheidungsfindung.
Erkenntnisbewertung	Fachliche Auswertung und Gewichtung der eingegangenen Erkenntnisse im Hinblick auf ihre Relevanz für das Verfahrensergebnis.
Bescheiderlass	Formale Herbeiführung und Bekanntgabe der behördlichen Entscheidung über den Antrag als Abschluss des Verwaltungsverfahrens.

3.3.3 Fähigkeitenlandkarte

Die nachfolgend dargestellte Fähigkeitenlandkarte (Abbildung 8) beschreibt die fachlichen Fähigkeiten des Produkts unabhängig von organisatorischen Zuständigkeiten, konkreten Prozessen oder technischen Lösungsentscheidungen. Sie stellt dar, was das Produkt fachlich leisten muss, um das Verfahren OSiP vollständig und regelkonform zu unterstützen.

Die Fähigkeiten sind hierarchisch strukturiert und bilden gemeinsam die Grundlage für die weitere Ableitung von Geschäftsprozessen, IT-Services und Architekturentscheidungen. Ergänzend zur grafischen Darstellung werden die einzelnen Fähigkeiten kurz in folgender Tabelle 8 erläutert, um eine einheitliche, fachliche Interpretation sicherzustellen und die Anschlussfähigkeit an nachgelagerte Architektur- und Umsetzungsartefakte zu gewährleisten.

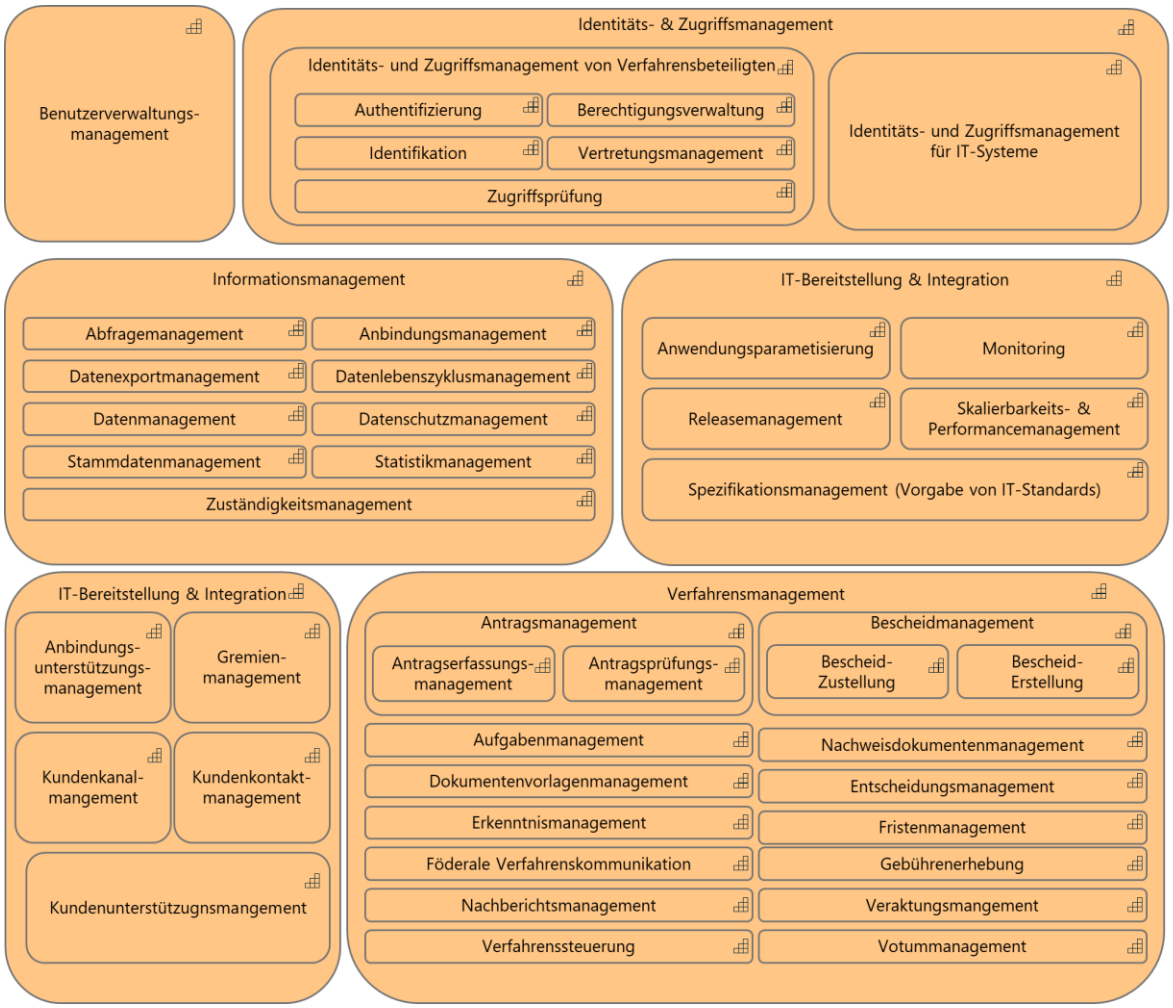


Abbildung 8: Hierarchische Fähigkeitenlandkarte des Produkts als Grundlage für Prozesse und Services

Tabelle 8: Tabellarische Erläuterung der in der Fähigkeitenlandkarte dargestellten fachlichen Fähigkeiten

Fähigkeit	Erläuterung
Antragsmanagement	Fähigkeit zur fachlichen Entgegennahme, Verwaltung und Bearbeitung von Anträgen als Ausgangspunkt des Verfahrens NEOSiP.
Antragserfassungsmanagement	Fähigkeit zur strukturierten Erfassung und formalen Anlage eines eingegangenen Antrags im Verfahren.
Antragsprüfungsmanagement	Fähigkeit zur fachlichen und formalen Prüfung eines Antrags auf Vollständigkeit, Plausibilität und Zulässigkeit.
Aufgabenmanagement	Fähigkeit zur fachlichen Steuerung, Zuweisung und Nachverfolgung verfahrensbezogener Aufgaben innerhalb des Verwaltungsprozesses.

Dokumentenvorlagenmanagement	Fähigkeit zur fachlichen Verwaltung und Bereitstellung standardisierter Dokumentenvorlagen für Bescheide und Mitteilungen.
Bescheidmanagement	Fähigkeit zur fachlichen Erstellung, Verwaltung und Bereitstellung behördlicher Bescheide als Ergebnis eines Verfahrens.
Bescheiderstellung	Fähigkeit zur fachlichen Erarbeitung und Finalisierung eines Bescheids auf Basis der Verfahrensentscheidung.
Bescheidzustellung	Fähigkeit zur formalen Übermittlung eines Bescheids an die betroffene Stelle oder Organisation.
Erkenntnismanagement	Fähigkeit zur fachlichen Entgegennahme, Verwaltung und Bewertung sicherheitsrelevanter Erkenntnisse von EKS zur Unterstützung der Entscheidungsfindung.
Föderale Verfahrenskommunikation	Beschreibt eine offene schriftliche Kommunikation im Rahmen des Verfahrens zwischen der zuständigen Stelle und Verfahrensbeteiligten. Diese Kommunikation ist an keine besonderen Strukturen und Vorgaben gebunden und kann für den Versand von allgemeinen Textnachrichten und nicht fachspezifischen Dokumentformaten genutzten werden.
Nachberichtsmanagement	Fähigkeit zur fachlichen Verarbeitung und Berücksichtigung nachträglich eingehender sicherheitsrelevanter Erkenntnisse im laufenden oder abgeschlossenen Verfahren.
Verfahrenssteuerung	Fähigkeit zur fachlichen Koordination und Steuerung des Gesamtverfahrens über alle Verfahrensschritte hinweg.
Entscheidungsmanagement	Fähigkeit zur fachlichen Vorbereitung, Herbeiführung und Dokumentation von Entscheidungen auf Basis von Anträgen, Erkenntnissen und fachlichen Prüfungen.
Fristenmanagement	Fähigkeit zur fachlichen Verwaltung, Überwachung und Einhaltung gesetzlicher und verfahrensspezifischer Fristen.
Votummanagement	Fähigkeit zur fachlichen Einholung, Verwaltung und Berücksichtigung von Stellungnahmen und Voten beteiligter Akteure im Entscheidungsprozess.
Nachweisdokumentenmanagement	Fähigkeit zur fachlichen Verwaltung, Zuordnung und Bewertung von eingereichten Nachweisdokumenten im Rahmen eines Antragsverfahrens.
Gebührenerhebung	Fähigkeit zur fachlichen Festsetzung, Verwaltung und Nachverfolgung von Gebühren im Zusammenhang mit der Durchführung eines Verwaltungsverfahrens.

Veraktungsmanagement	Fähigkeit zur fachlichen Zusammenführung, Ordnung und Archivierung aller verfahrensrelevanten Informationen und Dokumente in einer Verfahrensakte.

3.3.4 Geschäftsprozesse

Die Prozessdarstellung zeigt eine vereinfachte Business Process Model and Notation (BPMN)-Darstellung des ZSÜ-Prozesses und veranschaulicht die Abfolge der zentralen Schritte von der Antragseinreichung bis zur abschließenden Entscheidung und Dokumentation. Ziel ist es, den zukünftigen Soll-Prozess verständlich und nachvollziehbar darzustellen. Die Darstellung berücksichtigt sowohl automatisierte Abläufe als auch die wesentlichen Entscheidungspunkte und schafft damit eine Orientierung für die spätere technische Umsetzung. Als Quelle dienten die im Rahmen der Anforderungserhebung erhobenen Inhalte aus Interviews und Workshops.

Der Hauptprozess ist in drei Module gegliedert, die die funktionale Kernlogik des Systems strukturieren.

- Das erste Modul, Antragseinreichung, umfasst die Erfassung und Validierung der Antragsdaten.
- Das zweite Modul, Erkenntnisermittlung und Entscheidung, beinhaltet die Prüfung des Antrags, die Einholung externer Erkenntnisse sowie die Entscheidungsfindung.
- Das dritte Modul, Rückmeldung der Entscheidung und Dokumentation, umfasst die Mitteilung der Entscheidung, die Erstellung von Bescheiden und die Ablage im System.

Ergänzend zu diesen Kernmodulen wurden fünf Subprozesse identifiziert, die den Hauptprozess erweitern:

- Folgeantrag,
- Gebührenbescheid,
- Nachbericht,
- Änderungsmitteilung
- Löschung.

Diese Subprozesse sind fachlich eigenständig, jedoch eng mit den Hauptmodulen verzahnt. Die modulare Struktur unterstützt die klare Abgrenzung der Prozessphasen und erleichtert die spätere technische Modellierung. Die detaillierten Abläufe der drei Prozessmodule sowie der ergänzenden Subprozesse sind in den folgenden BPMN-Darstellungen (Abbildung 9 bis Abbildung 17) visualisiert.

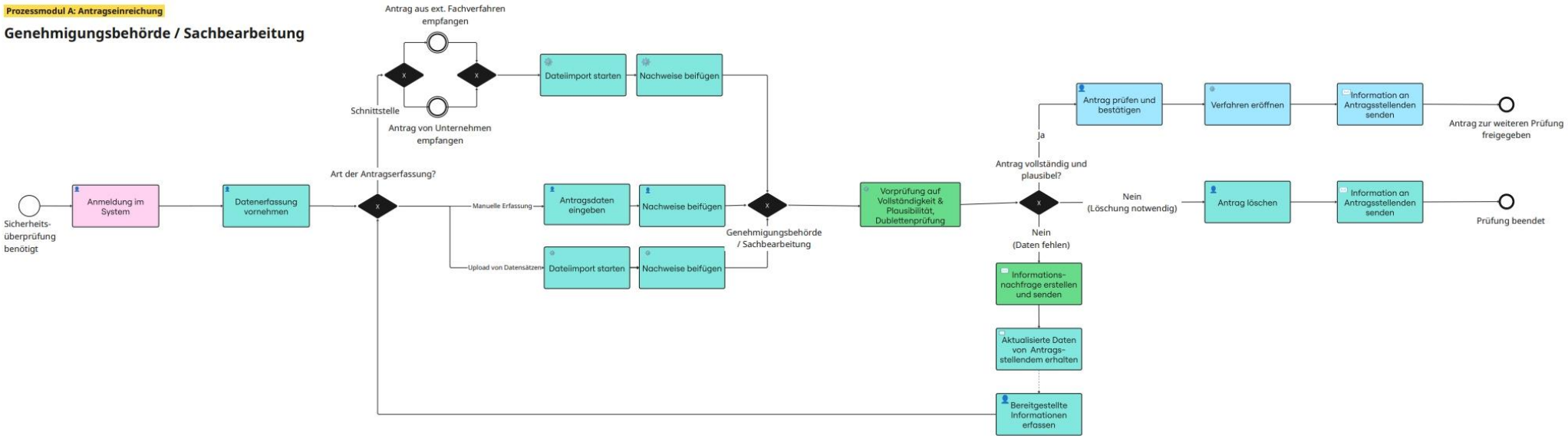


Abbildung 9: BPMN-Übersicht Prozessmodul A (Antragseinreichung) von der Datenerfassung bis zur Validierung als Start des Hauptprozesses.

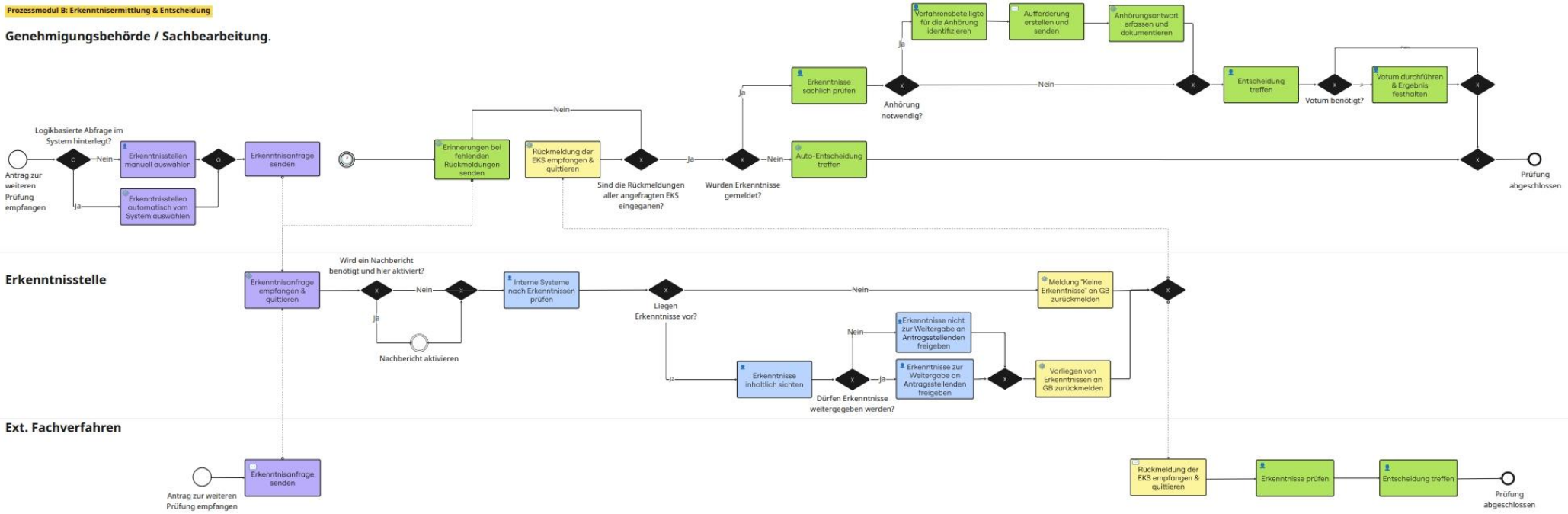


Abbildung 10: BPMN-Übersicht Prozessmodul B (Erkenntnisermittlung & Entscheidung) mit Anfrage an EKS, Bewertung und Entscheidungsvorbereitung

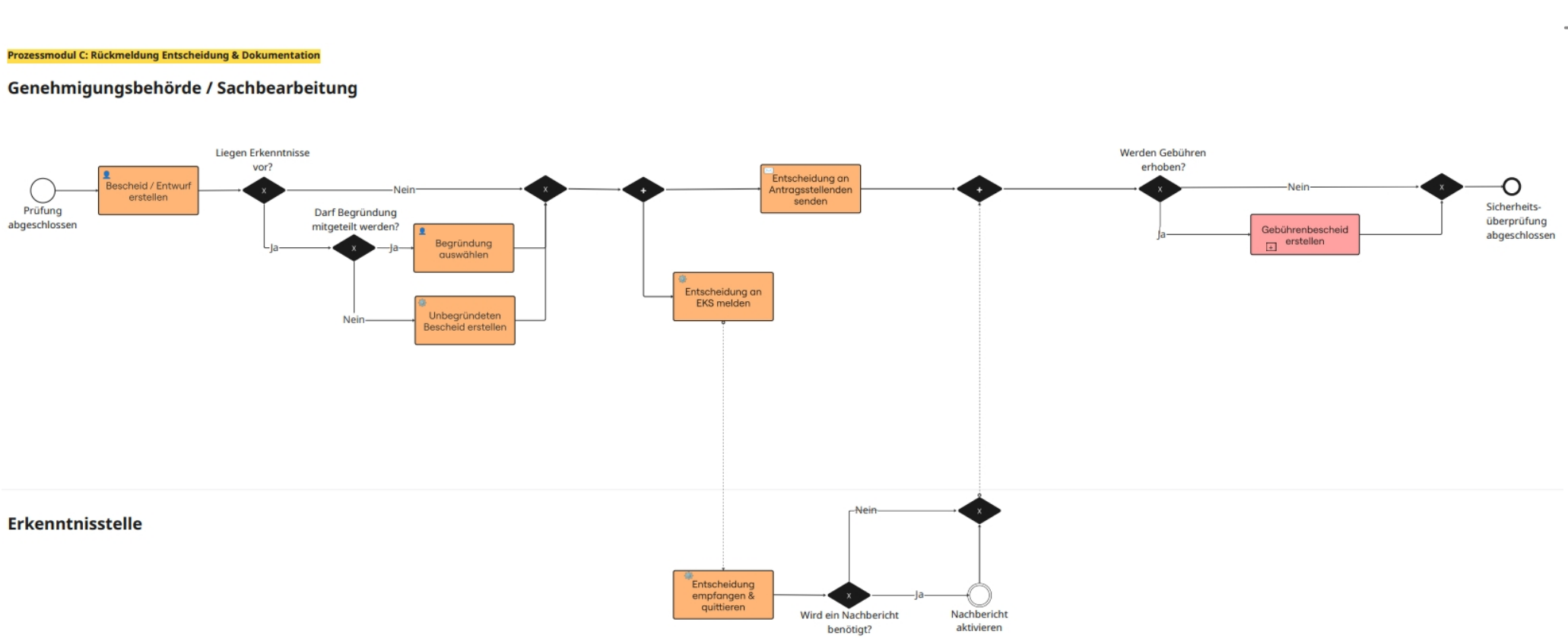


Abbildung 11: BPMN-Übersicht Modul C (GB) zur Rückmeldung der Entscheidung und Dokumentation inkl. Bescheiderstellung

Externe Fachverfahren

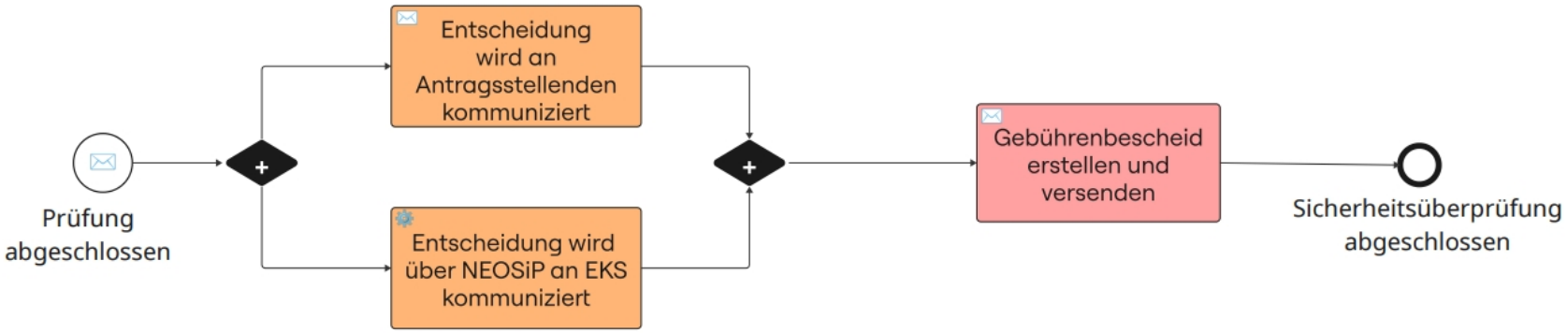


Abbildung 12: „BPMN-Variante des Moduls C für externe Fachverfahren mit angepassten Rollen/Schnittstellen

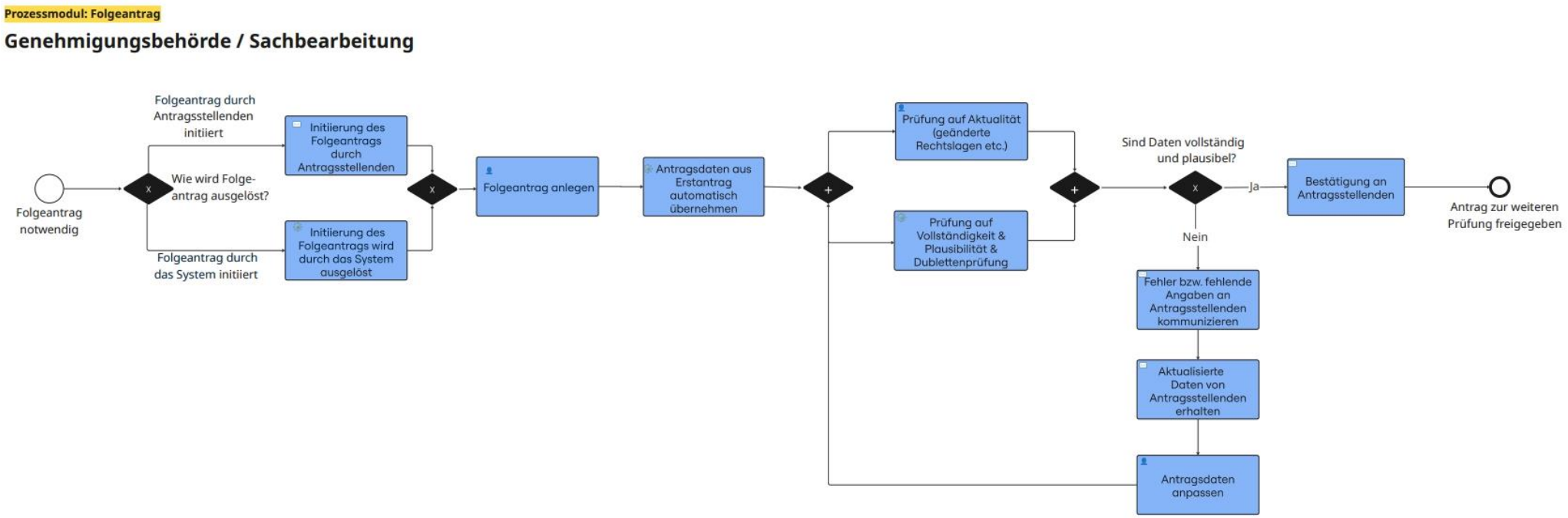


Abbildung 13: BPMN-Darstellung des Subprozesses Folgeantrag von der Initiierung bis zur Verknüpfung mit dem Ursprungsverfahren

Prozessmodul: Gebührenbescheid

Genehmigungsbehörde / Sachbearbeitung

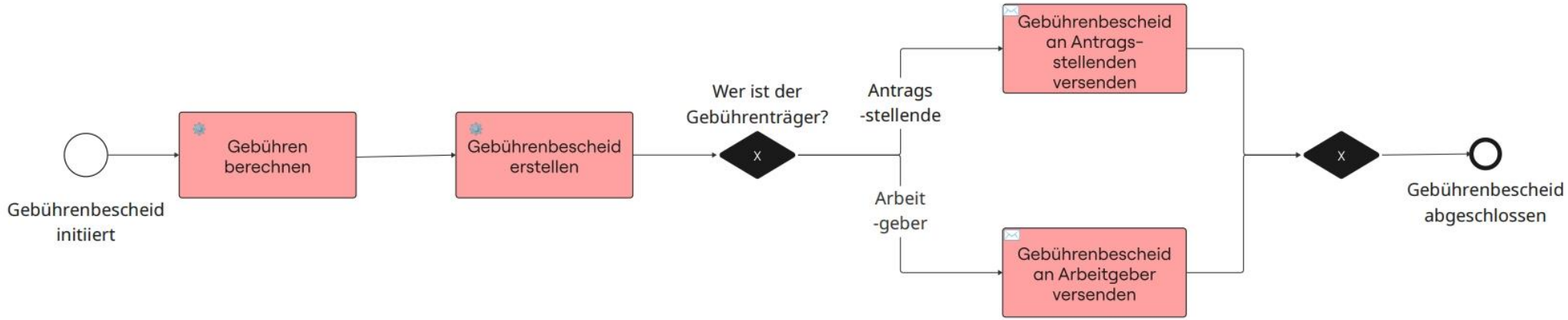


Abbildung 14: BPMN-Darstellung des Gebührenbescheids von der Berechnung bis zur Zustellung im Verfahrenskontext

Subprozess Nachbericht

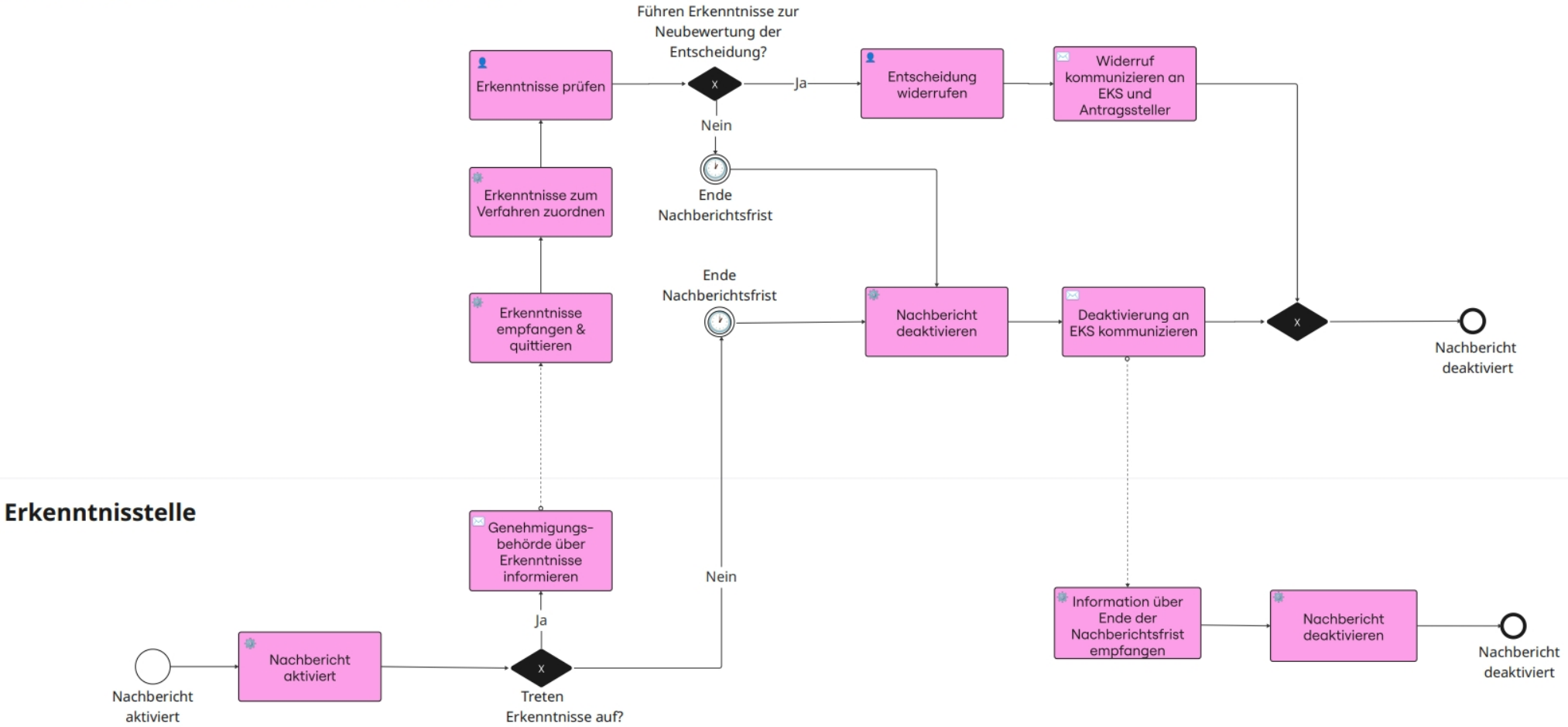


Abbildung 15: BPMN-Darstellung des Nachberichts mit Eingang, Prüfung und fachlicher Berücksichtigung im laufenden/abgeschlossenen Verfahren

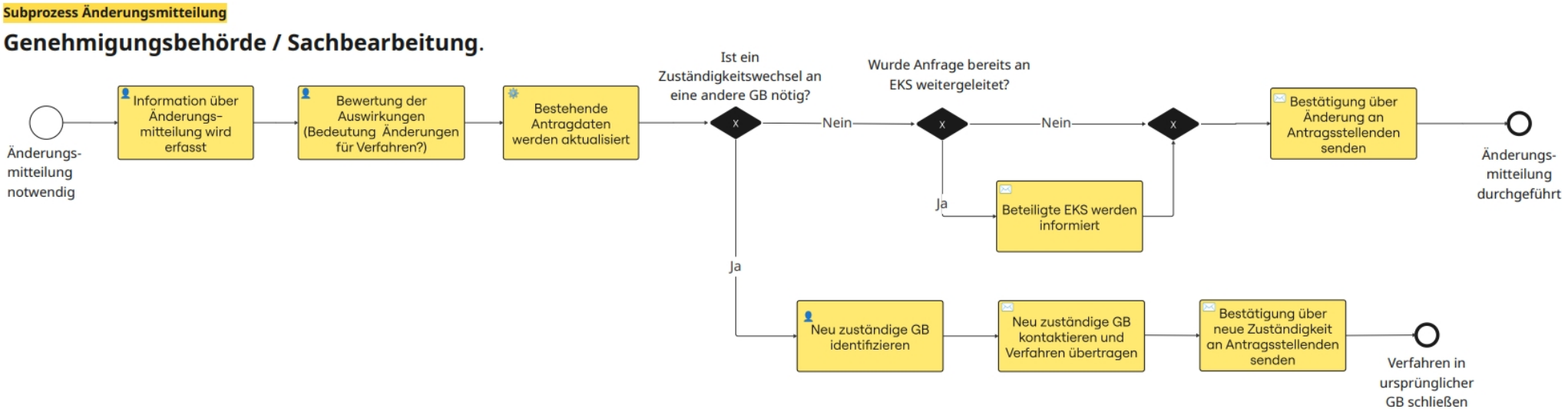


Abbildung 16: BPMN-Darstellung der Änderungsmitteilung mit Erfassung, Prüfung und Anpassung verfahrensrelevanter Daten

Subprozess Löschung

Genehmigungsbehörde / Sachbearbeitung.

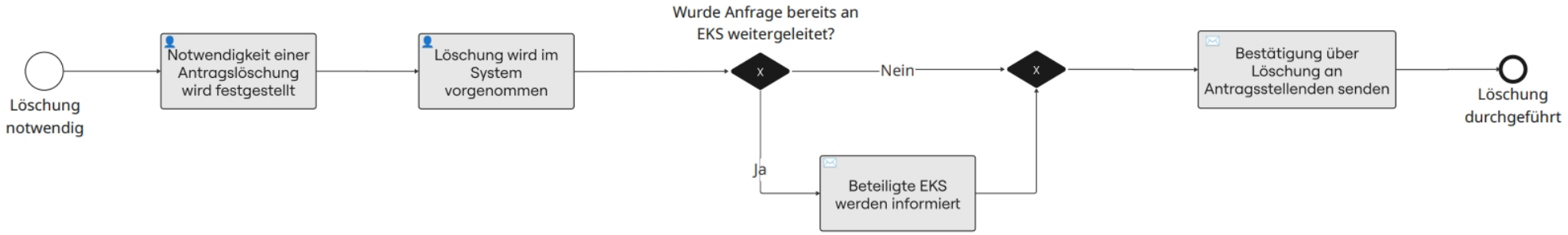


Abbildung 17: BPMN-Darstellung des Löschprozesses mit Kriterienprüfung, Auslösung und Nachweis der Löschung

3.4 Fachlicher und technischer Kontext für OSiP

Die Zielarchitektur ist in ein komplexes, fachliches und technisches Umfeld eingebettet, das durch eine Vielzahl beteiligter Akteure, Organisationen und bestehender IT-Systeme geprägt ist. Für ein belastbares Architekturverständnis ist es daher erforderlich, sowohl den fachlichen als auch den technischen Kontext explizit darzustellen und voneinander abzugrenzen.

Der fachliche Kontext beschreibt, aus welchen fachlichen Rollen heraus das System genutzt wird, welche Aufgaben und Verantwortlichkeiten die beteiligten Akteure wahrnehmen und welche fachlichen Informationen zwischen ihnen ausgetauscht werden. Er betrachtet das NEOSiP-System dabei bewusst als Blackbox und abstrahiert von technischen Umsetzungsdetails. Ziel ist es, die Einbindung der Zielarchitektur in die fachlichen Abläufe der Sicherheitsüberprüfung nachvollziehbar zu machen.

Der technische Kontext ergänzt diese Sicht um die konkrete technische Einbettung der Zielarchitektur. Er zeigt auf, welche IT-Systeme, Fachverfahren und Clients mit OSiP interagieren, über welche Schnittstellen der Datenaustausch erfolgt und über welche Infrastruktur- und Netzgrenzen hinweg Kommunikation stattfindet. Damit bildet der technische Kontext die Grundlage für das Verständnis der Integrations- und Betriebsanforderungen der Zielarchitektur.

Die getrennte Betrachtung von fachlichem und technischem Kontext ermöglicht es, fachliche Anforderungen und technische Rahmenbedingungen klar zu unterscheiden, ihre Wechselwirkungen jedoch gezielt sichtbar zu machen.

3.4.1 Fachlicher Kontext

Die Zielarchitektur fungiert aus fachlicher Sicht als vermittelnde Infrastruktur für den Austausch von Informationen zwischen AES, GB und EKS. Sie stellt den organisatorischen und fachlichen Rahmen für die Übermittlung von Anträgen, Informationen, Erkenntnissen und statusbezogenen Nachrichten bereit, ohne selbst fachliche Inhalte zu interpretieren, zu bewerten oder Entscheidungen zu treffen. Da auch ein Fachverfahren zentral für AES und GB bereitgestellt werden soll, tritt die FITKO an dieser Stelle auch in der Rolle eines Fachverfahrensherstellers auf.

GB interagieren mit der Zielarchitektur insbesondere im Kontext der Auf- und Entgegennahme von Anträgen, dem Versand von Anfragen an EKS und dem Empfang von Erkenntnissen. Die fachliche Verantwortung für Inhalte, Verfahren und Entscheidungen verbleibt dabei vollständig

bei den GB. Die Zielarchitektur übernimmt ausschließlich die Unterstützung des fachlichen Informationsaustauschs.[21]

EKS nutzen die Zielarchitektur als fachlichen Kommunikationskanal. Sie empfangen über die Infrastruktur Anfragen und stellen im Gegenzug Erkenntnisse bereit. Auch hier erfolgt keine fachliche Verarbeitung oder Bewertung innerhalb der Zielarchitektur selbst. Die Zielarchitektur dient lediglich als vermittelnde Ebene für den strukturierten Austausch zwischen den beteiligten Akteuren.[22]

Fachverfahrenshersteller nehmen im fachlichen Kontext die Rolle ein, die von ihnen entwickelten und betriebenen Fachverfahren technisch an die Zielarchitektur anzubinden. Die Nutzung der Zielarchitektur erfolgt dabei als fachlicher Kommunikationsweg zur Unterstützung der jeweiligen Anwendungsfälle. Eine fachliche Verantwortung innerhalb der Zielarchitektur selbst ist mit dieser Rolle nicht verbunden. Fachliche Logik, Prozesssteuerung und inhaltliche Bewertung verbleiben in den jeweiligen Fachverfahren und bei deren verantwortlichen Organisationen.

AES wie bspw. private Organisationen oder Onlinedienste nutzen die Zielarchitektur, um Anträge für Sicherheitsprüfungen von Bürger:innen an die GB zu versenden und die Entscheidung der Überprüfung zu empfangen. Dazu werden entweder eigenentwickelte Systeme verwendet, die an die Zielarchitektur angebunden werden müssen, oder es wird das zentral zur Verfügung gestellte Fachverfahren verwendet.

Die fachlichen Verantwortlichkeiten zwischen den beteiligten Akteuren und der Zielarchitektur sind dabei klar abgegrenzt. Die fachliche Bewertung von Anträgen, die inhaltliche Entscheidungsfindung sowie die Ableitung fachlicher Entscheidungen verbleiben vollständig bei den jeweils zuständigen Akteuren und Fachverfahren. Die Zielarchitektur trifft keine fachlichen Entscheidungen im Sinne einer inhaltlichen Prüfung oder Bewertung von Anträgen.

Gleichzeitig übernimmt die Zielarchitektur fachlich motivierte Steuerungsaufgaben zur Unterstützung des Kommunikationsprozesses. Hierzu zählen insbesondere die regelbasierte

[21] Mit bzw. nach dem Empfang der Erkenntnisse, die ggf. VS sind, trägt die jeweilige GB die Verantwortung hinsichtlich der ordnungsgemäßen Handhabung der VS. Die (technische) „Zuständigkeit" von NEOSiP zur Einhaltung weiterer geheimschutzrelevanter Anforderungen endet hiermit, wenn die VS die Anwendung verlässt oder die eingestufte Information zur Kenntnis genommen wurde, siehe Kapitel 3.2.3.3.

[22] Sofern es sich bei den Erkenntnissen um VS handelt, sind die EKS für korrekte Kennzeichnung der VS verantwortlich. NEOSiP als System muss ggf. dies technisch unterstützen. Im Wesentlichen muss NEOSiP die sichere Übertragung/Weitergabe von VS sicherstellen, siehe Kapitel 3.2.3.3.

Auswahl und Adressierung der jeweils zuständigen EKS auf Grundlage definierter, fachlicher Parameter, etwa in Abhängigkeit vom Anwendungsbereich oder relevanten zeitlichen und räumlichen Bezügen. Diese Steuerungslogik dient ausschließlich der korrekten und vollständigen Weiterleitung von Nachrichten und stellt sicher, dass Informationen an die jeweils fachlich zuständigen Stellen übermittelt werden.

Darüber hinaus stellt die Zielarchitektur sicher, dass übermittelte Informationen grundlegenden formalen und strukturellen Anforderungen genügen. Hierzu zählen unter anderem Prüfungen zur Sicherstellung der Datenintegrität, der formalen Gültigkeit sowie der technischen Unbedenklichkeit der übermittelten Inhalte.

Die im fachlichen Kontext betrachteten Informationsflüsse werden bewusst auf einer abstrahierten Ebene beschrieben. Es wird dargestellt, welche Arten von Informationen zwischen den Akteuren ausgetauscht werden und zu welchem fachlichen Zweck dies erfolgt. Aussagen zu Datenformaten, technischen Protokollen oder konkreten Implementierungen sind nicht Bestandteil dieser Betrachtung und werden in späteren Kapiteln adressiert.

Die Systemgrenze der Zielarchitektur ist in diesem Zusammenhang eindeutig definiert. Alle beschriebenen Rollen und Akteure befinden sich außerhalb dieser Grenze und interagieren mit der Zielarchitektur als externes System. Ein begleitendes, fachliches Kontextdiagramm in Abbildung 18 visualisiert diese Abgrenzung und stellt die Zielarchitektur sowie die externen Akteure und ihre fachlichen Informationsflüsse übersichtlich dar.

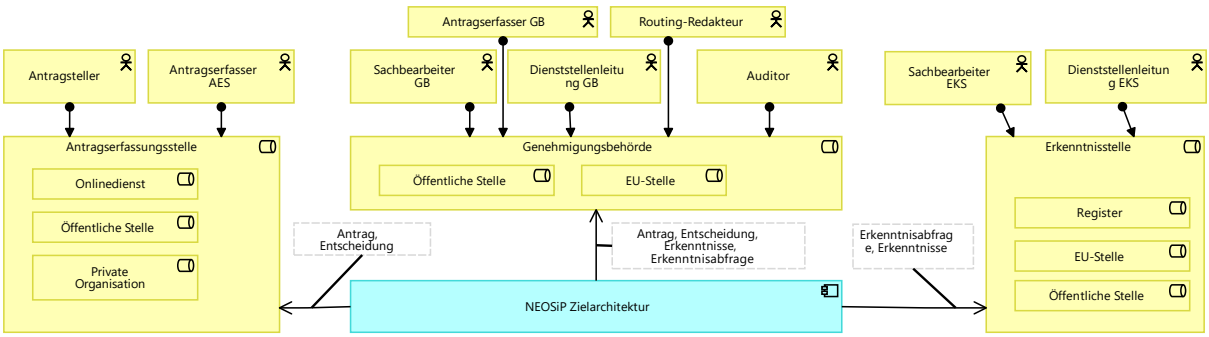


Abbildung 18: Kontextdiagramm zur fachlichen Systemgrenze mit externen Akteuren (AES, GB, EKS) und fachlichen Informationsflüssen; NEOSiP Zielarchitektur als vermittelnde Infrastruktur.

3.4.2 Technischer Kontext

Während in Kapitel 3.4.1 der fachliche Kontext der Zielarchitektur betrachtet wurde, richtet sich der Fokus dieses Kapitels auf die technische Einbettung der Zielarchitektur in ihre Systemumgebung. Ziel ist es, die technischen Systemgrenzen gegenüber externen Anwendungen und Infrastrukturen zu definieren und die grundlegenden technischen Kommunikationsbeziehungen darzustellen, über die ein Datenaustausch erfolgt.

Die Betrachtung des technischen Kontexts beschränkt sich dabei bewusst auf externe Systeme und deren Anbindung an die Zielarchitektur. Interne Komponenten, technische Detailausprägungen sowie konkrete Architekturentscheidungen sind nicht Gegenstand dieses Kapitels und werden in den nachfolgenden Abschnitten zur Zielarchitektur vertieft beschrieben. Externe Systeme werden daher in diesem Kapitel als Blackbox verstanden. Die Beschreibung beschränkt sich auf ihre Rolle als technische Kommunikationspartner der Zielarchitektur. Interne Struktur, technische Umsetzung und Betriebsdetails dieser Systeme sind nicht Gegenstand der vorliegenden Betrachtung.

Der technische Kontext bildet die Grundlage für das Verständnis der Systemintegration innerhalb der föderalen Systemlandschaft und schafft Transparenz über die technischen Abhängigkeiten und Interaktionspunkte der Zielarchitektur, ohne deren interne Ausgestaltung vorwegzunehmen.

3.4.2.1 Externe technische Systeme

Die Zielarchitektur interagiert im technischen Kontext mit einer Vielzahl externer Systeme, die entlang des Gesamtprozesses der Sicherheitsüberprüfung eingebunden sind. Diese Systeme unterscheiden sich hinsichtlich ihrer fachlichen Zuständigkeit, ihrer technischen Ausprägung sowie ihrer jeweiligen Betriebsverantwortung. Die nachfolgende Betrachtung ordnet die relevanten externen Systeme ein und beschreibt ihre Rolle im technischen Gesamtkontext.

Am Beginn des technischen Ablaufs stehen die technischen Systeme oder Anwendungen, über die AES-Anträge einreichen sowie Entscheidungen der Überprüfungen empfangen, welche im weiteren Verlauf unter „Antragsverarbeitung“ zusammengefasst werden. Diese Clients können in unterschiedlichen technischen Ausprägungen vorliegen, bspw. als Webanwendungen oder als angebundene Fachanwendungen. NEOSiP möchte im Rahmen der Neukonzeption eine eigens entwickelte Referenzimplementierung eines Fachverfahrens zur Verfügung stellen und dies zentral zur Nutzung bereitstellen.

Ein weiterer angebundener Systemtyp ist das Fachverfahren der GB. Diese technischen Systeme dienen der Entgegennahme, Bearbeitung und Verwaltung der eingehenden Anträge, der

Erkenntnisabfrage bei den EKS und der Bereitstellung von Überprüfungsentscheidungen. Diese Systeme werden im weiteren als „Erkenntnisverarbeitung“ bezeichnet. Der Betrieb und die fachliche Verantwortung dieser Systeme liegen bei den jeweiligen GB. Auch hierzu wird seitens der FITKO ein eigenentwickeltes Fachverfahren bereitgestellt.

Die Fachverfahren der EKS bilden einen weiteren wesentlichen Bestandteil des technischen Umfelds. Sie empfangen Anfragen über NEOSiP, verarbeiten diese entsprechend ihrer fachlichen Zuständigkeit und stellen die gewonnenen Erkenntnisse zur weiteren Verwendung bereit. Sie werden als „Erkenntnisermittlung“ bezeichnet. Auch diese Systeme werden eigenverantwortlich durch die jeweiligen EKS betrieben und liegen vollständig außerhalb der Zielarchitektur.

Das folgende technische Kontextdiagramm Abbildung 19 stellt die Architektur dar und visualisiert die angebundenen externen Systeme sowie deren grundlegenden technischen Kommunikationsbeziehungen.

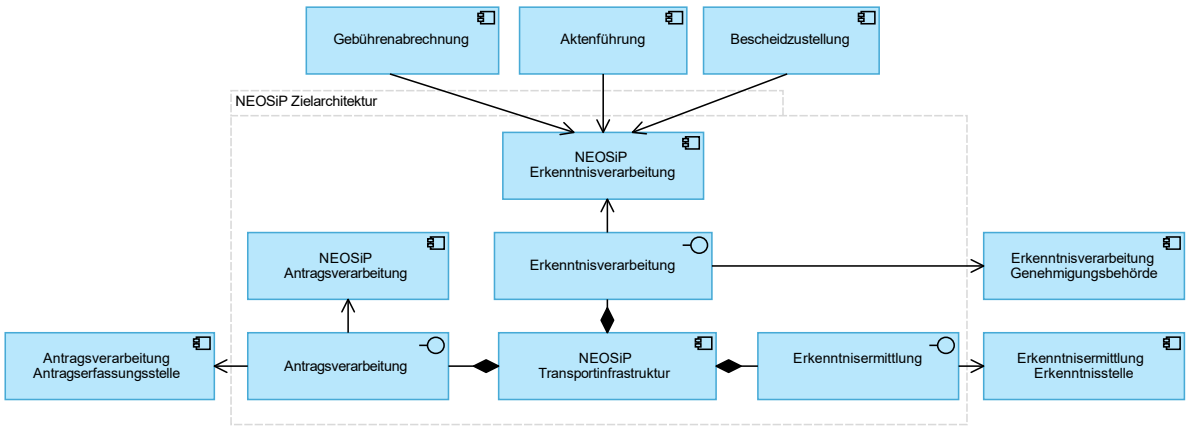


Abbildung 19: Darstellung des technischen Gesamtkontexts von NEOSiP mit angebundenen externen Systemen sowie der zentralen TI und den jeweiligen Kommunikationsbeziehungen.

3.4.2.2 Technische Rahmenbedingungen

Die Zielarchitektur ist in eine föderale, technische Systemlandschaft eingebettet, in der externe Systeme von unterschiedlichen Organisationen eigenverantwortlich betrieben werden. Diese föderale Struktur prägt die technischen Rahmenbedingungen maßgeblich und stellt besondere Anforderungen an die Gestaltung der Systemintegration. Die technische Kommunikation

erfolgt ausschließlich über klar definierte Schnittstellen an der Systemgrenze der Zielarchitektur.

Auch die technische Verortung der beteiligten Systeme ist heterogen. Die Systeme der AES befinden sich im Internet, wenn es um Unternehmensanwendungen geht und im Landesnetz, wenn es Onlinedienste sind. Die NEOSiP-Transportinfrastruktur, -Erkenntnisverarbeitung und –Antragsverarbeitung werden in eigenen Netzen betrieben. Die Fachverfahren der GB sind in unterschiedlichen Landesverwaltungsnetzen (LVN) verortet. Fachverfahren von EKS sind wiederum in weiteren organisatorisch und technisch getrennten Netzen angesiedelt, zu denen insbesondere speziell teilweise abgeschottete Netze zählen, in denen u.a. die Fachverfahren der LKÄ, des Verfassungsschutzes und der Nachrichtendienste betrieben werden. Die unterschiedlichen Netzbereiche sowie deren technische und organisatorische Trennung sind in Abbildung 20 dargestellt.

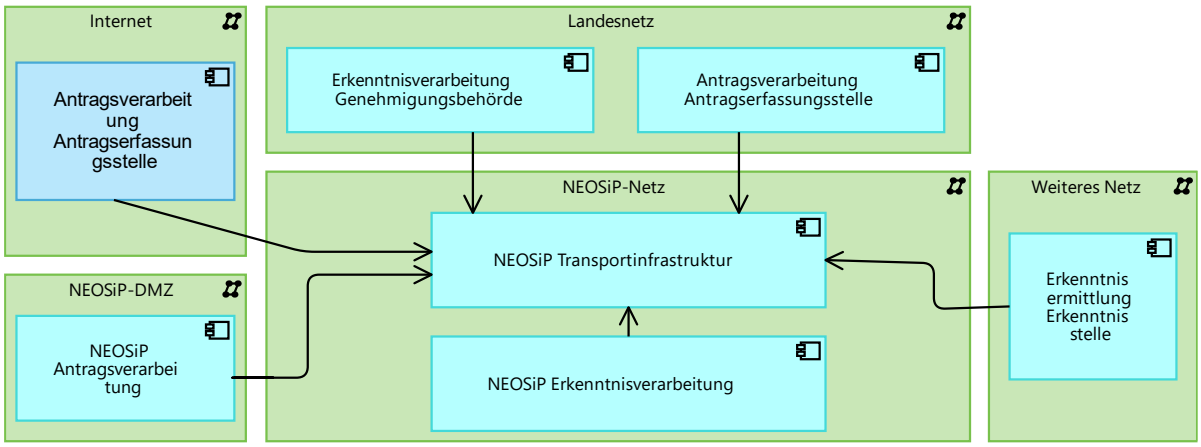


Abbildung 20: Grafische Darstellung der unterschiedlichen Netzbereiche und ihrer technisch-organisatorischen Trennungen.

Zwischen den genannten Netzen bestehen klare organisatorische und technische Trennungen. Direkte, netzinterne Kommunikationsbeziehungen zwischen externen Systemen können somit nicht vorausgesetzt werden. Die Kommunikation mit der Zielarchitektur erfolgt netzübergreifend über definierte technische Schnittstellen, die als einzige Kopplungspunkte zwischen den beteiligten Systemen dienen.

Darüber hinaus ist zu berücksichtigen, dass nicht davon ausgegangen werden kann, dass die beteiligten externen Systeme durchgehend verfügbar sind. Temporäre Nichtverfügbarkeit

einzelner Kommunikationspartner stellt eine technische Rahmenbedingung dar, die im Gesamtsystem zu berücksichtigen ist.

Die beschriebenen Rahmenbedingungen erfordern eine Integrationsfähigkeit, die sowohl eine schrittweise Anbindung weiterer externer Systeme als auch den Umgang mit einer variierenden Anzahl angebundener Systeme ermöglicht.

4 Zielarchitektur

Dieses Kapitel konkretisiert die Überführung der Anforderungen und der Ergebnisse der Untersuchung in ein konsistentes technisches Gesamtbild. Die Zielarchitektur wird dabei schrittweise aus verschiedenen Perspektiven hergeleitet:

- Grundlegende Architekturentscheidungen bilden die Basis und fließen direkt in die nachfolgenden Sichten ein.
- Die Bausteinsicht bietet eine Darstellung der Systembausteine und ihrer Verantwortlichkeiten.
- In der Laufzeitsicht wird das Zusammenwirken der Komponenten in operativen Szenarien betrieben.

Übergreifende Festlegungen zu Sicherheit, Kryptografie sowie Identitäts- und Rechtemanagement werden im Abschnitt Querschnittskonzepte behandelt.

Das Kapitel beschränkt sich auf das Zielbild und dient als verbindlicher Referenzrahmen für die Planung und Umsetzung. Es beschränkt sich bewusst auf die Zielarchitektur. offene Detailfragen, konkrete Umsetzungsmaßnahmen sowie die Migrations- und Transitionsplanung werden separat in den jeweiligen Handlungsfeldern adressiert.

4.1 Lösungsstrategie und architektonische Ableitung

Auf Basis der strategischen Ziele und Leitprinzipien (siehe Kapitel 1.30), sowie der Ergebnisse der Untersuchung (siehe Kapitel 3) folgt die Zielarchitektur dem Ziel, eine zukunftsfähige, sichere und föderationsfähige Plattform für die Durchführung von Zuverlässigkeits- und Sicherheitsprüfungen in der Bundesrepublik Deutschland bereitzustellen. Sie ist darauf ausgelegt, bestehende heterogene Systemlandschaften schrittweise einzubinden, ohne die bestehende fachliche Tätigkeit zu gefährden, und gleichzeitig eine einheitliche, deutschlandweit nutzbare Architekturgrundlage zu schaffen.

Die Zielarchitektur leitet sich dabei nicht nur aus funktionalen Anforderungen ab, sondern insbesondere aus den für das Vorhaben maßgeblichen Qualitätszielen. Diese orientieren sich

an den in Kapitel 1.3 beschriebenen strategischen Zielsetzungen und an einem qualitätsorientierten Architekturverständnis entlang von Sicherheits-, Wartbarkeits-, Zuverlässigkeits-, Leistungs- und Interoperabilitätsanforderungen.

Die Lösungsstrategie für die zentral zur Verfügung gestellten Komponenten wurde gemäß dem Betriebsmodell Software-as-a-Service (SaaS) gestaltet und soll perspektivisch durch eine zentrale Stelle verantwortet werden, während die fachliche Hoheit über Anträge, Erkenntnisse und Entscheidungen weiterhin bei den jeweils zuständigen Behörden verbleiben wird. Dieses Modell ermöglicht eine klare Trennung von fachlicher Verantwortung und technischer Bereitstellung und trägt somit den föderalen Rahmenbedingungen Rechnung.

Zugleich folgt die Lösungsstrategie dem Grundsatz, dass ein zentraler Betrieb nicht zu einer zentralen fachlichen Verfügungsmacht über Inhalte führen darf. Für die zentral betriebenen Komponenten ist daher architektonisch sicherzustellen, dass Betreiber grundsätzlich keine fachlichen Klartextinhalte einsehen oder verarbeiten können.

Bestehende Fachverfahren der GB und EKS werden nicht ersetzt, sondern über standardisierte Schnittstellen, klare Anschlussbedingungen und einen Datenformatstandard in die Zielarchitektur integriert. Durch ergänzende technische Hilfsmodule wie SDKs sollen zentrale Funktionalitäten bereitgestellt werden, die gemeinsame Funktionen bündeln und redundante Mehrfachimplementierungen vermeiden können. Die Zielarchitektur wird so ausgelegt, dass bestehende Systeme mit vertretbarem Aufwand eingebunden werden können. Die konkrete Migrationsstrategie, einschließlich möglicher Parallelbetriebe oder Ablöseszenarien, wird in einem separaten Migrationskonzept festgelegt, wie in Kapitel **Fehler! Verweisquelle konnte nicht gefunden werden.** beschrieben wird.

Vor dem Hintergrund des zugrunde gelegten mindestens hohen Schutzbedarfs folgt die Zielarchitektur einem Zero-Trust-Ansatz. Sicherheitsentscheidungen werden damit nicht aus Netzgrenzen oder impliziten Vertrauensannahmen abgeleitet, sondern aus überprüfbaren Identitäten, Kontextinformationen, technischen Zuständen und expliziten Berechtigungen. Für zentral bereitgestellte Komponenten bedeutet dies insbesondere, dass technische Betriebs- und Administrationsrechte strikt von der Möglichkeit zur Einsicht in fachliche Inhalte getrennt werden müssen.

Die zentralen Qualitätsmerkmale, die als Grundlage für die Gestaltung der Zielarchitektur herangezogen wurden, sind Sicherheit, Interoperabilität und Föderationsfähigkeit, Wartbarkeit, Leistungseffizienz und Zuverlässigkeit. Diese Auswahl spiegelt die strategischen Zielsetzungen

des Vorhabens wider und konkretisiert sie für die Architekturarbeit in einer Form, die für ADRs, Bausteinschnitt und Querschnittskonzepte anschlussfähig ist.

Die Ergebnisse aus der Bestandsanalyse bezüglich der zu antizipierenden Mengengerüste (siehe Kapitel 3.1.5) haben diesbezüglich aufgezeigt, dass sich hohe Anforderungen an die Leistungseffizienz und Skalierbarkeit der Transportinfrastruktur ergeben werden. In Hinblick auf Wartbarkeit, ist die Zielarchitektur darauf ausgelegt, eine wachsende Anzahl von beteiligten Behörden und Fachverfahren zu unterstützen und auf zukünftige fachliche oder rechtliche Anforderungen reagieren zu können.

Die in diesem Abschnitt beschriebene Lösungsstrategie bildet den Bezugsrahmen für die nachfolgenden Architekturentscheidungen. Die einzelnen ADRs konkretisieren die wesentlichen Richtungsentscheidungen, die Bausteinsicht überführt diese in funktionale Verantwortlichkeiten, und die Laufzeit- sowie Querschnittssichten präzisieren das Zusammenwirken der Komponenten unter den vorgegebenen Sicherheits- und Betriebsprämissen.

4.2 Architekturentscheidungen

Die Zielarchitektur basiert auf einer Reihe zentraler Architekturentscheidungen, die im Verlauf der Architekturarbeit getroffen wurden. Diese Entscheidungen adressieren unterschiedliche fachliche, technische und organisatorische Fragestellungen und prägen gemeinsam das in den folgenden Kapiteln beschriebene Zielbild. Sie bilden die Grundlage für die Ausgestaltung der Zielarchitektur sowie für die Ableitung weiterer Handlungsbedarfe.

Die Architekturentscheidungen wurden in Form von ADRs dokumentiert. Die detaillierte inhaltliche Auseinandersetzung mit einzelnen Entscheidungen erfolgt ausschließlich in den jeweiligen ADRs. Weitere Informationen zur Methodik finden sich in Kapitel 2.4. Das vorliegende Kapitel verfolgt demgegenüber das Ziel, die Architekturentscheidungen zusammenfassend darzustellen, thematisch zu ordnen und ihre Einbettung in die Zielarchitektur nachvollziehbar zu machen.

Die nachfolgende Tabelle 9 gibt einen vollständigen Überblick über alle im Rahmen der Zielarchitektur erstellten ADRs.

Tabelle 9: Liste der im Projekt dokumentierten ADRs mit ADR-ID und Titel

ADR-ID	Titel

ADR-000	Dokumentation von Architekturentscheidungen
ADR-001	Topologie der backendseitigen Kommunikationsinfrastruktur
ADR-002	Kommunikationskonzept
ADR-003	Festlegung des Endpunkts der Ende-zu-Ende-Verschlüsselung für das zentrale Fachverfahren
ADR-004	Auswahl der Ende-zu-Ende-Verschlüsselungsschicht
ADR-005	Authentizität und Integrität in der Ende-zu-Ende-Nachrichtenübermittlung
ADR-006	Authentizität: Identität öffentlicher Stellen
ADR-007	Authentizität: Identität privater Organisationen
ADR-008	Hilfsmodule zur vereinfachten Anbindung von Fachverfahren
ADR-009	Anschluss von externen Bestandssystemen an die Transportinfrastruktur

Die Architekturentscheidungen werden im Folgenden thematisch gruppiert. Die Cluster orientieren sich an den wesentlichen Gestaltungsdimensionen der Zielarchitektur und dienen dazu, Zusammenhänge zwischen einzelnen Entscheidungen sichtbar zu machen. Eine inhaltliche Wiederholung oder Bewertung der einzelnen Entscheidungen erfolgt dabei bewusst nicht. Die thematische Gliederung schafft vielmehr eine Lesebrücke zwischen der beschriebenen Zielarchitektur und den zugrundeliegenden ADRs.

4.2.1 Kommunikations- und Integrationsarchitektur

Ein zentraler Teil der Zielarchitektur wird durch Architekturentscheidungen geprägt, die die grundlegende Ausgestaltung der Kommunikation und Integration zwischen den beteiligten Systemen festlegen. Diese Entscheidungen definieren, wie der Nachrichtenaustausch strukturiert ist, welche Rolle zentrale Infrastrukturkomponenten einnehmen und nach welchen Prinzipien Systeme miteinander gekoppelt werden.

Im Fokus dieses Clusters stehen insbesondere die Topologie der backendseitigen Kommunikationsinfrastruktur sowie das übergeordnete Kommunikationskonzept. Die getroffenen Entscheidungen legen fest, dass der Nachrichtenaustausch über eine zentrale, vermittelnde Infrastruktur erfolgt (ADR-001) und auf einem asynchronen

Kommunikationsmodell basiert (ADR-002). Versand und Verarbeitung von Nachrichten sind dadurch zeitlich entkoppelt, was die Robustheit bei Nichtverfügbarkeit einzelner Kommunikationsparteien erhöht.

Nicht entschieden wurde die Festlegung der konkreten technischen Umsetzung der TI. Insbesondere ist offen, ob die TI als Eigenentwicklung realisiert oder auf bestehenden Lösungen aufgebaut wird. Hier besteht ein Handlungsbedarf, der in Kapitel **Fehler! Verweisquelle konnte nicht gefunden werden.** adressiert wird.

4.2.2 Sicherheit in der Nachrichtenübermittlung

Dieser Cluster definiert die Prinzipien zur Sicherstellung von Vertraulichkeit, Integrität und Authentizität der Kommunikation.

Im Mittelpunkt steht die Festlegung einer ende-zu-ende-gesicherten Nachrichtenübermittlung (ADR-004), bei der die Verschlüsselung bis in die fachlichen Endpunkte reicht (ADR-003). Zentrale Infrastrukturkomponenten, wie die TI, sind nicht in den Vertrauensraum der Verschlüsselung eingebunden und haben zu keinem Zeitpunkt Zugriff auf entschlüsselte Inhalte. Damit wird eine klare Trennung zwischen Transport und fachlicher Verarbeitung hergestellt. Die Verantwortlichen der TI erhalten somit zu keinem Zeitpunkt Zugriff auf die fachlichen Daten, wodurch die TI nicht zum Vertrauensanker für die fachliche Vertraulichkeit sowie die ende-zu-ende-gesicherte Authentizität und Integrität der Nachrichten wird. Dies unterstützt insbesondere die Umsetzung des Zero-Trust-Prinzips.

Die Architekturentscheidungen dieses Clusters definieren darüber hinaus, dass Authentizität und Integrität der Nachrichten konzeptionell eng an die E2EE gekoppelt sind (ADR-005). Die Sicherstellung dieser Schutzziele erfolgt nicht unabhängig, sondern auf Basis der gewählten Verschlüsselungsmechanismen. Dadurch wird ein konsistentes Sicherheitsmodell geschaffen, das die Nachrichtenübermittlung ganzheitlich absichert.

Die konkrete Auswahl der Ende-zu-Ende-Verschlüsselungsschicht wurde im Rahmen der Architekturarbeit getroffen und in ADR-004 festgelegt. Weiterer Handlungsbedarf besteht jedoch hinsichtlich der nachgelagerten Ausgestaltung des Kryptokonzepts sowie des Betriebs- und Schlüsselmanagements. Diese Aspekte werden in Kapitel 6116 weiter behandelt.

4.2.3 Vertrauensanker und Authentizität der Kommunikation

Ein weiteres Cluster der Architekturentscheidungen betrifft die Absicherung der Absenderschaft und Vertrauenswürdigkeit von Nachrichten innerhalb der Zielarchitektur. Die

Entscheidungen in diesem Bereich legen fest, auf welcher Grundlage Kommunikationspartner einander als legitim und vertrauenswürdig anerkennen und wie dieser Vertrauensnachweis technisch überprüfbar gemacht wird.

Im Mittelpunkt stehen dabei Entscheidungen zur organisationsbezogenen Authentizität der Kommunikation. Für öffentliche Stellen wird die Vertrauenswürdigkeit der Absenderschaft über bestehende staatliche Vertrauensinfrastrukturen sichergestellt (ADR-006). Die Architekturentscheidungen legen fest, dass hierfür Zertifikate aus der Verwaltungs-Public Key Infrastruktur (V-PKI) als kryptografischer Vertrauensanker genutzt werden. Für private Organisationen wird ein davon abgegrenzter Ansatz gewählt, der auf Zertifikaten aus einer öffentlichen PKI basiert (ADR-007). In beiden Fällen wird die Absenderschaft von Nachrichten auf Organisationsebene kryptografisch nachgewiesen und maschinenlesbar überprüfbar gemacht. Die konkrete technische Ausgestaltung dieser Mechanismen ist nicht Bestandteil dieses Kapitels.

Die Entscheidungen dieses Clusters definieren damit die grundlegenden Vertrauensanker der Zielarchitektur und legen fest, auf welcher Basis Kommunikationsbeziehungen als authentisch und vertrauenswürdig gelten. Sie schaffen die Voraussetzung für eine sichere Ende-zu-Ende-Kommunikation, ohne die Ausgestaltung des Identitäts- und Berechtigungsmanagements vorwegzunehmen. Die konkrete Modellierung und das Zusammenspiel der eingesetzten Mechanismen werden im Identitäts- und Vertrauensmodell in Kapitel 4.5.1 beschrieben.

4.2.4 Integration, Bestand und Weiterentwicklung

Das letzte Cluster der Architekturentscheidungen umfasst Festlegungen zur Anbindung bestehender und neuer Fachverfahren sowie zur langfristigen Weiterentwicklung der Zielarchitektur. Die Entscheidungen in diesem Bereich adressieren insbesondere die Frage, wie die Zielarchitektur in die bestehende Systemlandschaft integriert und wie gleichzeitig eine langfristig nachhaltige Entwicklung ermöglicht werden kann.

Im Fokus stehen Entscheidungen zur Anbindung von Bestandssystemen (ADR-009) sowie zur Unterstützung externer Fachverfahren durch Hilfsmodule (ADR-008). Die Architekturentscheidungen legen fest, dass Bestandssysteme temporär über geeignete Adapter an die Zielarchitektur angebunden werden können, bis die Anpassung an die neuen Anschlussbedingungen erfolgt ist. Diese Adapter sind dabei ausdrücklich als Übergangslösung zu verstehen und nicht als Bestandteil des dauerhaften Zielbilds

Ergänzend wird festgelegt, dass die Zielarchitektur durch die Bereitstellung von Software Development Kits (SDK) unterstützt wird, um die Anbindung neuer oder eigenentwickelter Fachverfahren zu vereinfachen. Die SDKs dienen dazu, Integrationsaufwände zu reduzieren, eine konsistente Umsetzung sicherheitsrelevanter Anforderungen zu fördern und die korrekte Nutzung der vorgesehenen Schnittstellen zu erleichtern.

Die Entscheidungen dieses Clusters reduzieren damit die Aufwände der Migration und der Anbindung in einem heterogenen Umfeld. Sie unterstützen eine kontrollierte Öffnung der Plattform für weitere Fachverfahren, ohne die Integrität oder Stabilität der Zielarchitektur zu gefährden.

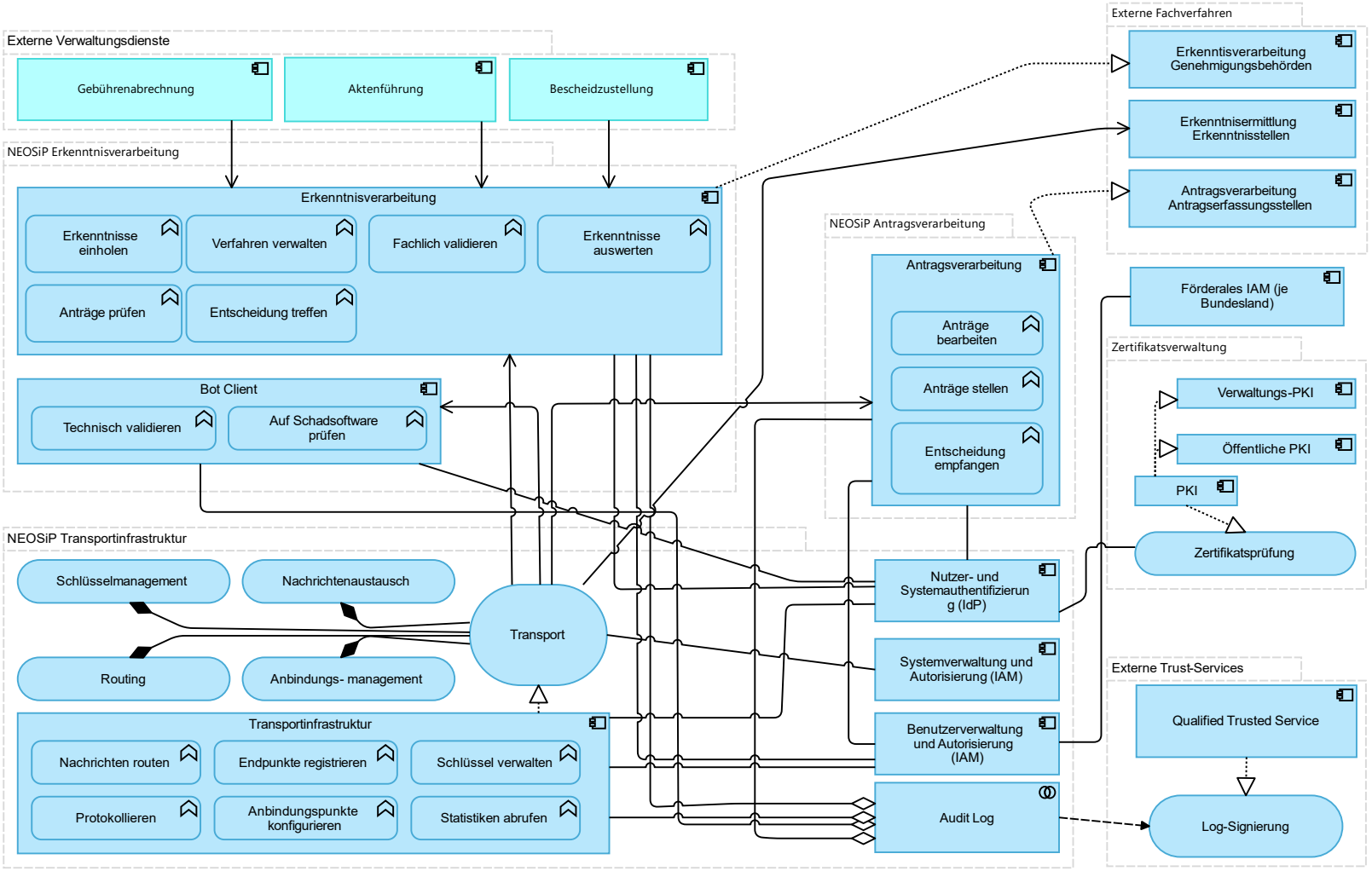


Abbildung 21: Darstellung der Kernfunktionen der drei Hauptkomponenten Antragsverarbeitung, Erkenntnisverarbeitung und Transportinfrastruktur sowie deren Kommunikationsbeziehungen untereinander.

4.3 Beschreibung der Hauptkomponenten

In diesem Kapitel wird die Architektur des Gesamtsystems in funktionalen Einheiten, den sogenannten Hauptkomponenten, dargestellt. Es erfolgt eine Beschreibung der Hauptkomponenten sowie eine Darlegung der Entscheidungen, die die Darstellung auf Basis der ADRs begründen. Ziel ist es, die Architektur in überschaubare Einheiten zu gliedern, deren spezifische Verantwortlichkeiten, Schnittstellen und Beziehungen zueinander transparent zu machen.

Die Zielarchitektur unterscheidet dabei zwei Klassen von Hauptkomponenten:

- die Transportinfrastruktur (TI) als gemeinsam genutzte, technisch vermittelnde Plattform für den sicheren Nachrichtenaustausch und
- die Fachverfahren als fachverarbeitende Systeme der AES, GB und EKS. Zu diesen Fachverfahren zählen sowohl bereits vorhandene, dezentral angebundene Fachverfahren als auch das zentral bereitgestellte Fachverfahren.

Das zentral bereitgestellte Fachverfahren ist nicht Teil der TI, sondern eine regulärer Teilnehmer an der TI. Es unterliegt denselben Anschlussbedingungen, Sicherheitsanforderungen und Kommunikationsstandards wie alle anderen angebundenen Fachverfahren. Die TI übernimmt daher ausschließlich Transport-, Zustell-, Routing- und technische Prüfaufgaben, während fachliche Verarbeitung, fachliche Entscheidungen und die Hoheit über fachliche Klartextinhalte in den Fachverfahren verbleiben.

Das weitere Kapitel strukturiert sich entlang der zentralen Hauptkomponenten für Antragsverarbeitung, Erkenntnisverarbeitung und Transport. Für jeden dieser Bausteine werden im Folgenden die technische Einbettung, die internen Strukturprinzipien, die wesentlichen Schnittstellen sowie die wesentlichen Rollen und Rechte beschrieben.

In Abbildung 21 wird grob aufgezeigt welche Kernfunktionalitäten die Hauptkomponenten erfüllen und wie diese Hauptkomponenten miteinander in Beziehung stehen.

4.3.1 Transportinfrastruktur

Die Transportinfrastruktur (TI) ist die zentrale, vermittelnde Komponente für den Nachrichtenaustausch zwischen allen beteiligten Systemen. Sie ermöglicht vor allem den Austausch von Anträgen, Anfragen und Erkenntnissen zwischen den GB, EKS und AES. Die TI ist dabei als technisch vermittelnde Plattform und nicht als fachverarbeitende Instanz zu

verstehen. Sie verarbeitet fachliche Nutzdaten ausschließlich in verschlüsselter Form und trifft keine fachlichen Entscheidungen.

Die TI nimmt Nachrichten entgegen, prüft diese auf technische Zulässigkeit, löst deren technische Zieladresse auf, hält sie bis zum Abruf durch berechtigte Empfängersysteme temporär vor und dokumentiert die hierfür erforderlichen technischen Zustandsübergänge. Fachliche Verfahrenszustände werden in der TI nicht geführt.

Architektonisch ist die TI in eine Datenebene und eine Steuerungsebene zu gliedern. Die Datenebene wird durch den Zustelldienst gebildet und umfasst die Annahme, Zustellung, temporäre Vorhaltung, Zustandsführung und technische Protokollierung von Nachrichten. Die Steuerungsebene umfasst die Verwaltung technischer Teilnehmer, Zustellpunkte, Kommunikationsbeziehungen, öffentlicher Schlüssel, technischer Empfangsparameter, transportbezogener Berechtigungen sowie Routing- und Kommunikationspolicies. Diese Trennung folgt dem Muster bewährter föderaler Transportinfrastrukturen wie FIT-Connect und wird hier vorwiegend an die Mehrparteienkommunikation und den hohen Schutzbedarf angepasst.

Im Unterschied zu ordinären Sender-Empfänger-Infrastrukturen muss die TI Kommunikationsbeziehungen zwischen AES, GB und EKS in verschiedenen Rollenbildern unterstützen. Hierzu sind eindeutig adressierbare technische Endpunkte bzw. Zustellpunkte vorzusehen, auf die Routing, Berechtigungen, technische Empfangsparameter und kryptographische Metadaten referenzieren. Zustellpunkte sind damit nicht nur adressierbare Ziele der Zustellung, sondern zudem die zentrale Referenz für zugelassene Kommunikationsbeziehungen und Schutzklassen im Sinne der VSA.

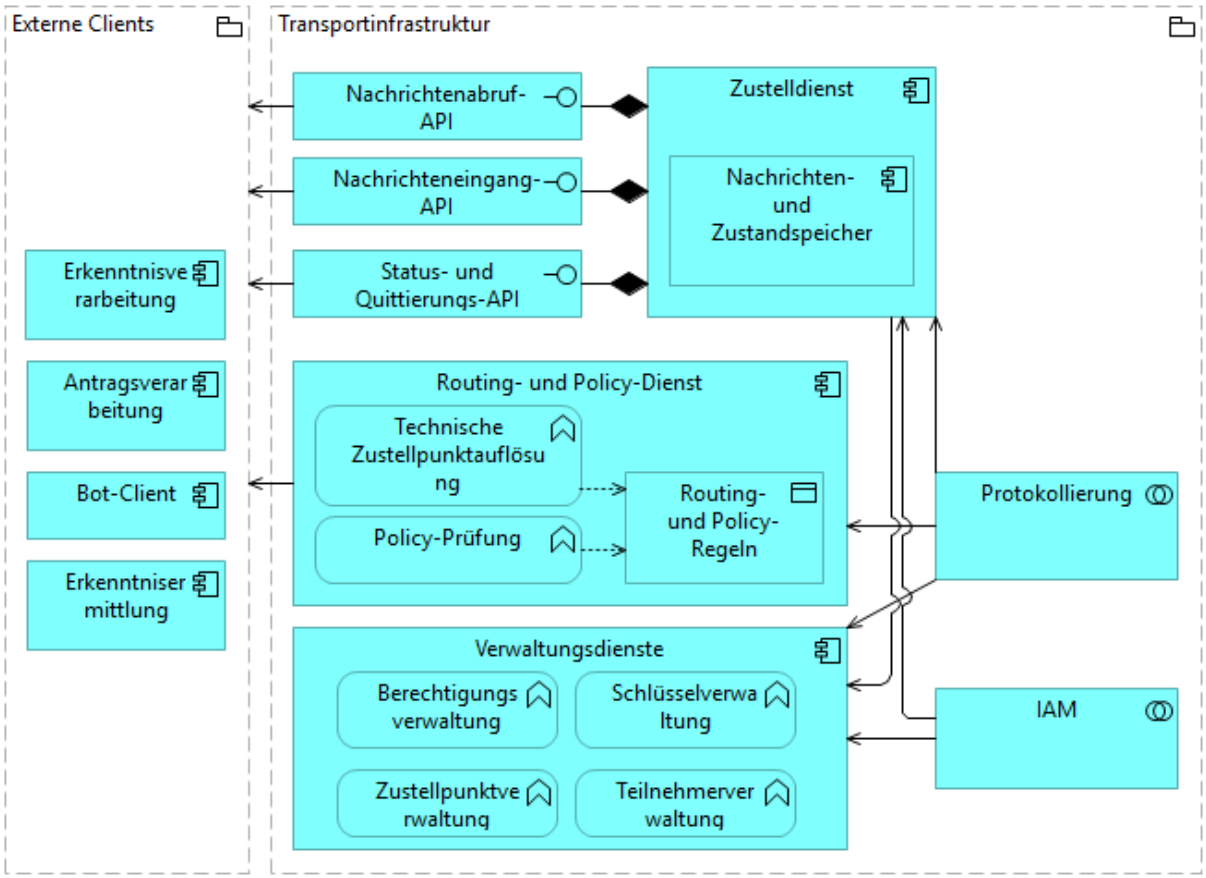


Abbildung 22: Schematische Darstellung der TI als vermittelnde Schicht zwischen angebundenen Fachverfahren, Routing-Mechanismen und Schnittstellen für ein- und ausgehende Nachrichten

Der Verantwortungsbereich der TI wird wie folgt abgegrenzt.

Innerhalb der Systemgrenze

- Nachrichtenannahme und Nachrichtenweiterleitung
- Technische Zustellpunktauflösung und Routing
- Temporäre Vorhaltung von Nachrichten
- Verwaltung technischer Kommunikationsbeziehungen
- Monitoring der Kommunikation
- Verwaltung technischer Zustell-, Prüf- und Fehlerzustände
- Quarantäne technischer Problemfälle
- Zentrale, unveränderbare Auditierung technischer Transportvorgänge
- Verwaltung und Bereitstellung öffentlicher Schlüssel sowie technischer Empfangsparameter

- Teilnehmer-, Zustellpunkt- und Verzeichnisverwaltung
- Bereitstellung eines technischen Ereignisprotokolls zu Transport- und Zustellereignissen

Außerhalb der Systemgrenze

- Ver- und Entschlüsselung fachlicher Inhalte
- Vorhaltung privater Schlüssel zur Entschlüsselung fachlicher Nutzdaten
- Fachliche Verarbeitung von Nachrichten
- Fachliche Bewertung von Anträgen, Erkenntnissen und Entscheidungen
- Fachliche Bewertung technischer Fehlerfälle
- Fachliche Verfahrenssteuerung und Aktenführung
- Fachliche Entscheidung darüber, welche Erkenntnisstellen in einem konkreten Verfahren zu beteiligen sind, soweit dies nicht bereits als technische Routing-Policy vorgegeben wurde

Die TI implementiert ein mehrschichtiges Sicherheitskonzept. Dieses ist in Tabelle 10 zusammengefasst.

Tabelle 10: Tabelle mit den Sicherheitsschichten der TI und ihren jeweiligen Schutzmechanismen

Schicht	Mechanismus	Zweck
Anwendungsschicht	Ende-zu-Ende-Verschlüsselung und Integritätsschutz auf Nachrichtenebene	Schutz der Fachinhalte, Nachweisbarkeit der Unverändertheit, Zero-Knowledge Prinzip
Transportschicht	mTLS	Authentizität der Kommunikationspartner, Schutz der Metadaten
Netzwerkschicht	Segmentierung, Firewalls	Isolation der Infrastruktur, Angriffsflächen-Minimierung
Infrastrukturschicht	Encryption at Rest	Schutz der vorgehaltenen Nachrichten und technischen Metadaten

Dieses mehrschichtige Sicherheitsmodell bildet die Grundlage für den technischen Aufbau der Komponente. Die nachfolgende **Fehler! Verweisquelle konnte nicht gefunden werden.**

detailliert diesen Aufbau in der Bausteinsicht und zeigt die funktionalen Einheiten, die das Sicherheitskonzept operativ umsetzen. Dabei fungieren die Eingangs- und Abrufschnittstellen sowie die validierenden Komponenten als erste Verteidigungslinie auf Netzwerk- und Transportebene, während die dahinterliegenden Speicher- und Queue-Komponenten die Datensicherheit auf Infrastrukturebene gewährleisten. Die validierenden Komponenten prüfen dabei ausschließlich Transport-, Identitäts-, Integritäts-, Schutzkennzeichnungs- und Routing-Metadaten sowie technische Formatanforderungen der Umschläge. Eine Prüfung fachlicher Klartextinhalte findet in der TI nicht statt.

4.3.1.1 Zustelldienst

Der Zustelldienst bildet die operative Datenebene der TI. Er ist für die Entgegennahme, technische Prüfung, persistente Vorhaltung, Zustandsführung, Bereitstellung zum Abruf sowie die technische Nachweisführung von Nachrichten verantwortlich.

4.3.1.1.1 Nachrichteneingang-API

Die Nachrichteneingang-API fungiert als zentraler Einstiegspunkt für alle eingehenden Nachrichten in die TI. Sie übernimmt die Aufgabe, verschlüsselte Nachrichten von authentifizierten und autorisierten Systemen entgegenzunehmen, technisch zu prüfen und bei erfolgreicher Annahme zur weiteren Verarbeitung zu persistieren.

Vor der Übernahme einer Nachricht erfolgt eine technische Prüfung des Kommunikationsvorgangs. Dabei werden insbesondere die Identität des Senders, die Zulässigkeit der adressierten Kommunikationsbeziehung, die Integrität des Nachrichtenumschlags, die Vollständigkeit der erforderlichen technischen Metadaten sowie die technische Erreichbarkeit bzw. Gültigkeit des adressierten Empfängers geprüft. Die Prüfung bezieht sich ausschließlich auf technisch auswertbare Umschlags- und Steuerungsinformationen. Fachliche Klartextinhalte werden nicht verarbeitet.

Architektonisch ist die Nachrichteneingang-API als horizontal skalierbare, zustandslose Komponente konzipiert, um Lastspitzen zuverlässig bewältigen zu können. Für robuste asynchrone Kommunikation sind fachverfahrensübergreifend eindeutige Nachrichten- und Korrelationskennungen, Regeln zur Idempotenz sowie Mechanismen gegen Replay- und Duplikatverarbeitung vorzusehen.

Es ist sicherzustellen, dass die zur Verschlüsselung benötigten empfängerbezogenen Zustellpunkt- und Schlüsselmetadaten vor dem eigentlichen Versand bereits aufgelöst wurden

oder zusammen mit der adressierten Zustellpunktreferenz eindeutig referenzierbar sind. Die Nachrichteneingangs-API selbst darf keine fachliche Empfängerauswahl nachholen.

4.3.1.1.2 Nachrichtenabruf API

Die Nachrichtenabrufs API bildet die standardisierte Schnittstelle, über die berechtigte Empfängersysteme ihre Nachrichten aus der TI abrufen können. Dabei wartet die API auf eingehende Abrufanfragen der zugewiesenen Empfängersysteme und stellt die für den jeweiligen Mandanten bestimmten Nachrichten kontrolliert bereit. Abrufbar sind nur Nachrichten, die sich im jeweils zulässigen technischen Zustand befinden, insbesondere im Status „abholbereit".

Die Anforderungen an Dokumentation, Authentifizierung und Transportverschlüsselung entsprechen grundsätzlich denen der Nachrichteneingang-API.

Abrufende Systeme können für sie bereitgestellte Nachrichten abfragen. Die API implementiert Paging-Mechanismen, um auch bei großen Nachrichtenmengen performante Abfragen zu gewährleisten. Das abrufende System quittiert die Nachrichtenabholung, sodass die Queue-Infrastruktur erfolgreich abgerufene Nachrichten als technisch zugestellt markiert und diese gemäß dem Löschkonzept sicher entfernt werden. Zusätzlich ist die Schnittstelle so auszugestalten, dass Wiederholungsabrufe kontrolliert, idempotent und revisionsfähig verarbeitet werden können.

4.3.1.1.3 Status- und Quittungs-API

Ergänzend ist eine getrennte Status- und Quittungs-API vorzusehen, über die technische Vorprüfungen, Zustellereignisse und Fehlerzustände an die TI zurückgemeldet oder aus ihr abgerufen werden können. Hierüber werden insbesondere Ergebnisse technischer Vorprüfungen, etwa Schema- oder Schadsoftwareprüfungen, sowie technische Zustell- und Abholquittungen verarbeitet.

Erst auf Basis definierter Statusrückmeldungen darf eine Nachricht – sofern das jeweilige Anschlussmodell dies vorsieht – in den Zustand „abholbereit" für den fachlichen Empfänger überführt werden. Statusmeldungen sind revisionsfähig und idempotent zu verarbeiten.

Durch diese explizite Trennung wird verhindert, dass technische Vorprüfungen implizit in die Abruflogik oder in Fachverfahren hineinmodelliert werden.

4.3.1.1.4 Nachrichten- und Zustandsspeicher

Der Nachrichten- und Zustandspeicher übernimmt die sichere, mandantenfähige Speicherung von verschlüsselten Nachrichteninhalten, technischen Zuständen und den für die operative Zustellung erforderlichen Metadaten. Er bildet die persistente Grundlage des Zustelldienstes und unterliegt strengen Datenschutz- und Sicherheitsanforderungen.

Ein fundamentales Designprinzip ist, dass die Verarbeitung von Fachinhalten ausschließlich in verschlüsselter Form erfolgt. Dabei hat diese Schicht zu keinem Zeitpunkt die Möglichkeit, verschlüsselte Inhalte zu entschlüsseln, da die dafür erforderlichen Schlüssel ausschließlich bei den beteiligten Behörden in deren Fachverfahren vorgehalten werden. Dieses Zero-Knowledge-Prinzip stellt sicher, dass selbst bei einer vollständigen Kompromittierung der Speicherschicht keine fachlichen Inhalte offengelegt werden können.

Ergänzend zur Ende-zu-Ende-Verschlüsselung der Nutzlasten wird auf Infrastrukturebene eine Verschlüsselung ruhender Daten für technische Metadaten, Systemprotokolle und zustellbezogene Zustandsdaten vorzusehen, wobei bei der Wahl des Verschlüsselungsverfahrens die Vorgaben und Empfehlungen des BSI einzuhalten sind. Dies schützt Daten vor unbefugtem Zugriff auf Speicherebene. Die Mandantentrennung ist auf Datenhaltungsebene logisch und revisionssicher durchzusetzen, sodass Daten verschiedener Organisationen nicht vermischt werden und Zugriffe strikt auf den jeweiligen Mandantenkontext beschränkt bleiben.

Zusätzlich sind die gespeicherten technischen Nachrichtenzustände so zu modellieren, dass mindestens zwischen „eingegangen“, „technisch validiert“, „in technischer Prüfung“, „abholbereit“, „zugestellt“, „fehlgeschlagen“, „quarantänisiert“ und „gelöscht“ unterschieden werden kann. Fachliche Verfahrenszustände, wie etwa „in Bearbeitung“, „bewertet“ oder „entschieden“, werden dagegen ausschließlich in den Fachverfahren geführt.

Die Datenverwaltung berücksichtigt umfassend die Anforderungen aus Datenschutz und Compliance. Das System implementiert Aufbewahrungsfristen gemäß gesetzlicher Vorgaben sowie ergänzender, fachlicher Festlegungen und setzt diese durch automatisierte Löschroutinen technisch durch. Nach Abruf der Daten und Quittierung durch den Empfänger werden Daten systematisch und unwiederbringlich gelöscht. Fristen zur maximal zulässigen Dauer der Zwischenspeicherung von Fachinhalten werden im Rahmen der Umsetzung festgelegt. Für technische Fehlerfälle und Quarantäne-Objekte sind gesonderte

Aufbewahrungs- und Löschregeln festzulegen. Eine sofortige Löschung ist hier aus Gründen der Nachvollziehbarkeit und Forensik nicht in jedem Fall sachgerecht.

Revisionssicherheit wird durch unveränderbare Speicherung von Audit-Protokollen gewährleistet. Sämtliche Datenzugriffe und -änderungen werden chronologisch protokolliert, wobei mindestens die ausführende Person oder das System, der Zeitpunkt und die Art der Operation erfasst werden. Diese Protokolleinträge bilden einen lückenlosen Audit-Trail für Compliance-Zwecke und werden signiert sowie verschlüsselt an eine zentrale Log-Archivierung übertragen. Statusänderungen werden vollständig versioniert, sodass frühere Systemzustände nachvollzogen werden können. Die Auswertung der Audit-Daten sollte zentral und komponentenübergreifend möglich sein, ohne dass dadurch die Trennung von Betriebs-, Sicherheits- und Fachrollen aufgehoben wird.

Neben Point-In-Time-Backup-Strategien (PITR) sind regelmäßig verschlüsselte, mandantengetrennte Sicherungen zu erstellen, um im Katastrophenfall eine zeitnahe vollständige Wiederherstellung zu ermöglichen. Die Integration in Business-Continuity- und Disaster-Recovery-Konzepte stellt sicher, dass definierte Recovery-Ziele (RTO/RPO) auch bei schwerwiegenden Störungsfällen eingehalten werden können.

4.3.1.2 Routing- und Policy-Dienst

Der Routing Dienst übernimmt die zentrale Aufgabe der regelbasierten, manipulationssicheren Adressierung von Nachrichten an die jeweils zuständigen Empfängersysteme. Er implementiert eine regelbasierte Zuständigkeitsauflösung und Routenermittlung auf Basis konfigurierbarer Kriterien und verweist dabei auf den passenden Zustellpunkt bzw. die zulässigenadressierbaren Zustellpunkte. Die Nachrichtenzustellung selbst erfolgt nicht im Routing- und Policy-Dienst, sondern im Zustelldienst.

Die Routing-Logik berücksichtigt dabei Kombinationen aus Bundesland, Anwendungsbereich, geografischen Bezügen sowie weiteren fachlichen Parametern, sofern diese als Meta-Daten abgebildet werden können. Diese Parameter müssen als minimierte, signifikante und technisch auswertbare Steuerungsmetadaten vorliegen. Die technische Zuständigkeitsauflösung darf nicht von der Entschlüsselung fachlicher Nutzdaten abhängen.

Soweit mehrere Erkenntnisstellen oder sonstige Kommunikationsparteien wie AES adressiert werden müssen, ist zwischen der technischen Ermittlung zulässiger Zielzustellpunkte und der fachlichen Entscheidung über die in einem konkreten Verfahren tatsächlich zu beteiligenden Stellen zu unterscheiden. Die fachliche Entscheidung verbleibt grundsätzlich außerhalb der TI,

sofern sie nicht bereits vorab in freigegebenen Kommunikations-Policies technisch vorgegeben wurde. Die Routing- und Policy-Logik gewährleistet insbesondere, dass Nachrichten nur an technisch zulässige und für den jeweiligen Fall freigegebene Zustellpunkte adressiert werden.

In einer Datenbank werden alle Routing-Konfigurationen integritätsgeschützt, versioniert und dauerhaft gespeichert. Der Zugriff auf Routing-Konfigurationen wird über ein rollenbasiertes Zugriffskontrollsystem gesteuert, das feingranular festlegt, welche Nutzer:innen und Systeme, welche Routing-Regeln einsehen oder bearbeiten dürfen. Routing-Regeln werden durch berechtigte Personen auf Anweisung zentral gepflegt. Für produktiv wirksame Änderungen ist aufgrund der Kritikalität der Routing-Entscheidungen ein Vier-Augen-Prinzip vorzusehen, bei dem Erstellung und Freigabe organisatorisch getrennt sind.

Nachvollziehbarkeit und Auditierbarkeit der Routing-Konfiguration wird durch umfassende Protokollierungsmechanismen sichergestellt. Jede Änderung an Routing-Regeln wird vollständig und chronologisch dokumentiert, wobei mindestens die ausführende Person, der Zeitpunkt und der geänderte Inhalt erfasst werden. Diese Protokolleinträge sind unveränderbar gespeichert und bilden einen lückenlosen Audit-Trail, der sowohl für Compliance-Zwecke als auch für die Fehleranalyse und Nachvollziehbarkeit von Zustellungsproblemen herangezogen werden kann. Die Routing-Datenbank unterstützt eine vollständige Versionierung aller Konfigurationen, sodass frühere Zustände rekonstruiert und bei Bedarf wiederhergestellt werden können.

Die Speicherung der Regeln erfolgt in einer mandantenfähigen Datenbankarchitektur, die sowohl mandantenspezifische als auch mandantenübergreifende Routing-Regeln unterstützt. Mandantenübergreifende Regeln sind dabei restriktiv zu handhaben und gesondert zu kennzeichnen, da sie systemweit wirksam werden können.

Um Anforderungen des Geheimschutzes bezüglich digitalem Labeling[23] von Verschlusssachen zu genügen, muss jeder Datentyp und Datensatz beim Übertragen in die Transportinfrastruktur ein entsprechendes Attribut setzen. So markierte Datensätze dürfen nur an Klienten ausgeliefert werden, die die VS-IT Voraussetzung vollständig erfüllen. Entsprechende

[23] Digitales Labelling BSI-VS-AP-0023-2020 Version 1.0

Schutzkennzeichnungen sind deshalb nicht nur im Nachrichtenumschlag, sondern auch in Zustellpunktmerkmalen und Routingpolicies konsistent zu berücksichtigen.

4.3.1.3 Teilnehmer-, Zustellpunkt- und Schlüsselverwaltung

Dieser Baustein verwaltet technische Teilnehmer, deren Identitäten und Berechtigungen, eindeutig adressierbare Zustellpunkte, technische Empfangsparameter sowie die für die Ende-zu-Ende-Verschlüsselung und Integritätsprüfung erforderlichen öffentlichen Schlüssel.

Technische Teilnehmer und Zustellpunkte sind dabei getrennt zu modellieren. Ein technischer Teilnehmer repräsentiert eine identifizierte und autorisierte Systemanbindung. Ein Zustellpunkt repräsentiert das adressierbare Ziel einer Nachrichtenübermittlung. Ein Teilnehmer kann mehrere Zustellpunkte betreiben, und ein Zustellpunkt kann zusätzliche Merkmale wie Schutzklasse, Mandantenzuordnung, unterstützte Kommunikationsbeziehungen, technische Erreichbarkeit und kryptographische Parameter aufweisen.

Öffentliche Schlüssel und sonstige empfangsseitige kryptographische Metadaten müssen versioniert, vertrauenswürdig referenzierbar und für berechtigte Sender vor dem Versand verfügbar sein. Schlüsselrotation, Sperrung und Gültigkeitsprüfung sind als reguläre Verwaltungsprozesse vorzusehen.

4.3.1.4 Rollen & Rechte

Folgende Rollen sind für diesen Baustein notwendig und in Tabelle 11 zusammengestellt.

Tabelle 11: Tabelle mit den zentralen Rollen innerhalb der TI und deren Berechtigungen, einschließlich administrativer, technischer und fachlicher Rechte

Rolle	Verantwortlichkeit	Zugriffsrechte
System-Administrator:in	Betrieb, Überwachung, Incident Management	Zugriff auf technische Metriken, Betriebslogs und Infrastrukturkonfigurationen. Kein Zugriff auf fachliche Klartextinhalte und kein Zugriff auf private Schlüssel zur Entschlüsselung fachlicher Nutzdaten.
Routing-Redakteur:in (Land/Zentral/Anwendungsbereich)	Pflege der Routing-Regeln für ein Bundesland, einen Anwendungsbereich oder eine Kombination aus diesen.	Erstellungs- und Bearbeitungsrechte für Routing-Regeln des zugeordneten Verantwortungsbereichs,

		Lesezugriff auf Audit-Logs des Routing.
Routing-Freigabeverantwortliche:r (Land/Zentral/Anwendungsbereich)	Freigabe produktiv wirksamer Routing-Änderungen im Vier-Augen-Prinzip	Freigaberecht für Routing-Regeln, kein alleiniger Bearbeitungs- und Freigabevollzug in Personalunion.
Security-Auditor:in (Intern/Extern)	Überprüfung der Einhaltung von Sicherheitsanforderungen	Lesezugriff auf Audit-Trails, Konfigurationen, Sicherheitsprotokolle
Fachverfahren von AES, GB und EKS	Ablage und Abholung von Nachrichten	Zugriff beschränkt auf die jeweils autorisierten Kommunikationsbeziehungen und auf eigene Nachrichten im Mandantenkontext.
Zustellpunktverantwortliche:r	Pflege und Freigabe technischer Zustellpunktkonfigurationen, Empfangsparameter und zugeordneter öffentlicher Schlüssel	Bearbeitungs- und Freigaberechte für zugewiesene Zustellpunkte und deren technische Parameter; kein Zugriff auf fachliche Inhalte

4.3.2 Zentral bereitgestelltes Fachverfahren

Das zentral bereitgestellte Fachverfahren ist eine gemeinsam betriebene, mehrmandantenfähige Fachverfahrenslösung für Organisationen, die kein eigenes Fachverfahren bereitstellen oder anbinden wollen. Es dient zugleich als Referenzimplementierung für die fachliche und technische Nutzung der TI.

Das Fachverfahren ist dabei nicht Bestandteil der TI, sondern ein regulärer Teilnehmer der Transportinfrastruktur. Es muss daher dieselben Anschlussbedingungen, Sicherheitsvorgaben, Authentifizierungsmechanismen, Autorisierungsregeln, Protokollierungsanforderungen und kryptographischen Prinzipien erfüllen wie jedes andere angebundene Fachverfahren. Ein privilegierter Sonderzugang zur TI ist nicht vorzusehen.

Aus fachlicher Sicht gliedert sich das Fachverfahren in zwei Bausteine:

- einen Baustein zur Antragsverarbeitung für AES und
- einen Baustein zur Verfahrens- und Erkenntnisverarbeitung für GB.

Ergänzend ist ein mandantennaher Bot-Client vorgesehen, mit dem technische Teilfunktionalitäten des Nachrichtenaustauschs und der technischen Vorprüfung automatisiert

werden können. Aufgrund der Anforderungen an Betreiberblindheit und Schlüsselhoheit ist dieser Bot-Client architektonisch von den zentral betriebenen Komponenten des Fachverfahrens zu unterscheiden.

4.3.2.1 Erkenntnisverarbeitung

Diese Hauptkomponente ermöglicht den Empfang und die Verarbeitung von Anträgen aus den AES sowie die Rückkopplung mit diesen im Rahmen von Nachforderungen, Rückfragen und der Entscheidungsbekanntgabe. Zudem werden mit dieser Hauptkomponente die eigentlichen ZSÜ-Verfahren gestartet und verwaltet, in deren Verlauf die EKS angefragt und eingehende Erkenntnisse gesichtet, bewertet und in die Verfahrensentscheidung einbezogen werden.

Architektonisch ist diese Komponente als mehrteilige Anwendung konzipiert, bestehend aus einem Nutzenden-Client, einem Administrations-Frontend und einem zentral betriebenen Backend. Aus kryptographischer Sicht ist die Komponente so auszulegen, dass fachliche Klartextverarbeitung ausschließlich im Mandantenkontext erfolgt, während zentrale Komponenten ohne Zugriff auf das hierfür erforderliche Schlüsselmaterial betrieben werden können. Frontend Komponente

Das Frontend soll in den Browsern der Nutzer ausgeführt werden. Es übernimmt dort die fachinhaltliche Anzeige-, Entschlüsselungs-, Verschlüsselungs- und Bearbeitungslogik. Die Entscheidung für diese Architektur ist dabei eine Konsequenz aus der Sicherheitskonzeption der Zielarchitektur. Da das Backend mit Zero-Knowledge arbeiten soll und somit keinen Zugriff auf kryptografische Schlüssel besitzen wird, wird es technisch nicht in der Lage sein, inhaltliche Daten zu verarbeiten oder fertig gerenderte Ansichten mit Klartextinhalten auszuliefern. Die Ent- und Verschlüsselung für die Darstellung und Verarbeitung müssen somit entsprechend zwingend auf die Endgeräte verlagert werden. Hiervon unberührt bleibt prozessbezogene Steuerungslogik auf Basis nicht-inhaltlicher Metadaten, die weiterhin zentral im Backend umgesetzt werden kann.

Dabei ist zwischen der Verarbeitung von Daten im Rahmen der Bearbeitung von Anträgen und Verfahren und Nachrichten in der Kommunikation zu AES und EKS zu unterscheiden. Nachrichten werden für die entsprechenden Kommunikationsparteien ver- und entschlüsselt und direkt über die TI übermittelt. Alle weiteren Daten werden mit dem Backend ausgetauscht und dort vorgehalten. Soweit diese weiteren Daten fachliche Inhaltsdaten enthalten, sind sie vor der Übermittlung an das Backend clientseitig zu verschlüsseln. Im Klartext dürfen im

Backend ausschließlich die für Workflow, Fristen, Zuordnung und Rechteprüfung zwingend erforderlichen Steuerungsmetadaten verarbeitet werden.

4.3.2.1.1 Backend Komponente

Das Backend soll als persistenter Datenspeicher für die Antrags- und Verfahrensdaten sowie als Workflow-Engine fungieren. Hierbei agiert es jedoch vollständig ohne Kenntnis der fachlichen Inhalte.

Nach dem Abruf von Nachrichten aus der TI durch hierfür vorgesehene mandantenseitige Komponenten und nach der clientseitigen Verarbeitung nimmt das Backend die verschlüsselten Inhaltsdaten sowie die zugehörigen Steuerungsmetadaten entgegen und persistiert diese. Es soll keinen Zugriff auf das kryptografische Schlüsselmaterial der Nutzenden besitzen, sodass unberechtigte keine Einsicht in diese Daten erhalten können.

Das Backend muss jedoch eine definierte Menge an Metadaten und Statusinformationen verarbeiten können, um beispielsweise die Zuordnung von Nachrichten zu Aktenzeichen, Fristenüberwachung oder Antragsstatus zu bewerkstelligen. Diese Trennung von Steuerungsdaten und Inhaltsdaten ermöglicht effiziente Workflows unter Berücksichtigung der Datensicherheit. Die Menge der im Klartext verarbeiteten Metadaten ist dabei nach dem Erforderlichkeitsprinzip eng zu begrenzen.

Ein integraler Bestandteil des Backends muss die revisionssichere Protokollierung aller Aktionen gemäß den Vorgaben in Kapitel 4.5.3 sein. Vor allem müssen Nutzerinteraktionen wie lesende Zugriffe auf Datensätze sowie ändernde Operationen, wie beispielsweise Speichern einer Bewertung oder Statuswechsel, protokolliert werden. Administrative und sicherheitsrelevante Aktionen sind hiervon getrennt auswertbar zu erfassen.

4.3.2.1.2 Rollen und Rechte

Tabelle 12: Tabelle mit Rollen der Genehmigungsbehörden innerhalb der Erkenntnisverarbeitung und den damit verbundenen Zugriffs- und Bearbeitungsrechten

Rolle	Verantwortlichkeit	Zugriffsrechte (Auszug)
Nutzer:in	Bearbeitung von Anträgen, Versand von Anfragen an EKS, Sichtung und Bewertung von Erkenntnissen.	Lesender Zugriff auf zugewiesene Vorgänge; schreibender Zugriff im Rahmen der zugewiesenen Bearbeitungsschritte; Versand

		fachlicher Nachrichten über autorisierte Systemfunktionen
Freigabeverantwortliche:r / Vorgesetzte:r	Validierung kritischer Entscheidungen (Vier-Augen-Prinzip), z. B. bei Versagungen.	Lesender Zugriff auf freizugebende Vorgänge; Recht zur Freigabe, Rückgabe oder Überstimmung im Rahmen definierter Befugnisse
Behördenadministrator:in	Verwaltung der Stammdaten der Behörde (z. B. lokale Fristenregelungen).	Administrativer Zugriff auf Konfigurationen. Kein inhaltlicher Zugriff.
Auditor:in	Nachträgliche Prüfung der Verfahrensabläufe auf Rechtmäßigkeit. Einsicht auf Statistiken.	Lesender Zugriff auf Audit-Logs und Metadaten.

4.3.2.2 Antragsverarbeitung

Der Baustein Antragsverarbeitung stellt die fachliche Benutzeroberfläche für die Einreichung und Nachverfolgung von Anträgen dar. Er richtet sich insbesondere an Antragserfassungsstellen, die über kein eigenes, an die OSiP-TI angebundenes Fachverfahren verfügen. Vorwiegend soll die Antragsverarbeitung von Antragserfassenden privater Organisationen eingesetzt werden.

Ziel dieses Bausteins ist es, eine zentral bereitgestellte, ohne lokale Fachverfahrensinstallation nutzbare Software bereitzustellen, die dennoch die hohen Sicherheitsanforderungen der Zielarchitektur erfüllt und zugleich die Anschlussbedingungen der TI einhält.

Die Architektur orientiert sich dabei analog zur Erkenntnisverarbeitung an einer strikten Trennung zwischen einer clientseitigen Logik im Browser und einem unterstützenden Backend. Der technische Ablauf der Antragsverarbeitung, einschließlich Frontend-Erstellung, Verschlüsselung, Transport und Backend-Persistierung, ist in **Fehler! Verweisquelle konnte nicht gefunden werden.** dargestellt.

4.3.2.2.1 Frontend Komponente

Analog zum Frontend der Verfahrens- und Erkenntnisverarbeitung soll auch die Benutzeroberfläche der Antragsverarbeitung als browserbasierte Anwendung realisiert werden. Sie stellt den vertrauenswürdigen Endpunkt für die Dateneingabe der Antragserfassungsstellen dar.

Die Authentifizierung erfolgt über das im IAM-Konzept definierte föderierte Identitäts- und Zugriffsmodell. Die Verschlüsselung der Antragsdaten erfolgt clientseitig im Browser der Nutzer:innen. Konkrete technologische Umsetzungsentscheidungen hierzu sind im Kryptokonzept in der Umsetzungsphase festzulegen.

4.3.2.2.2 Backend Komponente

Das Backend speichert die technischen und fachlichen Steuerungsinformationen der Vorgänge, insbesondere Antrags-ID, Zeitstempel, Zuständigkeiten, Aufgaben- und Bearbeitungsstatus, im erforderlichen Umfang im Klartext. Darüber hinaus werden verschlüsselte Antragsdaten vorgehalten, um eine spätere weitere Bearbeitung, Nachforderung oder Einsicht im Mandantenkontext zu ermöglichen.

Auch für diesen Baustein gilt, dass fachliche Inhaltsdaten zentral ausschließlich in verschlüsselter Form verarbeitet und gespeichert werden dürfen. Das Backend des zentral bereitgestellten Fachverfahrens darf keinen Zugriff auf das hierfür erforderliche private Schlüsselmaterial besitzen.

4.3.2.2.3 Rollen und Rechte

Die in diesem Abschnitt verwendeten Rollen sowie deren Verantwortlichkeiten und Zugriffsrechte sind in Tabelle 13 dargestellt.

Tabelle 13: Tabelle mit den Rollen Fachbehördenadministrator:in und Organisationsvertreter:in, einschließlich ihrer Verantwortlichkeiten in der Anwendung sowie der jeweils zugewiesenen Zugriffsrechte

Organisationsadministrator:in	Administration der Anwendung, Konfiguration organisatorischer Einstellungen und Fristen.	Administrativer Zugriff auf Konfigurationen. Kein genereller Zugriff auf fachliche Klartextinhalte anderer Nutzer:innen.
Antragserfasser:in	Erfassung, Bearbeitung und Einreichung von Anträgen für Antragstellende.	Erstellung, Bearbeitung und versandt neuer Anträge. Ansicht der

		versandten Anträgen und deren Status.

4.3.2.3 Bot-Client

Der Bot-Client ist als mandantennaher Anschlussbaustein des zentral bereitgestellten Fachverfahrens konzipiert. Er dient dazu, den Nachrichtenaustausch mit der TI und definierte technische Vorprüfungen teilweise zu automatisieren. Seine primäre Aufgabe ist es, eingehende Nachrichten automatisiert abzurufen, im Mandantenkontext technisch zu prüfen und den technischen Prüfstatus an die TI zurückzumelden.

Der Bot-Client kann insbesondere dazu genutzt werden, eingehende Nachrichten schematisch zu validieren und auf Schadsoftware hin zu prüfen, bevor sie für die weitere fachliche Verarbeitung freigegeben werden. Er übernimmt dabei keine fachliche Bewertung des Inhalts und trifft keine fachlichen Entscheidungen.

Da die Bot-Clients Zugriff auf fachliche Inhalte brauchen, ist es, im Gegensatz zu den zentral bereitgestellten Komponenten, vorgesehen, dass die Bot-Clients dezentral in der Hoheit des jeweiligen Mandanten betrieben werden können. Hierbei sind die Bot-Clients als Serveranwendungen innerhalb der Sicherheitszonen der Mandanten zu betrieben. Dies ist aus Sicht der Betreiberblindheit der bevorzugte Regelfall. Ein zentraler Betrieb durch Dritte ist nur dann vertretbar, wenn die Anforderungen an Betreiberblindheit, Schlüsselhoheit des Mandanten und Schutz vor Datenabfluss mindestens gleichwertig nachgewiesen werden. Dies bedarf eines gesonderten Sicherheits- und Kryptokonzepts. Die Bereitstellung des Software-Artefakts (Container-Image oder Installationspaket) kann zentral erfolgen, der operative Betrieb sollte jedoch grundsätzlich im Verantwortungsbereich des jeweiligen Mandanten bzw. dessen IT-Dienstleisters liegen.

Da fachliche Inhalte während der Prüfung temporär entschlüsselt vorliegen können, entstehen erhöhte Risiken für Datenabfluss im Arbeitsspeicher, auf Host-Systemen und in Betriebsartefakten. Für Implementierung und Betrieb des Bot-Clients sind daher zusätzliche Maßnahmen zur Härtung der Laufzeitumgebung, zur Minimierung von Datenpersistenz, zur Unterbindung unkontrollierter Abflüsse und zum Betrieb mit minimalen Rechten vorzusehen.

In der Umsetzungsphase muss noch ein entsprechendes Betriebskonzept entwickelt werden. Vorstellbar wäre hier die Nutzung von Trusted Execution Environments (TEEs), welche den

Zugriff durch den Betreiber stark reduzieren würden. Unabhängig vom konkreten Hosting-Modell ist sicherzustellen, dass privates Schlüsselmaterial mandantenseitig kontrolliert, geschützt gespeichert und für Administrator:innen möglichst nicht im Klartext zugänglich ist.

4.3.2.3.1 Ablauf der Datenverarbeitung

Die Bot-Clients sollen weitgehend autonom arbeiten. Der Ablauf könnte sich in die folgenden Schritte aufgliedern:

1. **Abruf:** Der Bot-Client fragt über die Nachrichtenabruf-API der TI neue Nachrichten für seinen Mandanten ab.
2. **Entschlüsselung:** Da die Nachrichten Ende-zu-Ende verschlüsselt sind, greift der Bot-Client auf sein eigenes kryptografisches Schlüsselmaterial zu, um diese zu entschlüsseln.
3. **Technische Prüfung**: Die Nachrichten werden gemäß dem jeweilig etablierten Prozess überprüft.
    - **Schema- bzw. Formatvalidierung:** Die Nachricht wird gegen das definierte Schema des Datenstandards validiert. Fehlerhafte Strukturen, die zu Verarbeitungsfehlern im Fachverfahren führen könnten, werden hier erkannt.
    - **Schadsoftwareprüfung** : Prüfung der Nachricht und insbesondere etwaiger Dateianhänge auf Schadsoftware.
4. **Technische Freigabe oder Quarantäne:** Das Ergebnis der Prüfung wird automatisiert kommuniziert. Der Bot-Client agiert hierzu über eine dezidierte Status-Schnittstelle mit der TI.

    - *Status Erfolgreich*: Nur wenn die technische Prüfung erfolgreich abgeschlossen wurde, meldet der Bot-Client den entsprechenden Status an die TI. Erst hierdurch kann die Nachricht – sofern das Anschlussmodell dies vorsieht – in den Zustand „abholbereit" für den fachlichen Empfänger überführt werden.
    - *Status Fehlerhaft*: Schlägt eine Prüfung fehl, wird die Nachricht technisch isoliert; die TI überführt sie in einen Fehler- bzw. Quarantänezustand.

- **Automatisierte Sender-Benachrichtigung**: Die TI erzeugt auf Basis des technischen Prüfung eine Rückmeldung an den Sender, damit dieser den Sendevorgang nachvollziehen und gegebenenfalls korrigieren kann.

4.3.2.3.2 Rollen und Rechte

Da der Bot-Client Zugriff auf Inhaltsdaten bekommen muss, braucht dieser stark definierte und eingeschränkte Rechte. So muss er die Nachrichten zwar lesen können und bricht somit die Vertraulichkeit auf der Kommunikationsstrecke, aber es ist nicht notwendig, dass er die ursprünglichen Nachrichten manipulieren kann und damit die Integrität gefährdet. Des Weiteren sollte die TI die ursprüngliche Nachricht weiter vorhalten und der Verteilung verantworten, sodass die Verfügbarkeit weiterhin durch diese gewährleistet bleibt. Eine detaillierte Ausarbeitung des Prozesses der Prüfung, der Statusmeldungen und der einhergehenden Abhängigkeiten über den Gesamtprozess hinweg ist im weiteren Verlauf des Projekts auszuarbeiten.

Als technische Systemkomponente ohne direkte Nutzerinteraktion, sind hier primär technische Identitäten relevant. Die in diesem Abschnitt vorgesehenen technischen Rollen sowie deren Berechtigungen sind in Tabelle 14 angerissen.

Tabelle 14: Tabelle mit den technischen Rollen des Bot-Clients und ihren jeweiligen Berechtigungen für Abruf, Validierung, Protokollierung und Statusmeldungen.

Rolle	Verantwortlichkeit	Zugriffsrechte
System User	Automatisierter Abruf und Vorprüfung von Nachrichten.	Zugriff auf für den Verwendungszweck freigegebenes kryptografisches Schlüsselmaterial, Zugriff auf Nachrichtenabruf-API, kein Zugriff auf Schnittstellen zur Datenlöschung und keine Berechtigung zur Änderung fachlicher Inhalte
System-Administrator:in	Installation, Konfiguration und Betriebskontrolle.	Zugriff auf Konfigurations- und Betriebsparameter sowie Logs; Kein erforderlicher lesender Zugriff auf private Schlüssel im Klartext

4.3.2.3.3 Auditierung und Protokollierung

Da der Bot-Client Nachrichten entschlüsseln können muss, unterliegt er besonderen Anforderungen an die Protokollierung. Die Protokollierung dient dem Nachweis, dass Nachrichten korrekt empfangen, erfolgreich geprüft und der Status dem Empfangssystem bekannt gegeben wurden.

Die Protokollierung erfolgt in Übereinstimmung mit dem Querschnittskonzept (siehe Kapitel 4.5.3) und unterscheidet streng zwischen technischen Betriebslogs und revisionsrelevanten Audit-Logs.

Obwohl der Bot-Client dezentral betrieben werden kann, müssen relevante Statusänderungen für das zentrale Protokoll nachvollziehbar sein. Dies geschieht durch explizite Statusmeldungen an die TI. Diese Statusmeldungen werden zentral nachvollziehbar gespeichert, während die detaillierten Protokolleinträge für die Fehleranalyse beim Mandanten verbleiben.

4.4 Laufzeitsicht

Die Laufzeitsicht beschreibt das Zusammenwirken der Hauptkomponenten im laufenden Betrieb. Im Mittelpunkt steht die dynamische Interaktion der beteiligten Komponenten sowie der zeitliche Ablauf zentraler Verarbeitungsschritte. Ziel dieses Kapitels ist es, nachvollziehbar darzustellen, wie Anträge, Anfragen, Erkenntnisse und Entscheidungen innerhalb der Zielarchitektur verarbeitet und zwischen den beteiligten Akteuren ausgetauscht werden.

Die Darstellung der Laufzeitsicht baut auf den in Tabelle 9 dargestellten Architekturentscheidungen und den Bausteinen aus Kapitel **Fehler! Verweisquelle konnte nicht gefunden werden.** auf und macht deren Auswirkungen auf den operativen Betrieb der Zielarchitektur sichtbar. Insbesondere das gewählte Kommunikationskonzept sowie die Entkopplung der Systemkomponenten prägen die beschriebenen Abläufe.

Die Laufzeitsicht betrachtet die Abläufe bewusst aus einer systemübergreifenden Perspektive. Sie beschreibt, welche Komponenten zu welchem Zeitpunkt miteinander interagieren, welche Informationen ausgetauscht werden und welche Rolle zentrale Infrastrukturbausteine dabei einnehmen. Dabei werden fachliche Verarbeitungsschritte, technische Zustandsübergänge und sicherheitsrelevante Interaktionen bewusst getrennt betrachtet, um die Verantwortlichkeiten der beteiligten Komponenten eindeutig einordnen zu können.

Zur Veranschaulichung der Laufzeitsicht werden im Folgenden ausgewählte Szenarien beschrieben, die typische und architektonisch relevante Nutzungssituationen der Zielarchitektur abbilden. Die Auswahl der Szenarien erfolgt exemplarisch und erhebt keinen Anspruch auf vollständige Abdeckung aller fachlichen Prozesse oder Sonderfälle. Ziel ist es vielmehr, anhand repräsentativer Abläufe die wesentlichen Interaktionsmuster, Kommunikationsprinzipien und sicherheitsrelevanten Eigenschaften der Architektur nachvollziehbar darzustellen.

4.4.1 Szenario 1: Erkenntnisabfrage

Das nachfolgende Szenario beschreibt den Ablauf einer Erkenntnisabfrage ausgehend von der Genehmigungsbehörde bis zur Weiterleitung der Anfrage an die zuständigen Erkenntnisstellen. Es veranschaulicht das Zusammenspiel der beteiligten Systemkomponenten entlang der Laufzeit und verdeutlicht insbesondere die Trennung von fachlicher Verarbeitung, Routinglogik und kryptografischer Absicherung.

Der Prozess beginnt mit der Auswahl eines Antrags durch eine Sachbearbeitung der Genehmigungsbehörde. Der Zugriff erfolgt über einen Webbrowser, in dem das Frontend der Verfahrens- und Erkenntnisverarbeitung ausgeführt wird. Das vom IAM zuvor ausgestellte Token wird bei den relevanten Backend-Aufrufen mitgeführt und dort vor der Auslieferung der erforderlichen Daten geprüft.

Die für die Bearbeitung erforderlichen fachlichen Inhaltsdaten werden im Mandantenkontext verarbeitet. Soweit eine clientseitige Entschlüsselung vorgesehen ist, erfolgt diese im Browser. Anschließend kann die Sachbearbeitung die Erkenntnisabfrage auslösen. Daraufhin werden die für die technische Adressierung erforderlichen Routinginformationen von der TI abgerufen. Die TI antwortet mit den gemäß den hinterlegten Routingregeln zu adressierenden Erkenntnisstellen sowie den für die Verschlüsselung benötigten öffentlichen kryptographischen Informationen der Empfänger. Die Anwendung erzeugt anschließend je Empfänger ein Ende-zu-Ende-verschlüsseltes Nachrichtenobjekt für die jeweilige Erkenntnisabfrage.

Die TI prüft im nächsten Schritt, ob die adressierten Empfänger den zuvor ermittelten Routingvorgaben entsprechen und ob die Nachrichten technisch zulässig sind. Ist dies der Fall, übernimmt sie die einzelnen Nachrichten in ihre Transportverarbeitung und speichert sie mandantenbezogen zur späteren Abholung durch die adressierten Erkenntnisstellen zwischen. Eine fachliche Inhaltsprüfung oder fachliche Bewertung der Erkenntnisabfrage findet dabei in der TI nicht statt.

Mit der temporären Vorhaltung der Nachrichten in der TI endet das betrachtete Szenario. Die fachliche Bearbeitung der Erkenntnisabfragen sowie die spätere Rückmeldung der Ergebnisse erfolgen asynchron und werden in dem folgenden Szenario betrachtet.

Dieses Laufzeitszenario verdeutlicht zentrale Architekturprinzipien der Zielarchitektur, insbesondere die konsequente Trennung von fachlicher Verarbeitung und Routinglogik, die clientseitige Umsetzung der Ende-zu-Ende-Verschlüsselung sowie die Rolle der TI als fachlich

blinder, regelbasierter Vermittler. Zugleich zeigt es, dass die TI zwar an der technischen Zuständigkeitsauflösung beteiligt ist, jedoch nicht selbst zur fachlichen Entscheidungsinstanz wird.

4.4.2 Szenario 2: Erkenntnisermittlung

Das nachfolgende Szenario beschreibt den Rücklauf der fachlichen Erkenntnisermittlung einer Erkenntnisstelle, beginnend beim Abruf der Erkenntnisabfrage aus der TI. Es baut auf dem vorhergehenden Szenario auf und zeigt, wie verschlüsselte Anfragen verarbeitet, fachliche Erkenntnisse ermittelt und die Ergebnisse an die Genehmigungsbehörde zurückgeführt werden.

Der Prozess beginnt mit dem Abruf neuer Nachrichten durch das Fachverfahren der jeweiligen EKS. Die EKS ruft hierzu regelmäßig neue Nachrichten von der TI ab.

Nach dem Abruf wird die Erkenntnisabfrage innerhalb der EKS als fachlicher Endpunkt der E2EE entschlüsselt und fachlich bearbeitet. Die konkrete Ausgestaltung dieses fachlichen Ermittlungsprozesses ist abhängig von der jeweiligen EKS und nicht Bestandteil der Zielarchitektur.

Nach Abschluss der Ermittlung wird eine Antwortnachricht mit den Erkenntnissen erzeugt. Diese Antwort wird Ende-zu-Ende-verschlüsselt und kann ausschließlich von der adressierten GB entschlüsselt werden.

Die verschlüsselte Antwort wird an die TI übermittelt. Auch hier übernimmt die TI die Rolle eines vermittelnden Systems. Sie prüft die formale Korrektheit der Adressierung und stellt die Nachricht anschließend zur Abholung für die Erkenntnisverarbeitung der GB, ohne Zugriff auf den fachlichen Inhalt zu erhalten.

Für die gesamte Kommunikation mit der TI kann die Erkenntnisermittlung das bereitgestellte SDK verwenden (siehe ADR-008).

Bevor die eingegangenen Nachrichten in der Referenzarchitektur für die fachliche Weiterverarbeitung freigegeben werden, werden sie einer technischen Vorprüfung unterzogen. Hierzu gehören insbesondere Schema- bzw. Formatvalidierung und Schadsoftwareprüfung. Diese Aufgabe übernimmt im Falle der Referenzimplementierung ein Bot-Client, der mandantenspezifisch betrieben wird und für diesen Zweck in die Ende-zu-Ende-gesicherte Kommunikation eingebunden ist. Erst nach erfolgreichem Abschluss dieser Prüfungen werden die eingegangenen Erkenntnisse für die fachliche Weiterverarbeitung in der

Verfahrens- und Erkenntnisverarbeitung freigegeben. Bei angebundenen Fremdfachverfahren muss eine funktional gleichwertige technische Vorprüfung vorgesehen werden. Diese hat jedoch so zu erfolgen, dass die Anschlussbedingungen, die Schlüsselhoheit des Mandanten und die Sicherheitsvorgaben der Zielarchitektur eingehalten werden.

Mit der technischen Freigabe und der anschließenden Übernahme der Nachricht in die fachliche Verarbeitung der GB ist das betrachtete Szenario abgeschlossen. Die endgültige Quittierung und Löschung der Nachricht aus der TI erfolgt gemäß dem vorgesehenen Abruf- und Löschkonzept. Die Herbeiführung einer Entscheidung durch die Sachbearbeitung wird im nächsten Szenario betrachtet.

Dieses Laufzeitszenario verdeutlicht die dezentrale fachliche Verantwortung der Erkenntnisstelle, die Ende-zu-Ende-verschlüsselte Rückmeldung der Ergebnisse sowie die Rolle der TI als fachlich blinder Vermittler. Gleichzeitig zeigt es die Einbindung des Bot-Clients als technische Prüfkomponente im Rücklauf zur GB im Kontext der Referenzimplementierung.

4.4.3 Szenario 3: Entscheidung

Das letzte Szenario beschreibt den Ablauf der Entscheidungsfindung in der Genehmigungsbehörde auf Basis der eingegangenen Erkenntnisse sowie die Rückmeldung der Entscheidung. Im gegebenen Szenario wird dabei davon ausgegangen, dass der Antrag nicht von einem Sachbearbeiter der Genehmigungsbehörde, sondern über die Antragsverarbeitung von einer privaten Organisation eingereicht wurde. Es baut auf den vorhergehenden Szenarien auf und schließt den fachlichen Bearbeitungszyklus eines Antrags ab.

Der Prozess beginnt, nachdem alle für einen Antrag relevanten Erkenntnisse von den zuständigen Erkenntnisstellen eingegangen und durch die Erkenntnisverarbeitung übernommen wurden. Die Erkenntnisse liegen der Genehmigungsbehörde vor und sind dem jeweiligen Vorgang eindeutig zugeordnet. Die Sachbearbeitung kann diese Informationen einsehen und in die fachliche Bewertung einbeziehen.

Auf Grundlage der vorliegenden Erkenntnisse trifft die zuständige Sachbearbeitung die Entscheidung über den Antrag. Die Entscheidung wird anschließend für die weitere Kommunikation vorbereitet und E2EE, sodass sie ausschließlich von der berechtigten empfangenden Stelle gelesen werden kann. Die Entscheidungsnachricht wird an die TI übermittelt, die diese nach technischer Prüfung zur Abholung für die adressierte Antragsverarbeitung bereitstellt. Etwaige nachgelagerte externe Folgeprozesse, wie

beispielsweise Gebührenabrechnung, können an dieser Stelle ausgelöst werden, sind jedoch nicht Bestandteil des hier beschriebenen Kernszenarios der Zielarchitektur.

Die Antragsverarbeitung ruft die Entscheidung aus der TI ab und stellt sie der berechtigten antragserfassenden Stelle innerhalb der privaten Organisation zur Verfügung, womit dieses Szenario endet. Eventuelle Folgeprozesse, wie Rechtsmittelverfahren, Mitteilungen an Antragstellende oder Archivierung, sind nicht Bestandteil dieses Szenarios.

4.5 Querschnittskonzepte

Dieses Kapitel beschreibt architektonische Querschnittskonzepte, die systemübergreifend wirken und nicht einem einzelnen Baustein zugeordnet werden können. Sie definieren grundlegende Mechanismen zur Steuerung von Identität, Zugriff, Vertrauen und Schutzbedarfen und prägen damit das Verhalten aller Komponenten der Zielarchitektur.

Die hier beschriebenen Konzepte legen fest, wie Akteure und Systeme eindeutig identifiziert werden, wie Berechtigungen durchgesetzt werden und wie Vertraulichkeit sowie Integrität der ausgetauschten Informationen systemweit gewährleistet werden. Sie bilden damit den verbindlichen Rahmen, innerhalb dessen sich die Bausteine der Zielarchitektur bewegen.

4.5.1 Identitäts- und Rechtemanagement (IAM)

Das Identitäts- und Rechtemanagement bildet einen zentralen Bestandteil der Sicherheitsarchitektur von NEOSiP und ist ein wesentliches Element des verfolgten Zero-Trust-Ansatzes. Es definiert die Mechanismen, mit denen natürliche Personen und technische Systeme eindeutig identifiziert werden und auf deren Basis Zugriffsentscheidungen getroffen werden können.

Das IAM-Konzept folgt dabei dem Prinzip der klaren Trennung von Authentifizierung und Autorisierung. Während die Authentifizierung die verlässliche Feststellung einer Identität zum Ziel hat, entscheidet die Autorisierung auf Grundlage dieser Identität sowie weiterer Kontextinformationen darüber, welche Aktionen im System zulässig sind. Die konkrete Durchsetzung dieser Entscheidungen erfolgt in den jeweils beteiligten Systemkomponenten und wird durch die im Folgenden beschriebenen Querschnittskonzepte unterstützt.

4.5.1.1 Authentifizierung von Nutzenden

Eine finale technologische Festlegung zur Authentifizierung natürlicher Personen ist noch nicht abschließend getroffen und muss in einem neuen weiteren ADR adressiert werden. Die im Folgenden beschriebenen technologischen Ansätze skizzieren eine mögliche Umsetzung. Ein entsprechender Handlungsbedarf zur finalen Entscheidung ist in Kapitel 6.7 hinterlegt.

Antragsverarbeitung

Für die Interaktion von Nutzer:innen mit der Antragsverarbeitungs-Komponente setzt die Architektur auf etablierte Standards. Die Authentifizierung könnte beispielsweise über OIDC abgebildet werden. Dies ermöglicht die Anbindung bestehender Identitätsanbieter (IdP) der Behörden, zentraler Verwaltungs-IdPs oder externer Systeme. Durch den Einsatz geeigneter Technologien verbleibt die Verwaltung der Identitäten bei den Quellsystemen. Dies gewährleistet, dass deren spezifische Sicherheitsrichtlinien (z. B. Passwortkomplexität, 2-Faktor-Authentisierung) direkt angewendet werden und Änderungen am Nutzerstatus, wie etwa eine Sperrung, sofort wirksam sind. Damit wird eine zentrale Voraussetzung des Zero-Trust-Modells erfüllt: Eine Identität gilt nur als gültig, wenn sie kontinuierlich überprüft wird und ihr Berechtigungsstatus nicht an langfristige Sessions gebunden ist. Kurzlebige Tokens, die an Nutzer:innen und Gerätekontexte gebunden sind, minimieren das Risiko unbefugter Wiederverwendung und ermöglichen eine kontinuierliche Neubewertung im laufenden Betrieb.

Erkenntnisverarbeitung

Für die Erkenntnisverarbeitung gelten erhöhte Sicherheitsanforderungen (z. B. im VS-NfD-Kontext oder in spezifischen Behördennetzen). Anstelle einer direkten client-seitigen Zertifikatsprüfung erfolgt die Authentifizierung hier über ein föderiertes Identitätsmanagement.

Das System nutzt perspektivisch ein zentrales, internes Identitätsmanagement, das als vertrauenswürdiger Broker fungiert. Dieses interne IAM verwaltet keine eigenen Nutzerdaten, sondern bindet die bestehenden Identitätsanbieter, wie z.B. die der beteiligten Behörden oder Bundesländer (z. B. BundID, Landes-IAMs), über sichere Protokolle (OIDC/ SAML) an.

Für die Authentifizierung der Web-Anwendung wird als potenzieller Standard OIDC Authorization Code Flow mit Proof Key for Code Exchange (PKCE) empfohlen. Folgender Ablauf ist damit möglich:

1. Der Sachbearbeiter greift auf die Anwendung zu und wird an das interne IAM weitergeleitet.
2. Das interne IAM leitet den Nutzer an den für ihn zuständigen IdP weiter.
3. Nach erfolgreicher Authentifizierung erhält das interne IAM eine Bestätigung und stellt ein Zugriffstoken (Access Token) für die Anwendung aus.
4. Die Anwendung nutzt dieses Token zur Autorisierung gegenüber dem Backend, wobei die Identität und Behördenzugehörigkeit manipulationssicher im Token (Claims) verankert sind.

4.5.1.2 Maschinenidentitäten und Systemkommunikation

Die Kommunikation zwischen technischen Komponenten (z. B. zwischen Fachverfahren und der TI) soll über Mutual TLS (mTLS) abgesichert werden. Hierbei weisen sich beide Kommunikationspartner durch X.509-Zertifikate aus. Dies stellt sicher, dass nur vertrauenswürdige, registrierte Systeme an der Kommunikation teilnehmen können.
mTLS stellt eine gegenseitige, zertifikatsbasierte Identifikation her, die kryptografisch beweist, welches System kommuniziert und welcher Behörde es zugeordnet ist. Die Zertifikate werden aus einer PKI ausgestellt und enthalten eindeutig zuordenbare Merkmale, sodass die Plattform sicherstellen kann, dass ein bestimmtes System tatsächlich das autorisierte Fachverfahren der jeweiligen Behörde ist. Zur Freischaltung eines Kommunikationsweges zwischen zwei Systemen werden die Zertifikate gegenseitig als vertrauenswürdig konfiguriert.

4.5.1.3 Dynamische Autorisierung (Policy-Based Access Control)

Für die Steuerung der Zugriffsrechte wird zunächst klassisches RBAC Modell umgesetzt. Jeder authentifizierten Identität (Nutzer oder System) werden eine oder mehrere fest definierte Rollen zugewiesen. Diese Rollen bündeln spezifische Berechtigungen für fachliche und technische Aktionen im System (siehe auch Rollenmodell in Kapitel 4.3.2.1.1).
Zuweisung:

- Anwendern (4.5.1.1) mit OIDC: Die Rollen werden als Attribute ("Claims") im ID-Token übermittelt und im IAM verwaltet.
- Maschinenidentitäten (4.5.1.2) mit Zertifikaten/mTLS*:* Die Identität aus dem Zertifikat wird im System einer Benutzerkennung zugeordnet, für die im IAM die entsprechenden Rollen hinterlegt sind.

Um die Anforderungen an Zero-Trust gemäß BSI zu erfüllen, erfolgt eine zusätzliche Autorisierungsentscheidung dynamisch zur Laufzeit durch eine Policy Decision Point (PDP).
Dabei wird nicht nur die zugewiesene Rolle, sondern auch aktuelle Kontextattribute (Attribute-Based Access Control, ABAC) geprüft. Dabei fungieren die Backend-Systeme fungieren als Policy Enforcement Points (PEP). Sie fragen bei jedem relevanten Zugriff die zentrale Policy-Entscheidung ab oder validieren kurzlebige Zugriffstokens, die diese Kontextprüfungen beinhalten.

4.5.1.4 Registrierung und Zertifikatausstellung für Antragstellende

Das Onboarding von Antragstellenden (z. B. Vertreter privater Organisationen) erfolgt in einem zweistufigen Prozess, der die Identitätsprüfung mit der technischen Befähigung zur verschlüsselten Kommunikation verknüpft.

Registrierung an IAM

Die initiale Registrierung und die laufende Anmeldung am System erfolgen über etablierte Identitätsanbieter mittels OIDC. Wie in 4.5.1.1 beschrieben dient ein internes IAM hierbei lediglich als Drehscheibe für freigegebene Identitätsanbieter.

Schlüsselerzeugung

Um an der E2EE Kommunikation teilnehmen zu können (siehe Kapitel 4.5.2), benötigen Antragstellende ein kryptografisches Schlüsselpaar, das ihre Identität technisch repräsentiert. Dazu erzeugt der Client (Browser) des Anwenders lokal ein Schlüsselpaar. Dabei ist wichtig, dass der private Schlüssel auf Client-Seite verbleibt und gemäß den Vorgaben sicher aufbewahrt wird. Anschließend wird der öffentliche Schlüssel zusammen mit dem gültigen OIDC-Token an das jeweilige Backend gesendet. Der Abschluss der Registrierung erfolgt durch eine Validierung der Registrierungssanfrage durch eine berechtigte Person. Bei positiver Entscheidung wird der öffentliche Schlüssel des Nutzers in einer internen Datenbank des Backendsystems hinterlegt und so die Kommunikation inkl. Nutzung der E2EE der Antragsdaten gestattet.

4.5.2 Sicherheit & Kryptografie

Die Sicherheitsarchitektur ist darauf ausgelegt, Daten auch in einer Umgebung zu schützen, in der einzelne Infrastrukturkomponenten potenziell kompromittiert sein könnten („Assume Breach"). Zentrales Element ist die kryptografische Entkopplung von Transport und Nachricht. Das System implementiert zwei voneinander unabhängige und getrennt verwaltete Verschlüsselungsschichten.

Transportverschlüsselung

Sie sichert die „Leitung" zwischen zwei technischen Punkten (z. B. zwischen einem Fachverfahren und der zentralen TI) mittels TLS. Sie schützt vor Angriffen auf der Netzwerkebene und verbirgt Metadaten vor externen Beobachtern.

Nachrichtenverschlüsselung

Sie sichert den eigentlichen Inhalt (die „Nachricht“) mittels E2EE direkt vom Sender zum finalen Empfänger.

Selbst wenn ein Angreifer die TI vollständig übernehmen würde, blieben die fachlichen Inhalte geschützt, da die Schlüssel für die Nachrichtenschicht niemals zentral vorliegen, sondern ausschließlich an den fachlichen Endpunkten verwaltet werden.

4.5.2.1 Dezentrales Schlüsselmanagement

Da der zentrale Betreiber keinen Zugriff auf Klartextdaten haben darf, muss das Schlüsselmanagement dezentral an den Endpunkten erfolgen. Kryptografische Schlüssel werden immer lokal in der Hoheit der Fachverfahren bzw. Clients erzeugt.

Schlüsselverwaltung

- Server-basiert (Backend Fachverfahren): Private Schlüssel werden in Hardware Security Modulen (HSM) oder gesicherten Vaults der jeweiligen Behörde gespeichert.
- Client-basiert (Browser): Für reine Web-Clients (z. B. Antragsstellung oder Antragsverarbeitung) erfolgt die Nutzung über die Web Crypto API, wobei Schlüsselmaterial so geschützt wird, dass es den Browserkontext nicht verlässt (Non-Exportable Keys).

4.5.2.2 Datenintegrität

Der Schutz vor unbemerktem oder unautorisiertem Verändern von Informationen ist neben der Vertraulichkeit eine zentrale Säule der Sicherheitsarchitektur. Das System stellt sicher, dass Daten wie Fachinhalte, Metadaten, Konfigurationen und Logs über ihren gesamten Lebenszyklus hinweg vollständig, korrekt und manipulationsfrei bleiben.
Integrität auf Transport- und Nachrichtenebene (Data in Transit) wird auf zwei Schichten erzwungen. Die Kommunikation zwischen allen Systemkomponenten erfolgt zwingend über mindestens TLS 1.3. TLS schützt nicht nur vor dem Mitlesen, sondern stellt über AEAD-Verfahren (Authenticated Encryption with Associated Data) sicher, dass Datenpakete auf dem Übertragungsweg nicht verändert, verworfen oder in veränderter Reihenfolge wiederholt werden können. Zum Schutz des fachlichen Payloads auf Nachrichtenebene wird E2EE eingesetzt und so Vertraulichkeit kryptografisch mit Integrität verknüpft. Jeder unbefugte Versuch, auch nur ein einzelnes Bit des verschlüsselten Ciphertexts in der TI zu verändern, führt zwangsläufig zum Fehlschlagen der Entschlüsselung beim Empfänger und damit zur direkten Abweisung der manipulierten Nachricht (siehe Kapitel 4.3.2.3.1).

Auch die Integrität der Datenhaltung (Data at Rest) Daten unterliegen strengen Integritätsprüfungen, um Manipulationen im Backend oder auf Datenbankebene zu verhindern (Encryption at Rest). Revisionsrelevante Audit-Logs (siehe Kapitel 4.5.3) werden nicht nur Write-Only erzeugt, sondern zusätzlich mit qualifizierten Zeitstempeln und digitalen Signaturen oder kryptografischen Hash-Ketten versehen. Dies macht nachträgliches Löschen oder Verfälschen von Log-Einträgen nachweisbar.
Die Integrität der Systemkonfiguration und Anwendungslogik wird durch signiertes Routing in der TI sichergestellt. Änderungen an den Routing-Regeln (4.3.1.2) werden kryptografisch signiert. Das System akzeptiert das Routing nur, wenn die Signatur der abrufenden Instanz valide ist, was unbemerktes Umleiten von Datenströmen ("Man-in-the-Middle") ausschließt.

4.5.3 Revisionssicherheit von Logdaten und Audit-Trails

Eine lückenlose und manipulationssichere Nachvollziehbarkeit von Aktionen ist eine zentrale nicht-funktionale Anforderung. Dieses Querschnittskonzept definiert, wie Protokollierungsdaten über alle Bausteine hinweg erzeugt, geschützt und gespeichert werden, um Compliance-Vorgaben wie sie bspw. durch BSI-Grundschutz und DSGVO vorgegeben werden und forensische Anforderungen zu erfüllen.
Das Audit-System arbeitet strikt nach dem Prinzip der „Systemblindheit“. Das bedeutet, dass Audit-Logs ausschließlich technische Metadaten und Statusinformationen enthalten (z. B. Zeitstempel, Message-IDs, Statusänderungen, Zertifikats-Fingerprints). Fachliche Inhaltsdaten oder entschlüsselte Informationen dürfen zu keinem Zeitpunkt in Audit-Logs geschrieben werden, um die Vertraulichkeit nicht zu gefährden.
Die TI protokolliert ausschließlich verbindungs- und routingrelevante Ereignisse (Wer hat wann an wen gesendet?). Diese Logs dienen dem Nachweis der Zustellung und der technischen Fehleranalyse, enthalten jedoch keinerlei fachliche Informationen.
Die Fachverfahren (z. B. bei Genehmigungsbehörden) fungieren als Audit-Instanz für die fachliche Bearbeitung. Da nur hier die Daten im Klartext vorliegen, sind sie für die Protokollierung von Nutzerinteraktionen (z. B. „Nutzer X hat Antrag Y genehmigt“) verantwortlich. Diese Trennung stellt sicher, dass keine sensiblen Inhaltsdaten in die Logs der zentralen Infrastruktur gelangen.
Jedes System unterscheidet dabei zwischen zwei Kategorien von Protokolldaten mit unterschiedlicher Schutzwürdigkeit und unterschiedlichen Aufbewahrungsfristen. Zum einen dienen technische System-Logs der Fehleranalyse und dem technischen Betrieb (z. B. Performance-Metriken, Stacktraces). Diese enthalten keine personenbezogenen Daten und unterliegen kurzen Löschfristen.

Zum anderen dienen Audit -und Sicherheits-Logs der rechtlichen Nachweisführung und Überwachung. Hier werden Aktionen der Anwender direkt protokolliert. Dazu gehören Identitäts-Events wie fehlgeschlagene Anmeldeversuche oder Informationen aus dem Umgang mit Nachrichten wie die Kommunikation mit der TI.
Kritische Audit-Trails werden digital signiert und mit qualifizierten Zeitstempeln versehen, um den Zeitpunkt und die Urheberschaft revisionssicher zu belegen.
Obwohl die Protokollierung zentral erfolgt, muss das System sicherstellen, dass Audit-Daten logisch mandantengetrennt auswertbar sind. Ein Auditor eines Bundeslandes darf nur Einsicht in die Audit-Spuren nehmen, die den eigenen Mandanten (Genehmigungsbehörde) betreffen, ohne Rückschlüsse auf das Verhalten anderer Mandanten ziehen zu können.

4.5.4 Zero-Trust

Die Zielarchitektur von NEOSiP orientiert sich am vom BSI beschriebenen Zero-Trust-Integrationsmodell. Zero Trust wird dabei nicht als isoliertes Sicherheitsfeature verstanden, sondern als übergreifendes Gestaltungsprinzip, das Identität, Kommunikation, Datenverarbeitung und Systembetrieb gleichermaßen betrifft.
Zur strukturierten Einordnung wird die Umsetzung entlang der vom BSI definierten Säulen sowie der Querschnittsfunktion Detektion und Reaktion in Tabelle 15 dargestellt.
Die folgende Tabelle verdeutlicht, dass zentrale Prinzipien einer Zero-Trust-Architektur und insbesondere die Verlagerung des Vertrauensankers auf Identitäten sowie die konsequente Absicherung von Daten durch Ende-zu-Ende-Verschlüsselung strukturell in der Zielarchitektur verankert sind.
Gleichzeitig verdeutlicht die Gegenüberstellung, dass einzelne Elemente des BSI-Integrationsmodells noch nicht vollständig abgebildet sind. Dies betrifft insbesondere:

- die weitergehende Ausgestaltung kontextbasierter Autorisierungsentscheidungen
- die detaillierte technische Ausgestaltung der Kommunikation zwischen PDP und PEP
- eine detaillierte Ausarbeitung von Micro-Segmentation
- sowie ein integriertes Konzept zur Detektion und automatisierten Reaktion

Zero Trust ist somit als architektonische Zielrichtung und Leitprinzip umgesetzt. Die vollständige Ausprägung aller vom BSI beschriebenen Integrationsdimensionen erfordert jedoch in einzelnen Bereichen eine weitere Konkretisierung, die jeweils als Handlungsbedarf ausgewiesen sind.

Tabelle 15: Einordnung entlang der Zero-Trust-Säulen des BSI

BSI Zero-Trust-Säule	Erfüllte Punkte	Offene Punkte	Referenz-kapitel
Identität (Identity)	**Natürliche Personen** - Föderierte Authentisierung über OIDC - Eindeutige Zuordnung zwischen Person und Organisation - Getrennte Authentifizierung und Autorisierung, dynamische Prüfung jeder sicherheitsrelevanten Aktion **Technische Systeme** - Zertifikatsbasierte Maschinenidentitäten via mTLS und X.509 - Gegenseitige Authentifizierung - Kein implizites Vertrauen aufgrund von Netzzugehörigkeit **Autorisierung** - Zentrale Entscheidungslogik mit technischer Durchsetzung in den Komponenten - Mandantenbezogene Rechte nach dem Prinzip minimaler Berechtigung	Kontextbasierte Zugriffsbewertung und das vollständiges Identitäts-Lifecycle-Management sind noch nicht abschließend spezifiziert	4.5.1 4.5.2
Gerät (Device / Endpoint)	**Browserbasierte Clients** - Entschlüsselung und kryptografische Operationen erfolgen bei den Endanwendern ausschließlich clientseitig im Browser unter Nutzung der WebCrypto API - Private Schlüssel sind nicht exportierbar und verbleiben im jeweiligen Endgeräte-Kontext **Technische Hilfskomponenten (Bot-Client)** - Der Bot-Client ist als eigenständige Systemkomponente mit eigener Maschinenidentität ausgeprägt und führt definierte Prüfprozesse innerhalb eines eng abgegrenzten Mandantenkontexts durch **Schlüsselmaterial** - Private Schlüssel verbleiben konsequent bei der für die Daten verantwortlichen Stelle und sind nicht zentral verfügbar	Mechanismen für eine weitergehende Bewertung des Gerätezustands (z.B. Integritätsnachweise oder Attestation) sind im aktuellen Konzept nicht spezifiziert und bedürfen weiterer Konkretisierung.	4.3.2.3 4.5.2

Netz (Network)	**Kein implizites Netzvertrauen** - Autorisierung erfolgt nicht aufgrund von Netzzugehörigkeit oder Standort, sondern ausschließlich auf Basis geprüfter Identitäten und Policies **Durchgängige Verschlüsselung** - Sämtliche Kommunikation nutzt TLS auf der Transportschicht. System-zu-System-Kommunikation nutzt zusätzlich mTLS Tunnel **Vermittelte Kommunikation** - Nachrichtenaustausch erfolgt ausschließlich über die TI - Direkte Punkt-zu-Punkt-Verbindungen sind nicht vorgesehen **Isolation zentraler Komponenten** - Zentrale Komponenten sind logisch getrennt und verarbeiten keine Klartext-Fachdaten	Explizite Modellierung von Mikrosegmentierung und netzinterner Verkehrsüberwachung bislang nicht weiter spezifiziert	4.5.2 ADR_001 ADR_004
Anwendung (Application / Workload)	**Klare Komponentenabgrenzung** - Trennung von Frontend, Backend, Transportinfrastruktur und unterstützenden Komponenten - Definierte Schnittstellen zwischen allen Bausteinen **Explizite Zugriffsdurchsetzung** - Backend-Komponenten agieren als Policy Enforcement Points und erzwingen zentrale Autorisierungsentscheidungen **Keine fachliche Vertrauensannahme** - Zentrale Komponenten, insbesondere die Transportinfrastruktur, können keine Klartext-Fachdaten verarbeiten **API-basierte Kommunikation** - Systeminteraktionen erfolgen ausschließlich über definierte, abgesicherte Schnittstellen	Feingranulare, kontextbasierte Zugriffsbewertung auf Anwendungsebene über attribut- und kontextbasierte Zugriffskontrolle (ABAC/PBAC) hinaus sind bislang nicht vollständig spezifiziert	4.5.1.3 4.5.2 ADR_001 ADR_002 ADR_004
Daten (Data)	**Ende-zu-Ende-Verschlüsselung** - Fachdaten werden ausschließlich clientseitig verschlüsselt und nur bei berechtigten Empfängern entschlüsselt - Zentrale Komponenten haben keinen Zugriff auf Klartextinhalte	Datenklassifizierung, Label-Durchsetzung und konsistente Umsetzung von Lösch- und Aufbewahrungsregeln	4.5.2 3.2.3.3 ADR_004

	Trennung von Inhalts- und Metadaten - Routing- und Systemmetadaten werden getrennt von fachlichen Nutzdaten verarbeitet **Verschlüsselung at Rest** - Persistierte Nachrichten und Systemdaten werden zusätzlich speicherseitig verschlüsselt **Mandantentrennung** - Daten unterschiedlicher Organisationen sind logisch voneinander getrennt	bedürfen weiterer Konkretisierung	
Querschnitt: Detektion & Reaktion (Visibility & Analytics)	**Protokollierung** - Systemblinde, revisionssichere Logs von Zugriffen und Statusänderungen (Systemblindheit: Logs enthalten keine Fachdaten)	Ein übergreifendes Konzept zur automatisierten Detektion und automatisierte Reaktion ist im Konzept als noch zu definierender Handlungsbedarf in Kapitel 6.8 identifiziert.	4.5.3

5 Migration von Bestandsprodukten

Gegenstand der Migration ist nicht allein die technische Datenübernahme, sondern die Transformation bestehender Verfahrens-, Sicherheits- und Kommunikationsmodelle in das einheitliche Zielbild. Ziel muss eine schrittweise Überführung der heutigen OSiP-Bestandsprodukte sein ohne dauerhafte Fortschreibung der bestehenden Heterogenität, ohne unkontrollierte Schattenarchitekturen und ohne sicherheitsrelevante Sonderpfade.

Die Migrationsstrategie soll insbesondere Daten aus der bestehenden Transportinfrastruktur, Daten aus vorhandenen OSiP-Fachverfahren, bestehende Schnittstellen, Datenformate, Prozesslogiken, Kommunikationsbeziehungen sowie Betriebs- und Sicherheitskonfigurationen berücksichtigen. Dabei sind perspektivisch laufende Verfahren, abgeschlossene Verfahren und historische Nachweisbestände zu migrieren.

Grundsätze

Für die Migration sollen die folgenden Grundsätze angewandt werden:

- iterative Migration sofern fachlich und betrieblich möglich
- klare Trennung von Übergangs- und Zielarchitektur
- temporäre Adapter statt dauerhafter Sonderintegrationen (siehe ADR-009)
- einheitliche Zielanschlussbedingungen für alle Kommunikationsparteien
- Minimierung zusätzlicher Vertrauensanker in der Übergangsphase
- durchgängige Nachvollziehbarkeit von Datenherkunft, Transformationsanwendungen und Verfahrenszustand
- definierte Exit-Kriterien für Altkomponenten und Adapter

Die Migration soll so geplant werden, dass bestehende Verfahren weiterhin bearbeitet werden können und zugleich die Zielarchitektur nicht durch dauerhaftes Mitschleppen historischer Schnittstellen, Datenmodelle oder Prozessvarianten belastet wird.

Datenmigration und Konsistenzsicherung

Für laufende Verfahren ist sicherzustellen, dass nach der Migration derselbe fachliche Verfahrenszustand, dieselbe Bearbeitbarkeit und dieselbe Zuständigkeit bestehen wie vor der Migration. Für abgeschlossene Verfahren ist zu entscheiden, ob diese vollständig in das Zielmodell transformiert, in einem Archivbestand beweisfähig erhalten oder lediglich referenziert werden.

Besonders kritisch sind Nachrichtenhistorien und Nachweisdaten. Für sie ist festzulegen, ob die ursprünglichen Nachrichtenketten unverändert erhalten bleiben müssen oder ob eine Transformation in ein neues Nachweisformat zulässig ist. Die Migration darf nicht dazu führen, dass Zustellnachweise, Bearbeitungsstände, Fristen, Beteiligtenrollen oder Entscheidungsgrundlagen nachträglich uneindeutig werden.

Migration von Schnittstellen, Datenformaten und Prozesslogiken

Für die Übergangsphase können Adapter und Datenkonverter eingesetzt werden. Diese dürfen jedoch keine dauerhafte Integrationsschicht für Altschnittstellen bilden. Jeder Adapter benötigt einen klaren Zweck, einen verantwortlichen Betreiber, definierte Sicherheitsanforderungen, Monitoring, Dokumentation und ein verbindliches Abschaltdatum beziehungsweise ein Exit-Kriterium.

Die Migration der Prozesslogiken umfasst insbesondere Statusmodelle, Zuständigkeitslogiken, Validierungsregeln, Eskalationspfade, Fristen, Entscheidungslogiken und Rückmeldeprozesse genaustens zu erheben. Dabei sollte insb. geprüft werden, welche Logiken fachlich notwendig sind und welche lediglich aus technischen oder historischen Zwängen des Bestandssystems entstanden sind. Dabei sind natürlich die gesetzlichen Grundlagen ausschlaggebend. Ziel ist die fachliche Harmonisierung der Verfahren, ohne notwendige anwendungsbereichsspezifische Unterschiede unzulässig zu nivellieren. Allerdings könnte und sollte in diesem Zuge fachlich ausgearbeitet werden, welcher gesetzliche Harmonisierungsbedarf erkannt wurde, um diesen an die entsprechenden Gesetzgebenden, Fachgremien oder Fachministerkonferenzen weiterzuleiten.

Sicherheits- und Vertrauensmodell der Transition

Da sich die Sicherheitsarchitektur grundlegend verändert, ist die Übergangsphase als eigenständiger sicherheitskritischer Zustand zu behandeln. Insbesondere ist zu klären, wo während Migration, Transformation und Validierung Klartext entstehen kann, welche Stellen Zugriff auf fachliche Inhalte erhalten, welche Schlüssel genutzt werden und wie Identitäten aus Bestandssystem und Zielarchitektur eindeutig gebunden werden.

Übergangskomponenten wie Datentransformations- oder Importskripte dürfen nicht zu verdeckten Vertrauensankern werden. Für jede temporäre Komponente ist daher festzulegen, welche Daten sie verarbeitet, welche Operationen sie ausführt, welche Protokolle sie evtl. schreibt, wer sie betreibt und wann sie außer Betrieb genommen wird.

Ein solches Sicherheitskonzept für die Migration sollte mindestens die folgenden Punkte behandeln:

- kryptographische Migrationspfade
- Schlüsselmanagement und Stilllegung alter Schlüssel
- Identitätsbindung zwischen Alt- und Zielsystemen
- Zugriffsschutz auf Migrationswerkzeuge und Transformationsumgebungen
- Protokollierung und evtl. eine Auditierbarkeit aller Migrationsschritte
- Schutz von Klartextphasen, sofern diese überhaupt unvermeidbar sind

Business Continuity und Cutover

Während der Transition müssen Bestandsprodukte und Zielarchitektur kontrolliert parallel betrieben werden. Für die Iterationen der Migration sind insb. Cutover-Strategien und Rückfallverfahren zu definieren. Die Bearbeitung sicherheitsrelevanter Verfahren darf durch die Migration nicht unkontrolliert unterbrochen, verfälscht oder in ihrer Nachvollziehbarkeit beeinträchtigt werden. Die Prozesse der ZSÜ sind hochgradig kritisch und können erhebliche praktische Konsequenzen nach sich ziehen.

Wissensmanagement

Relevantes Wissen aus Bestandssystemen, Fachverfahren, Betrieb, Support und Fachadministration sollte vorab strukturiert erfasst und dokumentiert werden. Dazu gehört insbesondere Wissen über Datenmodelle, Schnittstellenverhalten, fachliche Sonderfälle, Betriebsroutinen, Fehlerbilder, manuelle Umgehungslösungen und implizite Entscheidungsregeln.

Zielzustand

Der Zielzustand ist unter anderem dann erreicht, wenn:

- laufende Verfahren fachlich korrekt weitergeführt werden können
- abgeschlossene Verfahren nachvollziehbar erhalten bleiben
- Kommunikationsbeziehungen eindeutig in der Zielarchitektur abgebildet sind
- Fachverfahren die einheitlichen Anschlussbedingungen erfüllen
- Adapter und weitere Übergangskomponenten abgeschaltet oder verbindlich terminiert sind

- Sicherheits-, Betriebs- und Governance-Anforderungen der Zielarchitektur wirksam umgesetzt sind
- Betriebs- und Prozesswissen strukturiert und nachhaltig dokumentiert ist und nicht mehr nur personengebunden verfügbar ist

6 Weitere Handlungsfelder

Im Rahmen der Konzeption wurde deutlich, dass bestimmte Themen nicht abschließend innerhalb der Konzeptionsphase entschieden oder umgesetzt werden konnten. Diese Themen erfordern weiterführende konzeptionelle, organisatorische oder technische Klärungen und sind daher als eigenständige Handlungsfelder zu betrachten. Das vorliegende Kapitel bündelt diese identifizierten Handlungsfelder und formuliert hierzu konkrete Handlungsempfehlungen.

Die Ausführungen fokussieren sich jeweils auf die Ausgangslage, dem daraus resultierenden Handlungsbedarf sowie auf empfohlene nächste Schritte. Abhängigkeiten und Wechselwirkungen zwischen einzelnen Handlungsfeldern oder zu bestehenden Architekturentscheidungen werden ebenfalls benannt. Die konkrete Ausgestaltung und Umsetzung der empfohlenen Maßnahmen ist nicht Gegenstand dieses Dokuments und bleibt nachgelagerten Konzeptions-, Umsetzung- und Entscheidungsprozessen vorbehalten.

6.1 Konzeptionierung eines Datenstandards

Ausgangslage

Der Datenaustausch zwischen den beteiligten Systemen erfolgt im Bestand auf Basis unterschiedlicher, historisch gewachsener Datenstrukturen und -formate. Eine einheitliche, systemübergreifend abgestimmte Definition von Datenobjekten und deren Semantik liegt bislang nicht vor.

Darüber hinaus ist derzeit nicht verbindlich festgelegt, welche fachlichen Informationen in welcher technischen Form, mit welchen Codelisten, welchen Pflichtfeldern, welchen Erweiterungsmechanismen und welchen Versionierungsregeln zwischen AES, GB und EKS auszutauschen sind.

Handlungsbedarf

Ohne einen verbindlichen Datenstandard besteht das Risiko, dass bestehende Fragmentierungen auch in der Zielarchitektur fortbestehen oder neu entstehen. Dies führt zu erhöhtem Integrationsaufwand, redundanter Implementierung fachlicher Logik und erschwert die Weiterentwicklung und Anbindung zusätzlicher Systeme.

Darüber hinaus besteht das Risiko, dass dieselben fachlichen Sachverhalte in unterschiedlichen AWB unterschiedlich modelliert, interpretiert oder technisch repräsentiert werden.

Empfehlung

Es wird empfohlen, einen einheitlichen Datenstandard für den Datenaustausch zu konzipieren und verbindlich festzulegen. Der Datenstandard sollte fachliche und technische Aspekte trennen und unabhängig von konkreten Implementierungen oder Transportmechanismen definiert werden.

Dabei sollte der Datenstandard mindestens in die nachfolgenden Bestandteile gegliedert werden:

- ein fachliches Informationsmodell mit eindeutig definierten Datenobjekten, Attributen, Beziehungen und fachlichen Bedeutungen,
- eine technische Repräsentation der Austauschdaten einschließlich Syntax, Validierungsregeln und zulässiger Erweiterungen,
- eine geregelte Governance für Pflege, Versionierung, Freigabe und verbindliche Einführung des Standards.

Dabei sind insbesondere folgende Punkte zu berücksichtigen:

- Anforderungen aus Datenschutz, Informationssicherheit, Protokollierung, Schutzkennzeichnung und Datensparsamkeit
- Systematische Prüfung der Wiederverwendung, Anlehnung oder Abgrenzung zu bestehenden Datenstandards und Standardisierungsvorhaben
- Trennung zwischen fachlichen Inhaltsdaten, Routing-/Steuerungsmetadaten und transportbezogenen technischen Metadaten

Darüber hinaus ist ein dauerhaftes, verbindlich mandatieres Gremium einzurichten, in dem fachlich und technisch qualifizierte Vertretungen der Stakeholdergruppen aus AES, GB und EKS sowie der für Betrieb und Architektur verantwortlichen Stellen zusammenwirken. Dieses Gremium sollte gesetzliche und technische Rahmenbedingungen beobachten und insbesondere Änderungen am Standard bewerten und beschließen, Versionen und Übergangsfristen festlegen sowie die langfristige Pflege des Standards organisatorisch absichern.**Abhängigkeiten und Wechselwirkungen**

Der Datenstandard steht in enger Wechselwirkung mit der Migration, da insbesondere bei der Datenmigration des OSiP-Fachverfahrens ins NEOSiP-Fachverfahren Anpassungen an den Daten erforderlich sein könnten.

Die Konzeptionierung des Datenstandards sollte sich inbesondere an etablierten Austauschstandards wie XPolizei und dem dort zugeordneten Datenformat GPÜ orientieren.

6.2 Konzeptionierung eines übergreifenden Kommunikationsprozesses

Ausgangslage

Die Durchführung von Prüfungen erfolgt derzeit in den verschiedenen AWB auf Grundlage fachlich ähnlicher, in ihrer konkreten Ausgestaltung jedoch teilweise unterschiedlich gelebter Prozesse. Insbesondere unterscheiden sich Reihenfolge, Auslöser, Rückmeldewege, Statuslogiken und fachliche Sonderfälle zwischen den bestehenden Verfahrenskontexten. Ein übergreifend abgestimmtes, technisch einheitlich umsetzbares Prozessmodell liegt bislang nicht vor.

Für die Zielarchitektur ist dies von besonderer Bedeutung, da die TI und die angebundenen Fachverfahren auf ein konsistentes Verständnis der fachlichen Kommunikationsbeziehungen angewiesen sind. Ohne einen abgestimmten Kommunikationsprozess besteht das Risiko, dass technische Schnittstellen, Nachrichtenflüsse und Zustandsmodelle weiterhin anwendungsspezifisch ausdifferenziert und damit schwer vereinheitlichbar bleiben sowie fachliche Fehlerzustände auftreten.

Handlungsbedarf

Für die Umsetzung der TI ist eine Vereinheitlichung des übergreifenden ZSÜ-Kommunikationsprozesses erforderlich. Es bedarf eines gemeinsamen fachlichen Zielbildes dafür, wie Anträge, Nachweisforderungen, Verfahrensanfragen, Erkenntnismitteilungen, Rückfragen, Nachfolgeanträge, Statusmeldungen und Entscheidungen systemübergreifend ausgetauscht werden sollen.

Ohne eine solche Harmonisierung besteht das Risiko, dass die Zielarchitektur zwar technisch eine gemeinsame Transport- und Integrationsplattform bereitstellt, fachlich jedoch weiterhin durch voneinander abweichende Prozessverständnisse geprägt bleibt. Dies würde zum einen zu einem erhöhten Umsetzungsaufwand in den Fachverfahren, zu komplexen Sonderlogiken in den Schnittstellen sowie zu eingeschränkter Wiederverwendbarkeit technischer

Komponenten führen. Zum anderen könnte es zu fachlichen Fehleinschätzungen von Verfahrensstatus sowie fachlichen Fehlerzuständen führen.

Empfehlung

Es wird empfohlen, einen fachlich übergreifenden Kommunikationsprozess für ZSÜ zu konzipieren und als verbindliches Referenzmodell für die Zielarchitektur festzulegen. Ziel sollte nicht die vollständige Vereinheitlichung aller fachlichen Besonderheiten der einzelnen Anwendungsbereiche sein, sondern die Definition eines gemeinsamen prozessualen Kerns, der technisch einheitlich implementiert und bei Bedarf fachlich profiliert werden kann.

Dabei sind insbesondere folgende Punkte zu berücksichtigen:

- Definition eines fachlich übergreifenden Referenzprozesses mit klaren Prozessphasen, Zustandsübergängen, Kommunikationsereignissen und Verantwortlichkeiten
- Trennung zwischen einem verbindlichen prozessualen Kern und anwendungsbereichsspezifischen Varianten oder Ausprägungen
- Einheitliche Beschreibung der Rollen im Kommunikationsprozess, insbesondere von AES, GB und EKS, sowie ihrer jeweiligen Auslöser, Eingaben, Ausgaben und Rückkopplungen
- Berücksichtigung von Fristen und Eskalationen,
- Abstimmung des Prozessmodells mit dem zu etablierenden Datenstandard, dem Routing-Modell, dem Rollen- und Berechtigungskonzept sowie den Vorgaben zur Protokollierung

Abhängigkeiten und Wechselwirkungen

Das Handlungsfeld steht in enger Wechselwirkung mit der Konzeptionierung des Datenstandards, da ein einheitlicher Kommunikationsprozess die Grundlage für die Definition konsistenter Datenobjekte und Statusmodelle bildet. Ebenso bestehen direkte Abhängigkeiten zur Ausgestaltung der TI, insbesondere des Routing-Modells, der Zustelllogik und der technischen Ereignis- und Fehlerbehandlung.

6.3 Umfängliche Unterstützung der Anforderungen aus dem Geheimschutz

Ausgangslage

Es konnte noch nicht abschließend geklärt werden, ob die Anforderungen aus dem VS-konformen Austausch von Dokumenten und Informationen in der Konzeption abgebildet

werden sollen. Die bisherigen Erörterungen zu dem Thema haben gezeigt, dass perspektivisch maximal die Anforderung an eine VS-NfD-Unterstützung erforderlich sein könnte. Die Anforderungsgeber haben sich jedoch noch nicht eindeutig geäußert, sodass von einer perspektivisch wahrscheinlichen Anforderung ausgegangen wird. Die Zielarchitektur beschreibt zwar grundsätzlich eine sichere Kommunikationsinfrastruktur, diese ist aber noch nicht auf die VS-NfD-spezifischen Anforderungen ausgelegt (siehe Kapitel 3.2.3.3).

Die mit einer möglichen Unterstützung von VS-NfD verbundenen fachlichen, technischen, organisatorischen und regulatorischen Anforderungen wurden bereits umfangreich analysiert. Dabei wurde deutlich, dass eine VS-Unterstützung weitreichende Auswirkungen auf Architektur, Betrieb, Infrastruktur und Governance des Gesamtsystems hätte, auf der anderen Seite aber eine sinnvolle Erweiterung darstellen würde.

Handlungsbedarf

Daher ist für die weitere Ausgestaltung der Zielarchitektur eine verbindliche Klärung der künftig vorgesehenen VS-NfD-Einstufung erforderlich. Andernfalls besteht das Risiko, dass nachgelagerte Architektur- und Umsetzungsentscheidungen unter unklaren Annahmen erfolgen oder spätere Anpassungen mit hohem Aufwand verbunden sind.

Empfehlung

Es wird empfohlen, die Zielarchitektur grundsätzlich für den VS-konformen Austausch von Dokumenten und Informationen zu befähigen, da nur dies eine ganzheitliche Ende-zu-Ende-Digitalisierung des ZSÜ-Prozesses ermöglichen kann. Die hierfür zu beachtenden Anforderungen bestimmen fundamental weitere noch zu treffende Architekturentscheidungen in den Anfängen der Umsetzungsphase. Eine nachträgliche Befähigung der Zielarchitektur zu einem späteren Zeitpunkt der Umsetzung wird sehr wahrscheinlich zu großen Aufwänden führen. Aus diesen Gründen wird empfohlen, eine eigenständige Grundsatzentscheidung darüber herbeizuführen, ob NEOSiP grundsätzlich weiterführend für den Austausch von VS-NfD konzeptioniert werden soll. Diese Entscheidung muss auf den bereits vorliegenden Analysen aufbauen und insbesondere folgende Aspekte berücksichtigen:

- Fachlicher und organisatorischer Bedarf für den Austausch von VS-NfD
- Auswirkungen auf Betrieb, Infrastruktur und organisatorische Verantwortlichkeiten
- Regulatorische Anforderungen sowie notwendige Zulassungs- oder Genehmigungsverfahren

- Etablierung von Kommunikationswegen für Endsysteme die VS-NfD nicht unterstützen können.

Die Entscheidung sollte dokumentiert und als verbindliche Rahmenbedingung für die weitere Architektur- und Umsetzungsplanung festgelegt werden.

Abhängigkeiten und Wechselwirkungen

Eine mögliche Ausrichtung auf VS-NfD hat erhebliche Auswirkungen auf die Zielarchitektur und nachgelagerte technische Festlegungen, insbesondere auf die Ausgestaltung der Sicherheits- und Informationsarchitektur der TI. Sie konkretisiert weitere Anforderungen, innerhalb derer nachgelagerte technische Entscheidungen zu treffen sind.

6.4 Nachnutzung von bestehenden Transportinfrastruktur-Produkten

Ausgangslage

Die Zielarchitektur sieht eine zentrale TI als vermittelnde Komponente für den sicheren und entkoppelten Nachrichtenaustausch zwischen den beteiligten Systemen vor. Die grundlegende Rolle und Funktion der TI ist architektonisch klar beschrieben. Offen ist jedoch, wie diese Infrastruktur konkret umgesetzt werden soll, insbesondere ob eine Eigenentwicklung erfolgt oder auf einer bestehenden Lösung aufgebaut wird.

Dabei ist explizit zu prüfen, ob das bestehende IT-PLR-Produkt FIT-Connect ganz oder teilweise nachgenutzt werden kann. FIT-Connect ist ein Produkt des IT-Planungsrats und Teil des D-Stack. Es wird im offiziellen Produktkatalog des IT-PLRs als zentrale föderale Transportinfrastruktur bzw. Plattform für den sicheren Datenaustausch geführt.

Handlungsbedarf

Für die Umsetzung der Zielarchitektur ist eine Entscheidung über die konkrete Ausgestaltung der TI erforderlich. Ohne diese Entscheidung bleiben zentrale Fragen zur Implementierung, zum Betrieb, zur Wartbarkeit sowie zur Integration in bestehende Systemlandschaften ungeklärt.

Darüber hinaus bleibt ohne eine gesonderte Prüfung der Nachnutzbarkeit von FIT-Connect offen, ob im Projekt eine bereits vorhandene föderale Infrastruktur als Ausgangsbasis genutzt werden kann oder ob die OSiP-spezifischen Anforderungen eine eigenständige Lösung bzw. erhebliche Erweiterungen erfordern. Dies betrifft insbesondere Anforderungen aus der Ende-zu-Ende-Verschlüsselung bzgl. MLS, Mehrparteienkommunikation zwischen AES, GB und EKS,

dem Routing sowie gegebenenfalls Schutzkennzeichnung sowie weitere VS-bezogenen Rahmenanforderungen.

Empfehlung

Es wird empfohlen, eine gesonderte Entscheidungsfindung zur Umsetzung der TI durchzuführen. Dabei sollten unterschiedliche Umsetzungsoptionen systematisch betrachtet und bewertet werden, insbesondere die Nachnutzung von FIT-Connect, die Erweiterung oder Adaption von FIT-Connect oder einer vergleichbaren bestehenden Plattform wie bspw. NOOTS sowie eine Eigenentwicklung.

Zu berücksichtigen sind insbesondere:

- Erfüllung der funktionalen und nicht-funktionalen Anforderungen der Zielarchitektur
- Grad der Erfüllung der OSiP-spezifischen Anforderungen
- Auswirkungen auf Betrieb, Wartung und Weiterentwicklung
- Abhängigkeiten von Produkt-Governance, Roadmap und Releasezyklen einer nachgenutzten Lösung
- Aufwand für Anpassung, Erweiterung, Integration und gegebenenfalls Kompensation nicht erfüllter Anforderungen

Die Entscheidung sollte nachvollziehbar dokumentiert und als verbindliche Grundlage für die weitere Umsetzung der Zielarchitektur festgelegt werden.

Abhängigkeiten und Wechselwirkungen

Die Ausgestaltung der TI steht in enger Wechselwirkung mit mehreren Handlungsfeldern dieses Kapitels. Insbesondere die Entscheidungen zur VS-Unterstützung und zum Verschlüsselungsverfahren beeinflussen die Anforderungen an die TI maßgeblich.

Darüber hinaus bestehen zentrale Wechselwirkungen mit der Konsolidierung des übergreifenden Kommunikationsprozesses, der Konzeptionierung des Datenstandards sowie den Anschlussbedingungen für angebundene Fachverfahren.

6.5 Nachweisbarkeit und Zustimmung von Antragstellenden

Ausgangslage

Im aktuellen Verfahren gibt es einheitlichen digitalen Nachweis darüber, dass die antragstellende Person dem Antrag, den erfassten Daten und dem vorgesehenen

Verfahrensumfang zugestimmt hat. Es werden Anträge bspw. nicht durch die antragstellenden Personen oder auch nur die Antragserfassenden digital signiert.

Die Antragstellung erfolgt dabei über unterschiedliche Kanäle: teils direkt durch die antragstellende Person in einem Onlinedienst, teils indirekt durch Antragserfassende bei AES oder GB auf Grundlage papiergebundener oder mündlich aufgenommener Angaben. Für diese unterschiedlichen Entstehungskontexte existiert bislang kein einheitliches Nachweismodell, das belastbar dokumentiert, wer den Antrag inhaltlich erklärt hat, wer ihn technisch erfasst und eingereicht hat, auf welcher Grundlage die digitale Fassung erstellt wurde und auf welche Informationen und beteiligten Stellen (EKS und ggf. Register) sich die Erklärung der Antragstellenden konkret bezog.

Handlungsbedarf

Für die weitere Ausgestaltung des Verfahrens ist zu klären, wie Zustimmung, Identitätsbezug, Verantwortung und Nachweisbarkeit der Antragstellung künftig übergreifend abgesichert werden sollen.

Dabei ist insbesondere zwischen der direkten digitalen Erklärung durch die antragstellende Person, der Übernahme eines papiergebundenen oder persönlich aufgenommenen Antrags durch AES oder GB und der technischen Einreichung durch angebundene Organisationen bzw. Schnittstellen zu unterscheiden. Das Rechtsgutachten hat aufgezeigt, dass es hier unterschiedliche Rechtslagen gibt, die teilweise eine analoge Antragstellung einfordern, was einer zusätzlichen digitalen Umsetzung nicht widerspricht.

Es besteht das Risiko, dass Zustimmung, Nachweisbarkeit, Verantwortungszurechnung, Integrität der übernommenen Daten und rechtliche Belastbarkeit des Antrags langfristig uneinheitlich geregelt verbleiben. Dies betrifft insbesondere Fälle, in denen zwischen erklärender Person, erfassender Person und technisch einreichendem System mehrere Zwischenschritte liegen.

Empfehlung

Es wird empfohlen, eine Architekturentscheidung zu einem Nachweis- und Vertrauensmodell für die Antragstellung herbeizuführen. Dabei sollte ausdrücklich zwischen dem Nachweis der Willenserklärung einer natürlichen Person und dem Herkunfts- bzw. Integritätsnachweis durch eine Organisation unterschieden werden. Elektronische Siegel dienen bspw. dem Herkunfts-

und Integritätsnachweis von juristischen Personen, ersetzen aber nicht die Willenserklärung einer antragstellenden natürlichen Person.

Dabei sollte geprüft werden, ob eine einheitliche Vorgabe zur elektronischen Signatur für alle Antragsstellenden festgelegt werden sollte und welche rechtlichen und technischen Anforderungen hierfür maßgeblich sind. Technisch zu berücksichtigen sind insbesondere die folgenden Punkte:

- Gewünschtes Signaturniveau und rechtliche Verbindlichkeit
- Nutzbarkeit für natürliche Personen und Organisationen
- Integration in bestehende Antragsprozesse und Clients
- Abhängigkeiten zu Identitäts- und Authentifizierungslösungen

Die Entscheidung muss insbesondere mit den entsprechenden Landesrechten abgestimmt werden, sodass diese evtl. im Sinne einer Vereinheitlichung konsolidiert werden können.

Abhängigkeiten und Wechselwirkungen

Das Handlungsfeld steht in Wechselwirkung mit dem Identitäts- und Vertrauensmodell sowie mit den Anforderungen an Authentizität und Integrität von Antragsdaten. Zudem können sich Abhängigkeiten zu regulatorischen Vorgaben und externen Signaturdiensten ergeben, die bei der Entscheidungsfindung zu berücksichtigen sind.

6.6 Übergreifender prozessorientierter Machbarkeitsnachweis

Ausgangslage

Die Zielarchitektur beschreibt ein konsistentes Zielbild für die zukünftige Ausgestaltung des Produkts. Aufgrund der Komplexität der föderalen Systemlandschaft, der Vielzahl beteiligter Akteure sowie der vorgesehenen Sicherheits- und Integrationsmechanismen liegen zentrale Annahmen der Architektur bislang jedoch ausschließlich auf konzeptioneller Ebene vor. Eine praktische Validierung der Lösungsansätze hat bisher nicht stattgefunden.

Dies betrifft insbesondere die Frage, ob die technischen Kernprinzipien der Zielarchitektur durch die unterschiedlichen Teilnehmenden in der Praxis in hinreichend einheitlicher und wirtschaftlich vertretbarer Weise umgesetzt werden können. Bislang ist zudem nicht belastbar nachgewiesen, wie sich die Architektur bei Teilnehmenden mit unterschiedlichem Reifegrad, unterschiedlicher Integrationsfähigkeit und unterschiedlichen Betriebsmodellen tatsächlich umsetzen lässt.

Handlungsbedarf

Es wird empfohlen, einen exemplarischen Machbarkeitsnachweis umzusetzen, der ausgewählte technische Kernprinzipien der Zielarchitektur in einem begrenzten, aber prozessoral ganzheitlichen Szenario abbildet und überprüft. Die Erprobung sollte mit freiwilligen Teilnehmenden erfolgen, die sich proaktiv in die Validierung einbringen möchten. Sie ist nicht als produktionsnahe Einführung zu verstehen, sondern als gezielte Architekturvalidierung unter realitätsnahen Bedingungen.

Empfehlung

Es wird empfohlen, einen exemplarischen Machbarkeitsnachweis umzusetzen, der ausgewählte Kernaspekte der Zielarchitektur in einem begrenzten, aber prozessoral ganzheitlichen Szenario abbildet und überprüft.

Dabei sollten insbesondere folgende Fragestellungen betrachtet werden:

- Integrationsfähigkeit der Kernprinzipien in bestehende Systemlandschaften und Arbeitsabläufe auf Seiten von AES, GB und EKS
- Auswirkungen möglicher Transitions- und Migrationsszenarien, insbesondere im Hinblick auf technische, organisatorische und prozessuale Umstellungsaufwände
- Zusammenspiel von TI, Sicherheitsmechanismen und den vorgesehenen Anschluss- und Betriebsmodellen
- tatsächliche Umsetzbarkeit der vorgesehenen Fachverfahrensbausteine, insbesondere dort, wo zentrale Architekturprinzipien in Browser-Anwendungen oder mandantennahen Komponenten umgesetzt werden müssen
- Gewinnung belastbarer Erkenntnisse zur Abschätzung der Transitionsaufwände insgesamt sowie getrennt nach Stakeholdergruppen

Die Ergebnisse des Machbarkeitsnachweises sollten systematisch dokumentiert und für die weitere Ausgestaltung der Architektur sowie für nachgelagerte Entscheidungen genutzt werden. Dabei sollten die Erkenntnisse nicht nur technisch, sondern auch entlang der betroffenen Rollen, Prozessschritte, Betriebsannahmen und Aufwandskategorien ausgewertet werden.

Abhängigkeiten und Wechselwirkungen

Der Machbarkeitsnachweis steht in enger Beziehung zu mehreren Handlungsfeldern dieses Kapitels, insbesondere zur Migration, zur Ausgestaltung der TI sowie zur Entscheidung über das Verschlüsselungsverfahren. Erkenntnisse aus der Erprobung können Einfluss auf diese Handlungsfelder haben und sollten entsprechend frühzeitig in die weiteren Entscheidungsprozesse einfließen.

6.7 Architekturentscheidung zur Authentisierung natürlicher Personen an den OSiP-Fachverfahren

Ausgangslage

Für die zentral bereitgestellten OSiP-Fachverfahren zur Antragsverarbeitung und zur Erkenntnisverarbeitung ist noch nicht entschieden, wie sich nutzende natürliche Personen gegenüber dem System authentisieren sollen. Dies betrifft insbesondere zwei Gruppen: erstens Mitarbeitende von AES, die Anträge für Antragstellende erfassen, und zweitens Mitarbeitende von GB, die Anträge erfassen, Verfahren bearbeiten und Entscheidungen verantworten.

Gleichzeitig verarbeitet das Vorhaben sicherheitskritische Daten mit mindestens hohem Schutzbedarf. Für Zugriffe auf IT-Systeme fordert unter anderem das BSI eine angemessene Identifikation und Authentisierung.

Handlungsbedarf

Für die Zielarchitektur ist eine eigenständige Architekturentscheidung zur Authentisierung natürlicher Personen erforderlich. Ohne diese Entscheidung bleiben zentrale Fragen ungeklärt: auf welchen Vertrauensquellen die Anmeldung beruht, ob und wie föderierte Identitäten eingebunden werden, welche Vertrauensniveaus für AES und GB erforderlich sind, wie organisatorische Zugehörigkeit und Rollenbindung nachgewiesen werden und wie sich Authentisierung, Autorisierung und Protokollierung zueinander verhalten.

Gerade im Projektkontext ist dies wesentlich, weil OSiP-FV zentral bereitgestellt werden soll, die fachliche Verantwortung aber bei den angeschlossenen Organisationen verbleibt. In einem Zero-Trust-orientierten Modell dürfen Zugriffe nicht aus implizitem Organisationsvertrauen abgeleitet werden, sondern müssen identitäts- und kontextbezogen geprüft werden.

Empfehlung

Es wird empfohlen, eine gesonderte Architekturentscheidung zur Authentisierung natürlicher Personen an den OSiP-Fachverfahren zu erarbeiten und als verbindliche Grundlage für die weitere Fachverfahrens- und IAM-Konzeption festzulegen.

Diese Entscheidung sollte mindestens die folgenden Punkte festlegen:

- ein föderiertes Zielbild für die Authentisierung, bei dem OSiP-FV möglichst keine isolierten lokalen Identitätssilos aufbaut, sondern auf organisationsnahe oder verwaltungsnahe vertrauenswürdige Identitätsquellen aufsetzt,
- personenbezogene und organisationsgebundene Identitäten, damit nachvollziehbar ist, welche natürliche Person in welcher organisatorischen Rolle für welche AES oder GB handelt,
- eine Entscheidung, ob AES und GB dasselbe Authentisierungsmodell nutzen oder ob zwei interoperable, aber unterschiedlich ausgeprägte Modelle erforderlich sind,
- Regeln für erweiterte Authentisierung bei besonders schutzbedürftigen Vorgängen, etwa Freigaben, Versagungen, Vier-Augen-Schritten oder administrativen Änderungen,
- Vorgaben für Lebenszyklusprozesse wie Erstregistrierung, Rollenwechsel, Entzug von Berechtigungen oder Ausscheiden aus der Organisation,
- Anforderungen an revisionsfähige Protokollierung, ohne dabei schutzbedürftige Personenmerkmale offenzulegen.

Abhängigkeiten und Wechselwirkungen

Das Handlungsfeld steht in enger Wechselwirkung mit dem Rollen- und Berechtigungskonzept, dem Mandantenmodell des OSiP-Fachverfahrens, dem Protokollierungs- und Nachvollziehbarkeitskonzept sowie dem Kryptografie- und Schlüsselmanagement. Ebenso bestehen direkte Abhängigkeiten zur Frage, welche Organisationsattribute und Rolleninformationen aus externen Identitätsquellen übernommen werden können und welche innerhalb von OSiP-FV verwaltet werden müssen.

Darüber hinaus beeinflusst die Entscheidung zur Authentisierung die Nutzbarkeit und Anschlussfähigkeit des OSiP-Fachverfahrens für unterschiedliche Nutzungsgruppen erheblich. Für AES aus dem privaten Bereich kann ein anderes Vertrauens- und Registrierungsmodell erforderlich sein als für GB als öffentliche Stellen. Die Architekturentscheidung sollte deshalb ausdrücklich prüfen, ob ein gemeinsames föderiertes Modell mit differenzierten

Vertrauensniveaus ausreicht oder ob getrennte Zugangspfade mit einheitlicher nachgelagerter Rollen- und Rechteverarbeitung vorzusehen sind.

6.8 Detektion und Reaktion entsprechend Zero-Trust-Modell

Ausgangslage

Die Zielarchitektur von NEOSiP folgt dem Zero-Trust-Prinzip und entsprechend des „Positionspapier Zero-Trust 2023" des BSI umfasst dies eine auf dynamischen Zugriffsrichtlinien, kontinuierlicher Überwachung und Risikoanalysen beruhende Sicherheitssteuerung. Daraus ergibt sich die Notwendigkeit, sicherheitsrelevante Ereignisse nicht nur zu protokollieren, sondern systematisch zu erkennen, zu bewerten und mit geeigneten Maßnahmen zu beantworten.

In der aktuellen Konzeption sind die Voraussetzungen für Authentifizierung, Autorisierung und Protokollierung vorgesehen, ein übergreifendes Konzept für Detektion, Korrelation, Bewertung und Reaktion auf sicherheitsrelevante Ereignisse ist jedoch bislang nicht konkret definiert. Dies betrifft sowohl Ereignisse aus dem Identitäts- und Berechtigungskontext als auch sicherheitsrelevante Zustände technischer Identitäten, Schnittstellen, Konfigurationen und Kommunikationsbeziehungen.

Handlungsbedarf

Für den sicheren Betrieb der Zielarchitektur ist ein abgestimmtes Konzept zur Detektion sicherheitsrelevanter Ereignisse sowie zur regelbasierten Reaktion auf erkannte Auffälligkeiten erforderlich. Ohne eine solche Ausgestaltung besteht das Risiko, dass sicherheitskritische Zustände zwar technisch entstehen und protokolliert werden, jedoch nicht zeitnah erkannt, bewertet und wirksam adressiert werden.

Der Handlungsbedarf umfasst insbesondere die Frage, welche Ereignisse zentral zu erfassen sind**,** wie diese korreliert und priorisiert werden und welche Reaktionen automatisiert ausgelöst werden können**.**

Empfehlung

Es wird empfohlen, konkrete Maßnahmen zur Detektion und Reaktion im Kontext des Zero-Trust-Modells zu erarbeiten. Diese Maßnahmen sollten folgende Aspekte umfassen:

- Definition sicherheitsrelevanter Ereignisse und Zustände, einschließlich Authentifizierungs- und Autorisierungsereignissen, Richtlinienverstößen und ungewöhnlicher Zugriffsmuster.

- Festlegung von Mechanismen zur zentralen Erfassung, Korrelation und Auswertung dieser Ereignisse.
- Definition abgestufter Reaktionsmaßnahmen, beispielsweise Einschränkung oder Entzug von Berechtigungen, Sperrung technischer Identitäten oder organisatorische Eskalationen
- Klärung der Zuständigkeiten und Verantwortlichkeiten für Bewertung, Entscheidung und Umsetzung von Reaktionen
- Berücksichtigung bestehender Audit-, Logging-, Monitoring- und Betriebsprozesse

Zusätzlich sollten insbesondere folgende Ereignisquellen und Informationsobjekte einbezogen werden:

- sicherheitsrelevante Ereignisse natürlicher und technischer Identitäten,
- Auffälligkeiten in Kommunikationsmustern die die TI überwacht,
- Integritätsabweichungen und Richtlinienverletzungen,
- sicherheitsrelevante Zustände von Administrations-, Routing- und Schlüsselverwaltungsprozessen.

Abhängigkeiten und Wechselwirkungen

Der Handlungsbedarf steht in enger Wechselwirkung mit den Querschnittskonzepten zu Identitäts- und Rechtemanagement, der Auswahl des konkreten IAM, sowie Betrieb und Monitoring.

6.9 Integration des Projekts Föderale API-Autorisierungsinfrastruktur

Ausgangslage

Der IT-Planungsrat hat mit dem Projekt „Föderale API-Autorisierungsinfrastruktur“[24] (Projekt-ID: itPLR-25-004[25]) ein Vorhaben initiiert, das eine übergreifende API-Autorisierungsinfrastruktur für Querschnitts- und Basisdienste konzipieren soll. Ziel ist eine einheitliche Authentifizierung und Autorisierung nutzender Systeme in Maschine-zu-Maschine-Szenarien. Verantwortlich sind Sachsen-Anhalt und die FITKO.

Für OSiP ist dieses Projekt unmittelbar relevant, weil sowohl die Transportinfrastruktur als auch das zentral bereitgestellte Fachverfahren APIs für maschinelle Nutzung bereitstellen bzw.

[24] https://gitlab.opencode.de/sachsen-anhalt/mid/foederale-api-autorisierungsinfrastruktur
[25] https://www.it-planungsrat.de/beschluss/beschluss-2025-22

nutzen werden. OSiP sollte daher keine isolierte, basisdienstspezifische API-Autorisierung etablieren, wenn hierfür bereits ein föderales Zielbild entsteht.

Handlungsbedarf

Es ist zu klären, wie die OSiP-Zielarchitektur die Zielarchitektur der föderalen API-Autorisierungsinfrastruktur nutzen und in die eigenen Querschnittskonzepte integrieren soll. Dabei ist insbesondere zu prüfen, welche Teile des föderalen Zielbilds für OSiP verbindlich oder zumindest referenzierbar übernommen werden können, etwa im Hinblick auf Client-Registrierung, Token-basierte API-Autorisierung, Sicherheitsprofile, Berechtigungsmodell und Laufzeitinteraktion zwischen nutzenden Systemen und Basisdiensten.

Empfehlung

Es wird empfohlen, einen strukturierten Architekturabgleich mit dem Projekt „Föderale API-Autorisierungsinfrastruktur" einzuleiten und die dort entstehende Zielarchitektur als maßgebliches Referenzmodell für die API-Autorisierung von OSiP zu verwenden. Ziel sollte sein, OSiP so auszurichten, dass die APIs der TI und des zentral bereitgestellten Fachverfahrens die föderalen Autorisierungsstandards nach Möglichkeit direkt nutzen können und Abweichungen nur dort vorgenommen werden, wo dies aufgrund der OSiP-spezifischen Sicherheits- und Prozessanforderungen zwingend erforderlich ist.

Die Ergebnisse sollten in den betroffenen ADRs und Querschnittskonzepten nachvollziehbar nachgeführt werden. Besonders naheliegend ist dabei eine Überprüfung von ADR-006 und ADR-007 zur Identität öffentlicher bzw. privater Organisationen sowie von ADR-008 und ADR-009 zur vereinfachten Anbindung und zum Anschluss externer Bestandssysteme.

Abhängigkeiten und Wechselwirkungen

Das Handlungsfeld steht in enger Wechselwirkung mit dem IAM-Konzept und Trust-Diensten, mit dem Onboarding von Teilnehmenden, mit den Weiterentwicklunggesprächen mit der V-PKI, mit den Anschlussbedingungen für Fachverfahren sowie mit der Ausgestaltung der TI- und Fachverfahrens-APIs.

6.10 Integration und Nachnutzung des NOOTS

Ausgangslage

Derzeit entsteht das Nationale Once-Only-Technical-System (NOOTS). Das NOOTS dient dem automatisierten und rechtskonformen Nachweisabruf zwischen öffentlichen Stellen und

Registern im Rahmen der Registermodernisierung. Es soll dazu beitragen, dass Nachweise nach Zustimmung der betroffenen Person aus zuständigen Registern abgerufen werden können, anstatt mehrfach eingereicht werden zu müssen.

Registerabfragen sind ein zentraler Bestandteil an mehreren Stellen des ZSÜ-Prozesses. Für die Antragsteller und die Genehmigungsbehörden könnten Registerabfragen die Antragstellung deutlich vereinfachen. Auf der Seite der Erkenntniseinholung werden bereits jetzt vielfach Register abgefragt. Für OSiP ist das NOOTS in zweifacher Hinsicht relevant. Zum einen ist es für solche EKS relevant, die Register sind und sich perspektivisch an das NOOTS anbinden müssen oder sollen. Zum anderen ist es für das OSiP-Fachverfahren relevant, sofern dort im Rahmen der Antragstellung oder Antragsprüfung Nachweise aus Registern abgerufen werden sollen.

Handlungsbedarf

Es ist zu klären, inwieweit OSiP die Architektur des NOOTS integrieren oder nachnutzen können soll und an welchen Stellen dies fachlich, technisch und organisatorisch sinnvoll ist. Dabei ist insbesondere zu unterscheiden zwischen der Nutzung des NOOTS für den standardisierten Nachweisabruf im OSiP-Fachverfahren, der Anschlussfähigkeit solcher EKS, die Register darstellen oder registerähnliche Rollen einnehmen, sowie der Frage, ob und in welchem Umfang Architekturprinzipien, Anschlussmuster oder technische Komponenten nachgenutzt werden können.

Da das NOOTS zunächst auf OZG-bezogene Verwaltungsleistungen ausgerichtet ist, kann nicht vorausgesetzt werden, dass alle OSiP-Anwendungsfälle unmittelbar darüber abgebildet werden können. Zugleich wäre es architektonisch nachteilig, OSiP so auszugestalten, dass eine spätere Integration oder Nachnutzung unnötig erschwert wird. Daher ist frühzeitig zu prüfen, an welchen Stellen Synergien bestehen und wo Konflikte zwischen den jeweiligen Anforderungen und Architekturprinzipien entstehen können, etwa bei Sicherheitsmodell, Rollenbild, Transportmechanismus, Synchronität bzw. Asynchronität, Anschlussbedingungen und Verantwortungsgrenzen.

Empfehlung

Der bereits etablierte Austausch mit dem NOOTS sollte fortgeführt und durch eine nachvollziehbar dokumentierte Kompatibilitätsanalyse ergänzt werden. Deren Ergebnis sollte

als Grundlage für spätere Architekturentscheidungen, Anschlussbedingungen und die Ausgestaltung des OSiP-Fachverfahrens dienen.

Abhängigkeiten und Wechselwirkungen

Das Handlungsfeld steht in enger Wechselwirkung mit der Ausgestaltung der Transportinfrastruktur, mit den Anschlussbedingungen für Fachverfahren und Register, mit dem Sicherheits- und Krypto-Konzept sowie mit der Architektur des OSiP-Fachverfahrens. Besondere Relevanz besteht dort, wo OSiP einerseits eigenständige Kommunikations- und Verfahrensfunktionen bereitstellt, andererseits aber für den standardisierten Nachweisabruf auf externe Infrastrukturen anschlussfähig bleiben soll.

6.11 Initiale Erarbeitung eines Betriebskonzepts für den Bot-Client

Ausgangslage

Der Bot-Client ist als mandantennaher Anschlussbaustein des zentral bereitgestellten Fachverfahrens konzipiert. Er ist ein sicherheitskritischer Baustein, weil er eingehende Nachrichten vor ihrer fachlichen Weiterverarbeitung temporär im entschlüsselten Zustand verarbeiten kann. Sofern Bot-Clients ganz oder teilweise zentral unter Verantwortung eines zentralen Betreibers betrieben werden sollen, entsteht daraus ein besonders sensibles Betriebsmodell. Der Betreiber hätte potenziell Berührung mit Daten aus bundesweiten Quellen und müsste hierfür ein erhöhtes Maß an technischer, organisatorischer und rechtlicher Absicherung nachweisen. Für sensible Cloud- und Geheimschutzkontexte werden vom BSI Secure Enclaves, Trusted Execution Environments und Confidential Computing als mögliche technische Schutzmaßnahmen angeführt[26]. Zudem beschreibt das BSI Confidential Computing als Nutzung hardwarebasierter, attestierter Trusted Execution Environments zum Schutz der Vertraulichkeit und Integrität von Daten während der Verarbeitung.

Handlungsbedarf

Es sollte eine Erarbeitung eines Betriebskonzepts angefangen werden, das die grundsätzlichen Betriebsmodelle, Schutzmaßnahmen, Verantwortlichkeiten und Randbedingungen frühzeitig beschreibt. Ohne ein solches Betriebskonzept besteht das Risiko, dass die technische

[26] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Geheimschutz/Leitfaden_Cloud-Loesungen_Bundesverwaltung.html

Konzeption des Bot-Clients von nicht tragfähigen Betriebsannahmen ausgeht oder dass zentrale Sicherheits- und Datenschutzanforderungen erst spät berücksichtigt werden.

Es ist zu klären, unter welchen Rahmenbedingungen ein mandantennaher Betrieb der Regelfall bleiben soll, in welchen Ausnahmefällen ein zentraler Betrieb vertretbar wäre und welche zusätzlichen Schutzmaßnahmen dann erforderlich sind. Dabei ist nicht nur die Laufzeitumgebung des Bot-Clients zu betrachten, sondern auch deren Einbettung in Schlüsselmanagement, Monitoring, Incident Management, Update-Prozesse und Protokollierung.

Empfehlung

Es wird empfohlen, ein initiales Betriebskonzept für den Bot-Client zu erarbeiten, das die wesentlichen Betriebsoptionen und Sicherheitsannahmen strukturiert festlegt. Für zentrale Betriebsvarianten sollte das Betriebskonzept ausdrücklich festlegen, dass der Schutz des Bot-Clients nicht allein durch klassische Infrastrukturhärtung angenommen wird, sondern durch eine besonders geschützte Ausführungsumgebung ergänzt werden muss. TEEs und Confidential Computing zielen darauf ab, Daten während der Verarbeitung in isolierten, hardwaregestützt geschützten Umgebungen zu verarbeiten und ihre Exposition gegenüber Host-Betriebssystem, Hypervisor oder sonstig privilegierter Software zu reduzieren.

Abhängigkeiten und Wechselwirkungen

Das Handlungsfeld steht in enger Wechselwirkung mit der Ausgestaltung der TI, dem Sicherheits- und Krypto-Konzept, den Anschlussbedingungen für Fachverfahren, dem Rollen- und Rechtemodell sowie den Anforderungen an Auditierung und Protokollierung. Besondere Abhängigkeiten bestehen zum Schlüsselmanagement.

6.12 Weiterentwicklung der Verwaltungs-PKI

Ausgangslage

Mit ADR-006 wurde für die technische Authentisierung öffentlicher Stellen die Nutzung von X.509-Zertifikaten aus der Verwaltungs-PKI festgelegt.

Aus Sicht der Zielarchitektur deckt die heutige Version der Verwaltungs-PKI die in ADR-006 formulierten Anforderungen jedoch noch nicht vollständig ab. Für eine Zero-Trust-orientierte Infrastruktur mit stark automatisierter System-zu-System-Kommunikation werden

insbesondere intuitivere Self-Service-Prozesse, automatisierte Zertifikatsausstellung und -erneuerung sowie weiterentwickelte Transparenz- und Attributmechanismen benötigt.

Handlungsbedarf

Es besteht der Handlungsbedarf, die Weiterentwicklung der Verwaltungs-PKI frühzeitig mit dem zuständigen Produktmanagement der V-PKI abzustimmen. Ziel ist nicht die Ablösung der getroffenen ADR-Entscheidung, sondern die Klärung, wie die Verwaltungs-PKI perspektivisch so weiterentwickelt werden kann, dass sie die allgemeinen Anforderungen der OSiP-Zielarchitektur und die spezifischen Anforderungen aus ADR-006 besser unterstützt.

Dabei ist insbesondere zu prüfen, inwieweit die Verwaltungs-PKI künftig Funktionen eines moderneren IAM- und Trust-Ökosystems für öffentliche Stellen besser unterstützen kann. Hierzu zählen aus Projektsicht insbesondere automatisierte Lebenszyklusprozesse für Zertifikate, kryptographisch belastbare Attributbindung, verbesserte Betriebs- und Transparenzmechanismen sowie eine bessere Einbettung in Zero-Trust- und Governance-Modelle.

Empfehlung

Es wird empfohlen, einen strukturierten Austausch mit dem Produktmanagement der V-PKI einzuleiten. Gegenstand dieses Austauschs sollte sein, die für OSiP relevanten Anforderungen konsolidiert zu erläutern und gemeinsam zu bewerten, welche Weiterentwicklungen der Verwaltungs-PKI mittel- bis langfristig erforderlich oder anschlussfähig sind.

Im Fokus sollten dabei insbesondere folgende Themen stehen:

- automatisierte Zertifikatsausstellung, -erneuerung und -widerruf, insbesondere unter Nutzung standardisierter Verfahren wie ACME,
- Unterstützung kurzer Zertifikatslaufzeiten und stärker automatisierter Lebenszyklusprozesse,
- Einbettung kryptographisch gesicherter Attribute in Zertifikate oder eng daran gekoppelte Vertrauensmechanismen,
- Transparenz- und Auditierbarkeit von Zertifikatsausstellungen, etwa durch Certificate-Transparency-nahe Mechanismen,

Es ist festzuhalten, welche Anforderungen durch die bestehende Verwaltungs-PKI bereits erfüllt werden, welche Lücken aus Sicht der Zielarchitektur bestehen und welche Punkte nur durch produktseitige Weiterentwicklung der Verwaltungs-PKI adressiert werden können.

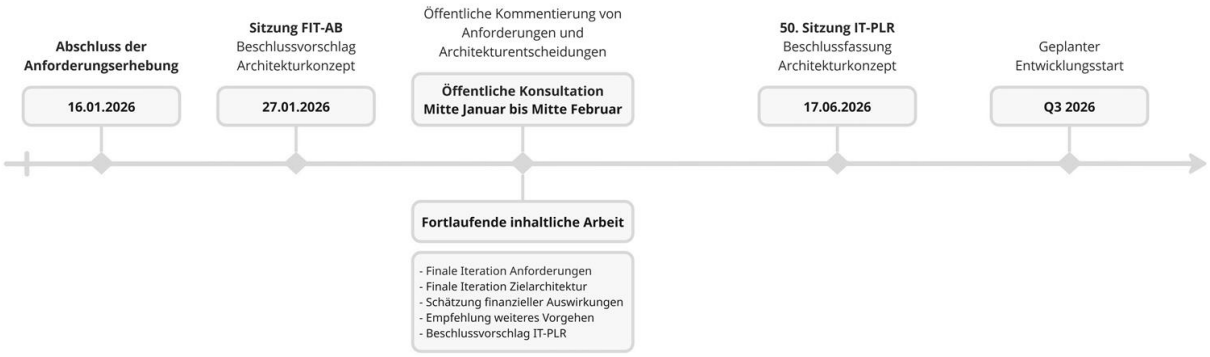
Abhängigkeiten und Wechselwirkungen

Das Handlungsfeld steht in enger Wechselwirkung mit ADR-006, mit dem Onboarding öffentlicher Stellen sowie mit den Querschnittsanforderungen an Authentizität, Zero Trust und automatisierte Systemkommunikation. Erkenntnisse aus dem Austausch können unmittelbaren Einfluss auf die Ausgestaltung der Anschlussbedingungen, des Zertifikatslebenszyklusmanagements und der zukünftigen Authentisierungsarchitektur haben.

7 Weiteres Vorgehen

7.1 Projekt-Roadmap

Die folgende Roadmap zeigt die zeitliche Planung des Vorhabens bis zur vorgesehenen Verabschiedung des Architekturkonzepts in der 50. Sitzung des IT-Planungsrates:



7.2 Logbuch zur Projekt-Roadmap

- **[26.03.2025] Beschluss IT-Planungsrat (46. Sitzung)**
  Der IT-Planungsrat fasst den Beschluss zur Neukonzeption von OSiP.[27]
- **[01.05.2025] Projektstart**

[27] vgl. Beschluss 2025/20 - Neukonzeption OSiP | IT-Planungsrat

Offizieller Beginn des Projekts zur Neukonzeption OSiP.

- **[27.06.2025] Erstes Treffen des Lenkungsausschusses**
  Der Lenkungsausschuss kommt erstmals zusammen.
- **[09.09.2025] Start des Aufbaus der operativen Arbeitsgruppen**
  Beginn der Einrichtung und Organisation der Arbeitsgruppen.
- **[30.09.2025] Abschluss der Bestandsanalyse**
  Die Bestandsaufnahme wird abgeschlossen.
- **[16.01.2026] Abschluss der Anforderungserhebung**
  Die Erhebung und Konsolidierung der Anforderungen ist abgeschlossen.
- **[Mitte Februar 2026] Start der öffentlichen Konsultation**
  Veröffentlichung der Anforderungen zur Kommentierung und Feedback-Einholung.
- **[19.05.2026] Sitzung FIT-AB**
  Vorstellung und Diskussion der Ergebnisse im Föderalen IT-Architekturboard.
- **[17.06.2026] 50. Sitzung IT-Planungsrat**
  Geplante Vorstellung der Ergebnisse und weiterer Beschlüsse.

- **[Q3 2026] Geplanter Entwicklungsstart**
  Start der Umsetzungsphase basierend auf den abgestimmten Beschlüssen.

Glossar

Das Glossar befindet sich in Begleitdokument 4 „Glossar" und auf der Plattform openCode[28].

Abbildungsverzeichnis

[28] https://gitlab.opencode.de/fitko/osip/neukonzeption-osip/-/blob/main/Glossar.md

Tabellenverzeichnis

Abkürzungsverzeichnis

2FA ..... Zwei-Faktor-Authentisierung
ADRs ..... Architecture-Decision-Records
AEAD ..... Authenticated Encryption with Associated Data
AES ..... Antragserfassungsstelle
APIs ..... standardisierte, dokumentierte Schnittstellen
AuthN ..... Authentifizierung natürlicher Personen
AWB ..... Anwendungsbereich
BAMAD ..... Bundesamt für den Militärischen Abschirmdienst

beispielsweise	bspw.
BfV	Bundesamt für Verfassungsschutz
BKA	Bundeskriminalamt
BND	Bundesnachrichtendienst
BO-Client	Back-Office-Client
BPMN	Business Process Model and Notation
BSI	Bundesamt für Sicherheit in der Informationstechnik
CI/CD	Continues Integration/Continues Delivery
Data Protection by Default	Datenschutz durch datenschutzfreundliche Voreinstellungen
Data Protection by Design	Datenschutz durch Technikgestaltung
d-NRW	d-NRW AöR Anstalt öffentlichen Rechts
DSFA	Datenschutz-Folgenabschätzung
DSGVO	Datenschutz-Grundverordnung
E2EE	Ende-zu-Ende-Verschlüsselung
EKS	Erkenntnisstellen
FITKO	Föderale IT-Kooperation
FO-Client	Front-Office-Client
GB	Genehmigungsbehörde
ggf.	gegebenenfalls
HSM	Hardware Security Modulen
i. d. R.	in der Regel
ICAP	Internet Content Adaptation Protocol
IdP	Identititätsanbieter
inkl.	inklusive
IT-NetzG	Gesetz über die Verbindung der IT-Netze von Bund und Ländern
LfV	Landesamt für Verfassungsschutz
LKA	Landeskriminalamt
LVN	Landesverwaltungsnetz
M2M	Machine-to-Machine
MFA	Mehrfaktorauthentisierung
mTLS	Mutual TLS
OIDC	OpenID Connect
OSiP	Online-Sicherheitsüberprüfung
PBAC	rollenbasiertes Zugriffskontrollsystem
PDP	Policy Decision Point
PEP	Policy Enforcement Points
PITR	Point-In-Time-Backup-Strategien
PKCE	Proof Key for Code Exchange
PoC	Proof of Concept
QR	Quick Response
SaaS-Modell	Software-as-a-Service-Modell
SAML	Security Assertion Markup Language
SDKs	Software Development Kits
SM/VC	Sicherer Messenger und Videokonferenzsysteme
SPA	Single Page Application

TEE	Trusted Execution Environment
TI	Transportinfrastruktur
TR	Technische Richtlinien
u.a.	unter anderem
vPKI	Verwaltungs-Public Key Infrastruktur
VS	Verschlusssachen
VSA	Verschlusssachenanweisung
WCAG 2.1 AA	Web Content Accessibility Guidelines
XSS	Cross-Site Scripting
ZKA	Zollkriminalamt
ZSÜ	Zuverlässigkeits- und Sicherheitsüberprüfungen