IT-PLANUNGSRAT

Frankfurt am Main
29.05.2026

Zielarchitektur föderale API-Autorisierungsinfrastruktur

- Kurzfassung -

Konzeption einer Basisinfrastruktur zur Realisierung eines durchgängigen föderalen Plattform-Ökosystems

Inhaltsverzeichnis

Hinweis zur Kurzfassung

Das vorliegende Dokument ist eine Kurzfassung des Konzepts zur Zielarchitektur der Föderalen API-Autorisierungsinfrastruktur. Es ist aus dem Hauptkonzept abgeleitet, das den vollständigen fachlichen, technischen und organisatorischen Rahmen der Zielarchitektur beschreibt. In dieser Kurzfassung sind Inhalte verkürzt, zusammengefasst oder weggelassen. Insbesondere detaillierte Prozessbeschreibungen, Detailinformationsflüsse, vollständige Use-Case-Listen, Datenmodellbeschreibungen, Pseudocode der Berechtigungslogik sowie ausführliche Bewertungen einzelner Standardlösungen sind nicht Bestandteil dieser Kurzfassung. Für vertiefende Inhalte wird durchgängig auf das Hauptkonzept verwiesen.

1 Einleitung

Die föderale Verwaltung steht vor der Herausforderung, eine wachsende Zahl digitaler Basisdienste sicher, einheitlich und wirtschaftlich miteinander zu verknüpfen. Dieses Kapitel erläutert, warum ein gemeinsames Fundament für die API-Autorisierung notwendig ist und was die Zielarchitektur zur föderalen API-Autorisierungsinfrastruktur leisten soll.

1.1 Projektkontext und Ausgangslage

Die föderale IT der öffentlichen Verwaltung wächst kontinuierlich: Basisdienste wie Postfächer, FIT-Connect, Bezahldienste oder NOOTS-Komponenten bilden zunehmend das technische Rückgrat digitaler Verwaltungsleistungen. Onlinedienste, Fachverfahren und Unternehmensanwendungen müssen sich gegenüber diesen Basisdiensten authentifizieren und autorisieren, heute jedoch mit basisdienstspezifischen Verfahren, ohne gemeinsame technische Muster.
Aus dieser Heterogenität ergeben sich vier wesentliche Probleme:

- **Mehrkosten und Komplexität in der Implementierung:** Jeder Basisdienst erfordert eine eigene Integrationslogik, da keine einheitlichen technischen Muster existieren. Betreiber von Onlinediensten und Fachverfahren müssen für jeden Basisdienst gesonderte Autorisierungsmechanismen entwickeln und warten.
- **Mehrkosten bei der Registrierung:** Das Fehlen automatisierter, standardisierter Registrierungsprozesse zwingt Betreiber zu manuellen, basisdienstspezifischen Onboarding-Verfahren, was den Integrationsaufwand erheblich erhöht.
- **Sicherheitsrisiken:** Ohne gemeinsame Sicherheitsvorgaben entstehen heterogene, teils unzureichend gesicherte Autorisierungslösungen, die die Gesamtsicherheit der föderalen IT-Landschaft gefährden.
- **Behinderung eines API-First-Ökosystems:** Die fehlende Standardisierung erschwert die skalierbare Nachnutzung von Basisdiensten und bremst die Entwicklung eines durchgängig interoperablen föderalen API-Ökosystems.

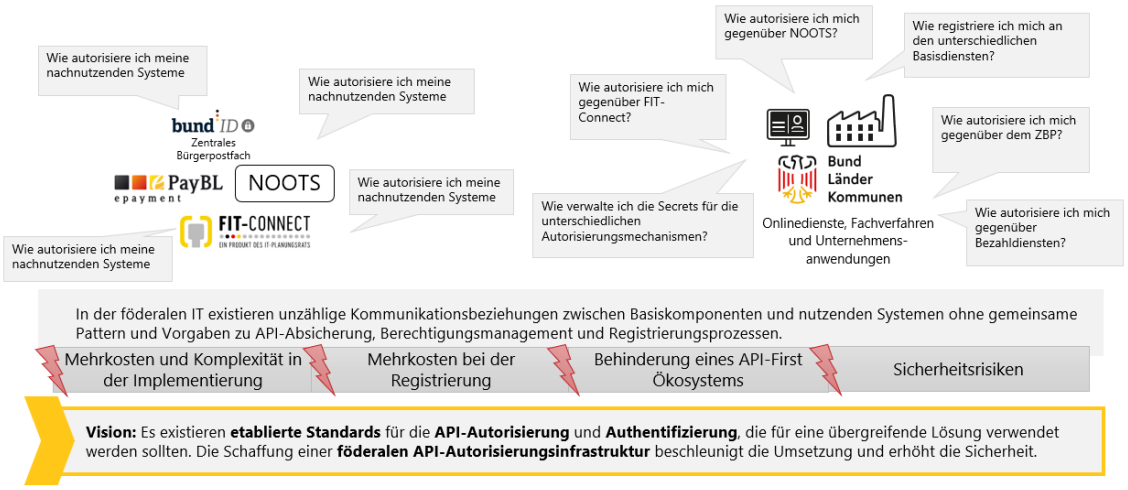

Abbildung 1: Ausgangslage

Das Projekt „Föderale API-Autorisierungsinfrastruktur" (Projekt-ID: itPLR-25-004) wurde durch Beschluss 2025/22 der 47. Sitzung des IT-Planungsrats vom 26. Juni 2025 initialisiert. Es ist dem Schwerpunktthema „Digitale Transformation" zugeordnet und adressiert die genannte Ausgangslage durch Schaffung eines gemeinsamen Fundaments für die API-Autorisierung. Eine erste Pilotierung im Kontext der Bezahldienste lieferte praktische Erkenntnisse, die in das Vorhaben eingeflossen sind.

Das Vorhaben umfasst zwei zentrale Liefergegenstände, deren Geltungsbereich bewusst unterschieden wird: Die **Sicherheitsvorgaben** definieren auf Basis des FAPI-2.0-Standards ein einheitliches Sicherheitsniveau für die API-Absicherung mit OAuth und OpenID Connect; ihr Geltungsbereich umfasst alle APIs der öffentlichen Verwaltung. Die **Zielarchitektur** (das hier in Kurzform dargestellte Dokument) beschränkt sich auf die APIs föderaler Basisdienste und legt dar, wie Betreiber, Integratoren und Nutzer in einer föderalen Autorisierungsinfrastruktur skalierbar, sicher und wirtschaftlich zusammenwirken können.

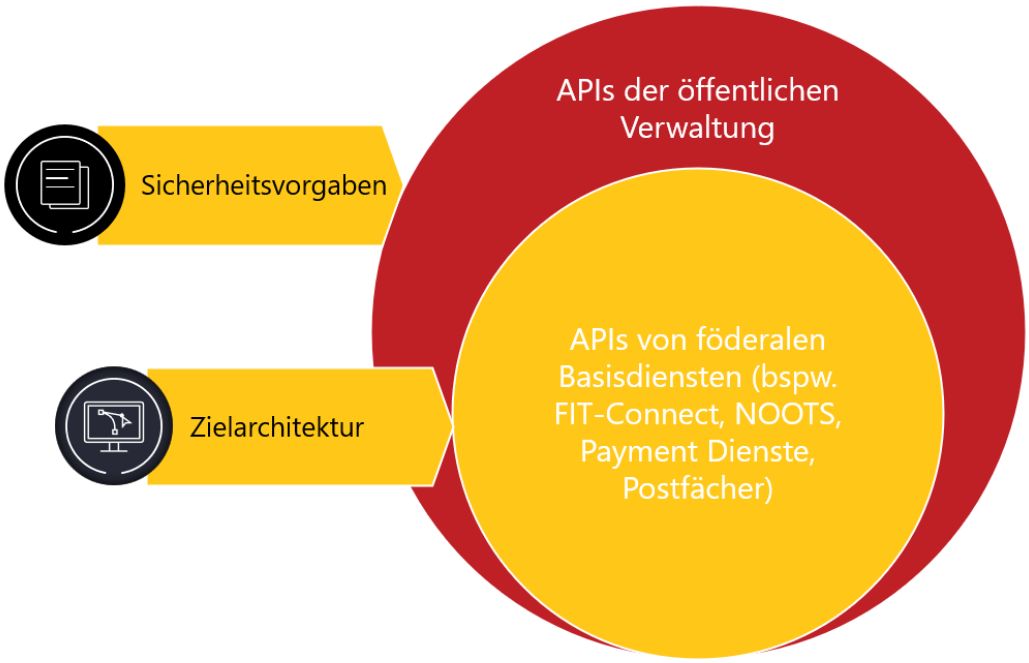

Abbildung 2: Fokus der Projektliefergegenstände

1.2 Umfang und Fokus der Zielarchitektur

Der Umfang der Zielarchitektur wird über drei komplementäre Wertströme definiert. Ein Wertstrom beschreibt dabei die Abfolge von Aktivitäten, die notwendig sind, um einem bestimmten Stakeholder einen konkreten Nutzen zu liefern. Aus der beschriebenen Ausgangslage ergeben sich drei Wertströme, die das Vorhaben adressiert:

- **APIs von Basisdiensten bereitstellen:** Betriebsorganisationen von Basisdiensten können ihre APIs auf standardisierte Weise im föderalen Kontext verfügbar machen, einschließlich der Beschreibung von Berechtigungsmodellen und der Veröffentlichung von Katalogin-formationen.
- **APIs von Basisdiensten in fachliche Anwendungen integrieren:** Betriebsverantwortliche Stellen und Software-Lieferanten können die benötigten APIs von Basisdiensten über einheitliche Prozesse beantragen, ihre Software registrieren und API-Clients automatisiert an allen relevanten Basisdiensten anmelden.
- **Angebote von Basisdiensten nutzen:** Basisdienstnutzer können zur Laufzeit sicher und nachvollziehbar auf Basisdienste zugreifen, unabhängig davon, welcher Basisdienst genutzt wird.

Die drei Wertströme sind komplementär zueinander: Erst ihr abgestimmtes Zusammenspiel schafft ein durchgängig anschlussfähiges föderales API-Ökosystem.

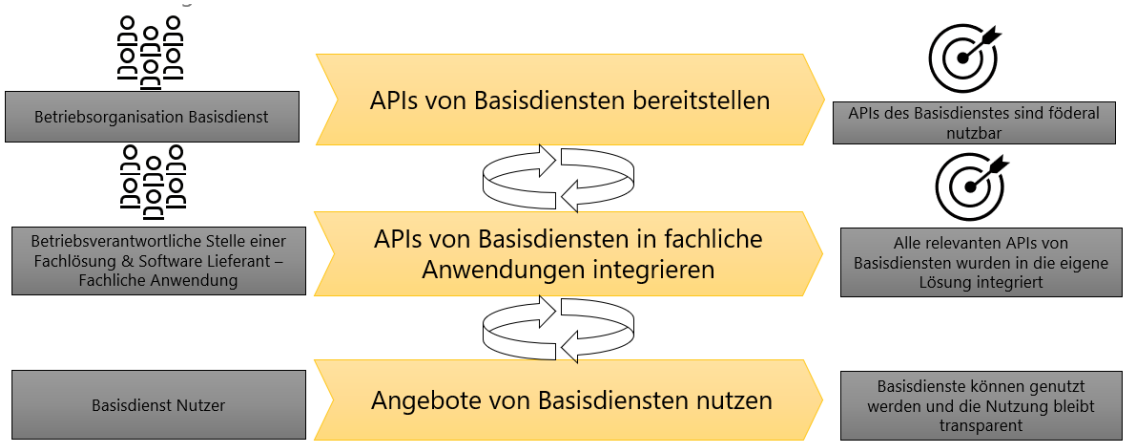

Abbildung 3: Umfang und Fokus der Zielarchitektur

1.3 Ziel des Dokuments

Das Hauptkonzept dient dem IT-Planungsrat als Entscheidungsgrundlage für den Aufbau einer föderalen API-Autorisierungsinfrastruktur. Es legt dar, wie eine solche Infrastruktur konzeptionell aussehen kann, welche organisatorischen und technischen Voraussetzungen für ihre Umsetzung erforderlich sind, welche Architekturentscheidungen getroffen wurden und wie der Übergang in den produktiven Betrieb gestaltet werden kann. Auf Basis dieses Dokuments soll der IT-Planungsrat ein Umsetzungsprojekt beschließen können, das die identifizierten Implementierungs- und Migrationsaufgaben durchführt und die föderale API-Autorisierungsinfrastruktur in den produktiven Betrieb überführt.

Die vorliegende Kurzfassung gibt einen verdichteten Überblick über die zentralen Inhalte des Hauptkonzepts.

2 Strategische Ausrichtung

Die strategische Ausrichtung beschreibt den übergeordneten Rahmen, der alle nachfolgenden Architektur- und Designentscheidungen der föderalen API-Autorisierungsinfrastruktur leitet. Sie beantwortet die Frage, wohin das Vorhaben führen soll, welche Ziele dabei im Vordergrund stehen und nach welchen Prinzipien gehandelt wird.

2.1 Architekturvision

Folgendes Vision Statement richtet als Nordstern die Konzeption der Zielarchitektur aus:

> *„Föderale Basisdienste sind nach einheitlichen Sicherheitsstandards absicherbar und wirtschaftlich integrierbar, unabhängig davon, wer sie betreibt oder nutzt. Eine gemeinsame Autorisierungsinfrastruktur schafft das technische Fundament für ein interoperables föderales Plattform-Ökosystem, in dem Mehrfachaufwände entfallen und Berechtigungen nachvollziehbar geregelt sind. Sie steht öffentlichen IT-Dienstleistern und privaten Unternehmen gleichermaßen offen und ermöglicht ein Innovationsökosystem, das den Verwaltungsalltag digital trägt."*

2.2 Projektspezifische Architekturziele

Das Vision Statement bildet die Grundlage für acht Architekturziele, die den Nutzen der Infrastruktur für Betreiber, Integratoren und die föderale IT-Landschaft insgesamt operationalisieren.

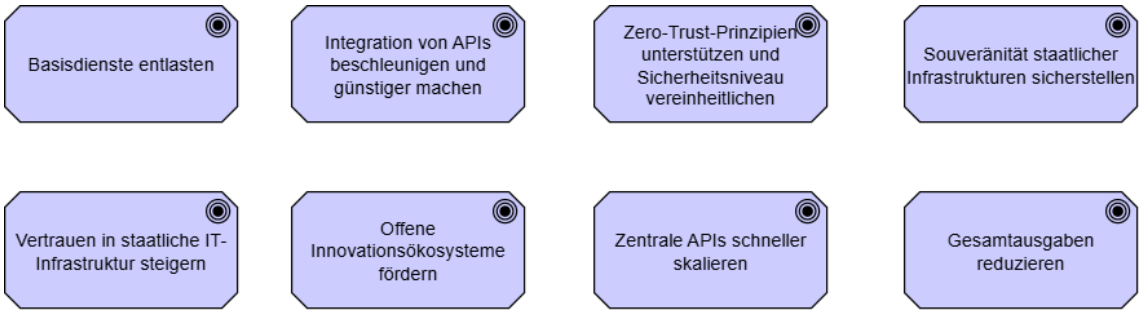

Abbildung 4: Projektspezifische Architekturziele

- **Basisdienste entlasten:** Die Infrastruktur übernimmt sicherheits- und berechtigungsbezogene Querschnittsfunktionen, die andernfalls jeder Basisdienst eigenständig um-setzen müsste. Basisdienst-Teams können sich dadurch auf ihre fachlichen Kernaufgaben konzentrieren.
- **Integration von APIs beschleunigen und günstiger machen:** Standardisierte Registrierungsprozesse und automatisierte Anbindungsverfahren reduzieren den Zeit- und

Kostenaufwand für die Integration föderaler Basisdienste; alle Anwendungen nutzen dieselben Muster und Schnittstellen.

- **Zero-Trust-Prinzipien unterstützen und Sicherheitsniveau vereinheitlichen:** Jede Anfrage wird unabhängig von Netzwerkherkunft oder institutioneller Zugehörigkeit authentifiziert und autorisiert. Einheitliche Sicherheitsvorgaben schaffen ein flächendeckendes, hohes Sicherheitsniveau.
- **Souveränität staatlicher Infrastrukturen sicherstellen:** Die Infrastruktur basiert auf offenen Industriestandards und Open-Source-Komponenten, um Abhängigkeiten von einzelnen Herstellern zu vermeiden. Dezentrale Betriebsmodelle verhindern, dass eine einzelne Stelle unkontrollierte Kontrolle über kritische Sicherheitsfunktionen erlangen kann.
- **Vertrauen in staatliche IT-Infrastruktur steigern:** Transparente, nachvollziehbare und revisionssichere Protokollierung aller Berechtigungsentscheidungen schafft Vertrauen bei Bürgerinnen, Bürgern und Unternehmen. Berechtigungen basieren auf klar definierten Regeln und Prozessen.
- **Offene Innovationsökosysteme fördern:** Standardisierter, diskriminierungsfreier Zugang zur Infrastruktur ermöglicht öffentlichen IT-Dienstleistern und privaten Unternehmen gleichermaßen die Integration föderaler Basisdienste in ihre Lösungen, auf einem Level Playing Field.
- **Zentrale APIs schneller skalieren:** Neue Basisdienste lassen sich durch standardisierte Infrastruktur deutlich schneller in das föderale Ökosystem einbinden. Einmalig definierte Sicherheitsvorgaben, Registrierungsprozesse und Berechtigungslogiken gelten für alle Basisdienste ohne Mehraufwand.
- **Gesamtausgaben reduzieren:** Die Bündelung von Querschnittsfunktionen vermeidet teure Mehrfachentwicklungen bei Bund, Ländern und Basisdienst-Betreibern. Standardisierte Komponenten und Prozesse senken den Betriebsaufwand durch Skaleneffekte.

2.3 Projektspezifische Architekturprinzipien

Die Architekturprinzipien bilden den verbindlichen Handlungsrahmen für alle Architektur- und Designentscheidungen im Rahmen der föderalen API-Autorisierungsinfrastruktur. Sie konkretisieren das Vision Statement und die Architekturziele auf der Ebene von Gestaltungsregeln, die bei Technologieauswahl, Prozesskonzeption und Bewertung von Lösungsalternativen anzuwenden sind.

Tabelle 1: Projektspezifische Architekturprinzipien

ID	Name	Erklärung

P-001	Offene Industriestandards und Best Practices nutzen	Funktionen, Datenmodelle, Schnittstellen und Architekturmuster werden, wo möglich, auf Basis etablierter offener Industriestandards umgesetzt. Auch neu aufkommende Entwicklungen werden genutzt, sofern sie sich in das bestehende Ökosystem einfügen.
P-002	Individualentwicklungen und verwaltungsspezifische Lösungen vermeiden	Etablierte Standardlösungen aus mehreren Branchen haben Vorrang gegenüber Individual- oder verwaltungsspezifischen Entwicklungen. Verwaltungsspezifische Lösungen sind nur bei nicht vermeidbaren, hochspezifischen Anforderungen ohne Bedarf außerhalb der Verwaltung zulässig.
P-003	Etablierte Verwaltungsinfrastruktur als zulässige Standardlösung berücksichtigen	Etablierte Komponenten der digitalen Verwaltungsinfrastruktur, die auf offenen Standards basieren und einer klaren Governance unterliegen, sind als Standardlösungen zulässig, sofern interoperabel ausgestaltet und ohne Bindung an proprietäre Insellösungen.
P-004	Verwaltungsspezifische Anforderungen in Standardisierungsprozesse einbringen	Anforderungen, die kein bestehender offener Standard abdeckt und die über eine einzelne Implementierung hinaus relevant sind, werden aktiv in Standardisierungsprozesse eingebracht. Eigenentwicklungen sind nur als befristete Übergangslösungen zulässig.
P-005	„Never trust, always verify" bei allen Zugriffen	Antwortende Systeme authentifizieren anfragende Systeme und verifizieren deren Autorisierungen. Für besonders kritische Informationen exponierter Systeme bestehen ergänzende Informationsquellen zu Veränderungstransaktionen, um Risikosituationen erkennen zu können.
P-006	Minimale Zugriffsberechtigungen und dynamische Zugriffsüberprüfungen	Systeme erhalten nur die zwingend benötigten Berechtigungen (Least Privilege). Der tatsächliche Zugriffsumfang hängt zusätzlich vom kontextuellen Vertrauenswert ab (Policy-based Access).
P-007	Nachvollziehbarkeit und Auditierbarkeit aller relevanten Systemaktivitäten	Relevante Ereignisse werden protokolliert, redundant gespeichert und manipulationsgeschützt vorgehalten. Informationen werden über Teilnehmergrenzen hinweg geteilt; betroffene Teilnehmer werden bei kritischen Ereignissen aktiv informiert.
P-008	Dezentralität und Redundanz von Sicherheitsmechanismen	Essenzielle Absicherungsfunktionen werden dezentral betrieben. Schutz eines Angriffsziels erfolgt über mehrere komplementäre Sicherheitsmechanismen, sodass die Kompromittierung

		einer Komponente keinen Angriffserfolg ermöglicht.
P-009	Open-Source-Priorisierung für kritische Komponenten	Bei vergleichbarer Eignung werden Open-Source-Lösungen bevorzugt. Voraussetzung sind ein tragfähiges Ökosystem und verfügbarer Support, also keine reine Lizenzierung verwaltungsspezifischer Lösungen.
P-010	Bündelung technischer Querschnittsfunktionen	Querschnittsfunktionen werden in spezialisierten Komponenten gebündelt und über lose gekoppelte Schnittstellen bereitgestellt. Das schließt eine zentral entwickelte Komponente, die als Sidecar in dezentralen Umgebungen läuft, ausdrücklich ein.
P-011	Flexibilität und Anpassbarkeit API-spezifischer Berechtigungsmodelle	Basisdienste können die berechtigungsrelevanten Informationen ihrer APIs flexibel an ihre fachlichen Anforderungen anpassen.
P-012	Automatisierung von Anbindungsprozessen	Alle Schritte des Anbindungsprozesses (von der Erstregistrierung bis zur Software-Registrierung an einer API) werden, soweit sicher und technisch praktikabel, vollständig automatisiert.
P-013	Ermöglichung effizienter und unterbrechungsfreier Backoffice-Verwaltungsprozesse	Backoffice-Prozesse werden so gestaltet, dass sie nicht durch manuelle Freigaben einzelner Nutzender unterbrochen oder verzögert werden.
P-014	Wiederverwendung und Bündelung vor Neuentwicklung	Vor Neuentwicklungen wird geprüft, ob bestehende föderale Lösungen nachgenutzt werden können. Bei Neuentwicklungen werden Bedarfe mehrerer Basisdienste gebündelt, um die IT-Landschaft zu konsolidieren.
P-015	Vertrauen basiert auf Protokollen und Prozessen, nicht auf Institutionen	Sicherheit und Vertrauenswürdigkeit werden durch Protokolle und Prozesse gewährleistet, nicht durch die Annahme, dass beteiligte Institutionen sich stets regelkonform verhalten.
P-016	Personenbezogene Daten minimieren	Es werden nur die unbedingt erforderlichen personenbezogenen Daten erhoben, verarbeitet und gespeichert (Datenminimierung gemäß DSGVO).
P-017	Dynamische Berechtigungssteuerung	Zugriffsrechte sind sofort und flexibel änder- oder entziehbar, ohne Verzögerung und ohne technische Hürden. Berechtigungen sind nicht statisch, sondern über zentrale oder verteilte Mechanismen kontrollierbar.

3 Geschäftsarchitektur

Die Geschäftsarchitektur konkretisiert die strategische Ausrichtung in Form von Wertströmen, Informationskonzepten und strategischen Fähigkeiten. Sie bildet die Brücke zwischen der Vision der Zielarchitektur und ihrer technischen Realisierung in der IT-Architektur.

3.1 Wertstrombetrachtung

Die in Kapitel 1.2 eingeführten drei Wertströme bilden den fachlichen Rahmen der Zielarchitektur. Sie beschreiben die Abfolge von Aktivitäten, die jeweils einem bestimmten Stakeholder einen konkreten Nutzen liefern.

3.1.1 Wertstrom „APIs von Basisdiensten in fachliche Anwendungen integrieren"

Auslösender Stakeholder dieses Wertstroms ist die betriebsverantwortliche Stelle einer fachlichen Anwendung beziehungsweise ihr Software-Lieferant. Das zentrale Wertversprechen besteht darin, alle benötigten APIs föderaler Basisdienste über einheitliche, weitgehend automatisierte Verfahren beantragen, die eigene Software registrieren und API-Clients an allen relevanten Basisdiensten anmelden zu können, ohne basisdienstspezifische Sonderverfahren.

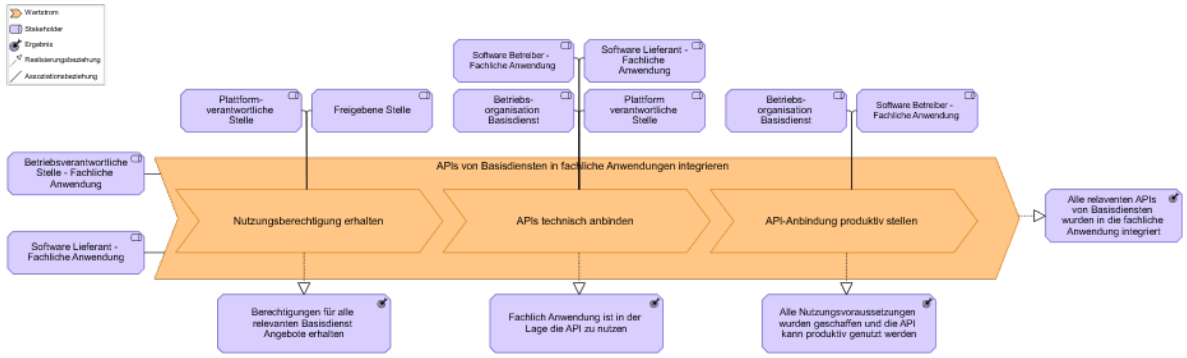

Abbildung 5: Wertstrom "APIs von Basisdiensten bereitstellen"

3.1.2 Wertstrom „APIs von Basisdiensten bereitstellen"

Auslösender Stakeholder ist die Plattformverantwortliche Stelle eines Basisdienstes. Das Wertversprechen liegt darin, die eigenen APIs auf standardisierte Weise im föderalen Kontext verfügbar zu machen, einschließlich der Beschreibung von Berechtigungsmodellen, der Veröffentlichung von Kataloginformationen sowie der durchsetzbaren Bindung an die föderalen Sicherheitsvorgaben. Im Ergebnis wird der Basisdienst für alle berechtigten Nutzer über einheitliche Mechanismen erreichbar.

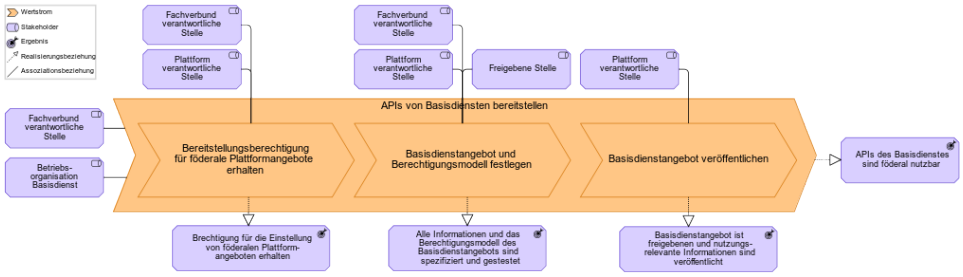

Abbildung 6: Wertstrom "APIs von Basisdiensten bereitstellen"

3.1.3 Wertstrom „Angebote von Basisdiensten nutzen"

Auslösender Stakeholder ist der Nutzer eines Basisdienstes, typischerweise vertreten durch die anfragende fachliche Anwendung beziehungsweise deren API-Client. Das Wertversprechen besteht im sicheren, nachvollziehbaren und standardisierten Zugriff auf den jeweiligen Basisdienst zur Laufzeit, unabhängig davon, welcher Basisdienst genutzt wird.

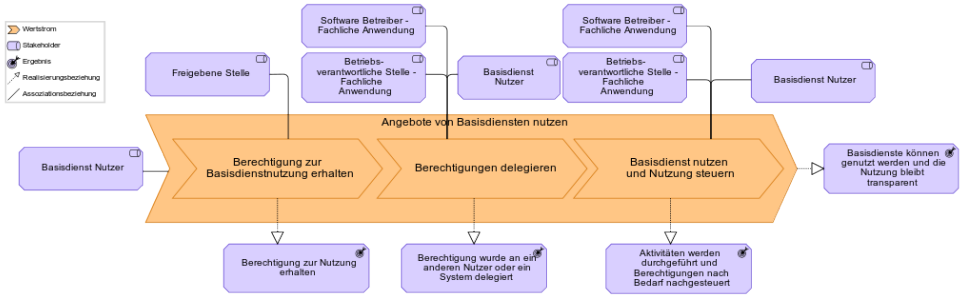

Abbildung 7: Wertstrom "Angebote von Basisdiensten nutzen"

3.1.4 Zentrale Beziehungen zwischen den Wertströmen

Die drei Wertströme greifen ineinander: Erst das Bereitstellen einer API durch den Basisdienst-Betreiber ermöglicht die Integration durch eine fachliche Anwendung, und erst die abgeschlossene Integration ermöglicht die Laufzeitnutzung. Die Wertströme teilen zentrale Informationsobjekte (insbesondere Software Statements, API-Beschreibungen und Berechtigungsregeln), deren Verwaltung in Kapitel 3.2 systematisch dargestellt wird.

3.2 Übersicht der Informationskonzepte

Die Zielarchitektur stützt sich auf eine Reihe zentraler fachlicher Informationskonzepte. Sie bilden den Begriffsrahmen, der allen Architektur- und Designentscheidungen zugrunde liegt.

3.2.1 Konzeptionelle Unterscheidung zwischen Berechtigungssteuerung auf API-Ebene und Anwendungsebene

Eine zentrale konzeptionelle Unterscheidung der Zielarchitektur betrifft die Ebenen der Berechtigungssteuerung: Auf der **API-Ebene** wird in einem groben Zuschnitt geregelt, welcher API-Client auf welche API überhaupt zugreifen darf. Auf der **Anwendungsebene** beziehungsweise **Ressourcenebene** wird feingranular bestimmt, welche konkreten Aktionen ein API-Client innerhalb der jeweiligen Anwendung ausführen darf, etwa auf einzelnen Datenfeldern oder Ressourcenpfaden.

Die Zielarchitektur konzentriert sich auf die API-Ebene. Die feingranulare Berechtigungssteuerung verbleibt in der Verantwortung der jeweiligen Basisdienste, da sie tiefes Verständnis der fachlichen Zusammenhänge der zu schützenden Anwendung voraussetzt, das auf übergreifender Konzeptebene nicht vorausgesetzt werden kann.

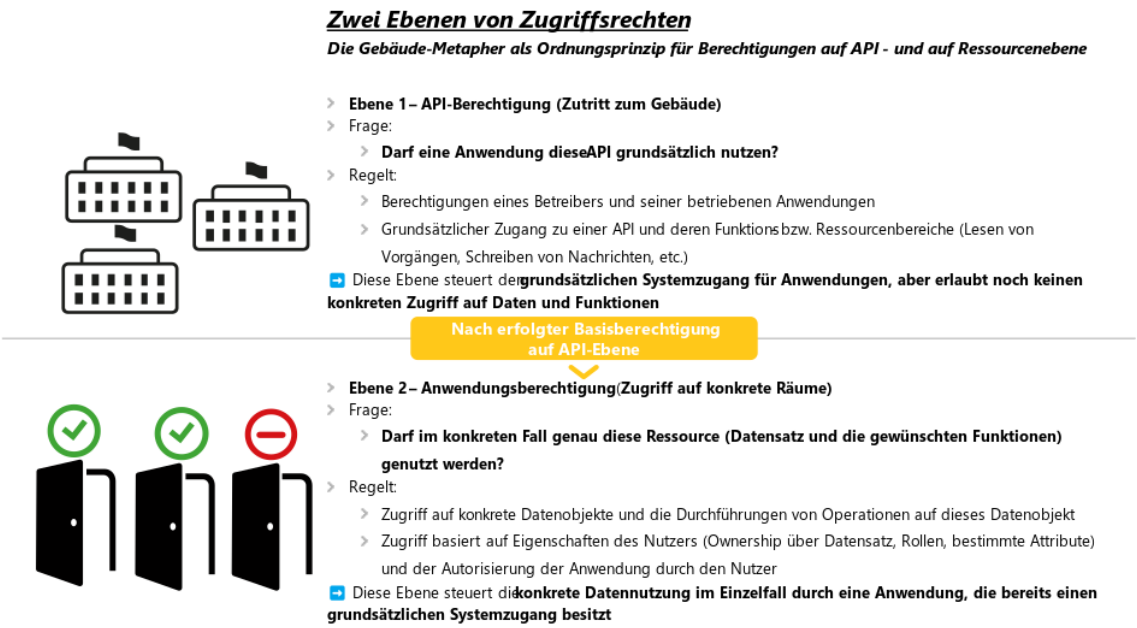

Abbildung 8: Zwei Ebenen der Berechtigungssteuerung

3.2.2 Information Concept Map

Die Information Concept Map gibt einen Überblick über die zentralen Informationskonzepte der Zielarchitektur und ihre Beziehungen zueinander.

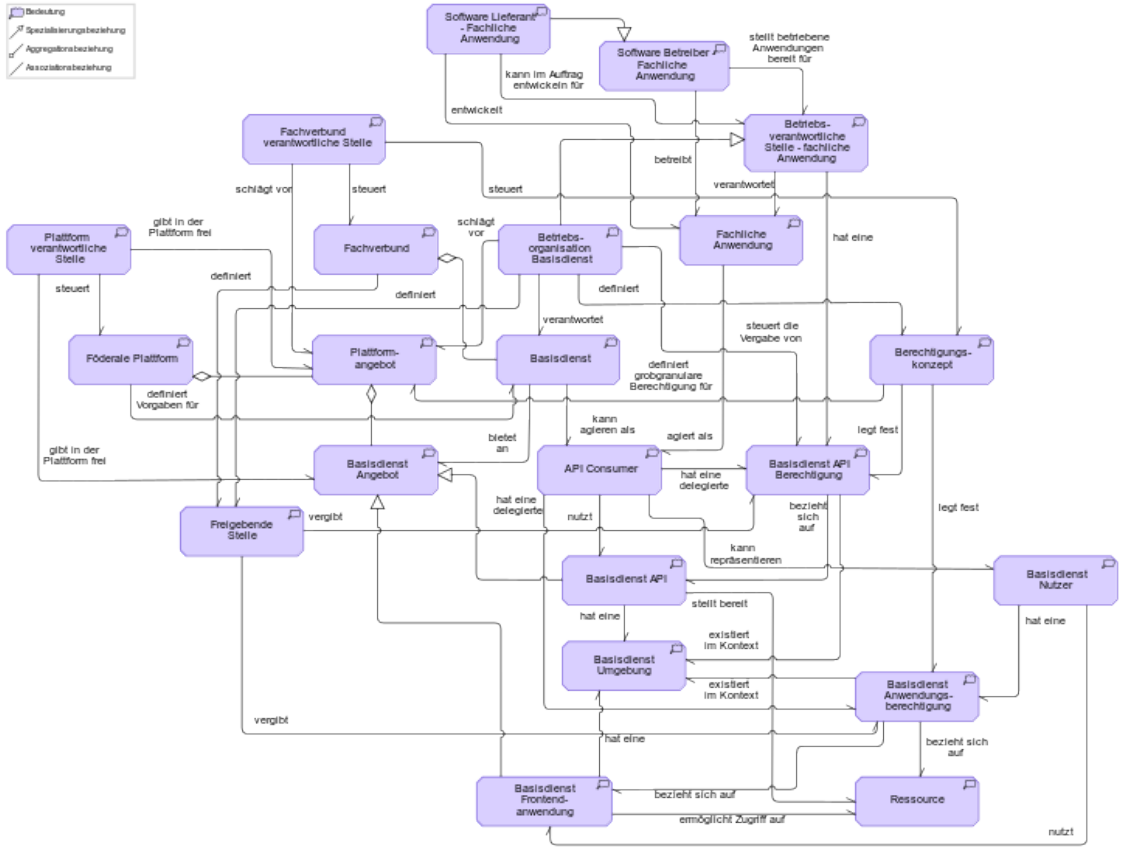

Abbildung 9: Information Concept Map

Die zugehörigen Informationskonzepte in Kurzbeschreibung:

Tabelle 2: Kurzbeschreibung der Informationskonzepte

Informationskonzept	Kurzbeschreibung
API-Consumer	Rolle einer Anwendung, die eine API nutzt oder integriert.
Basisdienst	System, das querschnittliche Funktionen für eine Vielzahl von Endnutzern (über Anwendungen) und/oder Systemen (über APIs) zentral für eine definierte Nutzergruppe bereitstellt.
Basisdienstangebot	Angebot eines Basisdienstes an andere Systeme oder Endnutzer; kann als API oder Anwendung ausgeprägt sein.
Basisdienst Anwendungsberechtigung	Berechtigung auf der Anwendungsebene eines Basisdienstes beim Zugriff durch Nutzer; umfasst grobgranulare und feingranulare Zugriffssteuerung auf konkrete Ressourcen.
Basisdienst-API	Maschinelle Schnittstelle, über die ein Basisdienst seine Funktionen anderen Anwendungen zur Nutzung bereitstellt.
Basisdienst-API-Berechtigung	Berechtigung auf API-Ebene eines Basisdienstes beim Zugriff durch Systeme; immer eine grobgranulare Zugriffssteuerung für den grundsätzlichen Zugriff auf eine API und ihre Bereiche.
Basisdienstumgebung	Betriebs- bzw. Bereitstellungsvariante einer API für spezifische Zwecke wie Produktivnutzung oder Testbetrieb bei der Implementierung der API-Anbindung.
Basisdienstnutzer	Person oder Organisation, die Zugriff auf die Ressourcen und Funktionen eines Basisdienstes hat.
Basisdienst-Frontendanwendung	Nutzeroberfläche eines Basisdienstes, entweder als eigenständige Anwendung oder als Interface zum direkten Zugriff auf die Basisdienst-API.
Berechtigungskonzept	Festlegung der Strukturen und Berechtigungslogik für den Zugriff auf Basisdienstangebote; kann einen Basisdienst oder einen kompletten Fachverbund umfassen und unterscheidet zwischen grobgranularer und feingranularer Berechtigungssteuerung.
Betriebsorganisation Basisdienst	Betriebsverantwortliche Stelle für einen Basisdienst, die alle Entscheidungen zu Betrieb, Weiterentwicklung und Ausgestaltung des Basisdienstes trifft.
Betriebsverantwortliche Stelle (Fachliche Anwendung)	Stelle, die den Betrieb einer Softwarelösung verantwortet und damit für alle Aspekte der Datenverarbeitung sowie die Einhaltung von Nutzungsbedingungen für die Einbindung von Basisdienst-APIs verantwortlich ist.
Fachliche Anwendung	Anwendung zur Unterstützung fachlicher Aufgaben oder Prozesse.

Fachverbund	Logisch abgegrenzter Verbund aus fachlichen, organisatorischen und technischen Komponenten, die auf Grundlage gemeinsamer Ziele, Regeln und Standards zusammenwirken; kann Fachverfahren, Register, Basisdienste, Infrastrukturen und Organisationen umfassen.
Fachverbundverantwortliche Stelle	Verantwortliche Stelle eines Fachverbunds; legt die Standards sowie organisatorische und technische Vorgaben fest, regelt das Angebot von Basisdiensten und die Zugangsregeln über alle Basisdienste des Verbunds hinweg.
Föderale Plattform	Gemeinsames föderales Angebot an abgestimmten Basisdiensten von Bund, Ländern und Kommunen.
Freigebende Stelle	Stelle, die mit der Erteilung von Berechtigungen für die Nutzung von Basisdienstangeboten betraut ist, sofern die Vergabe einen menschlichen Entscheidungsspielraum erfordert.
Plattformangebot	Angebotsklasse eines Basisdienstangebots für die föderale Plattform; kann mehrere funktional identische Basisdienstangebote gruppieren (z. B. Payment, Identitätsprovisionierung, Registerabruf) und auf einen gemeinsamen Standard oder Fachverbund referenzieren.
Plattformverantwortliche Stelle	Verantwortliche Stelle für den Zugang zur gemeinsamen Plattforminfrastruktur; steuert übergreifende Standards (API-Autorisierung, Berechtigungsverwaltung, Identitäten) und verantwortet die zentralen Infrastrukturen für die nahtlose Nutzung und Integration von Basisdiensten.
Ressource	Durch einen Resource Server (API-Provider) kontrolliertes, eindeutig identifizierbares Zielobjekt oder eine Zieloperation, dessen Zugriff durch Autorisierungsmechanismen gesteuert und das über eine Schnittstelle adressierbar ist.
Softwarebetreiber (Fachliche Anwendung)	Stelle, die im Auftrag einer betriebsverantwortlichen Stelle eine fachliche Anwendung betreibt.
Softwarelieferant (Fachliche Anwendung)	Stelle, die eine fachliche Anwendung als Standard- oder Individualsoftware entwickelt, im Auftrag Dritter oder als interne Leistung.

3.3 Ableitung der benötigten strategischen Fähigkeiten

Aus den Wertströmen und Informationskonzepten ergeben sich die strategischen Fähigkeiten (Capabilities), die eine föderale API-Autorisierungsinfrastruktur bereitstellen muss. Die folgende Übersicht zeigt die acht Top-Level-Fähigkeiten (sieben Kernfähigkeiten sowie eine unterstützende Fähigkeit). Jede Top-Level-Fähigkeit gliedert sich im Hauptkonzept in weitere Sub-Fähigkeiten, die hier nicht aufgeführt werden.

Tabelle 3: Strategische Fähigkeiten

Fähigkeit	Kategorie	Definition
API-Management	Kern	Die Fähigkeit, APIs als verwaltete Ressourcen zu beschreiben, bereitzustellen, ihren Lebenszyklus zu steuern und Zugriffsanfragen zur Laufzeit zu prüfen.
Workflow-Management	Kern	Die Fähigkeit, strukturierte Abläufe innerhalb der Plattform definieren, ausführen und über Aufgabenverwaltung steuern zu können.
Autorisierungsmanagement	Kern	Die Fähigkeit, Nutzern und Anwendungen auf Basis von Regeln Zugriffsrechte zu erteilen, zu prüfen und kontextabhängig durchzusetzen.
Identitätsmanagement	Kern	Die Fähigkeit, digitale Identitäten von Personen und Organisationen zu verwalten, zu authentifizieren, zu föderieren und attributbasiert zu beschreiben.
Berechtigungsmanagement	Kern	Die Fähigkeit, Regeln und Informationen zur Steuerung von Zugriffsberechtigungen zu verwalten und in der gesamten Infrastruktur konsistent verfügbar zu machen.
Logging und Monitoring	Kern	Die Fähigkeit, alle relevanten Ereignisse und Systemzustände zu erfassen, auszuwerten, Anomalien zu erkennen und auswertbare Berichte zu erzeugen.
Vertrauensinfrastruktur- und Zertifikatsmanagement	Kern	Die Fähigkeit, die kryptographische Vertrauensbasis der Infrastruktur durch Ausstellung von Vertrauensnachweisen, Verwaltung von Vertrauensbeziehungen und Schlüsseln zu schaffen.
Frontendbereitstellung	Unterstützend	Die Fähigkeit, Nutzern digitale Oberflächen für die Interaktion mit der Plattform bereitzustellen und in andere Frontends zu integrieren.

4 IT-Architektur

Die IT-Architektur überführt die Geschäftsarchitektur in eine konkrete technische Lösung. Sie beschreibt die Rahmenbedingungen, die Systemlandschaft, die technische Informationsarchitektur sowie die übergreifenden Prozesse und Use Cases, die durch die Infrastruktur unterstützt werden.

4.1 Rahmenbedingungen für die Konzeption der IT-Architektur

4.1.1 Architekturvorgaben

Die Konzeption der IT-Architektur folgt den in Kapitel 2 dargestellten projektspezifischen Architekturzielen und -prinzipien. Sie ist zudem an die Sicherheitsvorgaben der Föderalen API-Autorisierungsinfrastruktur (auf Basis FAPI 2.0) gebunden, die ein verbindliches Sicherheitsniveau für alle APIs der öffentlichen Verwaltung definieren.

4.1.2 Betrachtete Best Practices und Industriestandards

Die Zielarchitektur baut auf etablierten offenen Industriestandards und Best Practices auf. Zu den zentralen referenzierten Standards zählen:

- **OAuth 2.1** und **OpenID Connect** für die Identitäts- und Autorisierungsschicht,
- **FAPI 2.0** (Financial-grade API) der OpenID Foundation als Sicherheitsprofil,
- **Dynamic Client Registration** (RFC 7591/7592) für die automatisierte Software-Registrierung,
- **Software Statement Assertions (SSA)** als kryptographisch signierte Selbstauskunft von Softwareregistrierungen,
- **AuthZEN** der OpenID Foundation als Standardprotokoll zwischen Policy Enforcement Point und Policy Decision Point,
- **Shared Signals Framework (SSF)** der OpenID Foundation für den Austausch sicherheitsrelevanter Ereignissignale,
- **Security Event Tokens (SET)** nach RFC 8417,
- **DPoP** (Demonstrating Proof of Possession) für Sender-Constraining,
- **SCIM** (RFC 7644) für die standardisierte Bereitstellung von Identitäts- und Organisationsdaten,
- **Merkle-Tree-basierte Transparency Logs** als Stand der Technik für revisionssichere Protokollierung.

4.1.3 Dokumentation von Architekturentscheidungen

Wesentliche Architekturentscheidungen sind in Form von Architecture Decision Records (ADRs) dokumentiert und nachvollziehbar im Hauptkonzept hinterlegt. Die folgende Übersicht fasst die ADRs zusammen.

Tabelle 4: Architekturentscheidungen

ADR-Nr.	Titel	Kurzbeschreibung des Entscheidungsgegenstandes
ADR-001	Zu verwendender Autorisierungsstandard	Klärt den Autorisierungsstandard. Entschieden für OAuth 2.0 mit qualifiziertem Profil auf Basis von FAPI 2.0: weit verbreitet, formal analysiert, durch zertifizierte Implementierungen breit unterstützt.
ADR-002	Client-Authentifizierung	Klärt die Client-Authentifizierungsmethode am Authorization Server. FAPI 2.0 lässt mTLS und `private_key_jwt` zu. Entschieden für `private_key_jwt`: vollständig auf Applikationsebene umsetzbar, keine Abstimmungen mit Netzwerkbetriebsabteilungen erforderlich.
ADR-003	Sender-Constraining	Klärt den Mechanismus zur Bindung des Access Tokens an den rechtmäßigen Empfänger. Entschieden für DPoP: keine zusätzliche PKI-Infrastruktur erforderlich, breite Clientlandschaften unterstützt.
ADR-004	Absicherung und Vertrauenswürdigkeit von Public Keys	Klärt die Vertrauenswürdigkeit der Public Keys von API-Clients. Entschieden, den Public Key in der Software Statement Assertion zu verankern: kryptographisch signiert, auditierbar, ohne zusätzliche PKI-Systeme.
ADR-005	Prüfung der API-Autorisierung: Zentraler vs. Dezentraler OAuth-Server	Klärt die Verortung der Autorisierungsprüfung. Entschieden, die Wahl dem jeweiligen Fachverbund zu überlassen, da die Anforderungen stark zwischen Plattformangeboten variieren.
ADR-006	Absicherung der Schnittstellen zwischen Komponenten der zentralen Infrastruktur	Klärt die Schnittstellenabsicherung in der zentralen Infrastruktur. Entschieden für mTLS mit begrenzter interner PKI: robust, auditierbar, ohne Token-Verwaltungsaufwand.
ADR-007	Absicherung von Schnittstellen zwischen einheitlich bereitgestellten Komponenten der dezentralen Infrastruktur	Klärt die Absicherung dezentraler Schnittstellen (PDP, PIP). Entschieden, denselben Standard wie für externe API-Clients zu verwenden: kein zweiter Sicherheitsstack.

ADR-008	Berechtigungsarchitektur	Klärt die Aufteilung der Berechtigungsarchitektur zwischen Plattform- und Fachverbundebene. Entschieden für eine zweistufige Architektur: grobgranulare Zugangsentscheidungen zentral, feingranulare in Verantwortung der Fachverbünde.
ADR-009	Berechtigungsmodell für zentrale Regeladministration	Klärt das Berechtigungsmodell für die Verwaltung zentraler Berechtigungsregeln. Entschieden für ein ReBAC-Modell: bildet organisatorische Beziehungsstrukturen ab, ermöglicht kontrollierte Delegation.
ADR-010	Berechtigungsmodell für Plattformberechtigungen	Klärt das Berechtigungsmodell für API-Clients. Entschieden für ein regelbasiertes, attributgesteuertes Modell mit verteilter PDP-Nutzung: zentral gepflegte Attribute, dezentrale Entscheidungen ohne Laufzeitabhängigkeit zur Zentrale.
ADR-011	Externalisierung von Berechtigungen und Policy Decision Points	Klärt, ob Entscheidungen an externen PDP ausgelagert werden. Entschieden, die Nutzung des einheitlich bereitgestellten PDP verbindlich vorzuschreiben, sofern technisch möglich.
ADR-012	Prüfung der Gültigkeit von grobgranularen Berechtigungen	Klärt die Laufzeitprüfung grobgranularer Berechtigungen. Entschieden für die Kombination aus signiertem Token und PDP: lokal prüfbare Tokens plus ergänzende PDP-Entscheidungen.
ADR-013	Prüfung der Gültigkeit von feingranularen Berechtigungen	Klärt die Prüfung feingranularer Berechtigungen. Wahl des technischen Verfahrens beim Fachverbund; Plattform stellt einen wiederverwendbaren PDP bereit, ohne verbindliche Vorgaben.
ADR-014	Ownership von grobgranularen Berechtigungen	Klärt die Ownership grobgranularer Berechtigungen. Entschieden, dass die Organisation Eigentümer ist, da nur Organisationen im Verwaltungsumfeld dauerhaft identifizierbar.
ADR-015	System für Identifizierung von natürlichen Personen für das FöPD	Klärt die Identifizierung natürlicher Personen. Entschieden für die BundID: etabliertes staatliches Identifikationssystem, eIDAS-Anbindung bereits vorhanden.
ADR-016	System für Identifizierung von juristischen Personen für das FöPD	Klärt die Identifizierung juristischer Personen. Entschieden für Mein Unternehmenskonto (MUK): verwaltungsnaher, breit anschlussfähiger Identitätsanker.
ADR-017	Risikoadressierung von unzulässigen Veränderungen von grobgranularen Berechtigungen	Klärt die Adressierung des Risikos unzulässiger Änderungen. Entschieden für ein Transparency Log: manipulationssichere Protokollierung, dezentral prüfbar.

ADR-018	Vorgaben für dezentrale Komponenten der Basisdienste	Klärt den Umfang verbindlicher Architekturvorgaben für dezentrale Komponenten. Entschieden für einen gezielten Ansatz: Vorgaben nur für plattformkritische und sicherheitsrelevante Komponenten.
ADR-019	Scope der zentralen Nutzerautorisierung	Klärt den initialen Scope der zentralen Nutzerautorisierung. Entschieden, zunächst auf Verwaltungskunden zu begrenzen, da bestehende staatliche Identitätslösungen direkt anbindbar.
ADR-020	Logging von personenbezogenen Daten im Transparency Log	Klärt, ob personenbezogene Daten zentral protokolliert werden. Entschieden, das zentrale Log vollständig personen- und organisationsfrei zu halten. Personenbezogene Nachvollziehbarkeit ausschließlich in lokalen Audit-Logs.
ADR-021	Transparency Log	Klärt die revisionssichere Dokumentation sicherheitsrelevanter Änderungen. Entschieden für ein kryptographisch verkettetes Append-Only Transparency Log auf Basis einer etablierten Transparenzplattform.
ADR-022	Security Events: Format und Schnittstelle	Klärt Format und Schnittstelle für den organisationsübergreifenden Austausch sicherheitsrelevanter Ereignisse. Entschieden für das Shared Signals Framework (SSF) mit signierten Security Event Tokens (SET).
ADR-023	Verteilung von Policies und Attributen an verteilte PDPs	Klärt die Verteilung zentral verwalteter Policies und Attribute. Entschieden für ein selektives Polling-Modell mit lokalem Caching und optionalem Long-Polling: skalierbar, topologieunabhängig, „last known good state" ohne Inbound-Abhängigkeiten.

4.2 Übersicht der Systemlandschaft

Die folgende Abbildung zeigt die Systemlandschaft der föderalen API-Autorisierungsinfrastruktur im Überblick.

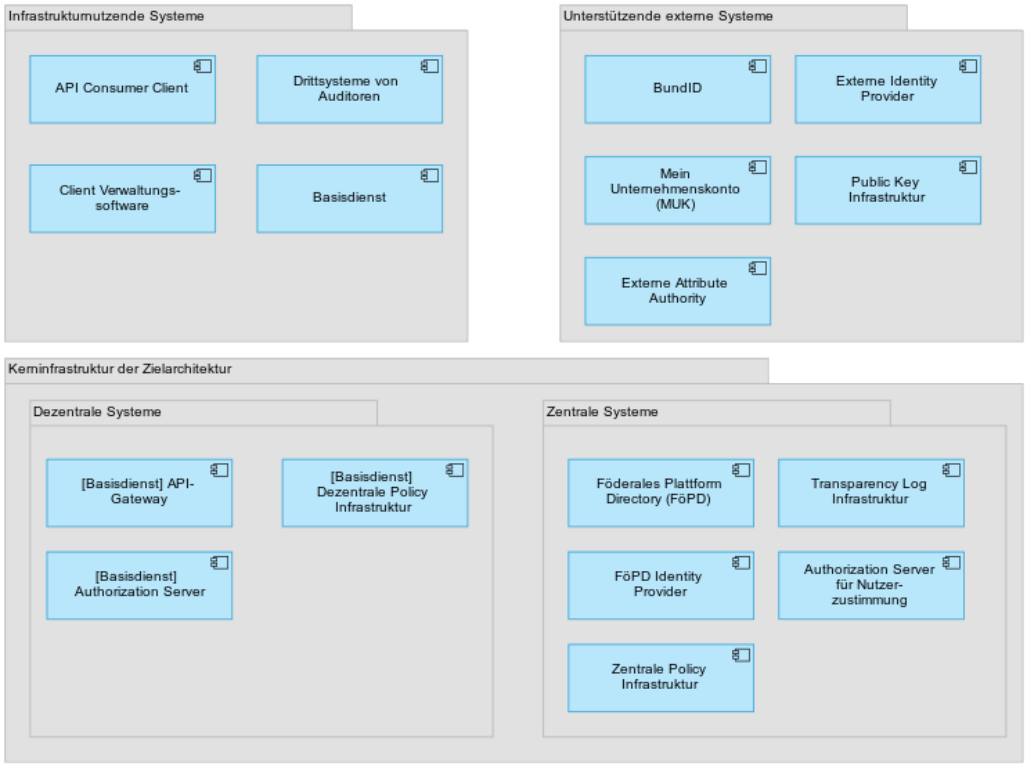

Abbildung 10: Übersicht der Systemlandschaft

4.2.1 Beschreibung der Systeme

Die Systeme der Zielarchitektur lassen sich in vier Kategorien einteilen.

Infrastrukturnutzende Systeme sind keine Bestandteile der Kerninfrastruktur, interagieren aber regelmäßig mit ihr.

Tabelle 5: Infrastrukturnutzende Systeme

System	Kurzbeschreibung
Basisdienst	Föderaler Basisdienst, der seine APIs über die Infrastruktur bereitstellt und die Vorgaben der Zielarchitektur einhält.
API Consumer Client	Software-Client, der im Auftrag einer fachlichen Anwendung APIs eines Basisdienstes nutzt.

Externe Client-Verwaltungssoftware	Software, die im Auftrag einer Organisation die Registrierung und Verwaltung von API-Clients beim FöPD durchführt.
Drittsysteme von Auditoren	Externe Prüfsysteme, die über die lesenden Schnittstellen der Infrastruktur Audit-Aufgaben wahrnehmen.

Unterstützende externe Systeme stellen Identitäts- oder Vertrauensgrundlagen bereit, die von der Infrastruktur genutzt werden.

Tabelle 6: Unterstützende externe Systeme

System	Kurzbeschreibung
BundID	Staatliches System zur Identifizierung natürlicher Personen, eIDAS-konform.
Mein Unternehmenskonto (MUK)	Staatliches System zur Identifizierung juristischer Personen.
Externe Identity Provider	Identity Provider von Behörden oder sonstigen juristischen Personen, die als föderierte Identitätsquellen integriert werden können.
Externe Attribute Authority	Externe Quelle für autoritative Attributinformationen (z. B. Behördenverzeichnisse, FIM-Datenfelder).
Public Key Infrastruktur	Bestehende föderale PKI (insbesondere V-PKI) zur Bereitstellung von Zertifikaten.

Zentrale Systeme der Kerninfrastruktur werden zentral betrieben und stellen die plattformweiten Funktionen der Infrastruktur bereit.

Tabelle 7: Zentrale Systeme der Kerninfrastruktur

System	Kurzbeschreibung
Föderales Plattform Directory (FöPD)	Zentrale Verwaltungs- und Registrierungsplattform für Organisationen, Software, APIs, Plattformangebote, Attribute und Berechtigungsregeln; autoritative Quelle (Single Source of Truth) der Plattform.
FöPD Identity Provider	Zentraler IdP für Nutzer der FöPD-Verwaltungsoberfläche, Föderierung mit BundID, MUK und externen IdPs.
Authorization Server für Nutzerzustimmung	Zentraler Authorization Server für Authorization-Code-Flows mit Nutzerinteraktion, stellt API-unspezifische Tokens mit Nutzerautorisierung aus.
Zentrale Policy-Infrastruktur	Verwaltung, Validierung und Verteilung der Berechtigungsregeln (Policy Administration Point, Policy Information Point, Policy Store / Policy Retrieval Point).

Transparency Log Infrastruktur	Append-only, kryptographisch verifizierbare Protokollierung sicherheitsrelevanter Ereignisse der zentralen Infrastruktur.
SSF-Monitoring-Infrastruktur	Zentrale Aggregations-, Korrelations- und Risikobewertungsschicht auf Basis des Shared Signals Framework.

Dezentrale Systeme der Kerninfrastruktur sind funktionaler Bestandteil der Plattform, werden aber in der Betriebsverantwortung der jeweiligen Basisdienste betrieben.

Tabelle 8: Dezentrale Systeme der Kerninfrastruktur

System	Kurzbeschreibung
[Basisdienst] Authorization Server	Lokaler Authorization Server eines Basisdienstes; stellt Access Tokens für API-Clients aus, agiert als Policy Enforcement Point bei der Token-Ausstellung.
[Basisdienst] Dezentrale Policy-Infrastruktur	Lokaler Policy Decision Point eines Basisdienstes mit lokalem Attribute Store; einzige Entscheidungsinstanz im Berechtigungsmodell.
[Basisdienst] API-Gateway	API-Gateway des Basisdienstes; agiert als Policy Enforcement Point zur Laufzeit-Validierung von Tokens.
[Basisdienst] SSF-Transmitter-Adapter	Adapter zur Übermittlung sicherheits- und administrativ relevanter Ereignisse des Basisdienstes an die zentrale SSF-Monitoring-Infrastruktur.

4.3 Technische Informationsarchitektur

4.3.1 Übersicht der zentralen Datenobjekte

Die zentralen Datenobjekte der Zielarchitektur konkretisieren die fachlichen Informationskonzepte aus Kapitel 3.2 in einer technisch implementierbaren Form.

Tabelle 9: Zentrale Datenobjekte

Datenobjekt	Kurzbeschreibung
Organisation	Juristische Person, die im FöPD als betriebsverantwortliche, nutzende, betreibende oder fachverbundverantwortliche Stelle registriert ist.
Natürliche Person	Physische Person, die im Kontext einer Organisation im FöPD agiert, etwa als Super-Admin oder delegierter Nutzer.
FöPD-Account	Konto einer Organisation oder natürlichen Person im Föderalen Plattform Directory, das Zugang zu den Funktionen des FöPD gewährt und die zugewiesenen Nutzungsattribute enthält.
FöPD-Zertifikat	Vertrauensanker für Software Statement Assertions, die vom FöPD herausgegeben werden.
Policy	Regelwerk für die Zugriffssteuerung auf API-Ressourcen.
Policy Entscheidungsinformationen	Zusammenstellung der für die Auswertung einer Policy benötigten Datensätze, etwa Attribute einer Person, Organisation oder Software sowie entscheidungsrelevante Kontextinformationen.
Policy Entscheidung	Zugriffsentscheidung auf Basis einer Policy und der Policy Entscheidungsinformationen.
Risikowert	Aggregierter Risikowert zu einem Subjekt der Infrastruktur, abgeleitet aus den mit diesem Subjekt verbundenen Sicherheitsereignissen.

Kataloginformationen von Plattformangeboten	Metadaten eines Plattformangebots eines Basisdienstes, die im FöPD veröffentlicht werden und die verfügbaren APIs, Berechtigungsmodelle und Nutzungsbedingungen beschreiben.
API-Consumer Software	Softwareprodukt einer betriebsverantwortlichen Stelle, das APIs von Basisdiensten nutzt und im FöPD registriert ist; Grundlage für die Ausstellung eines Software Statements.
API-Client	Technische Instanz einer API-Consumer Software, die für den Abruf von Access Tokens beim OAuth Server registriert ist.
Transparency Log	Fälschungssicheres, Merkle-Tree-basiertes Protokoll aller sicherheitsrelevanten Systemaktivitäten, das die Nachvollziehbarkeit und Auditierbarkeit der Plattform gewährleistet.
Client Authentifizierungsmittel	Kryptographisches Mittel, mit dem sich ein API-Client gegenüber dem OAuth Server authentifiziert.
Access Token	Zur Laufzeit ausgestelltes, sender-constrained Token, das einem API-Client den autorisierten Zugriff auf eine API-Ressource für eine begrenzte Zeit nachweist.
Nutzer Authentifizierungsnachweis	Nachweis der erfolgreichen Authentifizierung einer natürlichen Person gegenüber einem Identitätsprovider (BundID oder MUK).
Software Statement Assertion	Nachweis der Identität einer API-Consumer Software, ausgestellt auf Basis einer registrierten Software im FöPD und signiert durch das FöPD.
Nutzer Identitätsnachweis	Nachweis der Identität einer natürlichen Person, der nach erfolgreicher Authentifizierung ausgestellt wird und Identitätsattribute enthält.
API-Ressource	Durch einen Basisdienst bereitgestellter API-Endpunkt, für dessen Nutzung eine gültige Berechtigung und ein entsprechender Access Token benötigt werden.

4.3.2 Informationsverantwortungsmatrix

Die Verantwortung für die zentralen Datenobjekte ist im Hauptkonzept in Form einer detaillierten Informationsverantwortungsmatrix dargestellt. Sie weist jedem Datenobjekt einen Owner (System of Record) sowie verarbeitende und konsumierende Systeme zu und klärt geteilte Verantwortlichkeiten. Auf eine Wiedergabe dieser Matrix wird in der Kurzfassung verzichtet; sie ist im Hauptkonzept verfügbar.

4.3.3 Zentrale übergreifende Informationsflüsse

Die folgende Abbildung zeigt die übergreifenden Informationsflüsse in der Gesamtinfrastruktur auf konzeptioneller Ebene. Sie macht die Beziehungen zwischen FöPD, Basisdiensten, Identity Providern und Drittsystemen sichtbar. Detaillierte Datenflussdiagramme für die Kontexte API-Registrierung, API-Aufruf und Token-Austausch finden sich im Hauptkonzept.

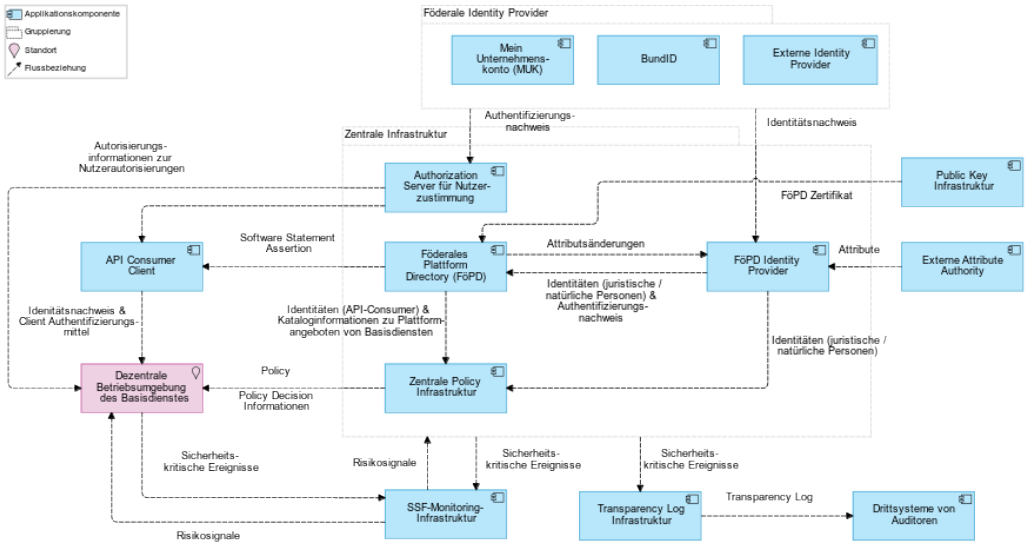

Abbildung 11: High Level Informationsflüsse in der Gesamtstruktur

4.4 Prozessübersicht und Darstellung der IT-Prozessunterstützung

Die Zielarchitektur unterstützt eine Reihe übergreifender Prozesse, die sich in Kernprozesse und Supportprozesse gliedern. Die folgenden Abbildungen geben einen Überblick auf die unterstützten Prozesse und den High-Level-Ablauf der Kernprozesse.

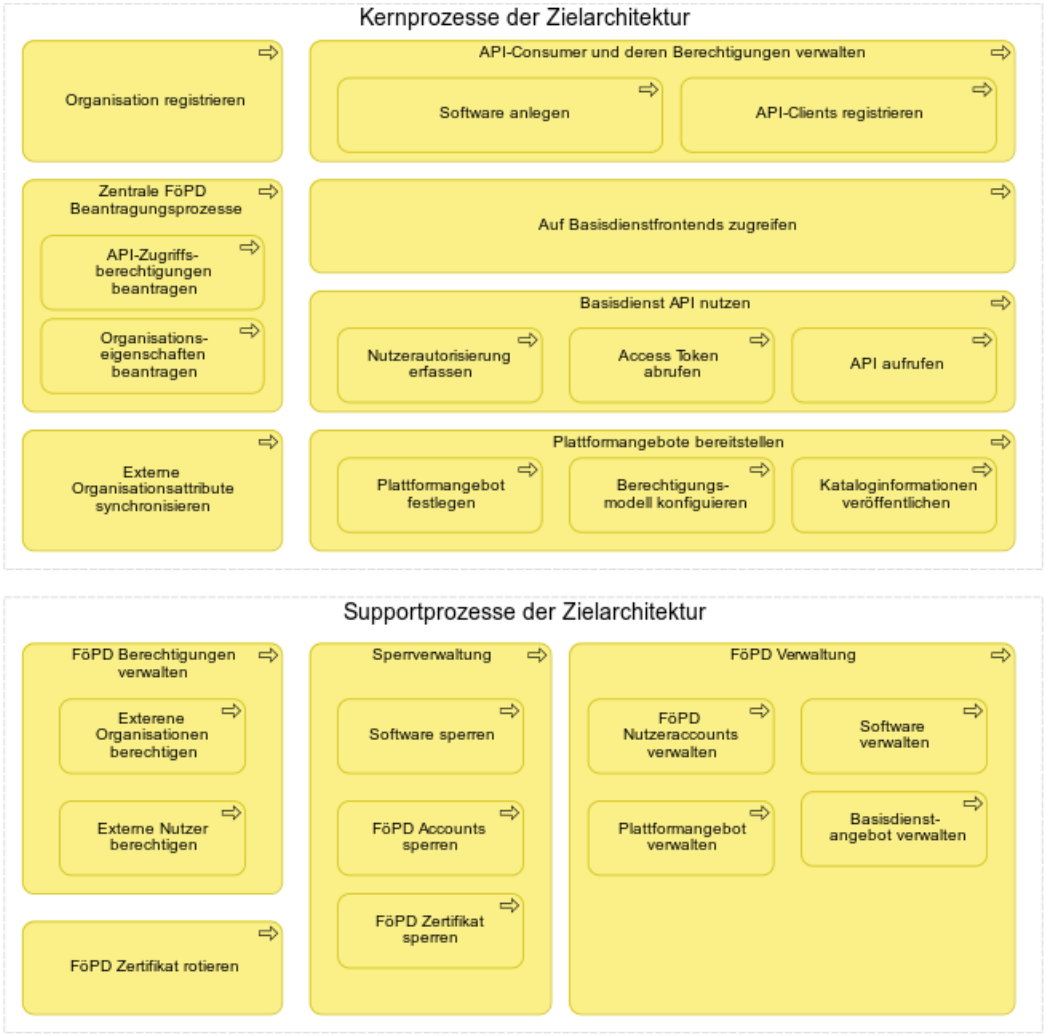

Abbildung 12: Landkarte der unterstützten Prozesse

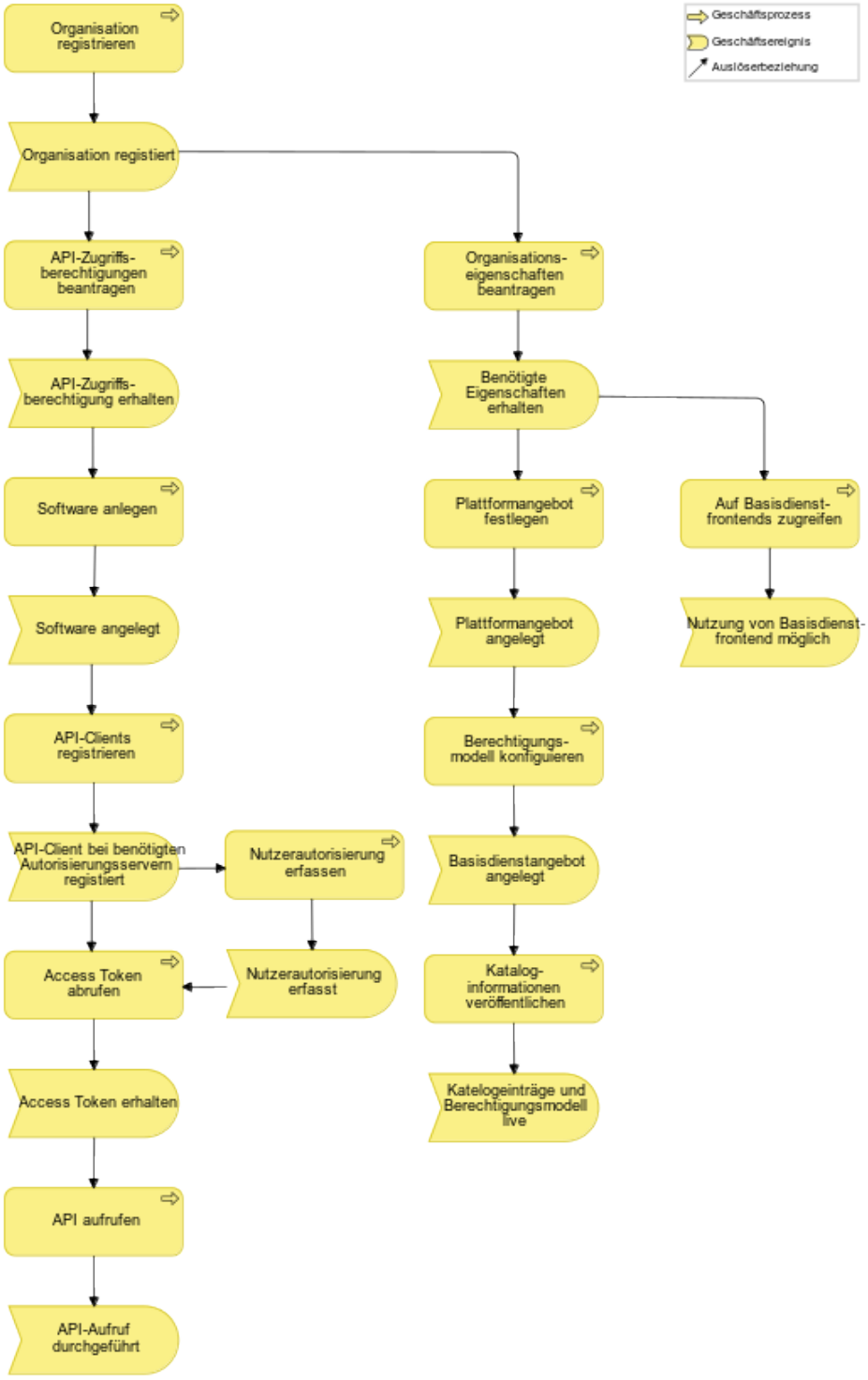

Abbildung 13: High Level Prozessablauf der Kernprozesse

Die detaillierte Beschreibung der einzelnen Prozesse (von „Organisation registrieren" über „API-Clients registrieren" bis „API aufrufen") erfolgt im Hauptkonzept. Sie umfasst pro Prozess Use-Case-Listen, Informationsflussdiagramme und Sequenzdiagramme. In dieser Kurzfassung wird auf die Wiedergabe dieser Prozessdetails verzichtet, da sie für die strategische Befassung nicht erforderlich sind.

Ergänzend zu den Kernprozessen bestehen Supportprozesse, die regelmäßige Pflege- und Verwaltungsaufgaben (z. B. Pflege des Plattformkatalogs, Pflege des Attributkatalogs, Verwaltung von Föderierungen) abdecken. Auch deren Beschreibung erfolgt im Hauptkonzept.

4.5 Übersicht der umzusetzenden Use Cases

Aus den Prozessen ergibt sich eine Reihe konkreter Use Cases, die durch die Systeme der Kerninfrastruktur umgesetzt werden müssen. Das Hauptkonzept enthält eine vollständige Use-Case-Übersicht, die jeden Use Case einem umsetzenden System, einem unterstützten Prozess, einer unterstützten Fähigkeit sowie den verwendeten Standardprotokollen und Schnittstellen zuordnet. In der Kurzfassung wird auf die Wiedergabe dieser Liste verzichtet; sie ist im Hauptkonzept verfügbar.

5 Querschnittliche Themen

Die querschnittlichen Themen behandeln Aspekte, die sich nicht einer einzelnen Komponente zuordnen lassen, sondern die Gesamtarchitektur durchziehen: das Berechtigungskonzept, das übergreifende Monitoring, die revisionssichere Protokollierung, Betriebsfragen, die Auswahl von Standardlösungen sowie die Behandlung von Middleware als bevollmächtigtem API-Consumer.

5.1 Berechtigungskonzept

5.1.1 Zielsetzung und Abgrenzung

Die Steuerung des Zugriffs auf APIs in einer heterogenen, behördenübergreifenden Infrastruktur erfordert ein flexibles Berechtigungskonzept. Die Breite der adressierten Nutzerschaft (sowohl auf Seiten der API-Anbieter als auch der API-Nutzer) geht mit einer Vielzahl möglicher Anwendungsszenarien einher, die sich weder vollständig antizipieren noch auf ein einheitliches Fachmodell reduzieren lassen.

Eine zentrale Aussage des Berechtigungskonzepts ist die Zwei-Ebenen-Logik: Die grobgranulare Zugangssteuerung („darf dieser Client diese API überhaupt nutzen?“) wird zentral standardisiert und einheitlich für alle Basisdienste umgesetzt. Die feingranulare Berechtigungssteuerung („welche konkreten Aktionen darf dieser Client innerhalb der Anwendung ausführen?“) verbleibt in der Verantwortung der jeweiligen Basisdienste. Sie setzt tiefes Verständnis der fachlichen Zusammenhänge der zu schützenden Anwendung voraus, das auf übergreifender Konzeptebene nicht vorausgesetzt werden kann. Die Zielarchitektur setzt damit bewusst keine technischen Vorgaben, die in die interne Verarbeitung und Berechtigungslogik einzelner Anwendungen eingreifen.

Für die Modellierung des Berechtigungssystems sind vier Leitlinien prägend. **Dezentralität:** API-Betreiber verwalten ihre Berechtigungsregeln fachlich eigenverantwortlich. **Flexibilität:** Das Modell ist fachdomänenunabhängig und unterstützt vielfältige Nutzungsszenarien. **Nachvollziehbarkeit:** Berechtigungsentscheidungen sind transparent und auf leicht verständliche Regeln zurückführbar. **Zentrales Vertrauen:** Das Föderale Plattform Directory (FöPD) stellt für die Berechtigungsverwaltung relevante Attributinformationen über Software-Instanzen als Single Source of Truth bereit.

Die Granularität der Berechtigungsprüfung bestimmt dabei den Zeitpunkt der Prüfung: Die grobgranulare Prüfung erfolgt einmalig am Authorization Server des Basisdienstes, wenn ein API-Client ein Access Token anfordert. Die feingranulare Prüfung erfolgt innerhalb der

Anwendung beziehungsweise des API-Dienstes selbst, bei jeder eingehenden, gültig authentifizierten Anfrage.

5.1.2 Berechtigungsmodell

Das Berechtigungsmodell ist regelbasiert und attributgetrieben. Es kombiniert Attribute-Based Access Control (ABAC) mit einem Policy-basierten Ansatz (PBAC). Anstatt einzelne Clients explizit zu berechtigen, definieren API-Betreiber Policies, die den Zugriff anhand von Attributen der anfragenden Software regeln.
Die Eckpfeiler des Modells sind:

- **Policy:** strukturiertes Regelwerk mit Effect (PERMIT oder DENY), Bedingungen (Conditions, UND-verknüpft), Scopes (nur bei PERMIT) und Exceptions (nur bei DENY);
- **API-Ressource:** verknüpft die Policy mit dem konkreten API-Endpunkt;
- **Conditions:** atomare, prüfbare Kriterien, die Eigenschaften des Subjekts oder Kontextvariablen abgleichen;
- **Scopes:** definieren die Menge möglicher Berechtigungen, die einem Client für die Nutzung einer API gewährt werden, und überbrücken die Lücke zwischen grobgranularer Zugangsentscheidung und feingranularer Anwendungslogik.

Drei zentrale Auswertungsprinzipien prägen das Modell:

- **Implicit Deny:** Trifft keine Policy zu, ist das Standardergebnis DENY. Berechtigungen müssen vollständig und explizit durch PERMIT-Policies erteilt werden.
- **DENY-Dominanz:** Eine zutreffende DENY-Policy überstimmt beliebig viele zutreffende PERMIT-Policies. Die Reihenfolge der Policies hat keinen Einfluss auf das Ergebnis.
- **Scope-Hoheit beim API-Betreiber:** Policies können ausschließlich Scopes referenzieren, die das API zuvor registriert hat. Eine Policy kann den Berechtigungsrahmen einer API nicht überschreiten.

Die in Berechtigungsregeln referenzierbaren Attribute werden in einem zentralen Attributkatalog des FöPD verbindlich definiert. Der Attributkatalog ist ein normativer, zentral verwalteter Bestandteil der Plattform; konkrete Attributzuordnungen zu Software-Instanzen und APIs werden über die Attribute-Verwaltung des FöPD bereitgestellt.

5.1.3 Systemkomponenten

Die Berechtigungsarchitektur unterscheidet die etablierten Komponentenrollen PAP, PIP, PRP, PDP und PEP mit klar getrennten Zuständigkeiten zwischen zentraler und dezentraler Schicht.

Zentrale Komponenten: Der **Policy Administration Point (PAP)** ist die zentrale Verwaltungsschnittstelle für Berechtigungsregeln und stellt die einzige autorisierte Schreibschnittstelle gegenüber dem Policy Store dar. Der **Policy Information Point (PIP)** ist die Informationsversorgungskomponente. Er bezieht Attributdaten aus dem FöPD und stellt sie den dezentralen PDPs zur Verfügung. Der **Policy Store / Policy Retrieval Point (PRP)** ist das zentrale Persistenzmedium für Policies und steuert deren selektive Verteilung an die zuständigen dezentralen PDPs. Diese funktionale Trennung ermöglicht eine zusätzliche Härtung der Systemarchitektur und reduziert die Angriffsfläche.

Dezentrale Komponenten: Der **Authorization Server (AS) des Basisdienstes** ist der lokale Vertrauensanker. Er fungiert als Policy Enforcement Point: Er stellt Access Tokens für Clients nur dann aus, wenn der lokale Policy Decision Point dies aufgrund einer Policy-Regel entscheidet. Das **API-Gateway des Basisdienstes** ist ebenfalls Policy Enforcement Point. Es prüft bei jeder Anfrage die Gültigkeit eines bereits ausgestellten Access Tokens. Der **Policy Decision Point (PDP) des Basisdienstes** ist die einzige Komponente, die Berechtigungsentscheidungen trifft. Er ist konzeptuell vom AS und API-Gateway vollständig getrennt und unterhält keine Online-Verbindung zur zentralen Plattform. Er empfängt die für seine Auswertungen erforderlichen Policies und Attributdaten vom zentralen Policy Store und PIP und verarbeitet sie lokal.

Die Kommunikation zwischen Policy Enforcement Points und Policy Decision Points erfolgt über das **AuthZEN-Protokoll** der OpenID Foundation als standardisierte REST-API. Durch die lokale Datenhaltung im PDP wird eine effiziente Regelauswertung ermöglicht und Single-Point-of-Failure-Risiken werden vermieden. Bei Ausfall der zentralen Komponenten bleibt der dezentrale PDP mit dem letzten konsistenten Datenstand entscheidungsfähig.

5.2 Übergreifendes Monitoring und Risikobewertung

Die föderale API-Autorisierungsinfrastruktur verteilt sicherheitsrelevante Entscheidungen und Ereignisse strukturbedingt über eine Vielzahl dezentral betriebener Komponenten. Authorization Server, API-Gateways und Policy Decision Points liegen in der Betriebsverantwortung der jeweiligen Basisdienste. Keine einzelne Komponente verfügt damit über einen vollständigen Sicherheitsblick auf das Gesamtsystem. Ziel ist eine föderale Signalschicht, die sicherheitsrelevante Ereignisse erkennt, korreliert und automatisierte Reaktionen ermöglicht.

Diese Funktion wird durch das **Shared Signals Framework (SSF)** der OpenID Foundation realisiert. SSF ist ein Standard für den sicherheitsgesicherten Austausch sicherheitsrelevanter Ereignissignale zwischen Systemkomponenten. Es unterscheidet zwischen Transmittern (Ereignisquellen) und Receivern (Ereignisempfängern), die über typisierte Streams verbunden sind. Ereignisse werden als Security Event Tokens (SETs) gemäß RFC 8417 übertragen, also als signierte JSON Web Tokens mit standardisierten Subject-Identifikatoren.

5.2.1 Grundarchitektur

Die SSF-Überwachungsinfrastruktur gliedert sich in drei Schichten.

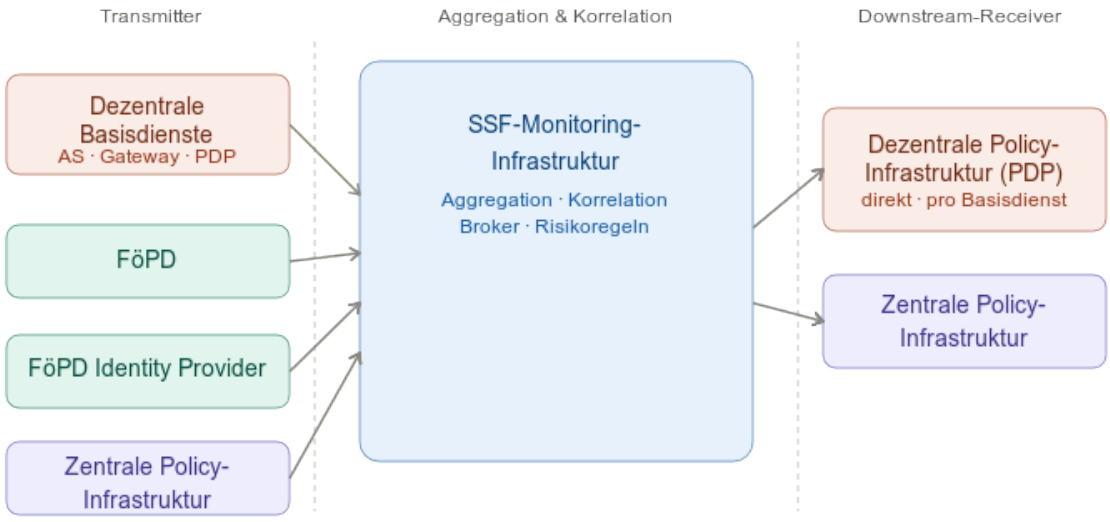

Abbildung 14: Schichten der SSF-Architektur

Schicht 1, Ereignisquellen (Transmitter): Alle zentralen und dezentralen Kerninfrastrukturkomponenten agieren als SSF-Transmitter. Die dezentralen Basisdienst-Komponenten übermitteln ihre Ereignisse über einen jeweils lokalen SSF-Transmitter-Adapter. Erfasst werden insbesondere Token-Ausstellungen und -Ablehnungen, Policy-Entscheidungen, abgelehnte API-Anfragen, Anomaliemuster, Registrierungsänderungen, Authentifizierungsereignisse und Föderierungsänderungen.

Schicht 2, Aggregation und Korrelation: Die zentrale SSF-Monitoring-Infrastruktur empfängt alle Streams und korreliert Ereignisse über Subjekte (API-Consumer-Clients, Organisationen) und Basisdienste hinweg. Sie bewertet Risikomuster und leitet aggregierte Risikosignale ab.

Schicht 3, Reaktion (Downstream-Receiver): Auf Basis der aggregierten Risikosignale werden parallele automatische Reaktionen ausgelöst, etwa die unmittelbare DENY-Aktivierung in dezentralen Policy-Infrastrukturen, die Aktivierung übergreifender DENY-Policies in der

zentralen Policy-Infrastruktur, administrative Workflows im FöPD oder die Übermittlung an externe Sicherheitssysteme.
Die zentralen Infrastrukturkomponenten schreiben ihre sicherheits- und administrativ relevanten Ereignisse parallel in das Transparency Log und über den SSF-Transmitter-Adapter in die SSF-Monitoring-Infrastruktur. Diese Parallelität ist architektonisch bewusst gewählt. Sie folgt der Trennung zwischen Beweissicherung (Kapitel 5.3) und operativer Reaktion.

5.2.2 Eventprofilierung

Das SSF definiert mit CAEP und RISC zwei Standardprofile, die primär auf natürliche Personen ausgerichtet sind. Im Kontext der föderalen API-Autorisierungsinfrastruktur stehen jedoch maschinelle Subjekte (registrierte Software, API-Consumer-Clients) und organisatorische Subjekte (Betreiber-Organisationen) im Vordergrund. Eine Spezifikation eines föderalen SSF-Eventprofils mit den entsprechenden Subject-Identifier-Konventionen und Event-Semantiken ist erforderlich. Diese und weitere offene Punkte sind in Kapitel7 zusammengeführt.

5.3 Revisionssichere Protokollierung und Auditierung

Kapitel 5.2 beschreibt mit der SSF-basierten Monitoring-Infrastruktur die Reaktionsfähigkeit des Gesamtsystems. Das vorliegende Kapitel richtet den Blick auf eine komplementäre, konzeptionell eigenständige Anforderung: die Beweissicherung. Operative Reaktionsfähigkeit und revisionssichere Beweissicherung sind zwei unterschiedliche Qualitäten, die unterschiedliche infrastrukturelle Antworten erfordern. Die SSF-Monitoring-Infrastruktur beantwortet die Frage „Was muss jetzt operativ reagieren?" Sie ist ein Streaming-System, ihre Signale sind aggregierte Urteile. Das Transparency Log beantwortet die Frage „Was ist in der zentralen Infrastruktur nachweislich passiert?" Es ist append-only, kryptographisch verifizierbar und unabhängig vom Vertrauen in den Betreiber prüfbar.
Diese Trennung ist im föderalen Kontext besonders bedeutsam: An der föderalen API-Autorisierungsinfrastruktur sind viele Betreiber mit unterschiedlichem Vertrauensniveau beteiligt. Ein Audit-System, das auf dem Vertrauen in den Betreiber des Logs basiert, genügt den Anforderungen einer föderalen Vertrauensarchitektur nicht.

5.3.1 Beweissicherung der zentralen Infrastruktur

Das Transparency Log erfasst ausschließlich Ereignisse der zentralen Infrastrukturkomponenten, nicht der dezentralen Basisdienst-Komponenten. Diese Scoping-Entscheidung folgt der Vertrauensarchitektur der Gesamtinfrastruktur: Die dezentralen Basisdienste sind Konsumenten der zentralen Infrastruktur. Sie vertrauen auf die Integrität der Daten, die sie vom FöPD und

der zentralen Policy-Infrastruktur erhalten, insbesondere auf Software Statements, Attributinformationen und Berechtigungsregeln. Das Transparency Log sichert genau diesen Vertrauensanker ab. Ob und in welchem Umfang Basisdienste eine eigene lokale Protokollierung betreiben, liegt in deren Betriebsverantwortung und ist nicht Gegenstand dieses Konzepts.

5.3.2 Eigenschaften des Transparency Logs

Das Transparency Log basiert auf einem kryptographisch verifizierbaren Merkle-Tree. Vier wesentliche Eigenschaften prägen es:

- **Append-only:** Einträge können nur hinzugefügt, nicht geändert oder gelöscht werden. Dies gilt auch gegenüber dem Betreiber des Logs.
- **Kryptographische Verifikation:** Jeder Zustand des Logs wird durch einen signierten Checkpoint repräsentiert. Jeder Eintrag kann durch einen Inclusion Proof als Teil des Logs nachgewiesen werden, die Konsistenz zwischen zwei Zuständen durch einen Consistency Proof.
- **Unabhängige Auditierbarkeit:** Externe Prüfinstanzen können das Log vollständig lesen, seine Integrität eigenständig verifizieren und Einträge prüfen. Die Lesbarkeit ist strukturell von der schreibenden Infrastruktur getrennt.
- **Kein Widerrufsrecht:** Da Einträge nicht gelöscht werden können, sind auch irrtümlich oder missbräuchlich vorgenommene administrative Akte dauerhaft nachweis-bar. Dies ist eine bewusste Designentscheidung zugunsten der Nachvollziehbarkeit.

5.3.3 Protokollierte Ereignisklassen

Drei Klassen von Ereignissen werden im Transparency Log erfasst:

- **Administrative Ereignisse des FöPD:** Ausstellung und Revokation von Software Statement Assertions, Sperrungen von Clients und Organisationen, Entzug und Wiederherstellung von API-Zugriffsberechtigungen, Registrierungsänderungen.
- **Berechtigungshistorie der zentralen Policy-Infrastruktur:** Erstellung, Änderung und Löschung von Policies, Replikationsstatus und ausgelieferte Policy-Versionen je PDP-Instanz.
- **Ereignisse des FöPD Identity Providers:** Änderungen an Organisationsattributen und deren Vertrauensstufen, Föderierungsänderungen externer IdP-Verbindungen.

Ausdrücklich nicht protokolliert werden Ereignisse der dezentralen Basisdienst-Komponenten sowie aggregierte Signale und abgeleitete Urteile der SSF-Monitoring-Infrastruktur.

5.3.4 Zugang für externe Auditoren

Das Transparency Log ist über eine lesende API für externe Prüfinstanzen zugänglich. Prüfinstanzen können das gesamte Log lesen und lokal verifizieren, Inclusion Proofs für einzelne Einträge anfordern, Consistency Proofs zwischen Log-Zuständen prüfen und die Signatur des Checkpoints gegen den öffentlichen Schlüssel des Log-Betreibers verifizieren. Dieser Zugang ist lesend und erfordert keine privilegierten Rechte.

5.3.5 Lösungsauswahl Tessera

Die Vorfestlegung der Implementierungsgrundlage erfolgt auf **Tessera** (transparency-dev/tessera). Die kryptographischen Anforderungen (Inclusion Proofs, Consistency Proofs, signierte Checkpoints) schließen sowohl Eigenentwicklungen als auch konventionelle Audit-Log-Lösungen strukturell aus. Tessera ist nach aktuellem Kenntnisstand die einzige bekannte Open-Source-Lösung, die einen allgemein verwendbaren, kryptographisch verifizierbaren Transparency Log mit beliebiger Log-Personality bereitstellt, aktiv weiterentwickelt wird und einen klaren Produktionspfad aufweist. Die Vorfestlegung erfolgt unter dem Vorbehalt eines konkreten Erprobungsbedarfs, da die bisherige Produktionserfahrung mit Tessera sich auf andere Ökosysteme (insbesondere Certificate Transparency und Sigstore) konzentriert.

5.4 Betriebsfragen

5.4.1 Umgang mit zentralen Systemen

Die zentrale Infrastruktur der föderalen API-Autorisierungsinfrastruktur wird unter der operativen Steuerung der Plattformverantwortlichen Stelle betrieben. Diese ist einer föderalen Steuerungsebene rechenschaftspflichtig, die als Auftraggeber und strategische Steuerungsinstanz agiert.

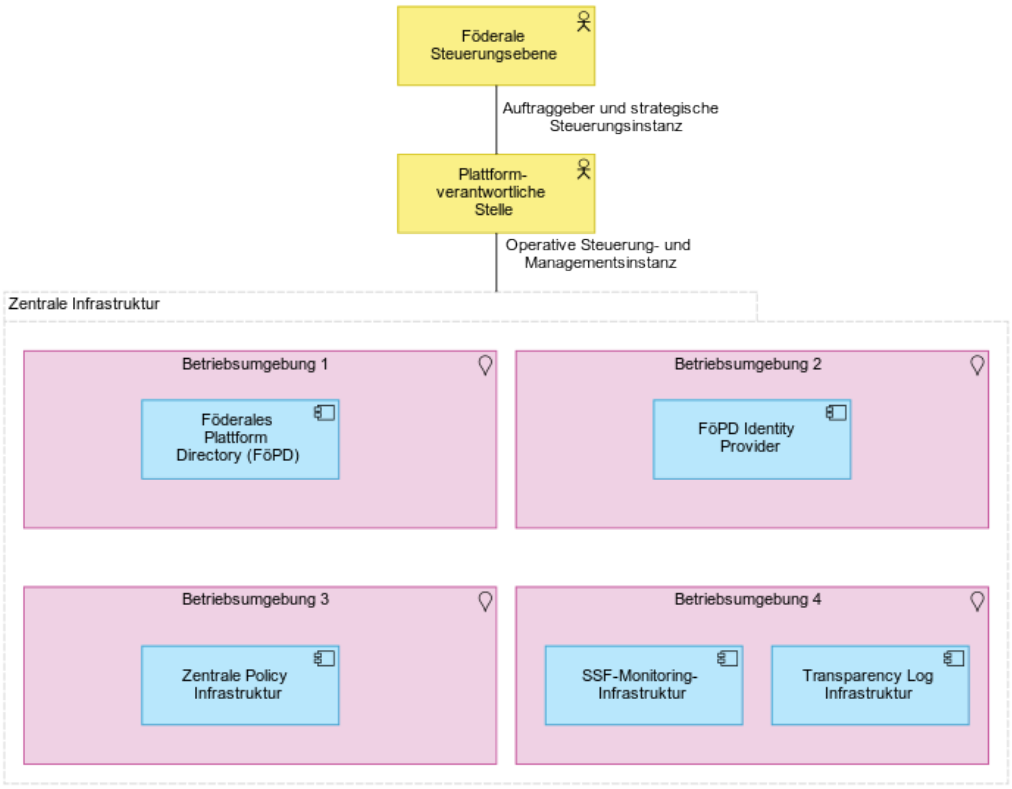

Abbildung 15: Verantwortlichkeiten und Strukturierung der Betriebsumgebungen der zentralen Infrastruktur

Die zentralen Systeme der Kerninfrastruktur werden in vier eigenständige Betriebsumgebungen gegliedert, die jeweils einen klar abgegrenzten Verantwortungsbereich adressieren.

Tabelle 10: Betriebsumgebungen der zentralen Infrastruktur

Betriebsumgebung	System(e)	Verantwortungsbereich
Betriebsumgebung 1	Föderales Plattform Directory (FöPD)	Verwaltung und Koordination: Registrierung von Organisationen, Software und API-Clients, Katalogverwaltung, Workflow-Steuerung sowie Ausstellung von Vertrauensnachweisen
Betriebsumgebung 2	FöPD Identity Provider	Identität und Authentifizierung: Verwaltung von Nutzeraccounts, Föderierung mit externen IdPs, Authentifizierung von Nutzern der Plattform

Betriebsumgebung 3	Zentrale Policy-Infrastruktur (PAP, PIP, Policy Store/PRP)	Autorisierungsregeln und Entscheidungsgrundlage: Verwaltung, Validierung und Distribution der Policies und Attributdaten an die dezentralen PDPs
Betriebsumgebung 4	SSF-Monitoring-Infrastruktur und Transparency Log Infrastruktur	Beobachtung und Nachweisführung: Operative Echtzeit-Risikobewertung sowie revisionssichere Protokollierung

Die Aufteilung in vier separate Betriebsumgebungen folgt drei architektonischen Leitgedanken: Erstens **gegenseitige Absicherung durch strukturelle Unabhängigkeit:** Die vier Betriebsumgebungen bilden ein System wechselseitiger Kontrolle, in dem alle Systeme ihre sicherheits- und administrativ relevanten Ereignisse sowohl an das Transparency Log als auch an die SSF-Monitoring-Infrastruktur melden. Zweitens **unabhängige Entwicklungsfähigkeit:** Die Cluster orientieren sich an vier orthogonalen Verantwortungsbereichen (Verwaltung, Identität, Autorisierung, Beobachtung), die jeweils eigenständige fachliche und technische Domänen darstellen, sodass jede Betriebsumgebung unabhängig weiterentwickelt werden kann. Drittens **kontraktbasierte Zusammenarbeit und Austauschbarkeit:** Die Architektur erzwingt eine präzise Definition der Schnittstellen und Datenkontrakte zwischen den Betriebsumgebungen, was die Kopplung auf das fachlich Notwendige reduziert.

5.4.2 Umgang mit dezentralen Systemen

Dezentrale Systeme der Kerninfrastruktur übernehmen zentrale Aufgaben der föderalen API-Autorisierungsinfrastruktur, liegen aber in der Betriebsverantwortung der jeweiligen Basisdienst-Betriebsorganisationen. Für die Bereitstellung dieser Systeme unterscheidet die Zielarchitektur zwei Modelle: verbindliche Bereitstellung und optionale Bereitstellung. In beiden Fällen wird eine zentral beschaffte, betreute und vorkonfigurierte Lösung bereitgestellt; bei optionalen Systemen können Basisdienst-Betreiber alternativ eigene Lösungen einsetzen, sofern diese die verbindlichen Schnittstellen einhalten.

Tabelle 11: Bereitstellungsmodelle der dezentralen Systeme

System	Bereitstellungsmodell
[Basisdienst] Authorization Server	Verbindlich
[Basisdienst] Dezentrale Policy-Infrastruktur (PDP, lokaler Attribute Store)	Verbindlich

[Basisdienst] API-Gateway	Optional
[Basisdienst] SSF-Transmitter-Adapter	Optional

Die Modellwahl folgt jeweils einer fachlich-technischen Begründung:

- **Authorization Server (verbindlich):** Der AS ist keine rein interne Komponente des Basisdienstes, sondern die direkte technische Schnittstelle zum gesamten API-Ökosystem. API Consumer Clients interagieren mit ihm bei der Client-Registrierung (DCR mit Software Statement Assertion), bei der Token-Anfrage und bei der Authentifizierung. Sein Verhalten wirkt damit unmittelbar auf alle Teilnehmer des föderalen Ökosystems. Die Sicherheitsvorgaben auf Basis FAPI 2.0 (Client-Authentifizierung, Sender-Constraining, Token-Binding) entwickeln sich im Laufe der Zeit weiter, sei es durch neue Standardversionen, Betriebserfahrung oder geänderte Bedrohungslagen. Eine einheitliche, zentral bereitgestellte Lösung ermöglicht es, solche Änderungen schnell, konsistent und zuverlässig in allen Basisdiensten durchzuziehen. Zusätzlich stellt die zentrale Bereitstellung sicher, dass die SSA-basierte dynamische Client-Registrierung als Fundament des föderalen Registrierungsmodells bei allen Basisdiensten interoperabel funktioniert.
- **Dezentrale Policy-Infrastruktur (verbindlich):** Zwei Kernfunktionen erfordern eine einheitliche Lösung. Erstens nutzt die Replikation zwischen zentraler Policy-Infrastruktur und dezentralem PDP einen infrastrukturspezifischen Kanal, der kein offener Standard ist. Über diesen Kanal werden Policies, Attributdaten und sicher-heitskritische Änderungen wie Client-Sperrungen an die dezentralen Instanzen ausgeliefert. Würde jeder Basisdienst die Replikation individuell implementieren, wäre das Risiko von Inkonsistenzen mit unmittelbaren Auswirkungen auf Berechtigungsentscheidungen zu hoch. Zweitens muss die Policy-Evaluierungslogik ökosystemweit semantisch identisch ausgewertet werden. Die Wahl der Regelsprache (Cedar, Open Policy Agent, DMN o. ä.) muss daher einheitlich sein. Eine zentral bereitgestellte Lösung erlaubt zudem die Weiterentwicklung oder den Austausch des Regelwerks, ohne dass jeder Basisdienst-Betreiber seine eigene PDP-Implementierung anpassen muss. Die AuthZEN-Schnittstelle ist zwar standardisiert und würde unterschiedliche PDP-Implementierungen erlauben; die Gründe für die verbindliche Bereitstellung liegen jedoch nicht in der externen Schnittstelle, sondern in der internen Datenhaltung und Regelkonsistenz.

- **API-Gateway (optional):** Im Gegensatz zum Authorization Server kommuniziert das API-Gateway ausschließlich über standardisierte Schnittstellen mit anderen Infrastrukturkomponenten: AuthZEN mit dem PDP, Token Introspection mit dem lokalen AS. Die Weiterleitung des API-Aufrufs an den Basisdienst ist eine basisdienstinterne Angelegenheit. Eine ökosystemweite Außenwirkung, die eine einheitliche Lösung erzwingen würde, gibt es nicht. Hinzu kommt, dass viele Basisdienste bereits über etablierte Lösungen mit vergleichbaren Funktionen verfügen, etwa das Sichere Anschlusskit (SAK) im NOOTS-Kontext, Standard-Gateways in Rechenzentrumsumgebungen oder Ingress Controller in Kubernetes-Umgebungen. Eine Vorschrift, diese bestehenden Lösungen durch ein einheitliches Gateway zu ersetzen, wäre weder verhältnismäßig noch praxisgerecht. Verbindlich bleibt die Einhaltung der Sicherheitsvorgaben (DPoP-Validierung, Token-Prüfung) und die korrekte Durchführung der AuthZEN-Abfrage; freigestellt ist allein die Wahl des Gateway-Produkts.
- **SSF-Transmitter-Adapter (optional):** In der Praxis ist der Adapter in den meisten Fällen kein eigenständiges Deployment-Thema. Bei Einsatz der verbindlich bereitgestellten Komponenten (AS, dezentrale Policy-Infrastruktur) sowie des optional bereitgestellten API-Gateways ist die SSF-Transmitter-Funktionalität bereits in diesen Komponenten integriert. Eine eigenständige Adapter-Komponente wird nur dann relevant, wenn ein Basisdienst eigene Gateway-Implementierungen einsetzt und zusätzlich basisdiensteigene Ereignisse, etwa fachliche Sicherheitsereignisse, an die SSF-Monitoring-Infrastruktur übermitteln muss. Verbindlich vorgegeben sind in allen Fällen das föderale SSF-Eventprofil (Struktur und Semantik der Security Event Tokens) und die Übermittlungsschnittstelle; freigestellt ist allein die technische Umsetzung (integrierter Adapter oder eigene Implementierung). Da das Shared Signals Framework noch ein relativ neuer Standard ist und Implementierungserfahrung in der Praxis begrenzt bleibt, kommt der zentral bereitgestellten Lösung darüber hinaus eine wichtige Bedeutung als Beispielimplementierung zu.

5.5 Standardlösungen und Nachnutzungsmöglichkeiten

Die Zielarchitektur untersucht für jedes identifizierte System der Kerninfrastruktur, ob primär eine Standardsoftwarelösung oder primär eine Individuallösung eingesetzt werden sollte. „Primär" bedeutet, dass auch eine Individuallösung Standardkomponenten für Teilfunktionen einsetzen kann (z. B. Workflow-Engines), und umgekehrt eine Standardsoftware-Lösung in Einzelfällen durch maßgeschneiderte Konfiguration oder Erweiterung ergänzt wird. Wo Standardsoftwarelösungen in Frage kommen und geeignete Open-Source-Lösungen existieren, werden diese gemäß Prinzip P-009 bevorzugt betrachtet. Eine verbindliche Festlegung auf ein

bestimmtes Produkt erfolgt (mit Ausnahme der Transparency Log Infrastruktur, vgl. Kapitel 5.3) nicht im Rahmen dieses Konzepts, sondern in einer nach-gelagerten Detailkonzeption.

5.5.1 Übersicht

Tabelle 12: Lösungsansätze zur Infrastruktur

System	Lösungsansatz	Wesentliche Begründung
Föderales Plattform Directory (FöPD)	Individuallösung mit Standardkomponenten	Fachlich hochspezifisch; OAuth-Server-Komponenten und Workflowsysteme als Standardkomponenten einsetzbar; Nachnutzung von IT-PLR-Produkten prüfen
FöPD Identity Provider	Standardsoftware	Etablierter Funktionsumfang in Open-Source-Lösungen verfügbar
Authorization Server für Nutzerzustimmung	Standardsoftware	Gleiche Anforderungen wie FöPD IdP und Basisdienst-AS
Zentrale Policy-Infrastruktur	Individuallösung mit Standardkomponenten	Fachspezifische Administration und Propagierung; Policy Engine als Standardkomponente
SSF-Monitoring-Infrastruktur	Individuallösung mit Standardkomponenten	Fachspezifische Integration und Eventprofil; CEP-Engine als Standardkomponente
Transparency Log Infrastruktur	Standardsoftware	Lösungsauswahl bereits erfolgt (siehe Kapitel 5.3)
[Basisdienst] Authorization Server	Standardsoftware	Etablierter Funktionsumfang in Open-Source-Lösungen verfügbar
[Basisdienst] Dezentrale Policy-Infrastruktur	Individuallösung mit Standardkomponenten	Fachspezifische Replikationslogik; Policy Engine als Standardkomponente
[Basisdienst] API-Gateway	Standardsoftware	Etablierter Funktionsumfang in Open-Source-Lösungen verfügbar
[Basisdienst] SSF-Transmitter-Adapter	Individuallösung mit Open-Source-Bibliotheken	Standard noch jung; Open-Source-Bibliotheken als Grundlage verfügbar

5.5.2 Wesentliche Empfehlungen

Aus der Bewertung leiten sich folgende Empfehlungen ab:

- **OAuth-/OIDC-Stack** (FöPD Identity Provider, zentraler Authorization Server für Nutzerzustimmung, Basisdienst-Authorization Server): gleiche Standardsoftware-Lösung für alle drei Rollen empfohlen, um Betriebs- und Know-how-Konsistenz zu erreichen. Bewertete Kandidaten sind Janssen (Linux Foundation) und Keycloak (CNCF). Janssen wird wegen des nativen SSA-Supports in der Dynamic Client Registration präferiert; Keycloak wird gemäß Prinzip P-009 als dokumentierter Fallback geführt.
- **Transparency Log Infrastruktur:** Tessera (Verweis auf Kapitel 5.3).
- **API-Gateway des Basisdienstes:** mehrere Open-Source-Kandidaten in Bewertung (Apache APISIX, Tyk, KrakenD, Gravitee). Die Auswahl erfolgt in der nachgelagerten Detailkonzeption.
- **FöPD:** Individuallösung mit Standardkomponenten. Als präferierter Nachnutzungskandidat wird das Self-Service-Portal von FIT-Connect betrachtet (Prinzip P-014). OAuth-Server-Komponenten (z. B. aus dem Janssen-Stack) können zur SSA-Generierung nachgenutzt werden; Workflow-Management-Systeme können die Antrags- und Freigabeprozesse unterstützen.
- **Zentrale und dezentrale Policy-Infrastruktur:** Individuallösung; für die Policy-Evaluierungslogik wird eine Standardkomponente eingesetzt. In Bewertung sind Cedar (AWS), Open Policy Agent (CNCF) und DMN-Engines (z. B. Camunda DMN, Drools). Für zentrale und dezentrale Policy-Infrastruktur soll dieselbe Engine eingesetzt werden, um eine semantisch identische Auswertung sicherzustellen.
- **SSF-Monitoring-Infrastruktur und SSF-Transmitter-Adapter:** Individuallösung mit Open-Source-Bibliotheken; die Eigenentwicklung wird als Open Source nachnutzbar bereitgestellt. Wegen der noch jungen Reife des SSF-Standards kommt der bereitgestellten Implementierung zugleich eine Bedeutung als Beispielimplementierung zu.

5.6 Middleware als bevollmächtigter API-Consumer

Middleware-Systeme verbinden Fachverfahren, Dokumentenmanagementsysteme und weitere Anwendungen mit zentralen Diensten und sind in der behördlichen IT-Praxis weit verbreitet. Die Zielarchitektur muss daher mit dieser Konstellation kompatibel sein, ohne ihre eigenen Sicherheits- und Nachvollziehbarkeitsmerkmale zu unterlaufen.

Im Grundprinzip behandelt die Zielarchitektur Middleware-Systeme als reguläre API-Consumer ohne privilegierte Stellung: Eine Middleware tritt gegenüber der Infrastruktur als registrierter

Software-Client mit eigenem Software Statement und eigenem Schlüsselmaterial auf, getrennt pro vertretener Fachanwendung.
Ein dynamischer Identitätswechsel zur Laufzeit, bei dem eine Middleware mit einem einzigen Software Statement flexibel verschiedene Fachverfahrenskontexte annähme, ist in diesem Konzept nicht vorgesehen. Er würde die Zurechenbarkeit von Zugriffen und das Zero-Trust-Prinzip unterlaufen.
Das Onboarding erfolgt über den allgemeinen Software-Statement-Registrierungsprozess des FöPD und wird von der jeweiligen Fachverantwortlichen Stelle genehmigt. Der Integrationsaufwand für bestehende Middleware-Systeme ist überschaubar, sofern diese bereits mandantenfähig sind und die Schlüsselpaar-basierte Authentisierung sowie die Dynamic Client Registration nach RFC 7591 unterstützen.

6 Transitionsbetrachtung

Die Einführung der föderalen API-Autorisierungsinfrastruktur betrifft eine Vielzahl bestehender und in Entwicklung befindlicher föderaler Basisdienste. Dieses Kapitel gibt einen Überblick über die identifizierten betroffenen Basisdienste und benennt mögliche Strategien für die schrittweise Anbindung.

6.1 Übersicht föderaler Basisdienste

6.1.1 Definition und Vorgehen

Als föderaler Basisdienst gelten Dienste, die drei Hartkriterien erfüllen. Erstens **Querschnittlichkeit:** Der Dienst wird domänenübergreifend für viele Verwaltungsleistungen genutzt, nicht für eine einzelne Fachdomäne. Zweitens **föderale Mitnutzung** durch mehrere Verwaltungsebenen (Bund, Länder, Kommunen). Drittens **etablierte oder koordinierende Trägerschaft** mit klaren Governance-Strukturen.

Eine konsolidierte autoritative Liste föderaler Basisdienste existiert nach Kenntnis der Autoren nicht; die folgende Übersicht wurde auf Basis öffentlich zugänglicher Quellen erstellt und stellt einen Versuch dar, die in Bund und Ländern bekannten und in Entwicklung befindlichen Basisdienste zusammenzufassen.

6.1.2 Angrenzende Domänen mit Anschlusspotenzial

Über den Kreis der hier betrachteten föderalen Basisdienste hinaus existieren angrenzende Domänen mit eigener Governance und etablierten Infrastrukturen, die zwar nicht im engeren Sinne als föderale Basisdienste der Verwaltungsdigitalisierung gelten, aber Anschlusspotenzial an die Zielarchitektur aufweisen. Im Bereich der Sozialversicherung ist insbesondere die Informationstechnische Servicestelle der Gesetzlichen Krankenversicherung (ITSG) mit zentralen Verfahren des elektronischen Datenaustauschs zu nennen, ergänzt durch das SV-Meldeportal. Im Bereich der Justiz koordiniert die Bund-Länder-Kommission für Informationstechnik in der Justiz (BLK) etablierte Komponenten wie das EGVP und den Verzeichnisdienst SAFE.

6.1.3 Übersicht der föderalen Basisdienste

Tabelle 13: Föderale Basisdienste

Basisdienste	Beschreibung
Basisregister für Unternehmen	Zentrales Register über Unternehmensbasisdaten zur Bereitstellung verifizierter Stammdaten.
Bezahldienste	Sammelkategorie föderaler Bezahlplattformen für Online-Dienste der öffentlichen Verwaltung.
BundID / DeutschlandID	Nutzerkonto Bund: Identifizierung natürlicher Personen für elektronische Verwaltungsleistungen.
DVC-IAM	Identitäts- und Zugriffsmanagementkonzept der Deutschen Verwaltungscloud.
DVDV	Deutsches Verwaltungsdiensteverzeichnis: zentrales Verzeichnis der elektronisch erreichbaren Behörden.
ELSTER	Gemeinsames eGovernment-Projekt aller Steuerverwaltungen von Bund und Ländern.
EUDI-Wallet	Staatlich getragene digitale Brieftasche für natürliche Personen auf Basis eIDAS 2.0.
European Business Wallet	Geplantes EU-weites Pendant der EUDI-Wallet für juristische Personen.
FIM	Föderales Informationsmanagement: Methode und Werkzeugbaukasten für die einheitliche Beschreibung von Verwaltungsleistungen.
FIT-Connect	Föderaler Antragsdatenübermittlungsdienst der FITKO.

GDI-DE	Föderal aufgebaute Geodateninfrastruktur Deutschland.
MUK	Mein Unternehmenskonto: bundesweit einheitliches Organisationskonto für Unternehmen.
NFK	Nationale Feedback-Komponente: mandantenfähige Lösung zur Erfassung anonymen Nutzendenfeedbacks.
NOOTS	National Once-Only Technical System: föderale Vermittlungsinfrastruktur für den rechtskonformen Datenaustausch.
OSiP	Online-Sicherheitsprüfung: föderal koordinierte Durchführung personenbezogener Prüfungen.
OZG-RE	Onlinezugangsgesetz-konforme Rechnungseingangsplattform des Bundes.
PVOG	Portalverbund Online-Gateway: föderale Vermittlungsinfrastruktur für Verwaltungsleistungsdaten.
Statistischer Verbund Bund-Länder	Föderaler Verbund der Statistischen Ämter des Bundes und der Länder.
ZSK	Zentrale Statistik-Komponente: Plattform zur Erfassung und Auswertung nicht-personenbezogener Statistikdaten.
ZaPuK	Zielarchitektur Postfach- und Kommunikationslösungen: föderale Zielarchitektur für eine einheitliche Postfach-Infrastruktur.

6.2 Mögliche Transitionsstrategien

Für die schrittweise Anbindung der bestehenden Basisdienste an die föderale API-Autorisierungsinfrastruktur kommen verschiedene Strategien in Betracht, die jeweils unterschiedliche Aspekte priorisieren. Im Umsetzungsprojekt sind die folgenden vier Strategien einzeln und in Kombination zu betrachten:

- **Erst mit den Willigen anfangen:** Eine Pull-Strategie setzt auf die Bereitschaft der Plattformverantwortlichen Stellen. Die Anbindung erfolgt zunächst dort, wo bereits eigenes Interesse, Modernisierungsdruck oder konkrete Anwendungsfälle bestehen. Frühe Erfolge erzeugen Lerneffekte und Multiplikatorwirkung.
- **Nach Erneuerungszyklen:** Eine opportunistische Strategie bindet Basisdienste dann an, wenn ohnehin eine größere Erneuerung, Neuvergabe oder Major-Release-Migration ansteht. Die Anpassungen lassen sich in den ohnehin laufenden Aufwand integrieren, wirtschaftlich vorteilhaft, aber zeitlich schwer planbar.
- **Nach strategischer Wichtigkeit:** Eine Priorisierungsstrategie nimmt zuerst diejenigen Basisdienste in den Blick, die als zentrale Querschnittsfunktionen besonders viele Anwendungsfälle und Nutzendengruppen betreffen, hohe Mengengerüste verarbeiten oder gesetzlichen Verpflichtungen unterliegen.
- **Nach Reifegrad:** Eine technikbezogene Strategie betrachtet den Ist-Stand der Basisdienste im Verhältnis zur Zielarchitektur. Dienste, die bereits OAuth-basierte Autorisierungsverfahren einsetzen oder eine moderne API-Architektur aufweisen, lassen sich mit deutlich geringerem Aufwand anbinden als Dienste mit proprietären Lösungen.

Die vier Strategien sind keine Alternativen, sondern Achsen, die in der konkreten Roadmap zu kombinieren sind. Die endgültige Auswahl und Planung kann erst im Rahmen eines Umsetzungsprojekts erfolgen, da intensive Abstimmungen mit den verantwortlichen Stellen der jeweiligen Basisdienste erforderlich sind.

7 Offene Fragen und Handlungsbedarfe

Die in den vorangegangenen Kapiteln dargestellte Zielarchitektur beschreibt den fachlichen, technischen und organisatorischen Rahmen einer föderalen API-Autorisierungsinfrastruktur. Ihre Realisierung wirft eine Reihe übergreifender Fragen auf, deren Klärung über den Geltungsbereich des vorliegenden Konzepts hinausgeht und im Rahmen eines Umsetzungsprojekts adressiert werden muss. Die ersten vier Abschnitte behandeln strukturelle und übergreifende Themen; die Kapitel 7.5 und 7.6 bündeln Konkretisierungsbedarfe der querschnittlichen Themen aus Kapitel 5; Kapitel 7.7 skizziert Erweiterungspotenziale.

7.1 Gemeinsame Governance-Struktur für Basisdienste

Die Realisierung der föderalen API-Autorisierungsinfrastruktur und ihre dauerhafte Wirksamkeit setzen eine Governance voraus, die über die klassische Betriebsverantwortung einzelner Basisdienste hinausgeht. Mehrere Themen lassen sich ausschließlich auf Architektur- und Querschnittsebene wirksam koordinieren. Konkrete Governance-Bedarfe der Zielarchitektur betreffen das Lifecycle- und Änderungsmanagement der Basisdienste, die Policy-Governance, die Attribut- und Identitäts-Governance sowie die übergreifende Architekturgovernance.

Die Zielarchitektur bewegt sich in einem etablierten und sich derzeit weiterentwickelnden Geflecht föderaler Governance-Strukturen: IT-Planungsrat, Föderales IT-Architekturboard, Föderales IT-Standardisierungsboard, DVC und DVC-Architekturboard, FIM, das Produktmanagement-Modell des IT-Planungsrats, sowie die im Aufbau befindlichen Strukturen der Deutschland-Architektur und des Deutschland-Stacks. Eine eigenständige Governance-Struktur für die föderale API-Autorisierungsinfrastruktur ist daher weder anzustreben noch realistisch erreichbar; vielmehr ist eine wirksame Verzahnung mit den bestehenden Strukturen erforderlich.

Aus der Verzahnung der Governance-Bedarfe mit den bestehenden Strukturen ergeben sich folgende offene Fragen:

- **Verortung der Governance der API-Autorisierungsinfrastruktur:** In welcher Konstellation der genannten Gremien werden die Architekturentscheidungen, die Standardpflege und die Migrationsplanung dauerhaft verankert?
- **Verortung im Produktmanagement-Modell:** Wie wird die Infrastruktur eingeordnet, also als eigenständiges Produkt mit eigenem Produktboard, als Querschnittsfunktion über mehrere Produktboards hinweg, oder über eine andere Konstellation?

- **Abstimmung zwischen den Governance-Strukturen:** Wie kann sichergestellt werden, dass die relevanten Strukturen (insbesondere IT-Architekturboard, IT-Standardisierungsboard, Produktmanagement-Modell, FIM, Deutschland-Architektur und Deutschland-Stack) konsistent ineinandergreifen?
- **Schnittstelle zur Deutschland-Architektur:** Wie wird die Zielarchitektur in die im Aufbau befindliche Governance der Deutschland-Architektur eingebettet?
- **Schnittstelle zum Deutschland-Stack:** Wie werden die Mechanismen der API-Autorisierungsinfrastruktur in die Standardisierung der Plattformkern-Dienste des Deutschland-Stacks eingebracht, sodass keine Parallelentwicklung entsteht?
- **Lifecycle-Prozess für die technischen Standards:** Wie wird die kontinuierliche Weiterentwicklung der Sicherheitsvorgaben, Schnittstellen und Architekturvorgaben im Rahmen des Föderalen IT-Standardisierungsboards organisiert, einschließlich angemessener Übergangsfristen?
- **Policy-Governance-Prozesse:** Welche Stellen, Prozesse und Werkzeuge sind für Redaktion, Abnahme, Veröffentlichung und Überwachung der Policies zu etablieren?
- **Attribut- und IdP-Governance:** Welche Stellen sind für die Pflege des Attributkatalogs verantwortlich, welche Anforderungen gelten an Identity Provider und Attribute Authorities, und wie wird die Konsistenz zu bestehenden Standards (insbesondere FIM-Datenfelder) sichergestellt?

7.2 Identity Provider von Behörden und sonstigen juristischen Personen

Die Wirksamkeit eines attributbasierten Berechtigungsmodells steht und fällt mit der Vertrauenswürdigkeit der Identitätsattribute, auf denen Berechtigungsentscheidungen beruhen. Das FöPD kann Clients anhand ihrer Software-Statement-Attribute unterscheiden (etwa nach Behördenzugehörigkeit oder fachlicher Rolle) nur insoweit, wie diese Attribute durch vertrauenswürdige Quellen abgesichert sind. Gegenwärtig fehlt im deutschen Verwaltungsraum eine flächendeckende, interoperable Infrastruktur für föderierte Identitätsdienste juristischer Personen.

Im Wissenschafts- und Hochschulbereich existieren mit DFN-AAI und eduGAIN seit Jahren funktionierende Föderationsmodelle, die belegen, dass eine dezentrale, institutionsübergreifende SSO-Infrastruktur in der Praxis skaliert. Wesentliche Erfolgsfaktoren sind ein klar definierter, verbindlicher Attributkatalog, eine zentrale Metadaten-Registry als Vertrauensanker, eine gemeinsame Governance-Struktur mit klaren Aufnahme- und Betriebsanforderungen sowie die konsequente Nutzung offener Standards. Diese Merkmale sind direkt auf den Verwaltungskontext übertragbar.

Im Justizbereich existiert mit S.A.F.E. eine föderale SSO-Infrastruktur, deren Attributkatalog (Organisations- und personenbezogene Attribute) ein wertvoller Referenzpunkt für die Federation-Konzeption ist; eine Anbindung von S.A.F.E. als föderierter Identity Provider für den Justizbereich an das FöPD ist erstrebenswert. Mein Unternehmenskonto (MUK) eignet sich aufgrund seines Designschwerpunkts (Authentifizierung von Unternehmen gegenüber Steuerbehörden) als Übergangslösung für privatwirtschaftliche Akteure, nicht als Grundlage einer skalierbaren Behörden-IdP-Infrastruktur.
Aus der Bestandsaufnahme ergeben sich folgende Empfehlungen, die an geeignete übergreifende Gremien gerichtet sind:

- Bund, Länder und Kommunen sollten ertüchtigt werden, institutionelle Identity Provider einzuführen und in eine gemeinsame FöPD-Federation nach dem Vorbild der DFN-AAI einzubringen.
- Ein normatives Behördenverzeichnis mit bestätigten fachlichen und örtlichen Zuständigkeiten sollte als organisatorische Grundlage geschaffen werden.
- Ein paritätisch besetztes Attributkatalog-Gremium sollte den normierenden Attributkatalog pflegen, versionieren und fortschreiben.
- Eine Federation-Betriebsstelle sollte benannt werden, die die zentrale Metadaten-Registry betreibt und Aufnahmeanträge prüft.
- Für Behörden ohne eigene IdP-Infrastruktur sollte ein mandantenfähiger Behörden-IdP als Übergangslösung bereitgestellt werden.

7.3 Verhältnis zu netzseitigen Sicherheitsarchitekturen

Die im vorliegenden Konzept formulierten Vorgaben beschreiben eine **applikationsbasierte Absicherung** der föderalen API-Kommunikation auf Basis von OAuth, FAPI 2.0 und ergänzenden Mechanismen wie Sender-Constrained Access Tokens. Die zugrunde liegenden Profile schließen Fragen der Netzarchitektur und netzseitigen Absicherung explizit aus dem Geltungsbereich aus.
In der Sicherheitsstandardlandschaft der öffentlichen Verwaltung lassen sich zwei Pole unterscheiden: Auf der einen Seite stehen netzarchitekturzentrierte Vorgaben, insbesondere der IT-Grundschutz-Baustein NET.1.1 sowie die Detailstandards 01 und 48 der DVC. Auf der anderen Seite stehen anwendungs- und cloudorientierte Vorgaben, insbesondere C5:2026 mit ausgebauten Anforderungen an Identitäts- und Berechtigungsmanagement, Kryptographie und Container Management sowie mit Zero Trust als Orientierungsmodell. Eine erhebliche Zahl

bestehender und in Entwicklung befindlicher Anwendungen wird heute in Verwaltungsnetzen betrieben, weil diese ein zentraler Bestandteil der etablierten Sicherheitsarchitektur sind.
Aus dem Verhältnis der applikationsbasierten Sicherheitsvorgaben zu den bestehenden netz- und cloudseitigen Standards ergeben sich folgende offene Fragen:

- **Bestandsintegration:** Wie kann sichergestellt werden, dass Basisdienste und API-Clients, die heute in Verwaltungsnetzen betrieben werden, ohne grundlegende Anpassungen ihrer Netzanbindung an die Infrastruktur angebunden werden können?
- **Schutzbedarfsbezogene Bewertung:** Für welche Schutzbedarfe und Szenarien sind die applikationsbasierten Sicherheitsmechanismen (gegebenenfalls in Kombination mit einer C5-konformen Bereitstellung) ausreichend, um einen sicheren Betrieb über das öffentliche Internet zu ermöglichen?
- **Aktualisierung von Empfehlungen:** Wie und in welchem Zeithorizont können auf Grundlage einer solchen Bewertung die einschlägigen Vorgaben von BSI (insbesondere zum IT-Grundschutz) und DVC (insbesondere Detailstandards 01 und 48) angepasst werden?
- **Konsistenz der kryptographischen Vorgaben:** Die in den Sicherheitsvorgaben referenzierten BSI-Vorgaben sind mit den entsprechenden Vorgaben der DVC-Detailstandards abzugleichen, um widersprüchliche Mindestanforderungen zu vermeiden.
- **Governance:** Es ist eine geeignete Form der Abstimmung zwischen den verantwortlichen Gremien (insbesondere BSI, DVC und der Trägerschaft des vorliegenden Konzepts) zu etablieren.

7.4 PKI-Infrastruktur

Die Verwaltungs-PKI (V-PKI) ist die etablierte föderale Vertrauensinfrastruktur des öffentlichen Sektors. Aus Sicht der föderalen API-Autorisierungsinfrastruktur stehen technische Modernisierungsbedarfe im Vordergrund: Heutige Beantragungs- und Austauschprozesse sind weitgehend manuell organisiert, Zertifikate werden mit langen Laufzeiten ausgestellt, und Mechanismen für eine automatisierte Lifecycle-Steuerung fehlen weitgehend. Die Architekturentscheidungen ADR-002 (Client-Authentifizierung mit `private_key_jwt`), ADR-003 (Sender-Constraining mit DPoP) und ADR-004 (Verankerung des Public Keys in der Software Statement Assertion) sind pragmatische Antworten auf den heutigen Stand: Sie erlauben einen schnellen, skalierbaren Aufbau der Infrastruktur, ohne dass deren Wirksamkeit von einer vorgängigen Modernisierung der V-PKI abhängt. Sie stellen jedoch keine grundsätzliche Abkehr von einer PKI-basierten Vertrauensinfrastruktur dar.

Eine technisch modernisierte V-PKI mit automatisierbaren Beantragungs-, Erneuerungs- und Austauschprozessen würde der föderalen API-Autorisierungsinfrastruktur an mehreren Stellen unmittelbaren Mehrwert bringen, insbesondere durch einen automatisierten Lifecycle für Zertifikate (z. B. ACME-basiert), eine erweiterte Nutzung von Zertifikaten in der Architektur (etwa für mTLS in der zentralen Infrastruktur, Signatur und Verschlüsselung), robuste Validierungsmechanismen, vereinfachtes Management der zentralen Zertifikate des FöPD und integrierte Bestellprozesse durch Verzahnung mit dem FöPD.
Aus dem Verhältnis zur V-PKI ergeben sich folgende offene Fragen:

- **Modernisierung der V-PKI:** In welchem Zeithorizont und unter welcher Federführung wird eine technische Modernisierung umgesetzt, insbesondere im Hinblick auf automatisierte Beantragungs- und Erneuerungsprozesse, robuste Validierungsmechanismen sowie die Vorbereitung auf Post-Quanten-Kryptographie?
- **Nachzug von Zertifikatsanwendungen in der Zielarchitektur:** Welche Komponenten und Schnittstellen sollen (sobald eine modernisierte V-PKI verfügbar ist) auf zertifikatsbasierte Mechanismen migriert oder durch solche ergänzt werden?
- **Verzahnung einer V-PKI-Registration-Authority mit dem FöPD:** Wie kann eine Registration Authority mit dem FöPD verzahnt werden, sodass Zertifikatsbestellungen automatisiert auf Basis der im FöPD validierten Identitäten erfolgen?
- **Verhältnis von Certificate Transparency zum Transparency Log der Zielarchitektur:** Wie wird eine etwaige Certificate-Transparency-Lösung der modernisierten V-PKI mit dem in Kapitel 5.3 beschriebenen Transparency Log abgestimmt, sodass keine Parallelinfrastrukturen entstehen?

7.5 Übergreifendes Monitoring und Risikobewertung

Die Umsetzung der in Kapitel 5.2 beschriebenen SSF-basierten Monitoring- und Risikobewertungsinfrastruktur erfordert die Klärung mehrerer offener Punkte:

- **Föderales SSF-Eventprofil:** Spezifikation der föderalen API-spezifischen Eventtypen als formales SSF-Profildokument, einschließlich SET-Struktur, Subject-Identifier-Konventionen und Event-Semantik. Zu klären ist, ob dieses Profil als eigenständige OpenID-Profilspezifikation oder als technischer Standard im IT-Standardisierungsboard verankert wird.
- **Risk-Score-Modell:** Definition, wie ein Risikowert für eine registrierte Software bzw. einen API-Consumer-Client berechnet, aggregiert und kommuniziert wird, einschließlich der Schwellenwerte für automatische Reaktionen.

- **Risikoregeln und Eskalationspfade:** Spezifikation der Korrelationsregeln und Schwellenwerte sowie der automatischen Reaktionsketten, insbesondere die Abgrenzung zwischen dem direkten SSF-Kanal zum PDP (unmittelbare Einzelentscheidung) und dem zentralen Policy-Pfad (übergreifende DENY-Policies).
- **Datenschutz und Protokollierungspflichten:** Klärung, welche Ereignisdaten über Basisdienst-Grenzen hinweg übertragen und aggregiert werden dürfen, insbesondere im Hinblick auf personenbezogene Daten und die DSGVO. Das SSF sieht Privacy-Controls auf Stream-Ebene vor, deren Konfiguration im föderalen Kontext zu definieren ist.

7.6 Revisionssichere Protokollierung und Auditierung

Die Umsetzung der in Kapitel 5.3 beschriebenen Transparency-Log-Infrastruktur erfordert die Klärung folgender offener Punkte:

- **Erprobung und Reife von Tessera für diesen Use Case:** Tessera ist als Go-Bibliothek für beliebige Log-Personalities konzipiert und technisch geeignet. Die bisherige Produktionserfahrung konzentriert sich jedoch auf andere Ökosysteme (insbesondere Certificate Transparency und Sigstore); eine konkrete Erprobung im Kontext der föderalen API-Autorisierungsinfrastruktur ist erforderlich.
- **Eintragungsschema:** Definition des konkreten Eintragsformats: Felder eines Logeintrags pro Ereignisklasse (SSA-Ausstellung, Policy-Änderung, administrative Ereignisse, IdP-Föderierungsänderungen) sowie das Serialisierungsformat.
- **Datenschutz und Protokollierungspflichten:** Klärung, welche Datenfelder personenbezogene Daten enthalten können, und wie der Konflikt zwischen DSGVO (insbesondere Recht auf Löschung) und der append-only Natur des Transparency Logs aufzulösen ist.
- **Witness-Infrastruktur:** Prüfung, ob und wie eine Witness-Infrastruktur zur weiteren Stärkung der Manipulationsresistenz eingesetzt werden soll. Witnesses sind unabhängige Parteien, die den Checkpoint des Logs gegenzeichnen.
- **Aufbewahrungsfristen:** Definition der gesetzlichen und betrieblichen Aufbewahrungsfristen unter Berücksichtigung der einschlägigen Vorgaben (BSI-Grundschutz, Haushaltsrecht, DSGVO).

7.7 Erweiterungspotenziale für künftige Anwendungsfelder

Die in diesem Konzept beschriebene Zielarchitektur adressiert die als prioritär identifizierten Kernherausforderungen der föderalen Verwaltung im Bereich der API-Autorisierung. Der Scope wurde bewusst eng gefasst, um eine zügige und konsensfähige Umsetzung zu ermöglichen. Die Architektur ist jedoch auf Erweiterbarkeit ausgelegt; im Umfeld der föderalen Verwaltung

sowie in der internationalen Standardisierungslandschaft zeichnen sich bereits heute Entwicklungen ab, die für künftige Erweiterungen relevant werden können:

- **Autorisierung für KI-Anwendungen und agentische Systeme:** Mit der zunehmenden Verbreitung KI-gestützter Anwendungen (insbesondere agentischer Systeme, die im Auftrag einer Person oder Organisation autonome Handlungen ausführen) entstehen neue Anforderungen an Authentifizierung und Autorisierung. Die hier beschriebene Architektur bietet mit Software Statements und attributbasierten Berechtigungsregeln bereits eine geeignete Grundlage; eine spezifische Konzeption für agentische Systeme ist eigenständig zu entwickeln.
- **Nutzerzentrierte Datenhaltung und dezentrale Berechtigungsverwaltung:** Das SOLID-Protokoll verfolgt einen komplementären Ansatz, in dem Daten in nutzerseitig kontrollierten Datenspeichern verbleiben und Anwendungen nur auf Grundlage individueller Berechtigungen Zugriff erhalten. Eine Verzahnung mit der föderalen Architektur könnte langfristig erprobt werden.
- **Übertragung der Architekturmuster auf weitere Anwendungsdomänen** außerhalb der heute betrachteten Basisdienste sowie die Verzahnung mit angrenzenden europäischen Initiativen.

Eine Erweiterung der Zielarchitektur unter Wahrung der etablierten Architekturprinzipien ist Aufgabe der etablierten Architekturgovernance.

8 High Level Umsetzungsroadmap

Die Roadmap beschreibt einen inkrementellen Weg von der technischen Erprobung zur produktiven Integration der föderalen API-Autorisierungsinfrastruktur. Es handelt sich explizit um eine High Level Roadmap, die den Weg zum Ausbau der Infrastruktur aufzeigt, ohne detaillierte zeitliche Vorgaben festzulegen. Die konkrete Phasenplanung erfolgt im Rahmen des Umsetzungsprojekts.

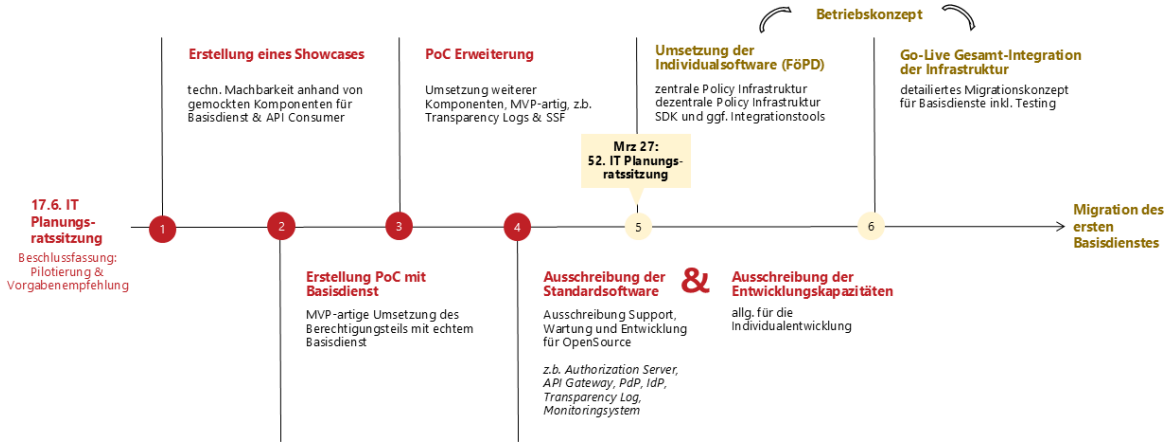

Abbildung 16: High Level Umsetzungsroadmap

Phase 1 (Showcase): In Phase 1 steht die Validierung der technischen Machbarkeit der Zielarchitektur im Fokus. Ein Showcase validiert zentrale Architekturannahmen wie Policy-Handling, Autorisierung und Schnittstellen möglichst früh im Projekt. Dabei kommen imaginäre Komponenten für Basisdienste und API-Clients in einer kontrollierten Umgebung zum Einsatz.

Phase 2 (Proof of Concept): Phase 2 legt den Fokus weiterhin auf die Validierung zuvor getroffener Annahmen. Ein PoC soll basierend auf realen Basisdiensten in Testumgebungen die technische Machbarkeit weiter untermauern. Zentrale technische Aspekte sind die dynamische Client-Registrierung sowie die Autorisierung.

Phase 3 (MVP): Die Ergebnisse der vorigen Phasen werden in Phase 3 kontinuierlich Richtung MVP weiterentwickelt, anhand dessen der Mehrwert der Infrastruktur klar ersichtlich wird. Die wichtigsten Funktionen werden prototypisch implementiert beziehungsweise in dieser Phase erstellt.

Phase 4 (Beschaffung): Phase 4 beschreibt die Beschaffung von Standardsoftware und Entwicklerkapazitäten für die folgenden Projektphasen. Insbesondere werden Ausschreibungen für Standardsoftware, Enterprise-Support und Entwicklungsleistungen vorbereitet und durchgeführt. Ziel ist es, sowohl Umsetzungs- als auch Betriebsfähigkeit sicherzustellen.

Phase 5 (Realisierung): In Phase 5 erfolgt die Realisierung der Individualsoftware (insbesondere FöPD). Zentrale und dezentrale Komponenten werden implementiert und über klar definierte Schnittstellen integriert. Darüber hinaus werden Integrationshilfen (beispielsweise SDKs) für Basisdienste erstellt, um die Adoption zu erleichtern.

Phase 6 (Produktivüberführung und Migration): Zum Abschluss werden die Komponenten in Phase 6 schrittweise in den produktiven Betrieb überführt. Ein detailliertes Migrations- und Testkonzept stellt sicher, dass bestehende Basisdienste kontrolliert angebunden werden können. Aufbauend auf der produktiven Infrastruktur können die ersten Basisdienste integriert werden, deren Auswahl im Laufe der Umsetzungsaktivitäten erfolgt und den Überlegungen aus Kapitel 6 folgt.

9 Anhang

9.1 Externe Referenzen auf Projektartefakte

Die folgenden Projektartefakte sind außerhalb dieses Dokuments verfügbar und werden durch diese Kurzfassung referenziert:

- **Hauptkonzept zur Zielarchitektur** der föderalen API-Autorisierungsinfrastruktur: vollständige Fassung mit allen in dieser Kurzfassung verkürzten oder weggelassenen Inhalten (Prozessbeschreibungen, Detailflüsse, vollständige Use-Case-Listen, Datenmodellbeschreibungen, vollständige Bewertungstabellen).
- **FöPD-Mockup:** Mockup-Design der Kernkomponente: Föderale Plattform Directory (FöPD): https://chart-willow-37308320.figma.site

Alle weiteren Artefakte sind im Open-Code-Repository des Projekts verfügbar:
https://gitlab.opencode.de/sachsen-anhalt/mid/foederale-api-autorisierungsinfrastruktur

Abbildungsverzeichnis

Tabellenverzeichnis