

Frankfurt am Main
28. Mai 2026

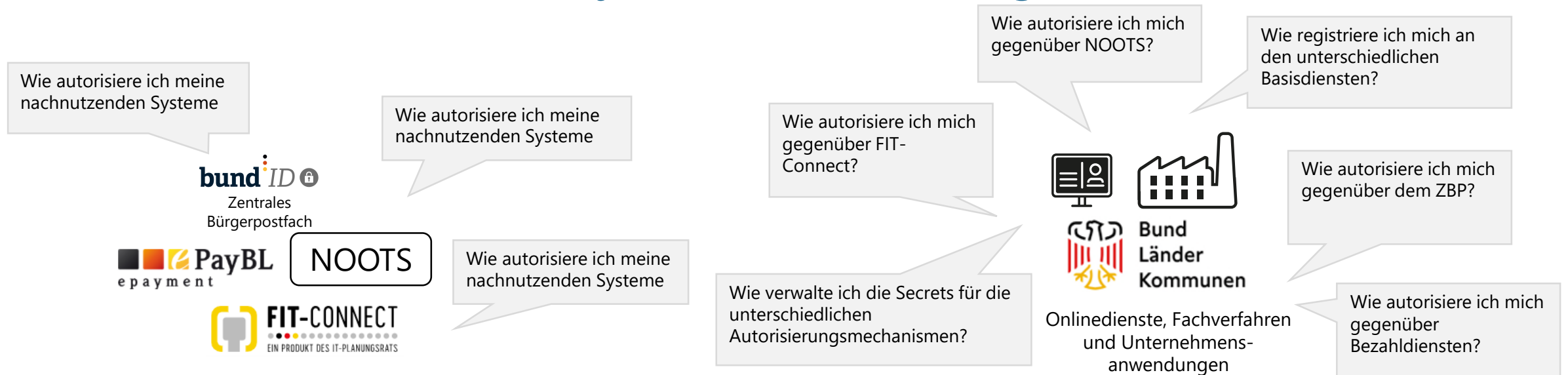
Föderale API- Autorisierungsinfrastruktur

Begleitpräsentation

Andreas Altmann
Sachsen-Anhalt

Alexander Hoose
FITKO

Der Bedarf nach einer föderalen API-Autorisierungsinfrastruktur besteht bei vielen Diensten und Projekten der Verwaltung



In der föderalen IT existieren unzählige Kommunikationsbeziehungen zwischen Basiskomponenten und nutzenden Systemen ohne gemeinsame Pattern und Vorgaben zu API-Absicherung, Berechtigungsmanagement und Registrierungsprozessen.

Mehrkosten und Komplexität in der Implementierung

Mehrkosten bei der Registrierung

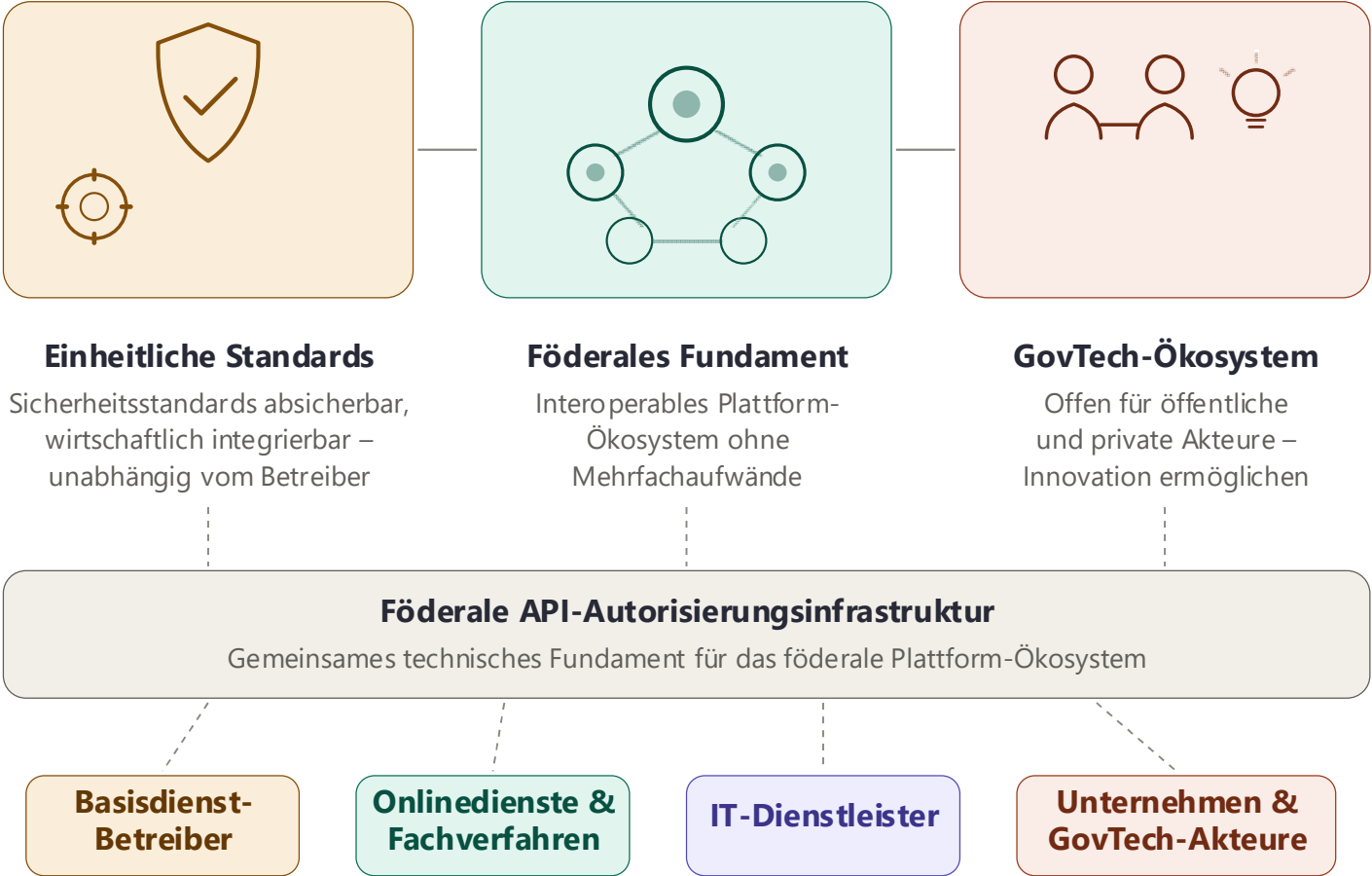
Behinderung eines API-First Ökosystems

Sicherheitsrisiken

Projektziel: Es existieren **etablierte Standards** für die **API-Autorisierung** und **Authentifizierung**, die für eine übergreifende Lösung verwendet werden sollten. Die Schaffung einer **föderalen API-Autorisierungsinfrastruktur** beschleunigt die Umsetzung und erhöht die Sicherheit.

Vision der föderalen API-Autorisierung: Autorisierungsstandards als Grundlage für ein lebendiges GovTech-Ökosystems, offen für alle

Vision Statement der Zielarchitektur



Föderale Sicherheitsvorgaben und eine Zielarchitektur bilden das Fundament für die API-Autorisierungsinfrastruktur

Erarbeitete Artefakte



Sicherheitsvorgaben

Föderale Sicherheitsvorgaben für die Absicherungen von APIs mit OAuth und OpenID Connect auf Basis des FAPI 2.0 Standards sowie internationalen Best Practices mit dem Ziel ein **einheitliches Sicherheitsniveau in der föderalen Architekturlandschaft** zu gewährleisten.



Zielarchitektur

Zielarchitektur für eine föderale API-Autorisierungsinfrastruktur für die APIs von föderalen Basis-komponenten, die Betreibern von fachlichen Anwendungen (bspw. Onlinedienste, Fachverfahren oder auch Anwendungen der Wirtschaft und von Start-Ups) es ermöglichen sollen, **skalierbar**, **sicher** und **wirtschaftlich** auf diese APIs zuzugreifen.



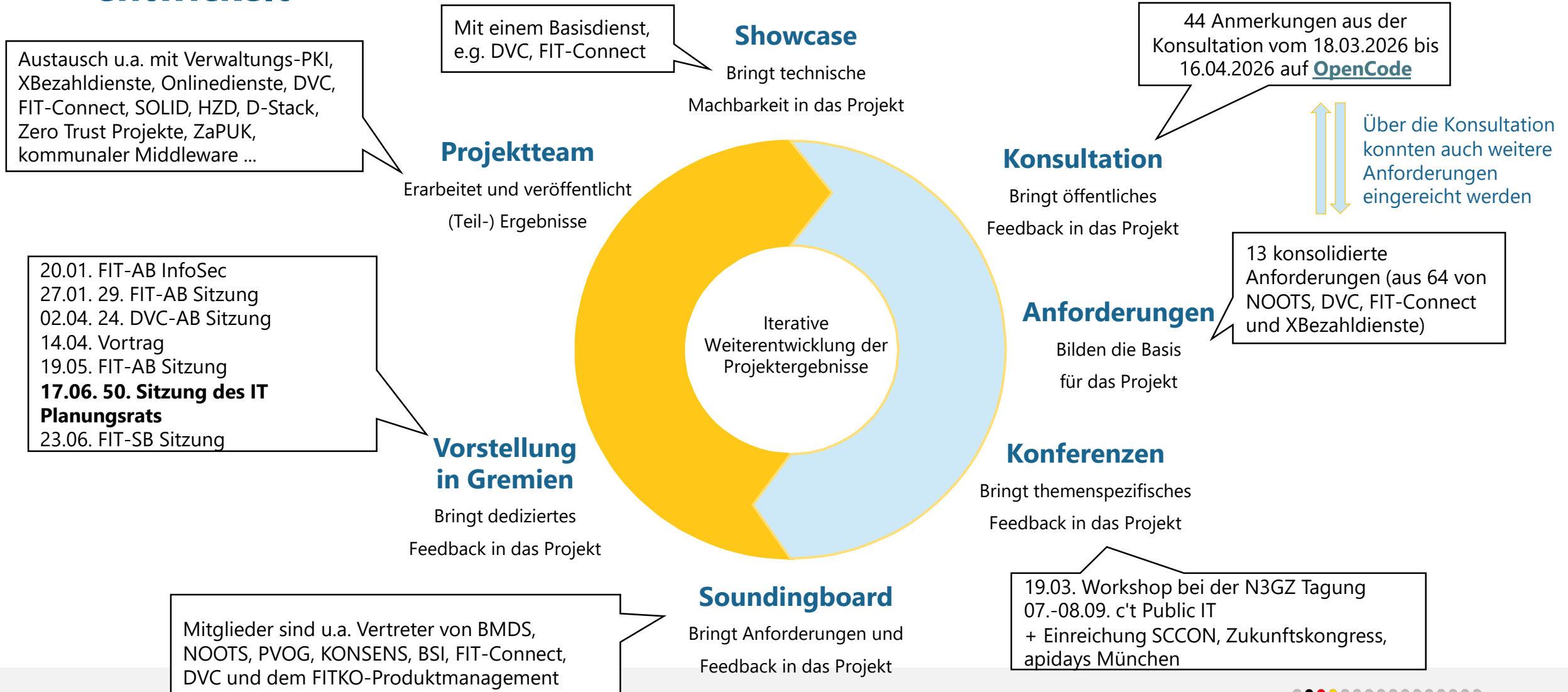
Architektonischer Kern der Zielarchitektur

- › Systemlandschaft: Gemeinsam wo sinnvoll, eigenständig wo nötig
- › **Berechtigungskonzept: Regeln zentral, Prüfung dezentral**
- › **Transparenz & Monitoring: Lückenlose, manipulationssichere Nachvollziehbarkeit**

Unterstützende Artefakte

- › Anforderungsliste, Architekturprinzipien, Architekturentscheidungen (ADR) & **Glossar**

Projektergebnisse wurden iterativ durch diverses Feedback validiert und entwickelt



Sicherheitsvorgaben und Zielarchitektur adressieren unterschiedliche Ebenen in der öffentlichen Verwaltung

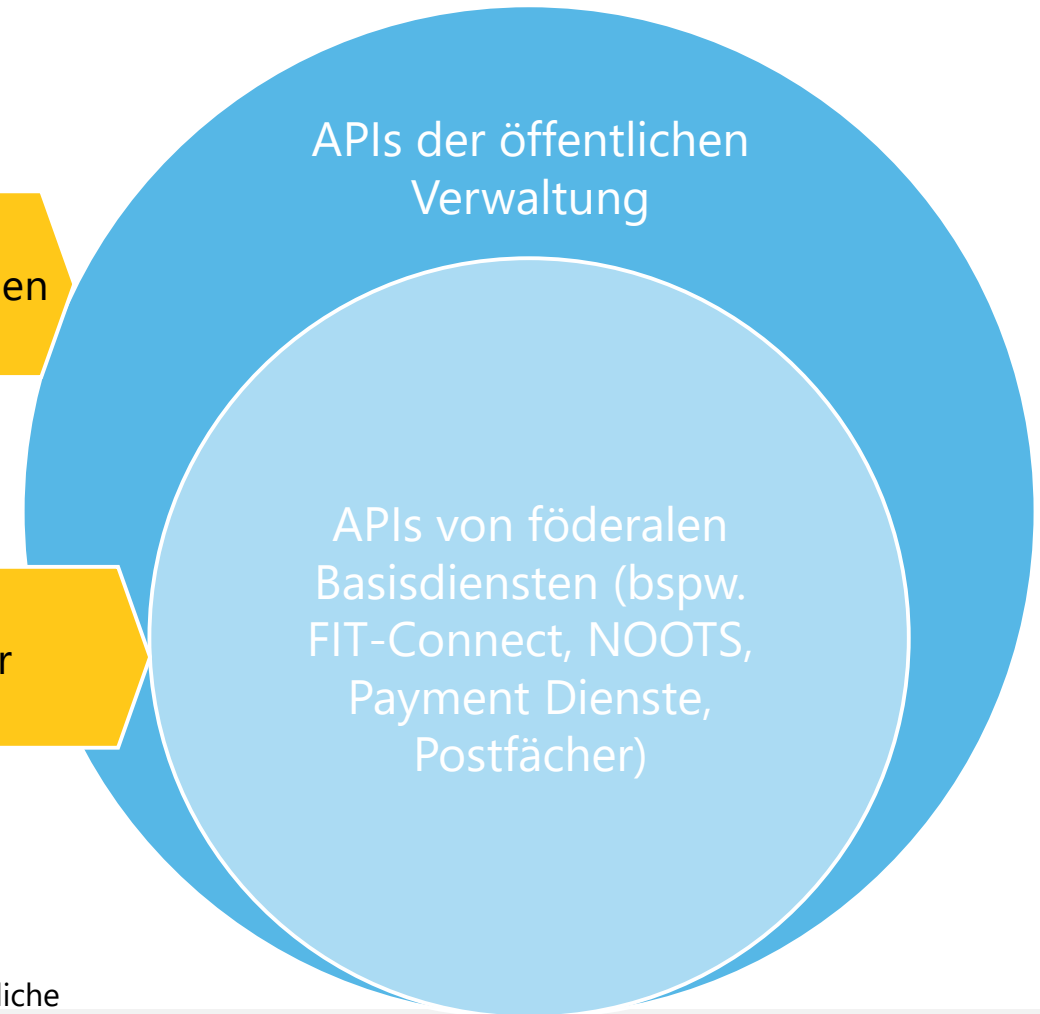
- Geltungsbereich der föderalen Sicherheitsvorgaben liegt auf allen APIs der öffentlichen Verwaltung
- Die Zielarchitektur beschränkt sich auf die APIs föderaler Basisdienste*
 - Die Zielarchitektur unterliegt jedoch selber den föderalen Sicherheitsvorgaben



Sicherheitsvorgaben



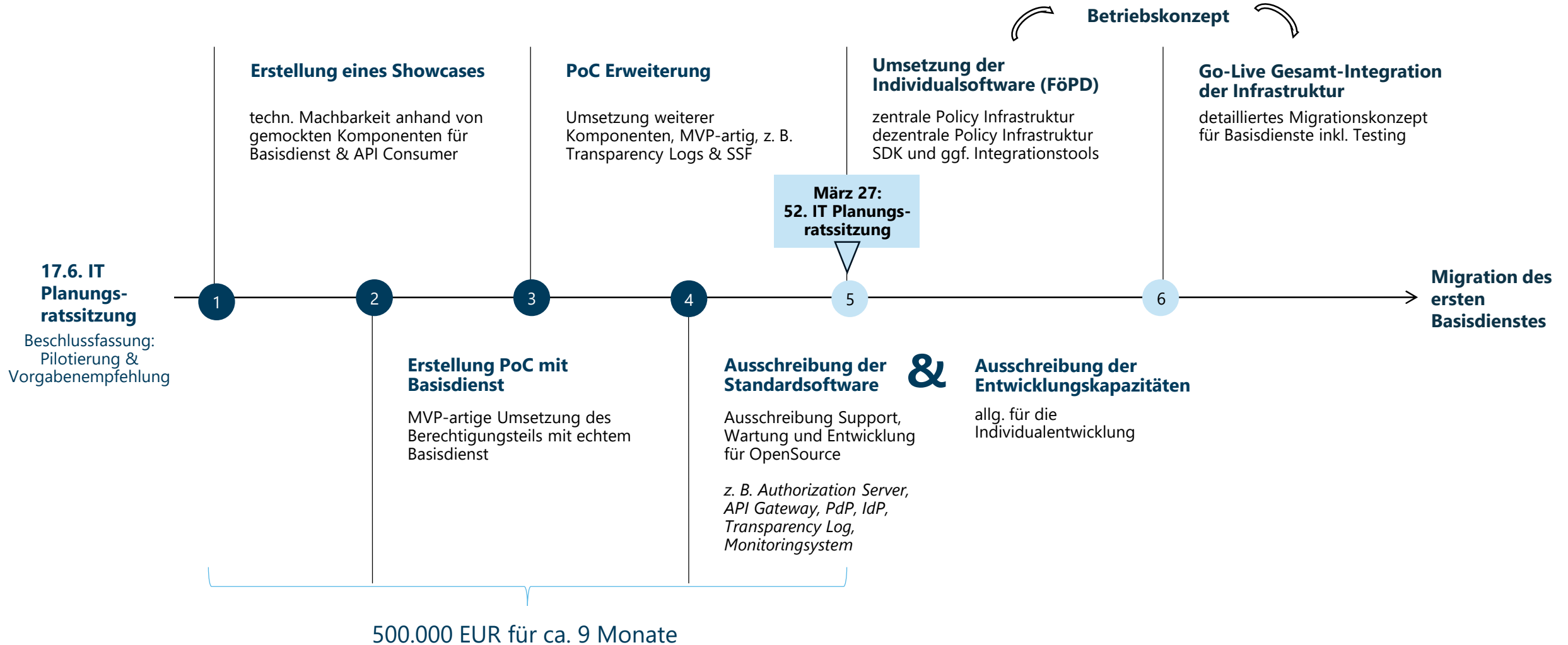
Zielarchitektur



* Basisdienste sind zentral bereitgestellte Softwarelösungen, welche querschnittliche Funktionen für fachliche Prozesse der Verwaltung bereitstellen

Beschluss in der 50. Sitzung des IT-Planungsrats als Start für Pilotierung

Roadmap 2026



Eckpunkte zum Projekt

Stand 08.05.2026

› Rahmenbedingungen

- › Laufzeit: Juli 2025 bis Juni 2026
- › Schwerpunktthema: Digitale Transformationen
- › Verantwortliches Bundesland: Sachsen-Anhalt (Andreas Altmann) mit Vorhabensleitung durch die FITKO (Alexander Hoose)

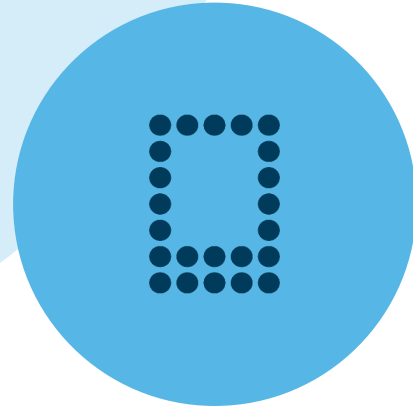
› Projektergebnisse zur 50. Sitzung des IT-Planungsrats (17.6.2026)

- › Zielarchitektur als Langfassung und Kurzfassung,
- › Vorgaben inkl. Rahmendokument, Vorgaben für 2 Sicherheitsstufen und deren Attacker Modelle
- › Mockup und User Stories für das Föderales Plattform Directory (FöPD) als zentrales Self-Service-Portal und Single Source of Truth der föderalen API-Autorisierungsinfrastruktur
- › Glossar
- › Präsentation

› Öffentliche Dokumentation online in OpenCode:

<https://gitlab.opencode.de/sachsen-anhalt/mid/foederale-api-autorisierungsinfrastruktur>

Kontakt



Andreas Altmann

Ministerium für Infrastruktur und Digitales des
Landes Sachsen-Anhalt

E-Mail: andreas.altmann@sachsen-anhalt.de

Tel.: +49 (0)391 567 7266

Alexander Hoose

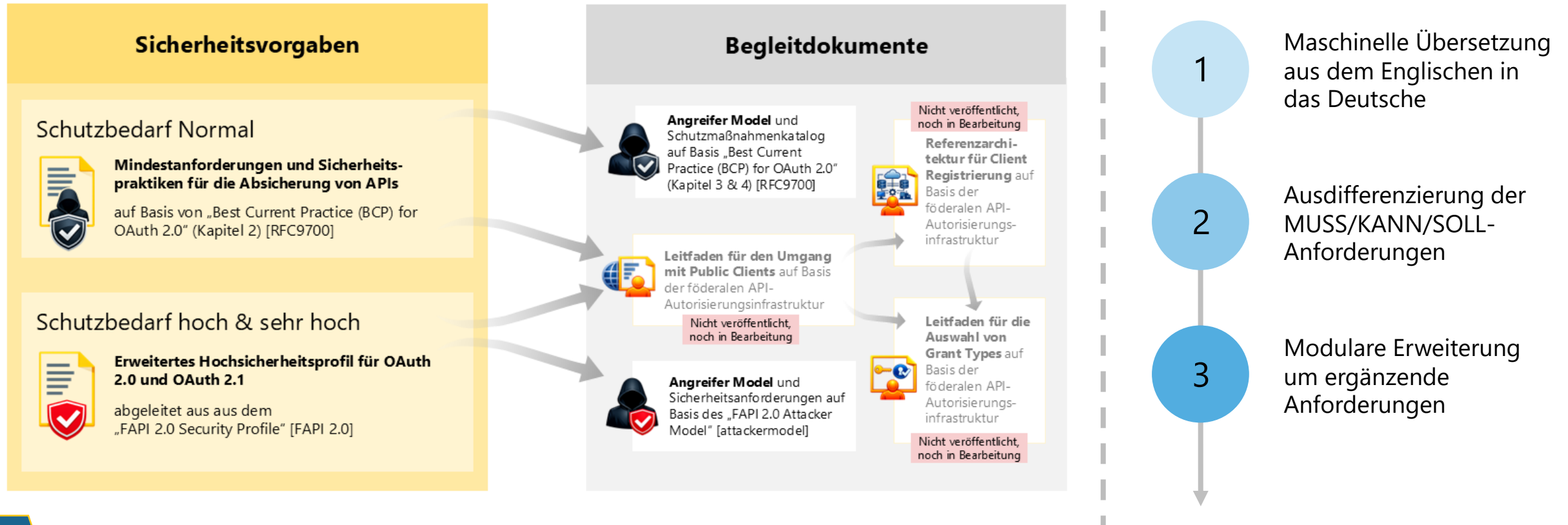
FITKO, Föderales IT-Architekturmanagement

E-Mail: alexander.hoose@fitko.de

Anhang

Ausgearbeitete Sicherheitsvorgaben

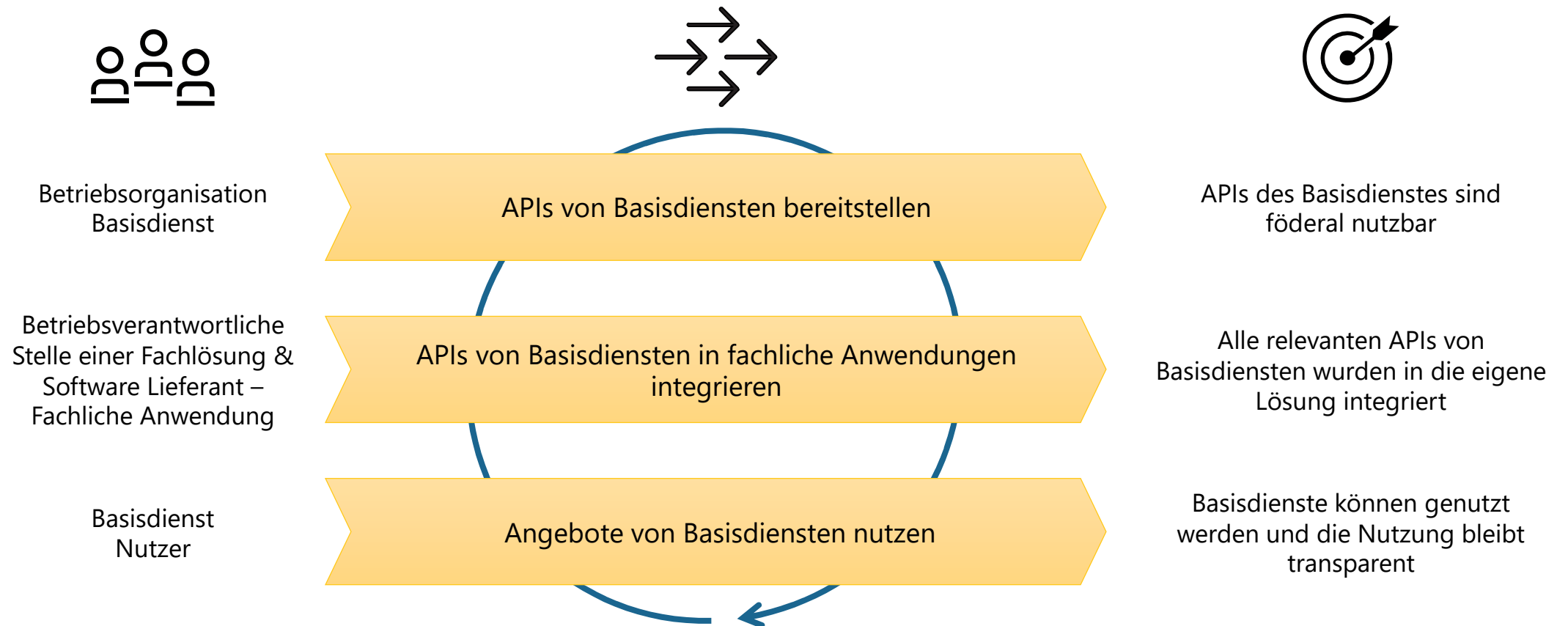
Vorgehen und Ergebnisse



Die Sicherheitsvorgaben sind eng an **etablierten Standards** ausgerichtet und wird ggf. auf die Bedarfe der föderalen IT **angepasst oder erweitert**. Unterschiedliche Schutzbedarfe werden adressiert, indem unterschiedliche Standards herangezogen werden. Die Kerndokumente des Sicherheitsprofils werden durch Begleitdokumente in den passenden Kontexten ergänzt.

Fachlicher Umfang der Zielarchitektur

Betrachtung der zentralen Wertströme



Die Wertströme sind **komplementär** zueinander und erst das **abgestimmte Zusammenspiel** ermöglicht eine **durchgängige Anschlussfähigkeit der föderalen API-Ökosystems**

Prozessübersicht aus der Zielarchitektur

Prozesslandkarte der föderalen API-Autorisierungsinfrastruktur*

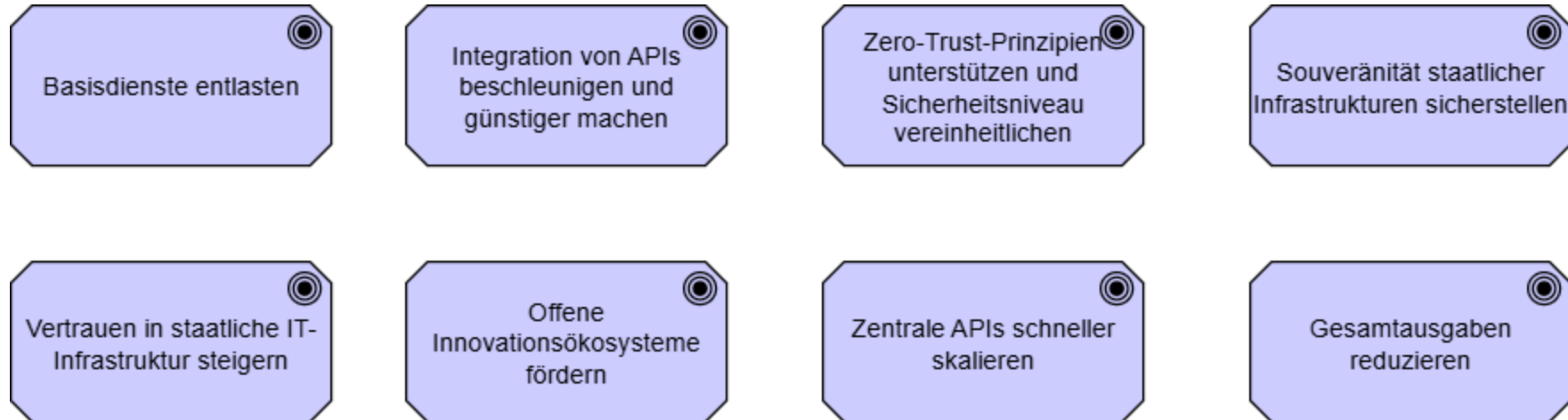


- **Kernprozesse** tragen unmittelbar zur Erbringung des Plattformnutzens bei
- **Supportprozesse** unterstützen den laufenden Betrieb der Infrastruktur

* Im Rahmen dieses Konzepts werden nur solche Prozesse benannt, die für das Verständnis und die Konzeption der Zielarchitektur relevant sind. Eine vollständige Betrachtung aller Betriebsprozesse ist nicht Gegenstand des Projekts

Projektspezifische Architekturziele

Acht Ziele operationalisieren die strategische Ausrichtung des Projekts.

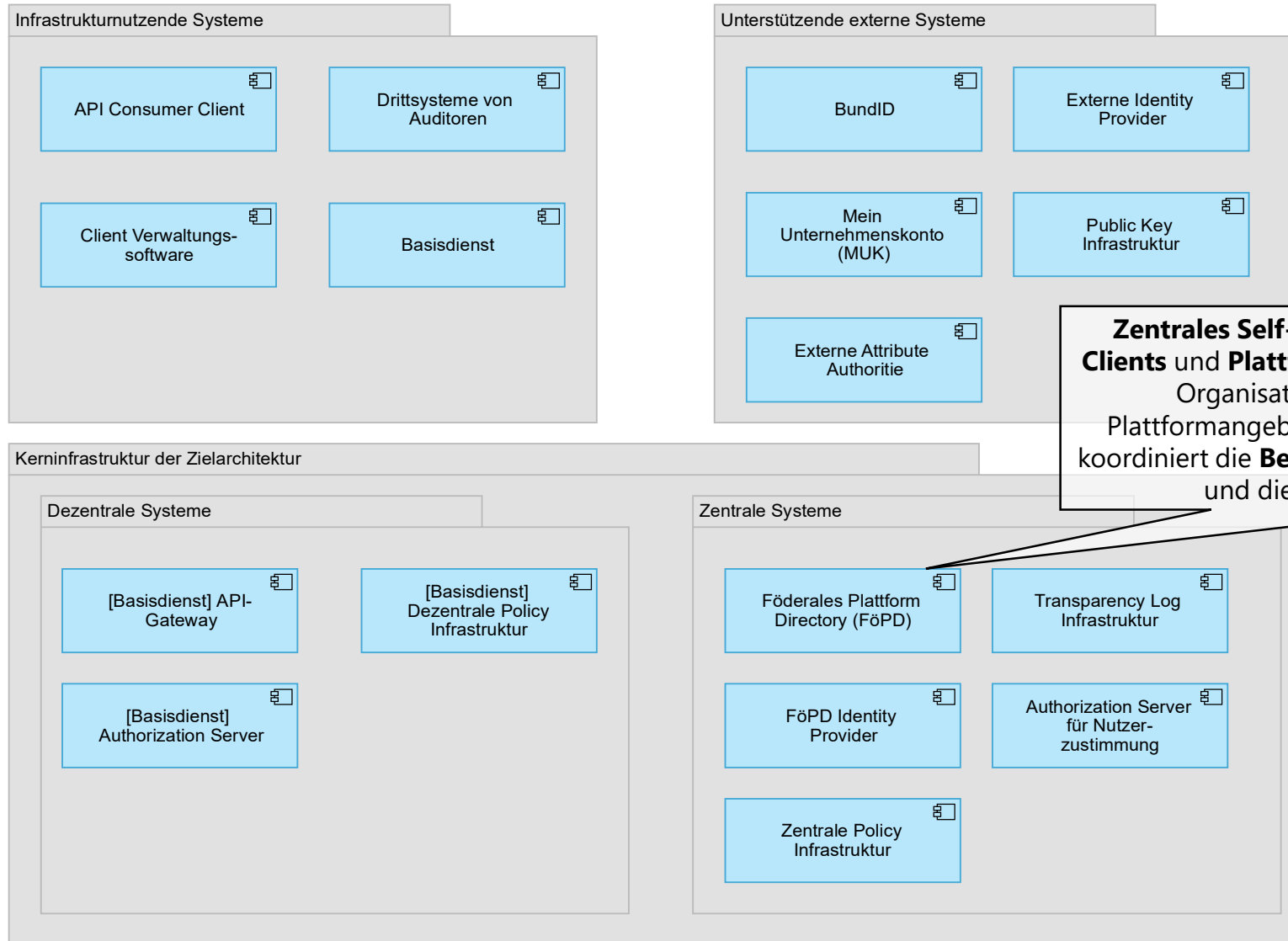


Prinzipienüberblick

Die projektspezifischen Architekturprinzipien bilden den verbindlichen Handlungsrahmen für alle Architektur- und Designentscheidungen im Rahmen der föderalen API-Autorisierungsinfrastruktur.

- Offene Industriestandards und Best Practices nutzen
- Individualentwicklungen und verwaltungsspezifische Lösungen vermeiden
- „Never trust, always verify“ bei allen Zugriffen
- Minimale Zugriffsberechtigungen und dynamische Zugriffsüberprüfungen
- Nachvollziehbarkeit und Auditierbarkeit aller relevanten Systemaktivitäten
- Dezentralität und Redundanz von Sicherheitsmechanismen
- Open-Source-Priorisierung für kritische Komponenten
- Bündelung technischer Querschnittsfunktionen
- Flexibilität und Anpassbarkeit API-spezifischer Berechtigungsmodelle
- Automatisierung von Anbindungsprozessen
- Ermöglichung effizienter und unterbrechungsfreier Backoffice-Verwaltungsprozesse
- Wiederverwendung und Bündelung vor Neuentwicklung
- Vertrauen basiert auf Protokollen und Prozessen, nicht auf Institutionen
- Personenbezogene Daten minimieren
- Dynamische Berechtigungssteuerung

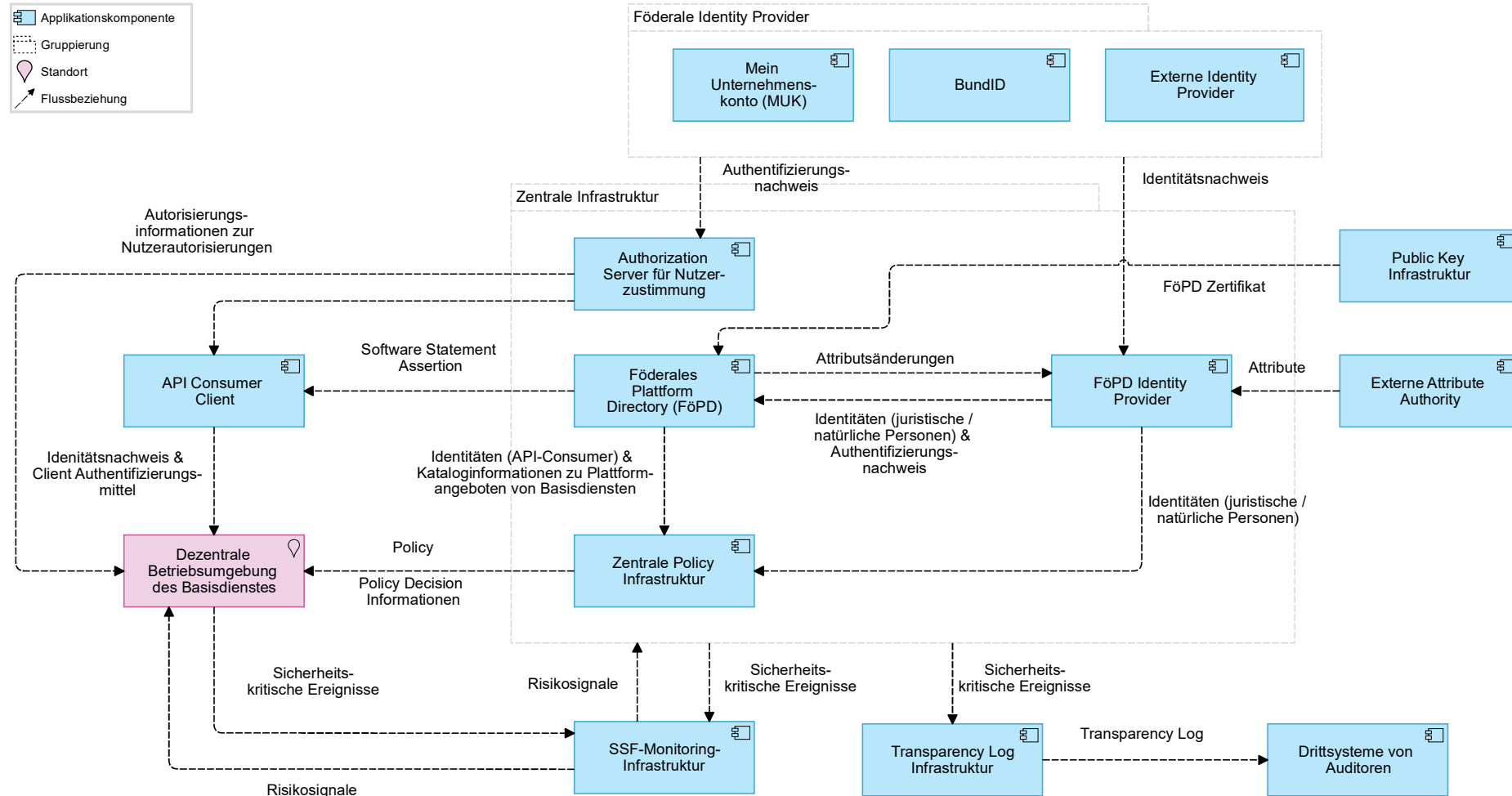
Überblick über die wesentlichen Architekturbausteine



Zentrales Self-Service-Portal und **Single Source of Truth** für **API-Clients** und **Plattformangebote**. Das FöPD steuert die Registrierung von Organisationen, API-Consumer-Software, API-Clients und Plattformangeboten, **stellt Software Statement Assertions aus** und koordiniert die **Beantragungsprozesse für API-Zugriffsberechtigungen** und die **Vergabe von Organisationseigenschaften**.

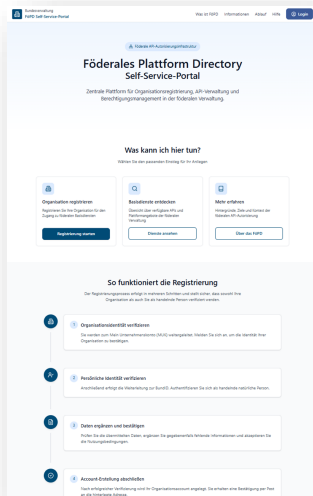
- **Dezentral betriebene Systeme:** Werden zentral beschafft, betreut, vorkonfiguriert und für den dezentralen Betrieb beim Basisdienst bereitgestellt
- **Zentral betriebene Systeme:** Werden zentral für alle Basisdienste und Clients betrieben.

High Level Informationsfluss der föderalen API-Autorisierungsinfrastruktur

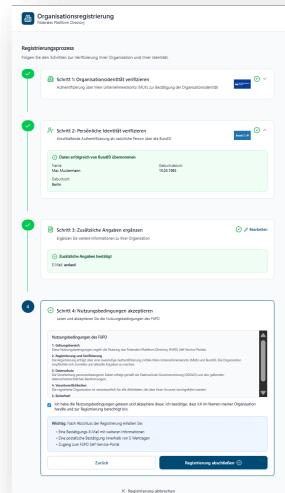


Mockup-Design der Kernkomponente*: Föderale Plattform Directory (FöPD)

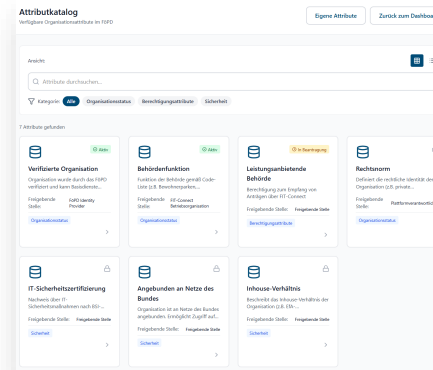
Das Föderale Plattform Directory (FöPD) unterstützt zentrale Kernprozesse der föderalen API-Autorisierung



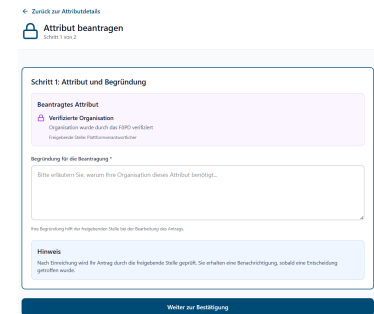
FöPD Landing Page



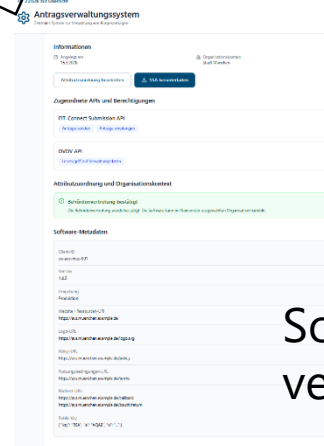
Registrierung



Beantragungs-
übersicht



Beantragung



Software-
verwaltung

* Die hier aufgeführten Mock-ups deuten zentrale Interaktion und Designs im Plattform Directory an und stellen keine Vollständigkeit in Sinne der gesamten föderalen API-Autorisierungsinfrastruktur dar. Im Zielbild sollen alle Prozesse aus Kapitel 4.4 „Prozessübersicht und Darstellung der IT-Prozessunterstützung“ der Zielarchitektur der föderalen API-Autorisierungsinfrastruktur abgebildet werden.