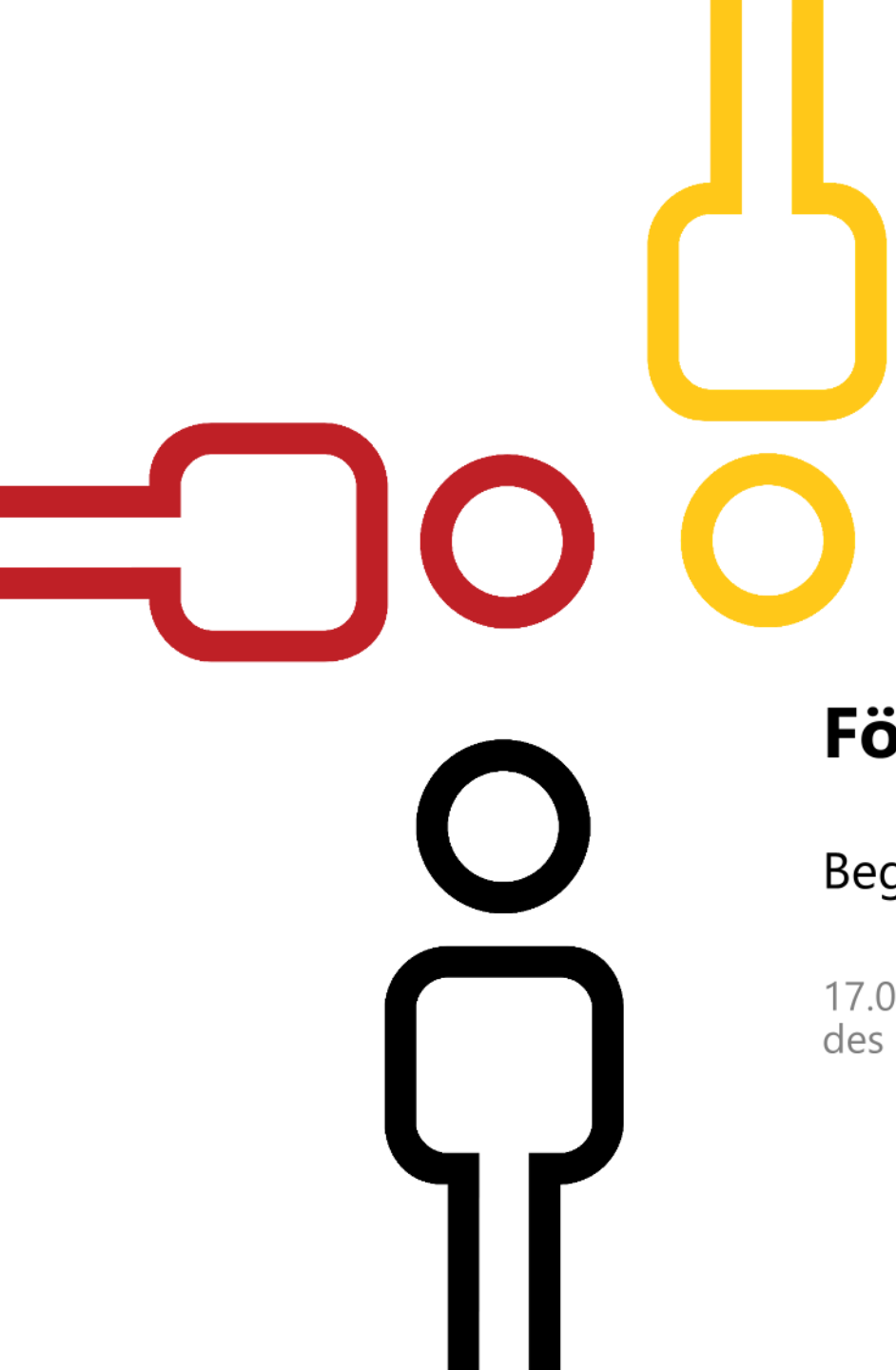


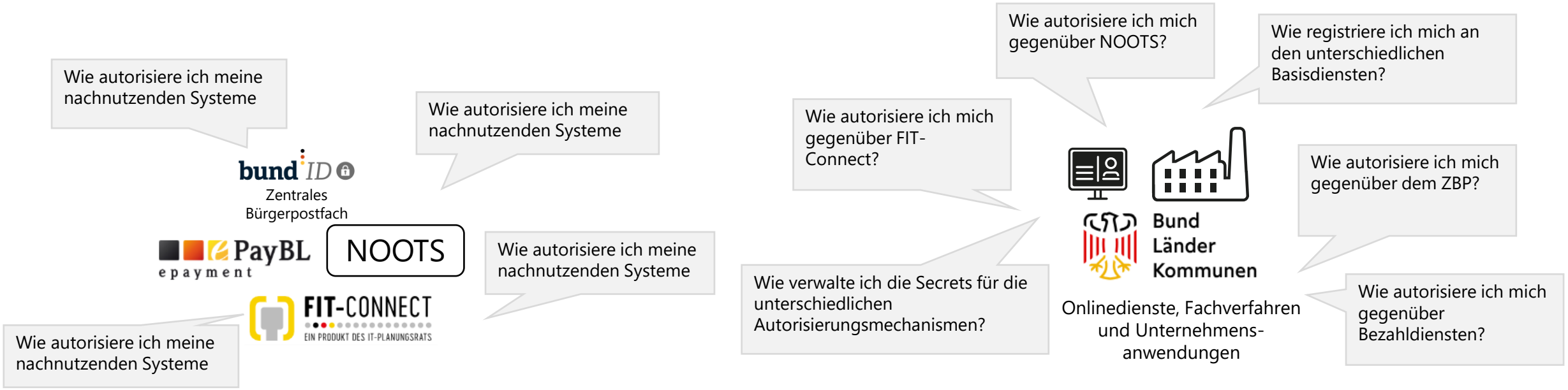
Föderale API-Autorisierungsinfrastruktur

Begleitpräsentation

17.06.2026 | [redacted] 50. Sitzung des IT-Planungsrats

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.

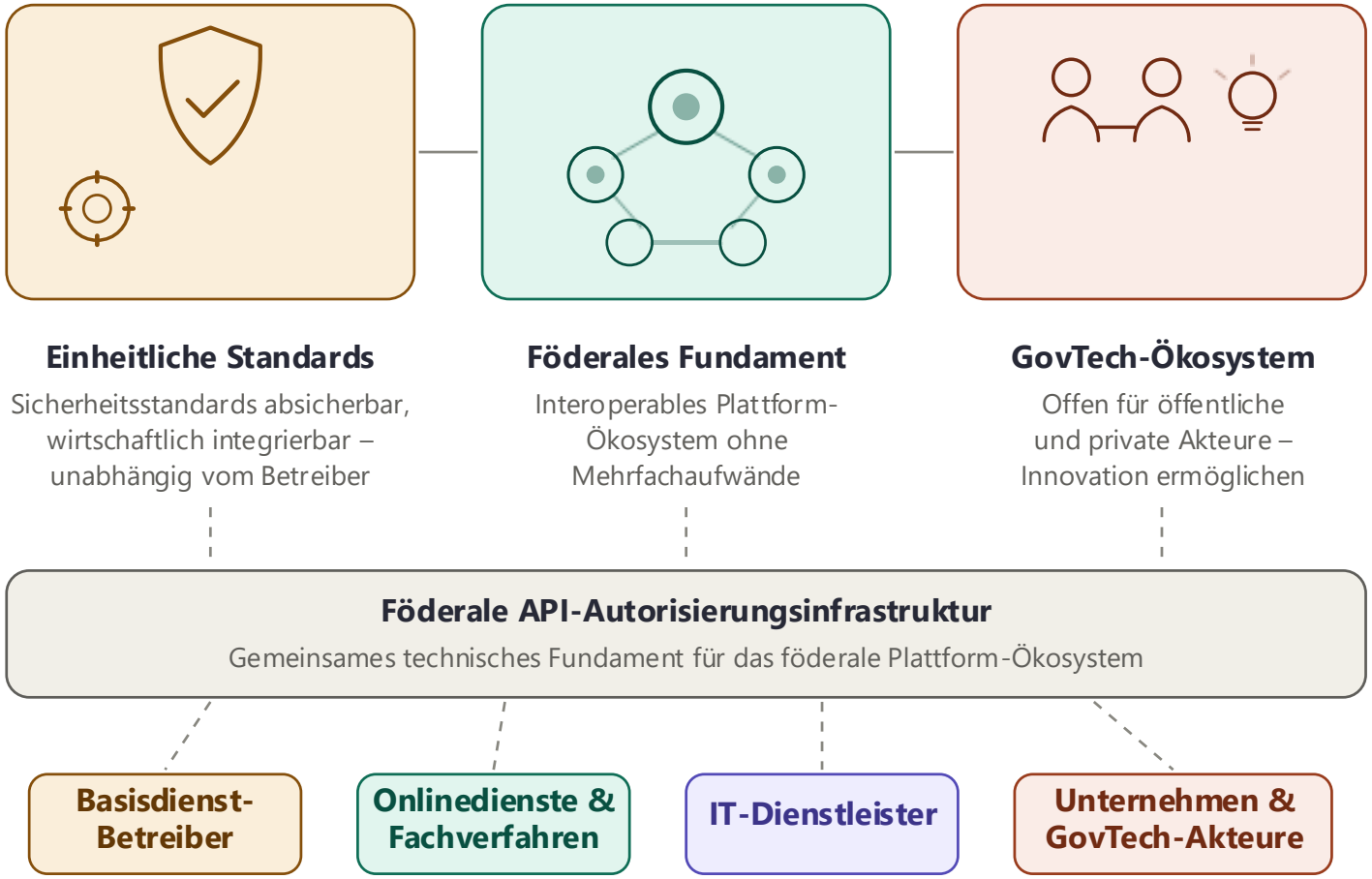
- Mehrkosten und Komplexität in der Implementierung
- Mehrkosten bei der Registrierung
- Behinderung eines API-First Ökosystems
- Sicherheitsrisiken

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.

FITKO

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

FITKO

Projektergebnisse wurden iterativ durch diverses Feedback validiert und entwickelt

Mit einem Basisdienst, e.g. DVC, FIT-Connect

Showcase

Bringt technische Machbarkeit in das Projekt

44 Anmerkungen aus der Konsultation vom 18.03.2026 bis 16.04.2026 auf **OpenCode**

Austausch u.a. mit Verwaltungs-PKI, XBezahldienste, Onlinedienste, DVC, FIT-Connect, SOLID, HZD, D-Stack, Zero Trust Projekte, ZaPUK, kommunaler Middleware ...

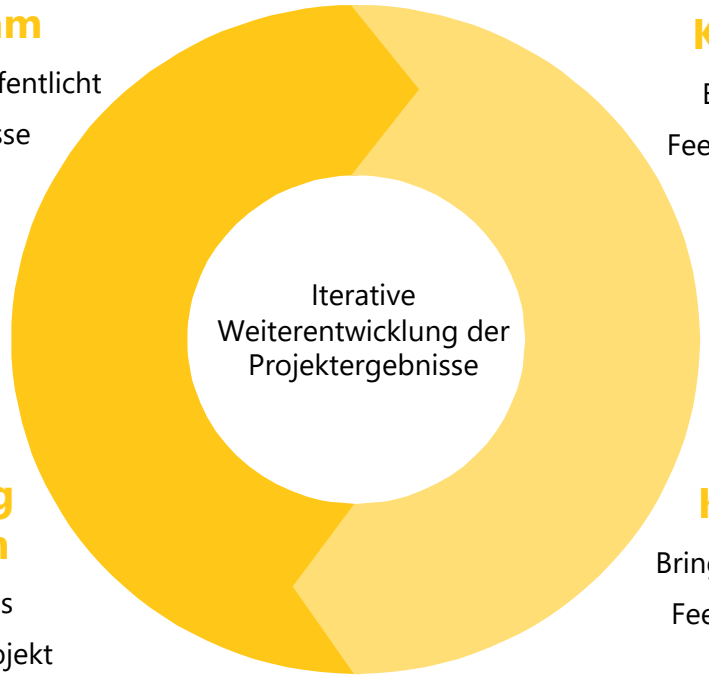
Projektteam

Erarbeitet und veröffentlicht (Teil-) Ergebnisse

Konsultation

Bringt öffentliches Feedback in das Projekt

Über die Konsultation konnten auch weitere Anforderungen eingereicht werden



13 konsolidierte Anforderungen (aus 64 von NOOTS, DVC, FIT-Connect und XBezahldienste)

Anforderungen

Bilden die Basis für das Projekt

20.01. FIT-AB InfoSec
27.01. 29. FIT-AB Sitzung
02.04. 24. DVC-AB Sitzung
14.04. Vortrag
19.05. FIT-AB Sitzung
17.06. 50. Sitzung des IT Planungsrats
23.06. FIT-SB Sitzung

Vorstellung in Gremien

Bringt dediziertes Feedback in das Projekt

Konferenzen

Bringt themenspezifisches Feedback in das Projekt

19.03. Workshop bei der N3GZ Tagung
07.-08.09. c't Public IT
+ Einreichung SCCON, Zukunftskongress, apidays München

Mitglieder sind u.a. Vertreter von BMDS, NOOTS, PVOG, KONSENS, BSI, FIT-Connect, DVC und dem FITKO-Produktmanagement

Soundingboard

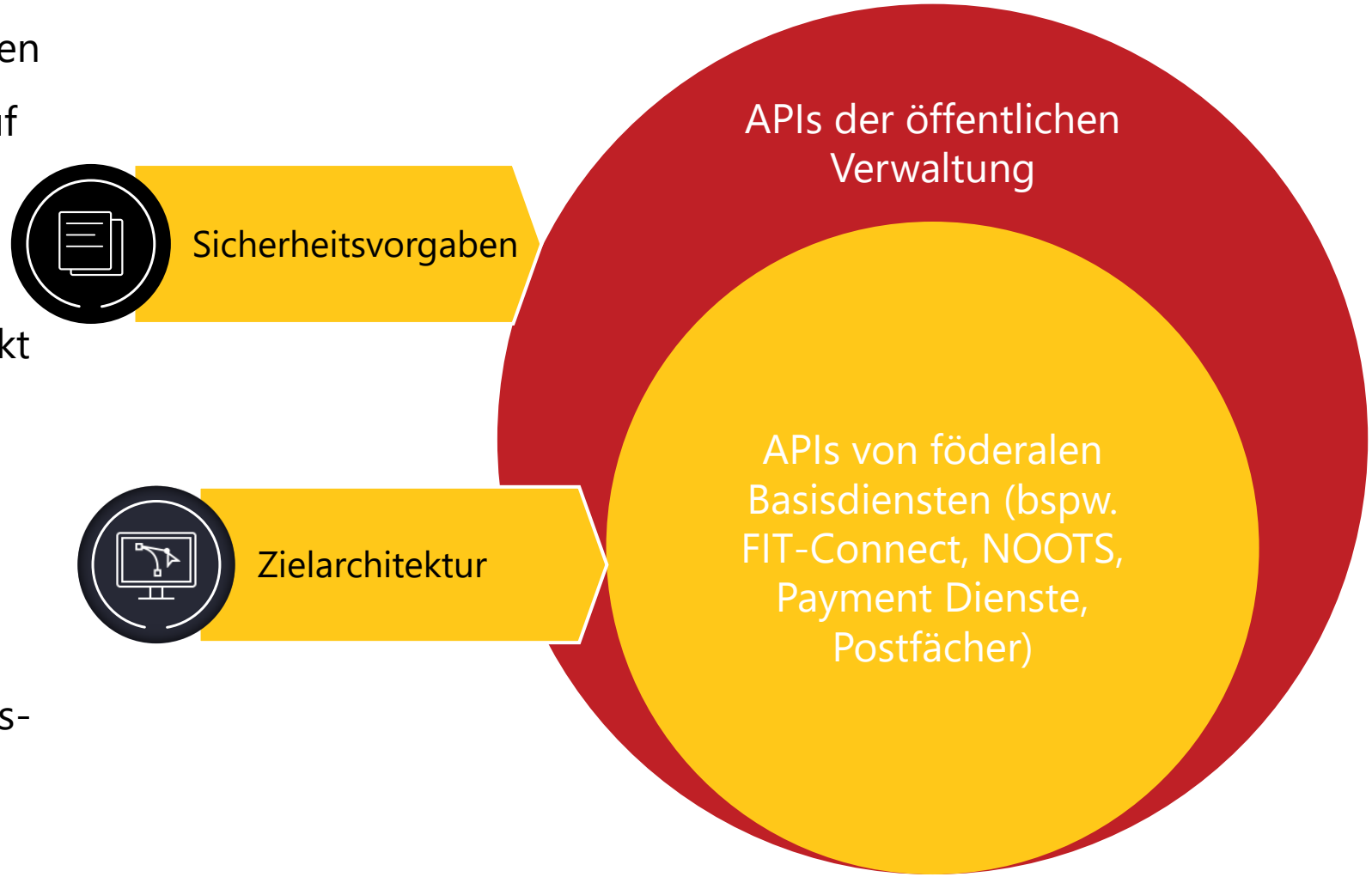
Bringt Anforderungen und Feedback in das Projekt

6. Soundingboard im Mai / Anfang Juni

FITKO

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 Sicherheits-vorgaben

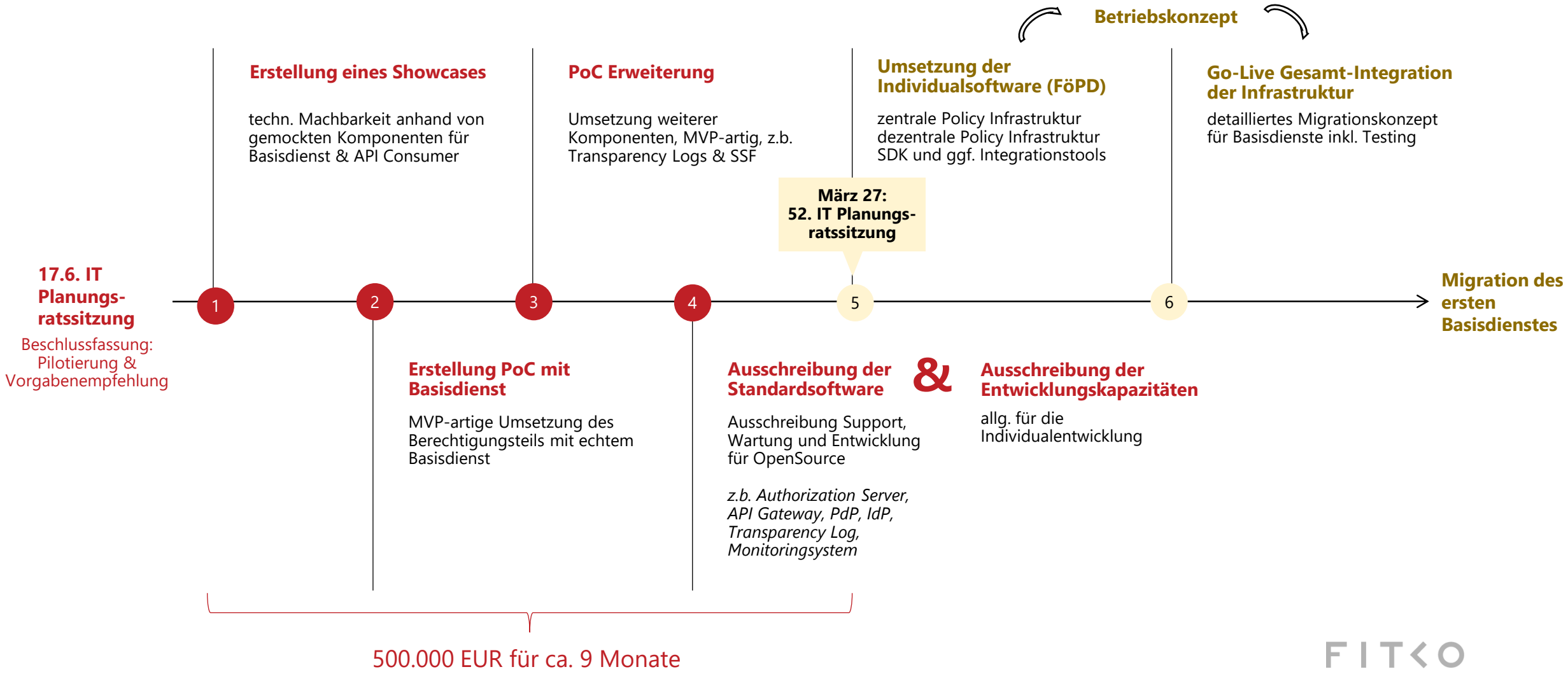


*Basisdienste sind zentral bereitgestellte Softwarelösungen, welche querschnittliche Funktionen für fachliche Prozesse der Verwaltung bereitstellen

FITKO

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

Roadmap 2026



FITKO

Eckpunkte zum Projekt

Stand 08.05.2026

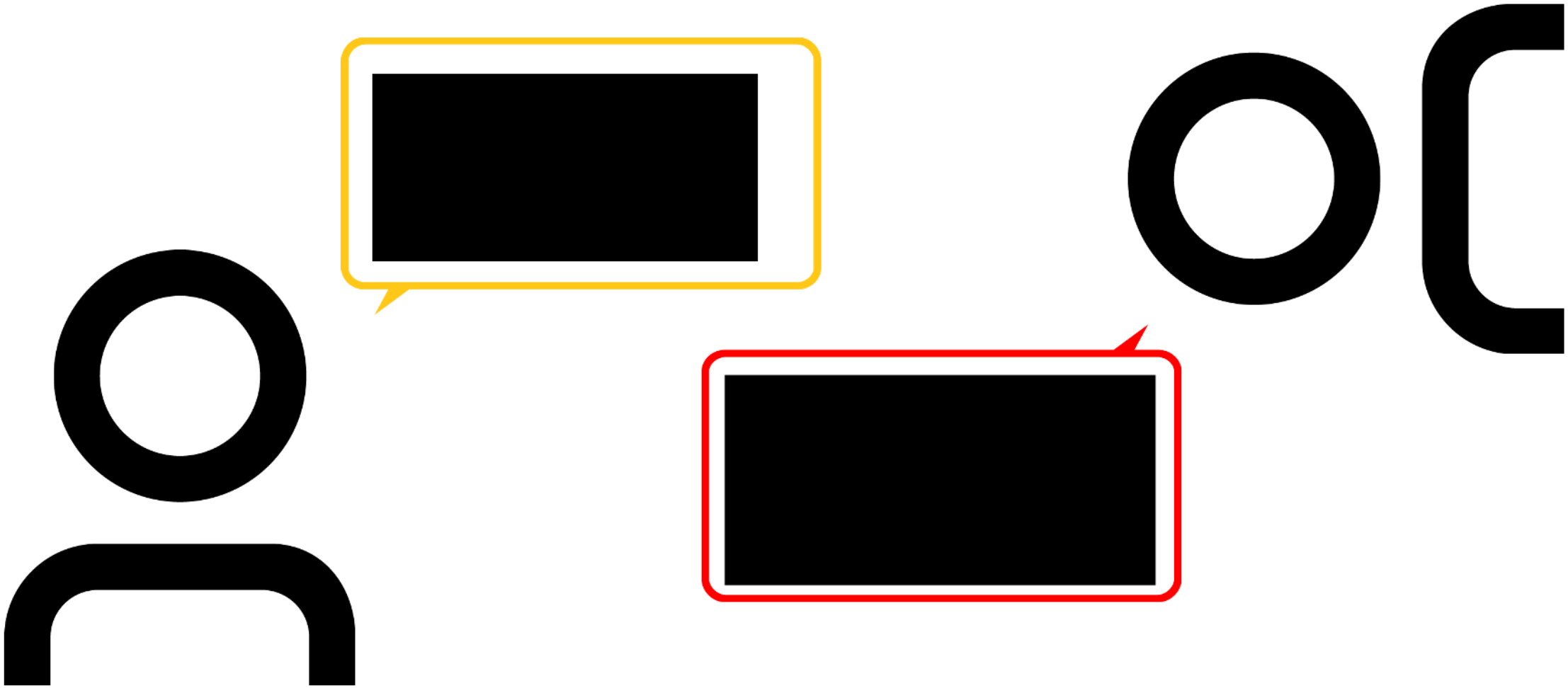
- **Rahmenbedingungen**
  - Laufzeit: Juli 2025 bis Juni 2026
  - Schwerpunktthema: Digitale Transformationen
  - Verantwortliches Bundesland: Sachsen-Anhalt [redacted] mit Vorhabensleitung durch die FITKO [redacted]
- **Projektergebnisse zur 50. Sitzung des IT-Planungsrats (17.6.2026)**
  - Zielarchitektur 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

Digitale Verwaltung. Intelligent vernetzt.

www.fitko.de



FITKO

Anhang

Ausgearbeitete Sicherheitsvorgaben

Vorgehen und Ergebnisse

Sicherheitsvorgaben

Schutzbedarf Normal

Mindestanforderungen und Sicherheits-praktiken für die Absicherung von APIs

auf Basis von „Best Current Practice (BCP) for OAuth 2.0" (Kapitel 2) [RFC9700]

Schutzbedarf hoch & sehr hoch

Erweitertes Hochsicherheitsprofil für OAuth 2.0 und OAuth 2.1

abgeleitet aus aus dem „FAPI 2.0 Security Profile" [FAPI 2.0]

Begleitdokumente

Angreifer Model und Schutzmaßnahmenkatalog auf Basis „Best Current Practice (BCP) for OAuth 2.0" (Kapitel 3 & 4) [RFC9700]

Leitfaden für den Umgang mit Public Clients auf Basis der föderalen API-Autorisierungsinfrastruktur

Nicht veröffentlicht, noch in Bearbeitung

Angreifer Model und Sicherheitsanforderungen auf Basis des „FAPI 2.0 Attacker Model" [attackermodel]

Nicht veröffentlicht, noch in Bearbeitung

Referenzarchi-tektur für Client Registrierung auf Basis der föderalen API-Autorisierungs-infrastruktur

Leitfaden für die Auswahl von Grant Types auf Basis der föderalen API-Autorisierungs-infrastruktur

Nicht veröffentlicht, noch in Bearbeitung

Vorgehen

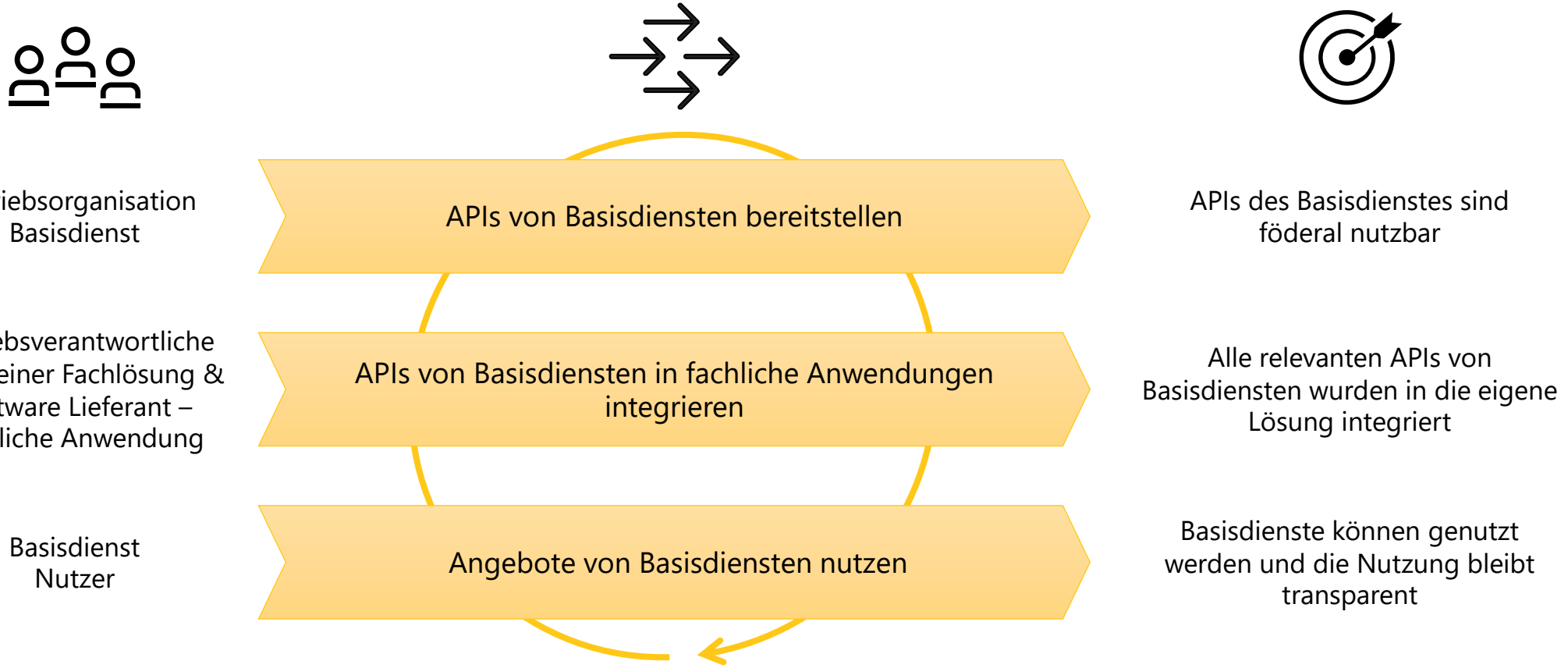
1. Maschinelle Übersetzung aus dem Englischen in das Deutsche
2. Ausdifferenzierung der MUSS/KANN/SOLL-Anforderungen
3. Modulare Erweiterung um ergänzende Anforderungen

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.

FITKO

Fachlicher Umfang der Zielarchitektur

Betrachtung der zentralen Wertströme



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

FITKO

Prozessübersicht aus der Zielarchitektur

Prozesslandkarte der föderalen API-Autorisierungsinfrastruktur*

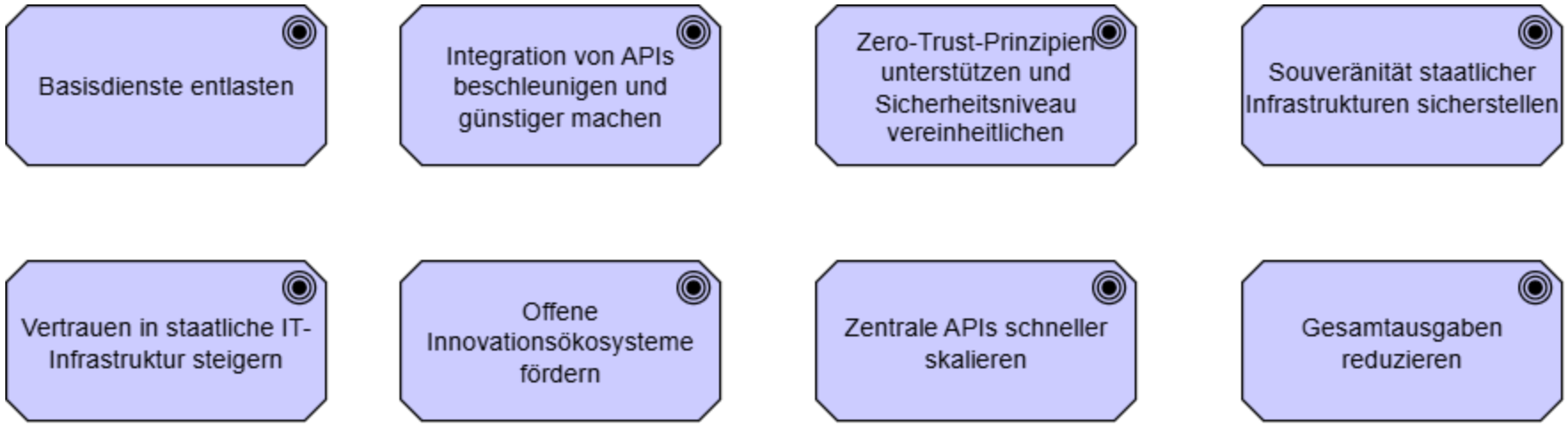
- **Kernprozesse** tragen unmittelbar zur Erbringung des Plattformnutzens bei
- **Supportprozesse** unterstützen den laufenden Betrieb der Infrastruktur

*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

FITKO

Projektspezifische Architekturziele

Acht Ziele operationalisieren die strategische Ausrichtung des Projekts.

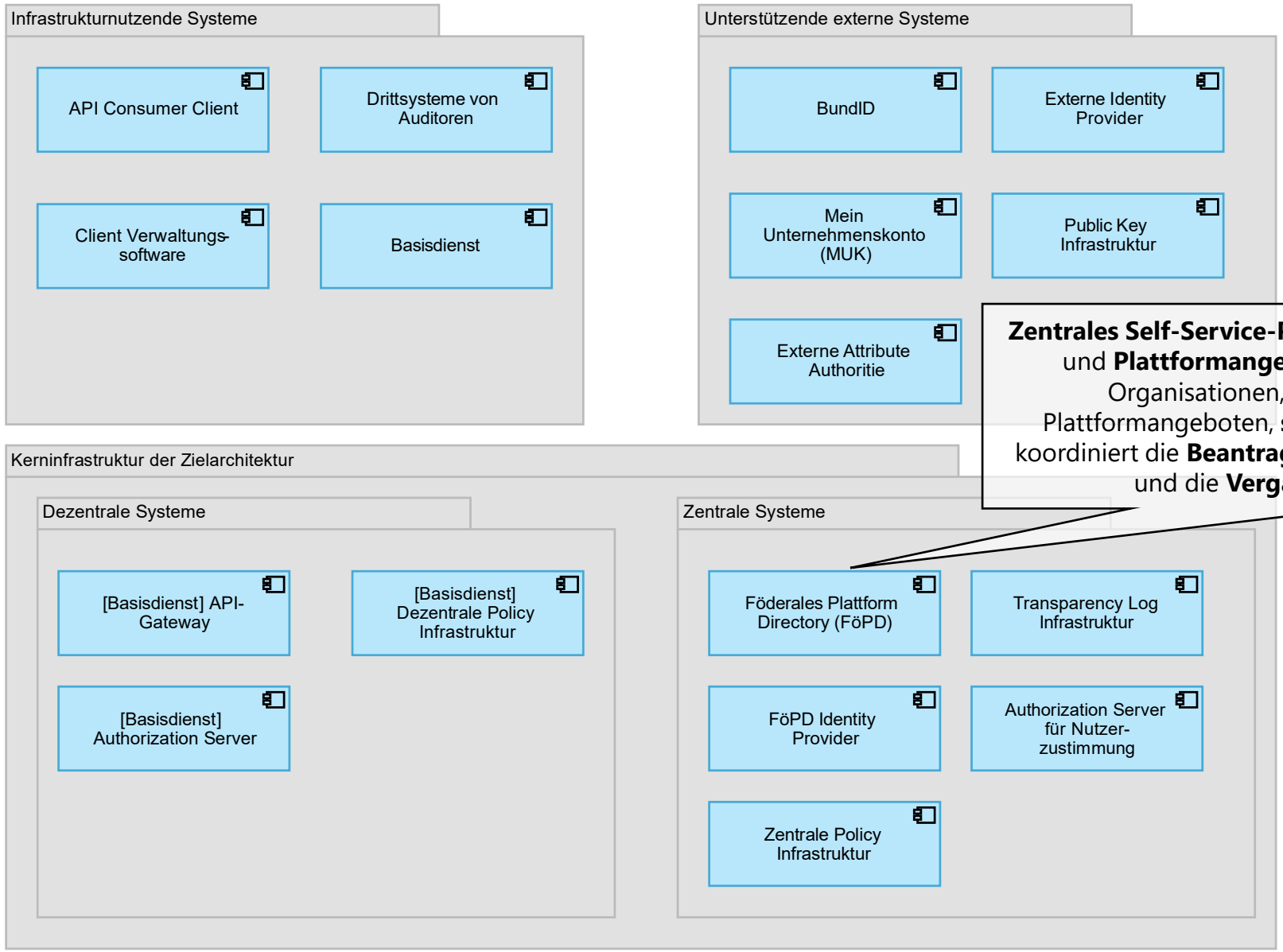


Prinzipienüberblick

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

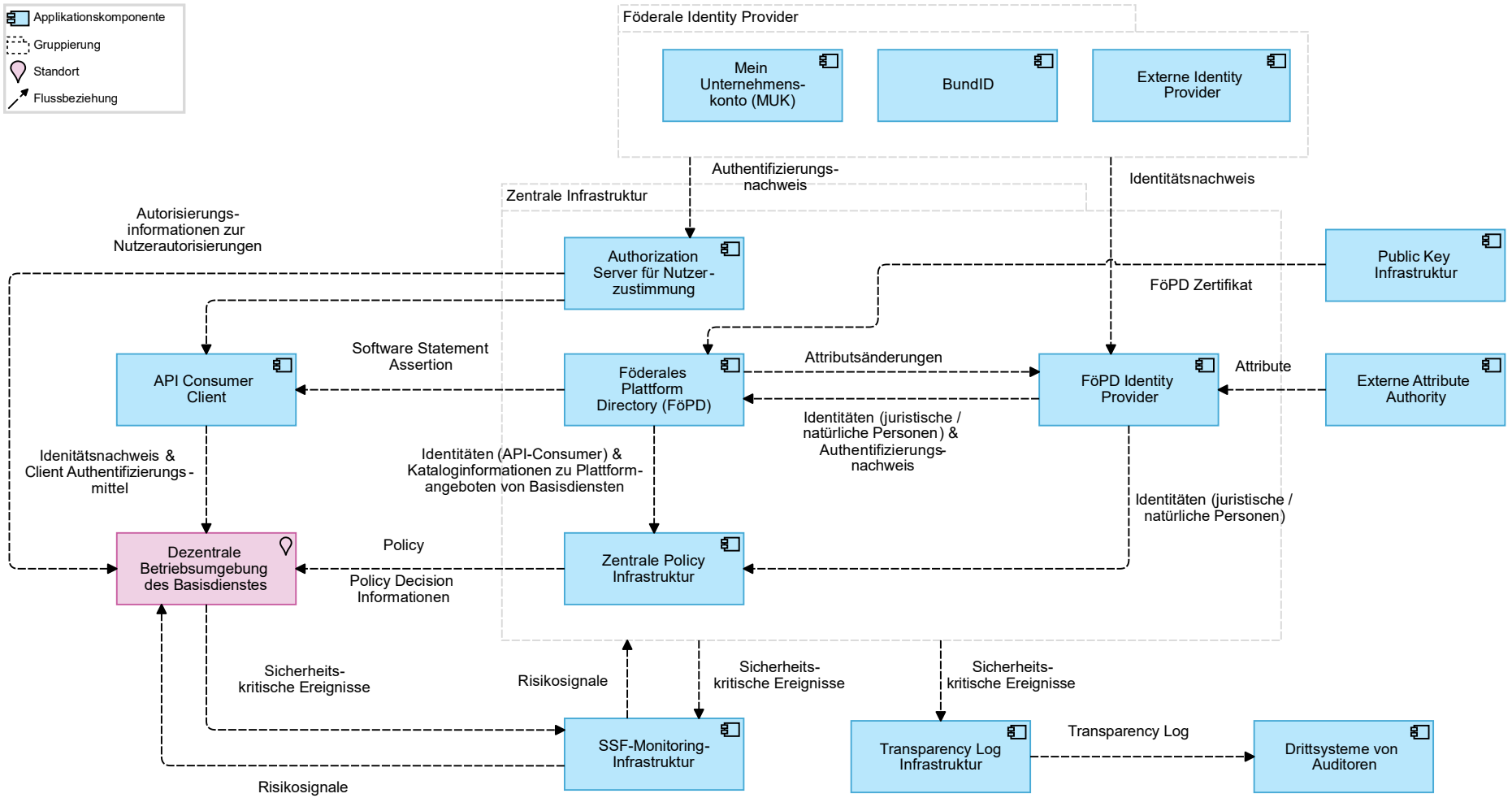


Zentrales Self-Service-Portal und **Single Source of Truth** für **API-Clients** und **Plattformangebote**. Das FöPD steuert die Registrierung von Organisationen, API-Consumer-Software, API-Clients und Plattformangeboten, **stellt Software Statement Assertions aus** und koordiniert die **Beantragungsprozesse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

FITKO

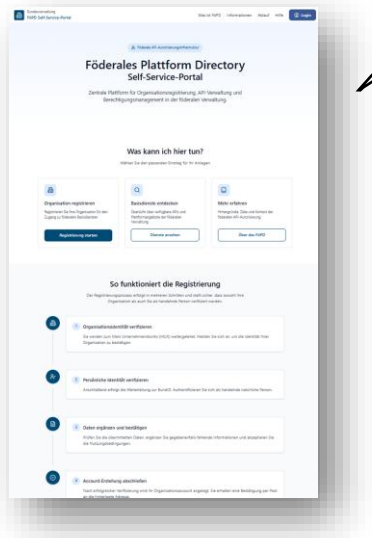
High Level Informationsfluss der föderalen API-Autorisierungsinfrastruktur



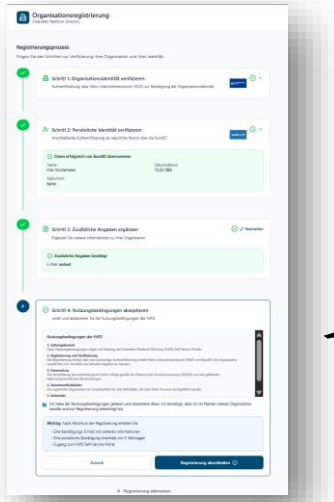
FITKO

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

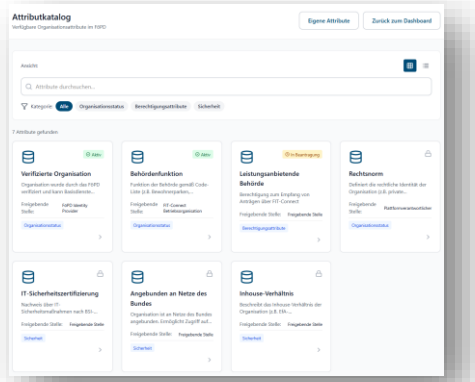
Das Föderale Plattform Directory (FöPD) unterstützt zentrale Kernprozesse der föderalen API-Autorisierung



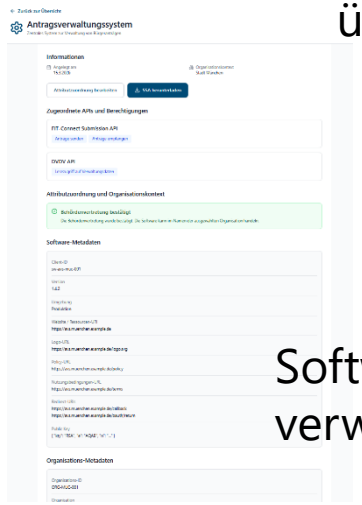
FöPD Landing Page



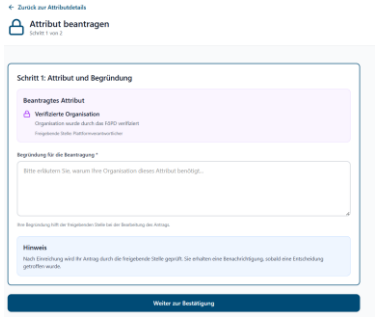
Registrierung



Beantragungs-übersicht



Software-verwaltung



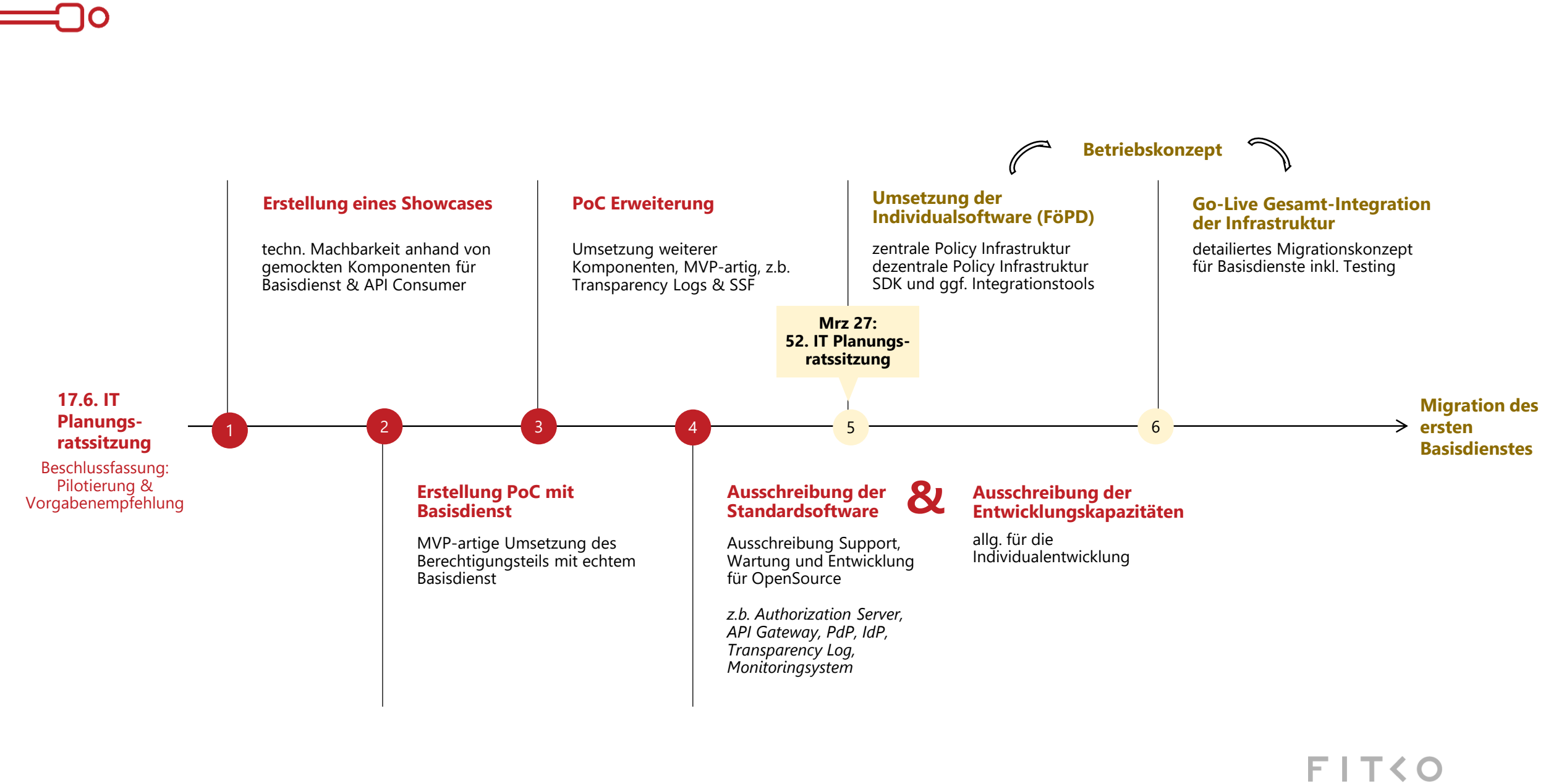
Beantragung

*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.

Kontakt

Digitale Verwaltung. Intelligent vernetzt.

www.fitko.de


Betriebskonzept
Erstellung eines Showcases
techn. Machbarkeit anhand von gemockten Komponenten für Basisdienst & API Consumer
PoC Erweiterung
Umsetzung weiterer Komponenten, MVP-artig, z.b. Transparency Logs & SSF
Umsetzung der Individualsoftware (FöPD)
zentrale Policy Infrastruktur
dezentrale Policy Infrastruktur
SDK und ggf. Integrationstools
Go-Live Gesamt-Integration der Infrastruktur
detailiertes Migrationskonzept für Basisdienste inkl. Testing
Mrz 27: 52. IT Planungs-ratssitzung
17.6. IT Planungs-ratssitzung
Beschlussfassung: Pilotierung & Vorgabenempfehlung
1
2
3
4
5
6
Migration des ersten Basisdienstes
Erstellung PoC mit Basisdienst
MVP-artige Umsetzung des Berechtigungsteils mit echtem Basisdienst
Ausschreibung der Standardsoftware
&
Ausschreibung der Entwicklungskapazitäten
Ausschreibung Support, Wartung und Entwicklung für OpenSource
z.b. Authorization Server, API Gateway, PdP, IdP, Transparency Log, Monitoringsystem
allg. für die Individualentwicklung