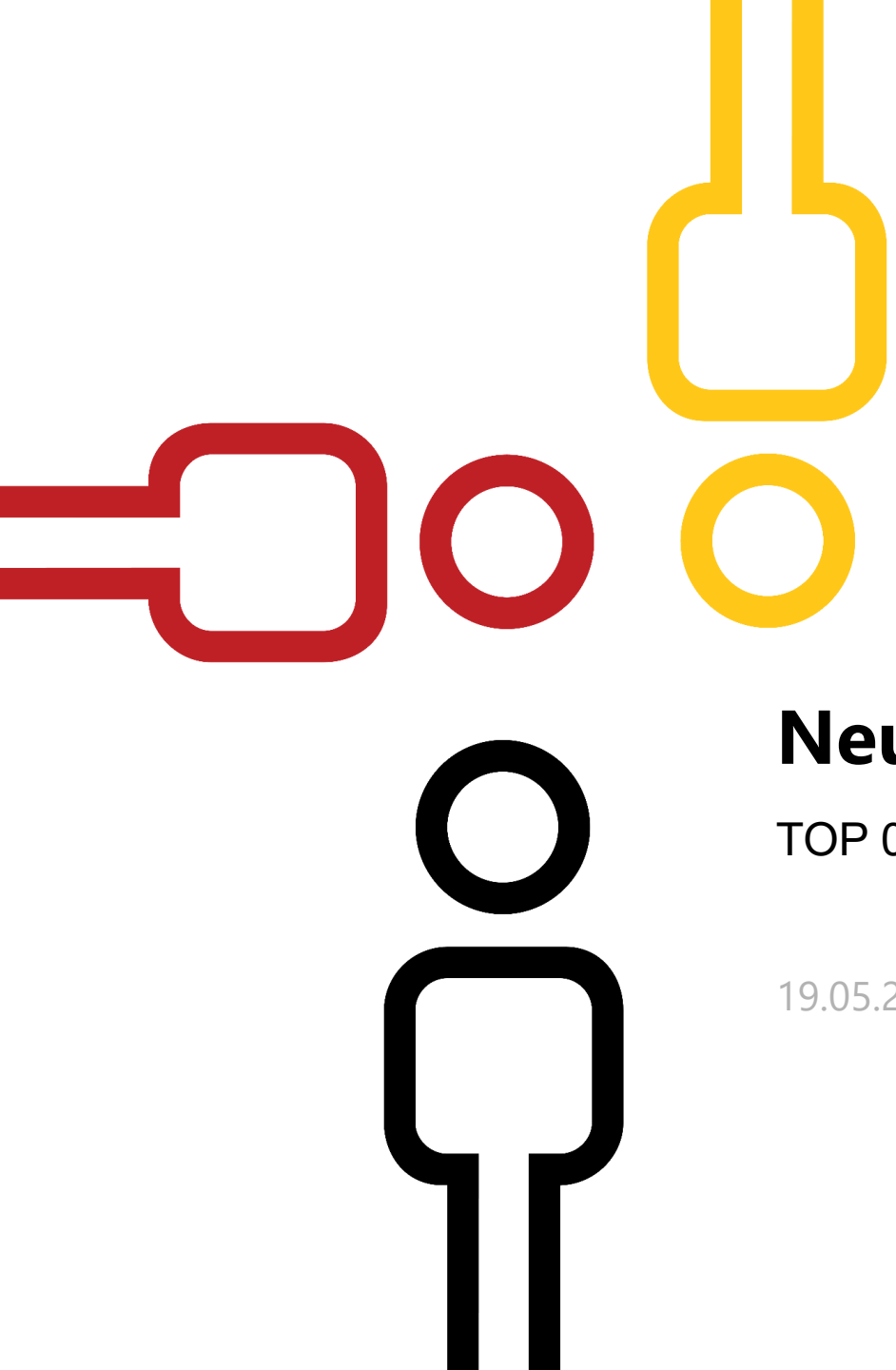


Neukonzeption OSiP

TOP 05

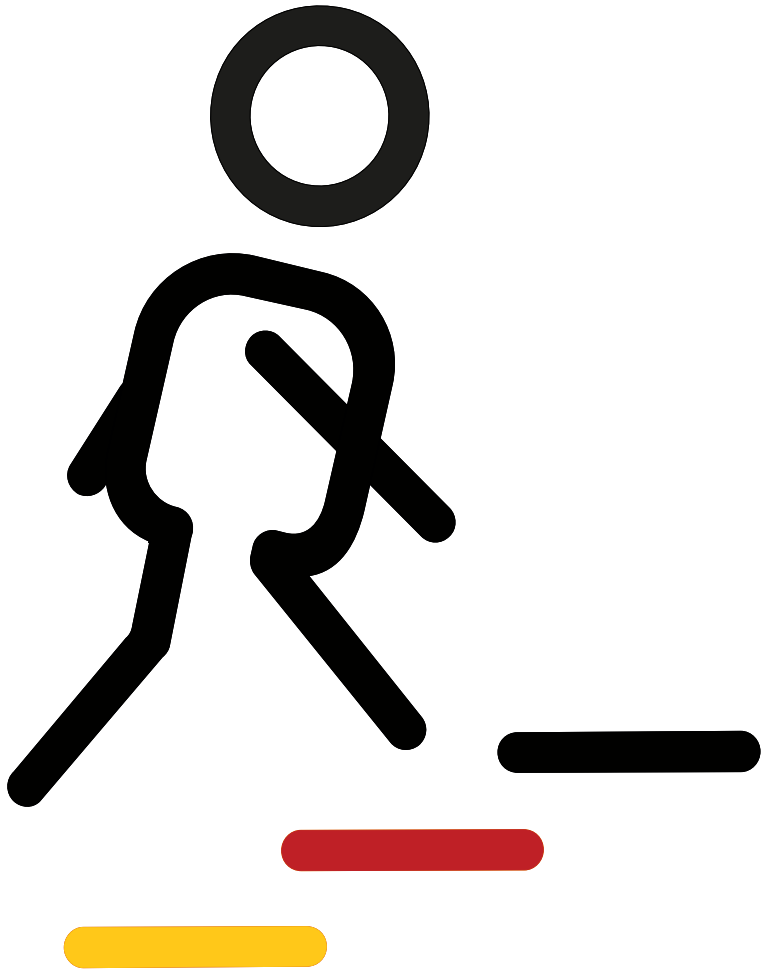
19.05.2026 / FIT-AB / FITKO Architekturmanagement

FITKO

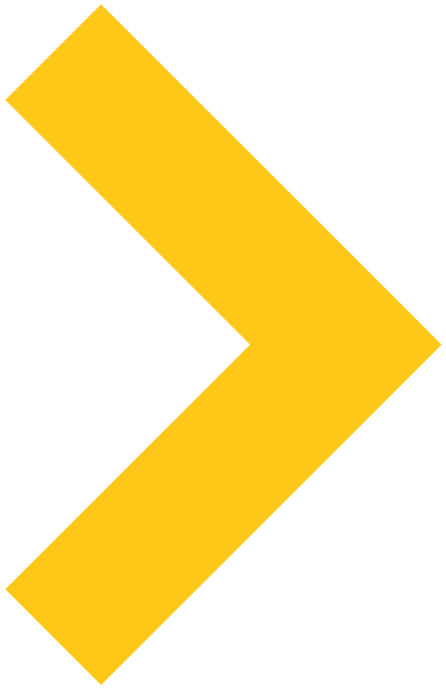
Projektteam

[redacted]

Agenda



1. Der Auftrag
2. Das Kontext
3. Das Architekturkonzept
4. Die offenen Herausforderungen
5. Die Planung

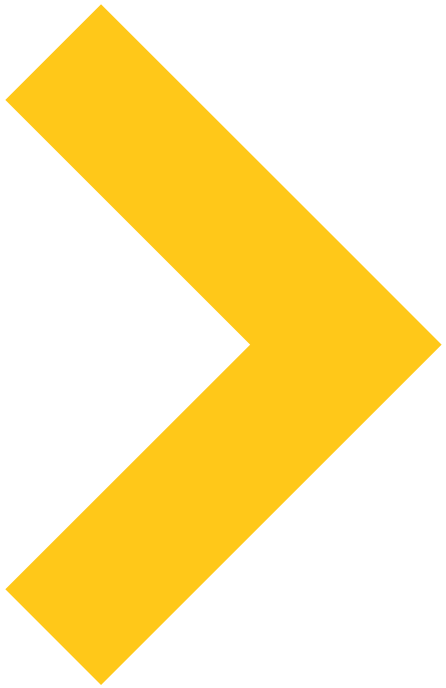


Der Auftrag

Der Auftrag

IT-Planungsrat | 26.03.2025 | 46. Sitzung | Beschluss 2025/20

- Der IT-Planungsrat **beauftragt die FITKO mit der Umsetzung der vorgelegten Planung zu Neukonzeption, Neuentwicklung und Rollout** des Produkts Online-Sicherheitsprüfung (OSiP).
- Der IT-Planungsrat beauftragt die FITKO, unter Einbeziehung der relevanten Fachbehörden und Erkenntnisstellen, eine übergreifende Architektur für eine Zuverlässigkeits- und Sicherheitsprüfung zu erarbeiten, mit den Zielen,
  - eine **medienbruchfreie** und **Ende-zu-Ende-verschlüsselte** Lösung zu entwickeln, die die Prinzipien **Secure- und Data-Protection-by-Design** berücksichtigt und einen **Zero-Trust-Ansatz** verfolgt,
  - die **Komplexität des Betriebs zu reduzieren**,
  - **Robustheit, Effizienz** und **Skalierbarkeit** des Produkts zu steigern sowie
  - die **Homogenisierung von Schnittstellen** für die **unmittelbare Anbindung, Authentifizierung** und **Adressierung** von Fachverfahren und Behördensystemen zu erreichen.
- Nach Abschluss der Konzeptionsphase bittet der IT-Planungsrat die FITKO um die **Vorlage des Architekturkonzepts** zu seiner **49. Sitzung** sowie, falls erforderlich, eines **aktualisierten Umsetzungs- und Finanzierungsplans für die Entwicklung**.



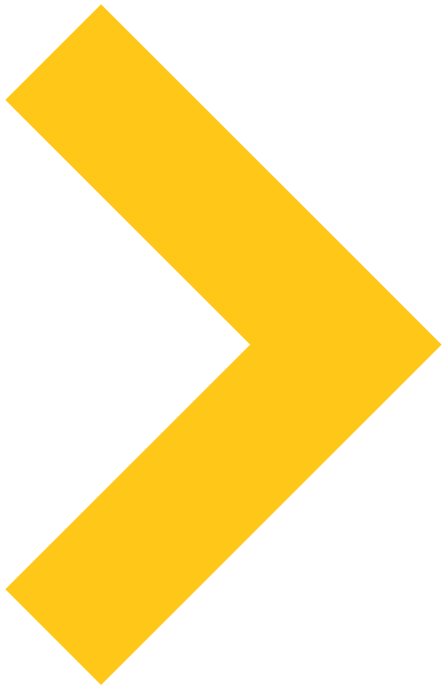
Der Kontext

Der Kontext

Zuverlässigkeits- und Sicherheitsprüfung (ZSÜ)

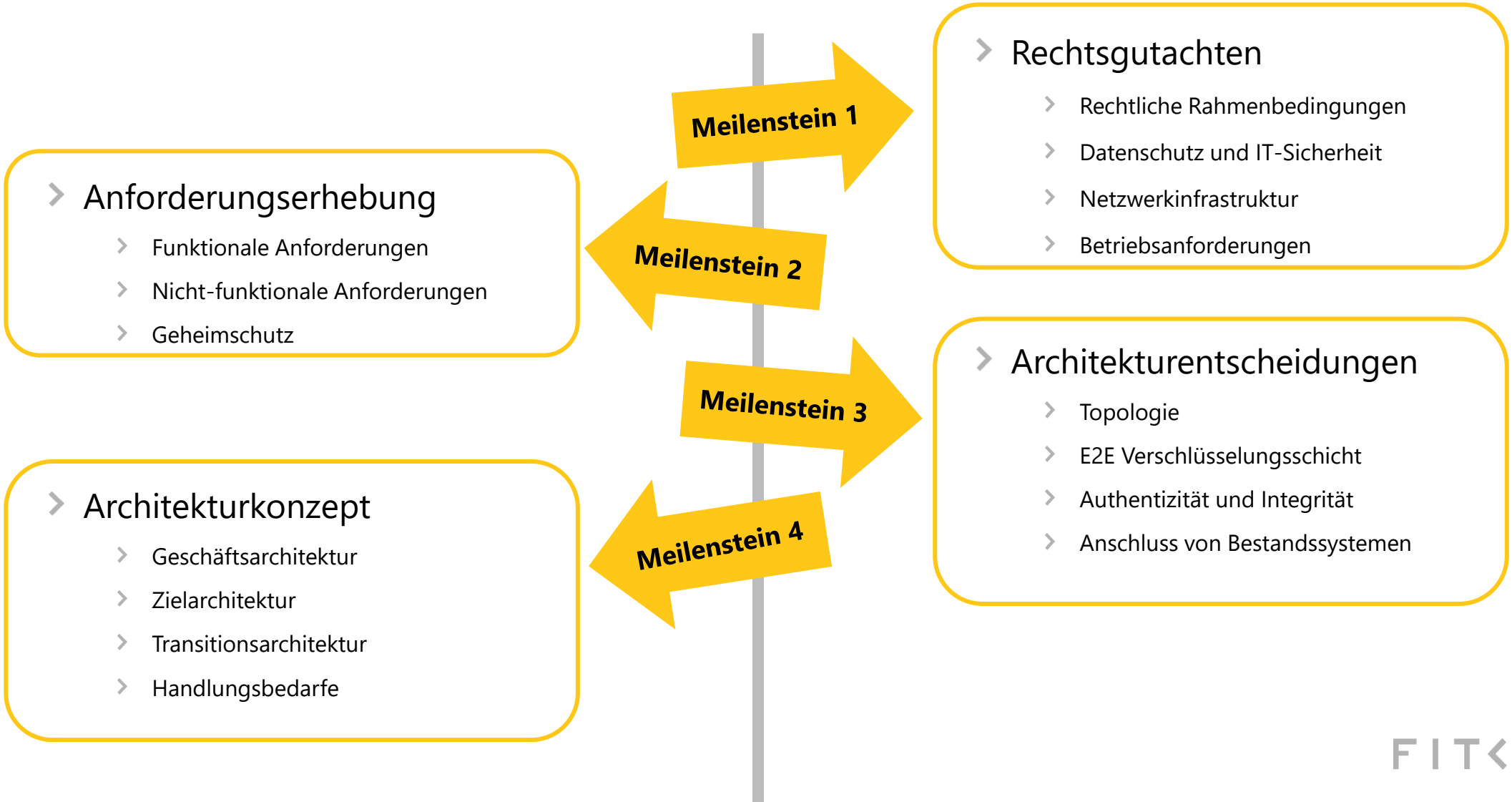
Einschätzung von Personen die mit einer **sicherheitsempfindlichen Tätigkeit** betraut werden sollen oder denen **Zugang zu sicherheitsrelevanten Bereichen** gewährt werden soll.

- 15+ Anwendungsbereiche (bspw. Waffenerwerb, Einbürgerung, Luftsicherheit)
- Verschiedenste Rechtsgrundlagen, Länder- und Bundesgesetze (bspw. Luftsicherheitsgesetz, Staatsangehörigkeitsgesetz, Waffengesetz)
- Fachliche Verantwortung bei Genehmigungsbehörden (bspw. Kreispolizeibehörden, Bezirksregierungen, Landeskriminalämter)
- Erkenntnisse von Polizeien und Registern (bspw. LKA, BKA, LfV, BND, ZStV, BPol, S.I.S)



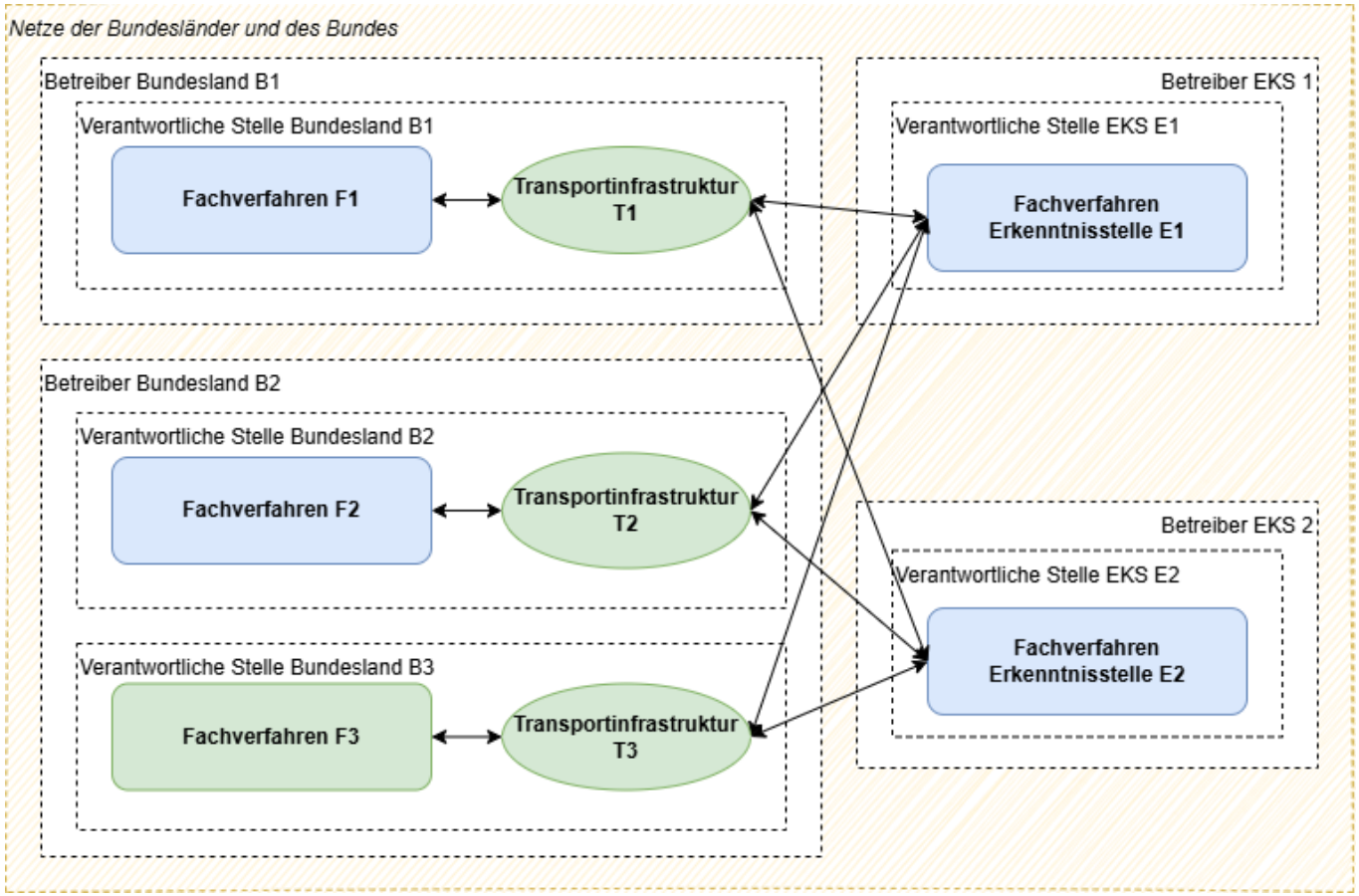
Das Architekturkonzept

Architekturartefakte



- Anforderungserhebung
  - Funktionale Anforderungen
  - Nicht-funktionale Anforderungen
  - Geheimschutz
- Rechtsgutachten
  - Rechtliche Rahmenbedingungen
  - Datenschutz und IT-Sicherheit
  - Netzwerkinfrastruktur
  - Betriebsanforderungen
- Architekturentscheidungen
  - Topologie
  - E2E Verschlüsselungsschicht
  - Authentizität und Integrität
  - Anschluss von Bestandssystemen
- Architekturkonzept
  - Geschäftsarchitektur
  - Zielarchitektur
  - Transitionsarchitektur
  - Handlungsbedarfe

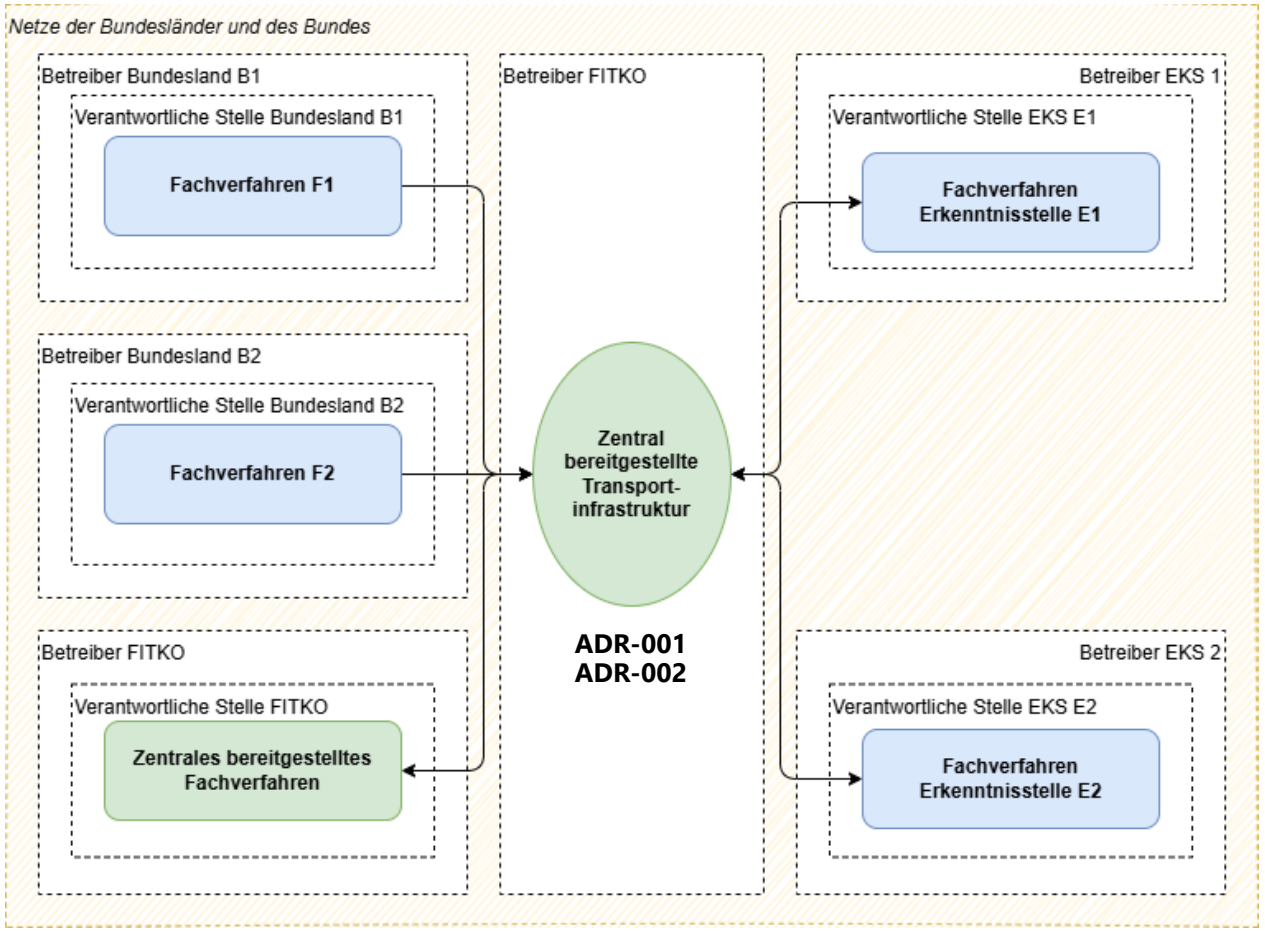
Betriebsmodel Bestandssystem



FITKO entwickelt Software und Länder betreiben eigenverantwortlich

- Eine Instanz der Transportinfrastruktur pro Bundesland
- Eigenverantwortlicher Betrieb durch Länder aber teilweise abgegeben
- Unterschiedliche Versionsstände
- Keine DevOps-Möglichkeiten für Entwicklungsunternehmen

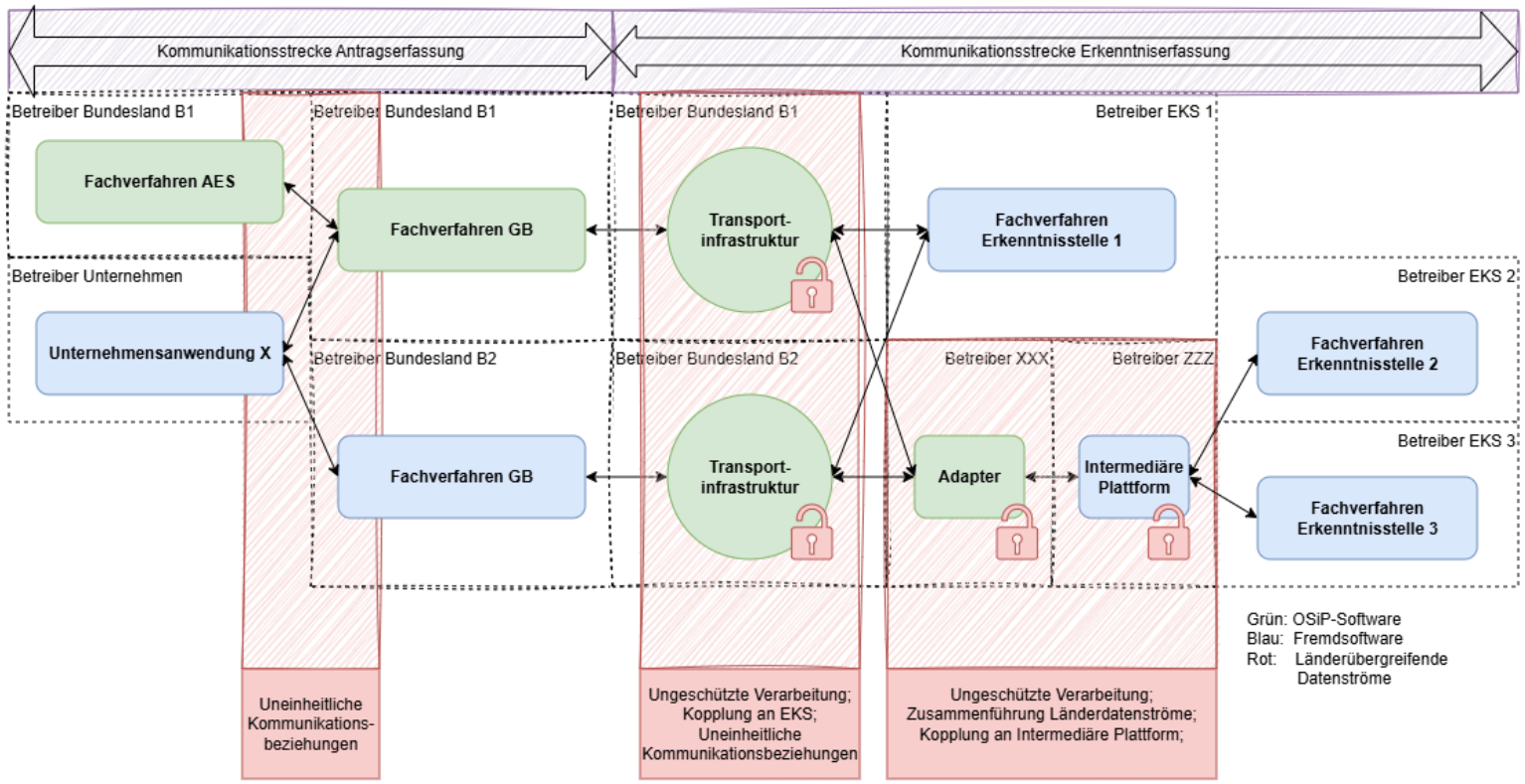
Betriebsmodel Neukonzeption



FITKO entwickelt Software und betreibt zentral

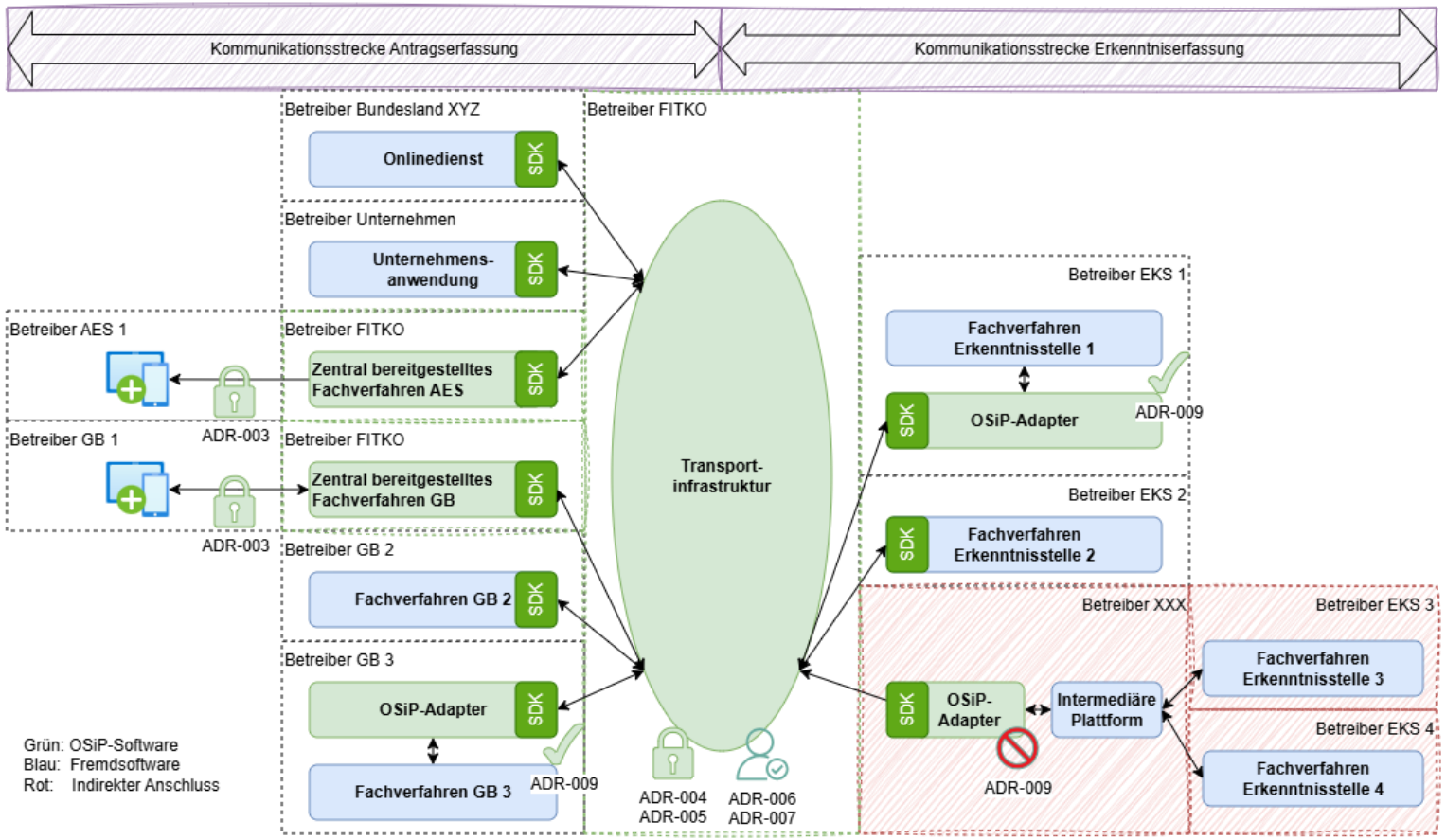
- Eine zentrale Transportinfrastruktur für alle Länder
- Zentral bereitgestelltes Fachverfahren für manche Länder
- Verantwortung Betrieb bei FITKO
- Einheitliches Release-Management
- DevOps Möglichkeiten

Architektur Bestandssystem



1. Uneinheitliche Kommunikationsbeziehungen für Antragserfassung
2. Ungesicherte Datenverarbeitung in Transportinfrastruktur
   - Vertraulichkeit und Integrität nicht gegeben
3. Uneinheitliche Kommunikationsbeziehungen für Erkenntniserfassung
   - Schnittstellen, Sicherheitsmechanismen
4. Kopplung an EKS
   - Transformation und Validierung
5. Gemeinsame Adapter
   - Unklare datenschutz-/rechtliche Verarbeitung
   - Zusammenführung von ungeschützten Datenströmen

Architektur Neukonzeption



- ADR-003 E2EE bis Gerät für zentrales Fachverfahren
- ADR-004 MLS
- ADR-005 E2EE zwischen fachliche verantwortlichen Stellen
  - Keine zentrale Fachlogik
  - Direkte Anbindung Fachverfahren
- ADR-006 V-PKI für öffentliche Stellen
- ADR-007 PKI für private Organisationen
- ADR-008 Bereitstellung SDKs
- ADR-009 Übergangsweise Bereitstellung von Adaptern
  - Betrieb nur in Vertrauenszone der Fachstelle
  - Nur mit Migrationsplanung

Die offenen Herausforderungen

Die offenen Herausforderungen

Konsoli-dierung

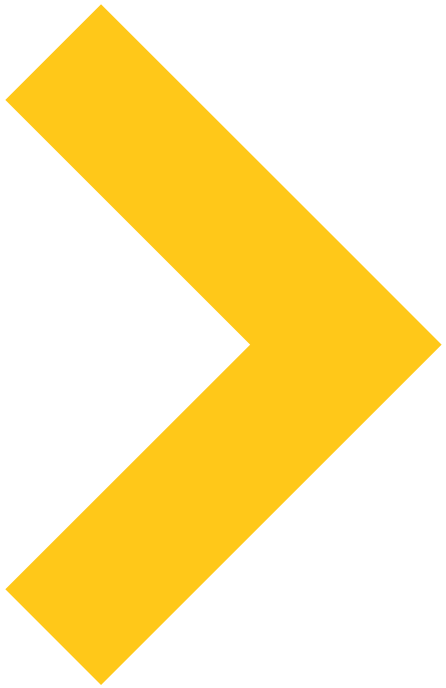
1. Einheitliche Schnittstellen, Datenformate und Prozesse
   - Gemeinsame Gremien, zentrales Releasemanagement, einheitliche Anschlussbedingungen
2. Migrationsplanung für Bestandssysteme
   - Bereitstellung SDKs und übergangsweise Adapter
3. AuthN von natürlichen Personen für zentral bereitgestellte Fachverfahren
   - Sachbearbeiter private Organisationen und öffentliche Stellen
4. Nachweisbarkeit und Zustimmung von Antragstellenden

Nach-nutzung

1. Nachnutzung von FIT-Connect
   - Nur für Antragserfassung zwischen AES und GB
   - Evtl. auch für Erkenntnisübermittlung zwischen EKS und GB
2. Umsetzung Anforderungen der Föderalen API-Autorisationsinfrastruktur
   1. OSiP hat min. hohen Schutzbedarf
3. Perspektivische Integration von NOOTS
   - Nachweise bei Antragserfassung

Geheim-schutz

1. E2E-Digitaler Prozess für VS-Erkenntnisse
   - AuthN und AuthZ von Sachbearbeitenden
   - Schutzklassen und VS-Kennzeichnung von Daten



Die Planung

Roadmap 2026-2027

https://gitlab.opencode.de/fitko/osip/neukonzeption-osip

- **Abschluss Konsolidierung**
  - Anforderungen
  - ADRs
  - Architekturkonzept

- **Abschluss Proof-of-Concept**
  - Umsetzung mit progressiven GB und EKS
  - Ermittlung Personal- und Ressourcenaufwände

2026 — Q4 — 2027 — Q1 — Q4 — 2028

- **Abschluss Abstimmungsphase**
  - Bestandsanalyse Fachverfahren
  - Mengengerüste
  - Finanzierungsbedarfe Fachverfahren
  - Datenformat
  - AWB und übergreifende Prozesse

Offene Diskussion

Da ist zu viel Sicherheit im Architekturkonzept!

OSiP Stakeholder