



Hohe Düne

18./19.03.2026

# Willkommen zum 14. Fachkongress 2026



**FACHKONGRESS**



DES IT-PLANUNGSRATS



**IT-PLANUNGSRAT**

# Digitale Verwaltungsstruktur – Interoperabilität, Skalierbarkeit & sichere M2M-Kommunikation in der Praxis

Deep Dive ins IT-Planungsrat-Portfolio:  
DVDV und Governikus



Hohe Düne  
19.03.2026

Dr. Clemens Fell  
Produktmanagement DVDV

Dr. Jan Wittmann  
Produktmanagement Governikus

# Digitale Verwaltungsstruktur – DVDV

Interoperabilität, Skalierbarkeit und  
sichere M2M-Kommunikation in der  
Praxis



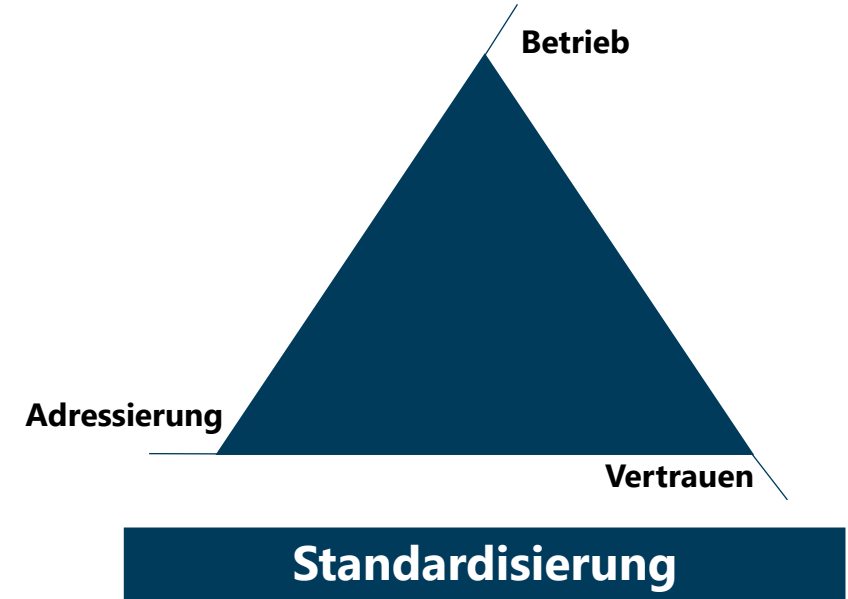
Dr. Clemens Fell  
Produktmanagement DVDV

# Agenda

- Ausgangslage & Zielbild
- DVDV im Überblick
- Technische und operative Sicht
- Nutzung & Mehrwert
- Erfahrungen, Herausforderungen und Entwicklungsperspektiven

# Interoperabilität im Föderalismus: Standards reichen nicht

- **Ausgangslage:** Föderale IT-Landschaft, viele Fachverfahren/Betreiber, trotzdem **durchgängige M2M-Kommunikation** erforderlich
- **Standards (XÖV/OSCI)** definieren Datenformate – lösen aber nicht die Betriebsfragen
- Drei Voraussetzungen für produktive Interoperabilität:
  - **Adressierung** (wohin?)
  - **Vertrauen** (wer?)
  - **Betrieb** (wie stabil/aktuell?)
- **Zielbild:** Verwaltungsübergreifende Kommunikation, die auffindbar, sicher und aktuell ist





# DVDV im Überblick

# DVDV als Infrastruktur-Baustein: Adressierung & Vertrauen

- **Nicht-öffentliches Infrastruktur-Verzeichnis** (föederal getragen) mit technischen Verbindungsdaten
- **Zweck:** Adressierbarkeit von E-Government-Diensten und **eindeutige Authentifizierung** der Kommunikationspartner
- **Ergebnis: vertrauenswürdige Behandlung** der ausgetauschten Daten (operativ abgesichert)
- **Praktische Nutzung:** Fachverfahren nutzen DVDV für **technische Adressierung** und **OSCI-gestützten Austausch** (XML/XÖV-Kontexte)





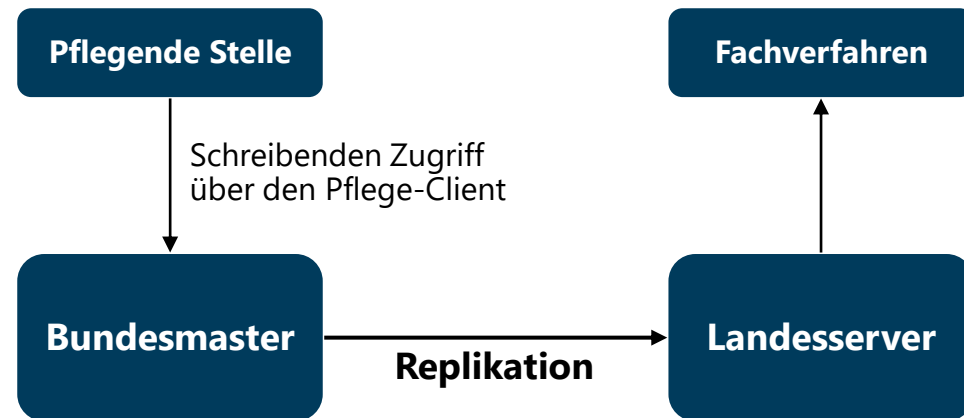
# Technische und operative Sicht

# Integration scheitert selten an Technologie – meist an Betriebsstabilität, Sicherheitspflege und Verantwortlichkeiten

- Erfolg hängt **an korrekten und aktuellen Service-Einträgen** – nicht an „noch einer Schnittstelle“
- Nutzung erfolgt **fördert über Landesserver**: performant, entkoppelt, skalierbar
- Sichere Kommunikation ist **laufender Betrieb**: Zertifikate, Signaturen, Berechtigungen müssen kontinuierlich stimmen
- Zentrale Ausfallursachen sind **Änderungen ohne saubere Pflege**: Endpunkte wechseln, Zertifikate laufen ab, Zuständigkeiten sind unklar
- Konsequenzen: **klare Verantwortlichkeiten und nachvollziehbare Change-Prozesse** sind Voraussetzung für Vertrauen und Stabilität

# Konsistenz durch zentrale Schreibhoheit – Skalierung und Resilienz durch föderiertes Lesen

- **Schreiben (Referenz):** nur im **DVDV-Bundesmaster** durch berechnigte Pflegende Stellen
- **Lesen (Skalierung):** Abfragen laufen über **Landesserver**, nicht über den Bundesmaster
- **Replikation** Bundesmaster → Landesserver: Lastverteilung + Ausfallsicherheit (gegenseitiges Einspringen)
- **Sicherheitsprinzip:**
  - Bundesmaster nicht am Internet
  - Rollen/Rechte über IAM



# DVDV ist nur so gut wie die Pflegeprozesse – Datenqualität ist eine Betriebsaufgabe

- Änderungen kommen aus Behörden/Betreiber (z.B. Portale): Endpunkte, Kontakte, Parameter, Zertifikate
- Rolle „Pflegerische Stelle“: prüfen, validieren, pflegen (Governance + Qualitätssicherung)
- Herausforderung bundesweit:
  - **Datenqualität & Pflegefähigkeit** in der Fläche (Melden/Ändern sauber möglich?)
  - **Governance & Verantwortungsketten** (Rollen klar, Validierung verbindlich)
  - **Skalierung in der Föderation** gelingt nur mit einheitlichen Pflege-/Change-Prozessen



# Nutzung & Mehrwert

# Mehrwert im Betrieb: weniger bilaterale Abstimmung, mehr Skalierung



**Interoperabilität:** verlässliche Parameterbasis statt individueller Abstimmung



**Wiederverwendbarkeit:** ein Dienst → viele Konsumenten ohne neue Adressierungslogik



**Skalierbarkeit/Resilienz:** föderiertes Lesen + zentrale Schreibhoheit (Bundesmaster) → performant & Konsistenz



**Sicherheits- & Compliance-Fähigkeit:** klare Rollen-/Rechte, nachvollziehbare Changes

# Kontakt

## Dr. Clemens Fell

Produktmanagement DVDV, Marktplätze

Clemens.Fell@fitko.de

+49 (69) 401270 196

<https://www.fitko.de/produktmanagement/dvdv>



# Produktfamilie Governikus

Infrastruktur für Datentransport,  
Identitäten und Vertrauensdienste



Dr. Jan Wittmann  
Produktmanager Governikus


# Governikus in der föderalen Digitalstrategie




**Digitale  
Transformation**




**Digitale  
Infrastruktur**



**Digitale  
Anwendungen**



**Datennutzung**



**Informationen-  
sicherheit**

# Agenda

- Strategische Zielbilder
- Technische Basisfähigkeiten
- Einordnung Governikus
- Datentransport, Identitäten, Trust Services
- Cloud, Interoperabilität, Architektur
- Steuerung im PM-Modell

# Strategische Zielbilder des IT-Planungsrats und ihre technische Bedeutung

**Diese Ziele kennen wir alle – aber was bedeuten sie eigentlich konkret auf technischer Ebene?**

- Digitale Souveränität ist ein zentrales Leitprinzip der föderalen IT-Steuerung.
- Interoperabilität ist Voraussetzung für durchgängige digitale Prozesse.
- Cloud-Orientierung für flexible, skalierbare und moderne Betriebsmodelle.
- Wiederverwendbarer Basisdienste statt isolierter Einzellösungen.

# Technische Basisfähigkeiten für föderale Verwaltungsdigitalisierung

Welche technischen Fähigkeiten muss Verwaltung besitzen, um genau das leisten zu können?

Sicherer Datentransport

Sichere Identitäten

Sichere Daten/-nutzung/-integrität

- Diese Fähigkeiten werden von vielen unterschiedlichen Fachverfahren gleichartig benötigt.
- Sie ermöglichen eine sichere und standardisierte Zusammenarbeit zwischen Behörden.
- Erst durch diese Infrastruktur wird die praktische Umsetzung strategischer Zielvorgaben möglich.



# Sicherer Datentransport als Voraussetzung föderaler Zusammenarbeit

## Wie tauschen Ihre Behörden heute sensible Daten föderal und rechtssicher aus?

- Vertraulichkeit, Integrität und Nachweisbarkeit als Grundanforderungen
- Medienbrüche und Insellösungen in der Praxis
- Standardisierter, interoperabler Datentransport notwendig
- Technische Basis: Verschlüsselung und Zertifikate
  - realisiert durch Dienste der Anwendung Governikus
  - gemäß nationalen und europäischen Richtlinien und Standards/Normen

# Vertrauenswürdige digitale Identitäten

## Wie stellen wir sicher, dass digitale Identitäten organisationsübergreifend vertrauenswürdig sind?

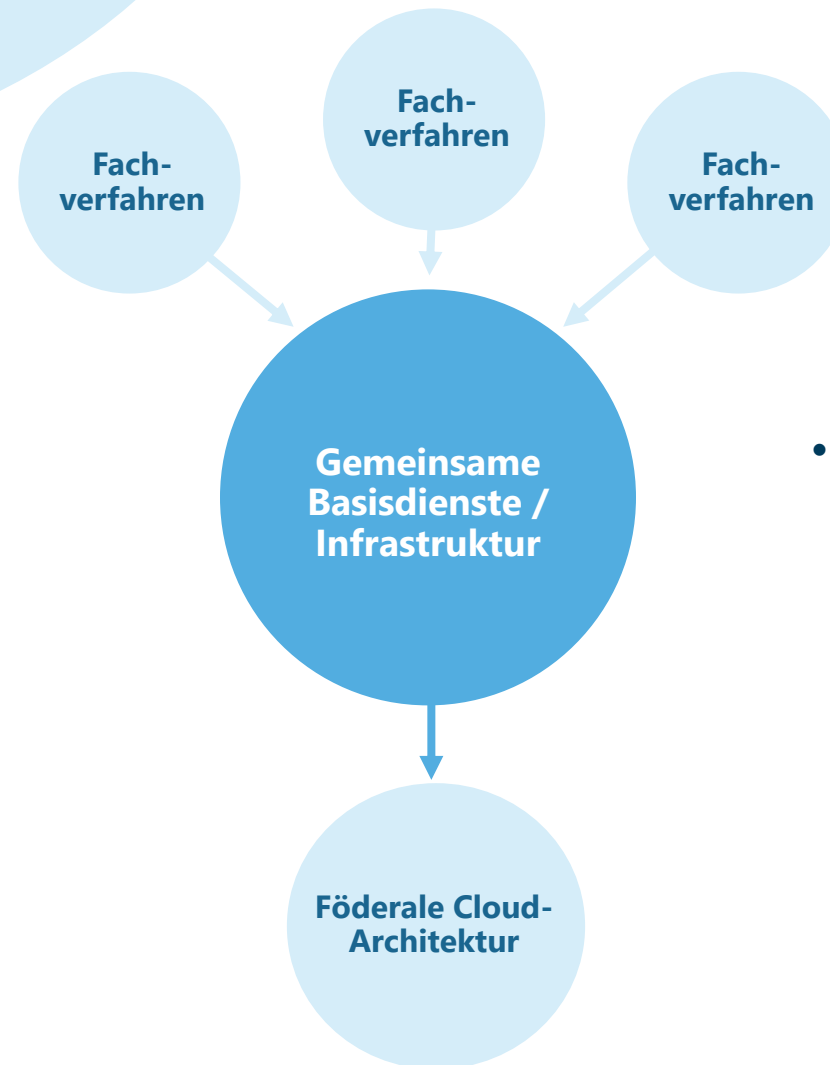
- Eindeutige, überprüfbare Identitäten als Voraussetzung digitaler Prozesse
- Vertrauensdienste und eID als Grundlage
- Organisationsübergreifende Prüfung notwendig
- Rechtssichere Authentifizierung für OZG-Leistungen
  - unterstützt durch Komponenten der Anwendung Governikus

# Sichere Daten und Trust Services als Grundlage rechtssicherer Digitalisierung

## Welche Nachweise brauchen wir in der Verwaltung wirklich: Unveränderbarkeit, Signatur, Siegel, Prüfung?

- Schutz vor Manipulation und Verlust
- Integrität, Vertraulichkeit und Nachweisbarkeit
- Revisions sichere Dokumentation
- Digitale Souveränität über Verwaltungsdaten
  - realisiert durch Trust-Services der Anwendung Governikus

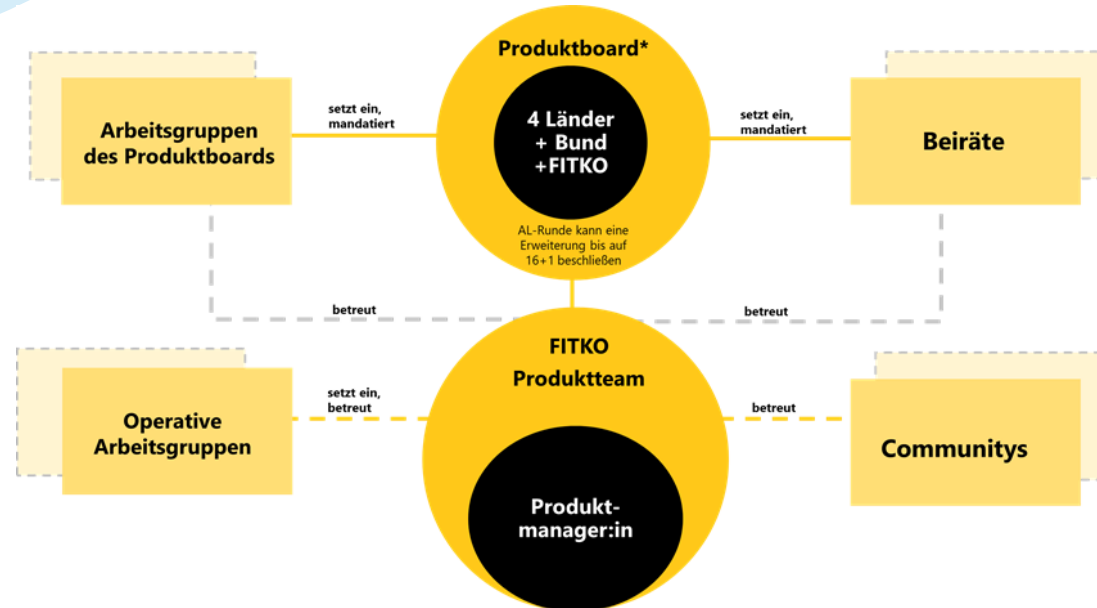
# Warum gemeinsame Infrastruktur Voraussetzung für föderalen Cloud-Betrieb ist



- Infrastrukturbausteine wie Governikus stellen diese gemeinsamen Basisdienste in der Praxis bereit.



# Steuerung im PM-Modell des IT-Planungsrats



- Einordnung im PM-Modell der FITKO (Steuerungsansatz 3)
- Steuerung durch ein Produktboard (7 Länder + Bund)
- Governikus als Produktverantwortlicher

# Kontakt

## **Dr. Jan Wittmann**

Produktmanager

[Jan.wittmann@fitko.de](mailto:Jan.wittmann@fitko.de)

+49 (69) 401270 197

[www.fitko.de](http://www.fitko.de)

## **Janine Lindemann**

Leitung Project Management Office

[Janine.lindemann@governikus.de](mailto:Janine.lindemann@governikus.de)

+49 (151) 23629212

[www.governikus.de](http://www.governikus.de)

# Danke!



## Noch Fragen ?