abraxas

IAM PTI

Identity und Access Management als Schlüssel zur sicherern Zusammen-arbeit von Polizeikorps

Silvano Fari | 17.03.26 | öffentlich

Rückblick

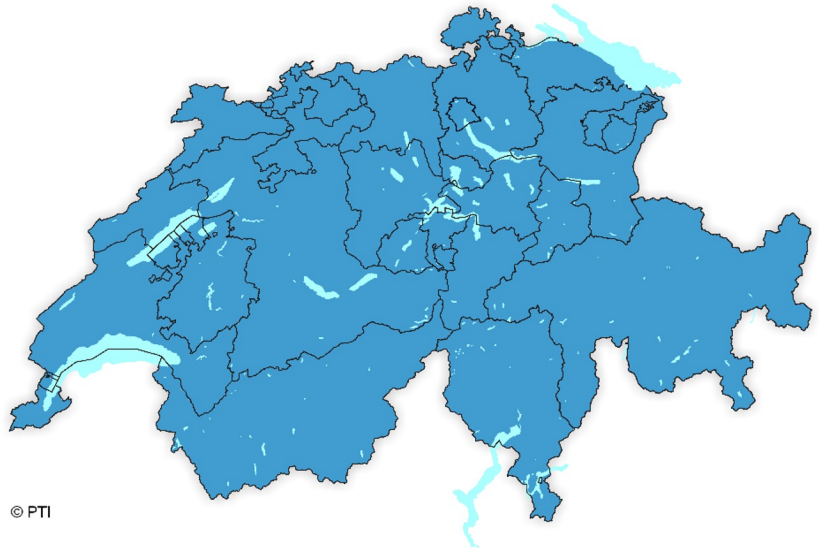
Ursprung IAM HPI/PTI

- **2017**: Start des Projekts *IAM HPI/PTI* (KKJPD)

- **Zielsetzung**
  - Vermeidung redundanter, manueller Benutzerverwaltungen
  - Einführung eines **Single Sign-On (SSO)**
  - **Beteiligung aller Korps inkl. Bund**

- **Umsetzungsansatz: Drei Phasen**

- **Produktivsetzung 2018**
  - Mit Anbindung der Applikationen IMP & OAWR
  - Gefolgt von weiteren Applikationen

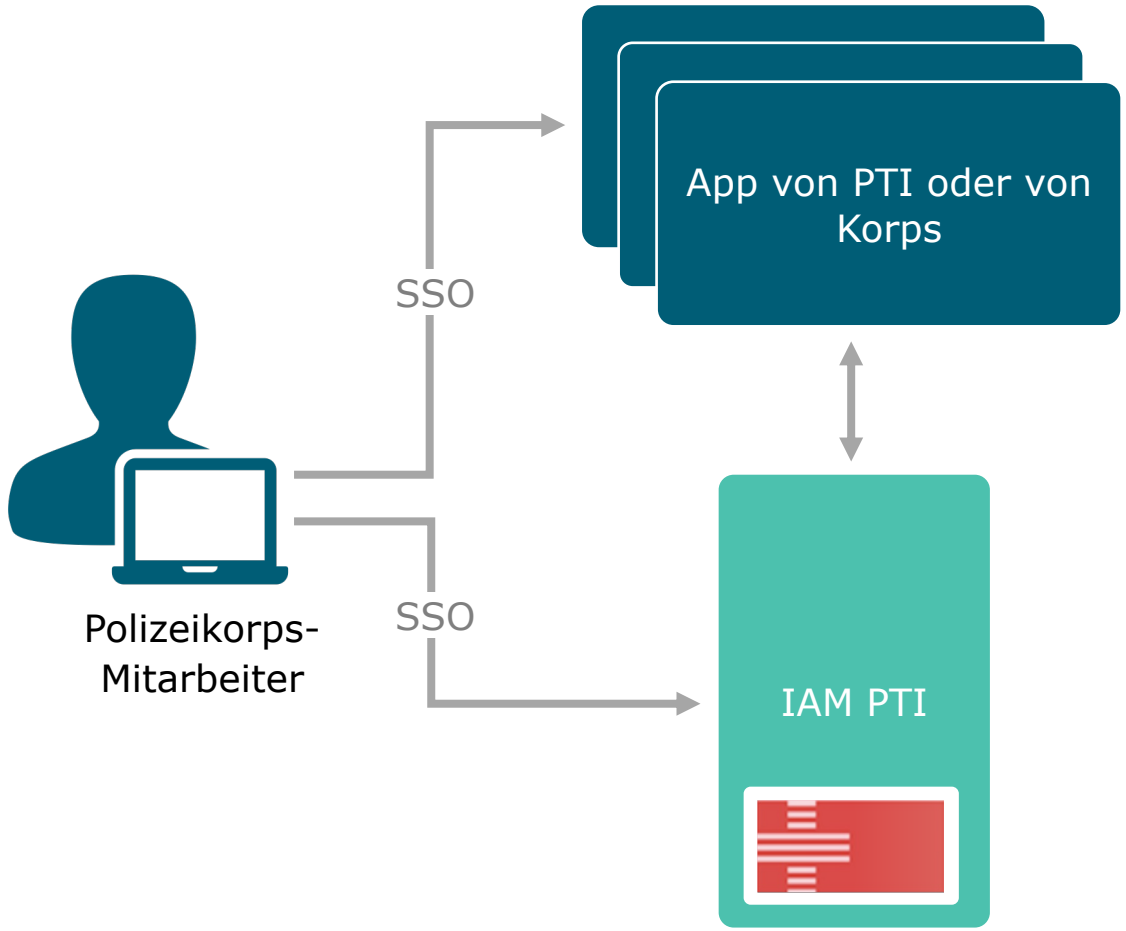


Agenda

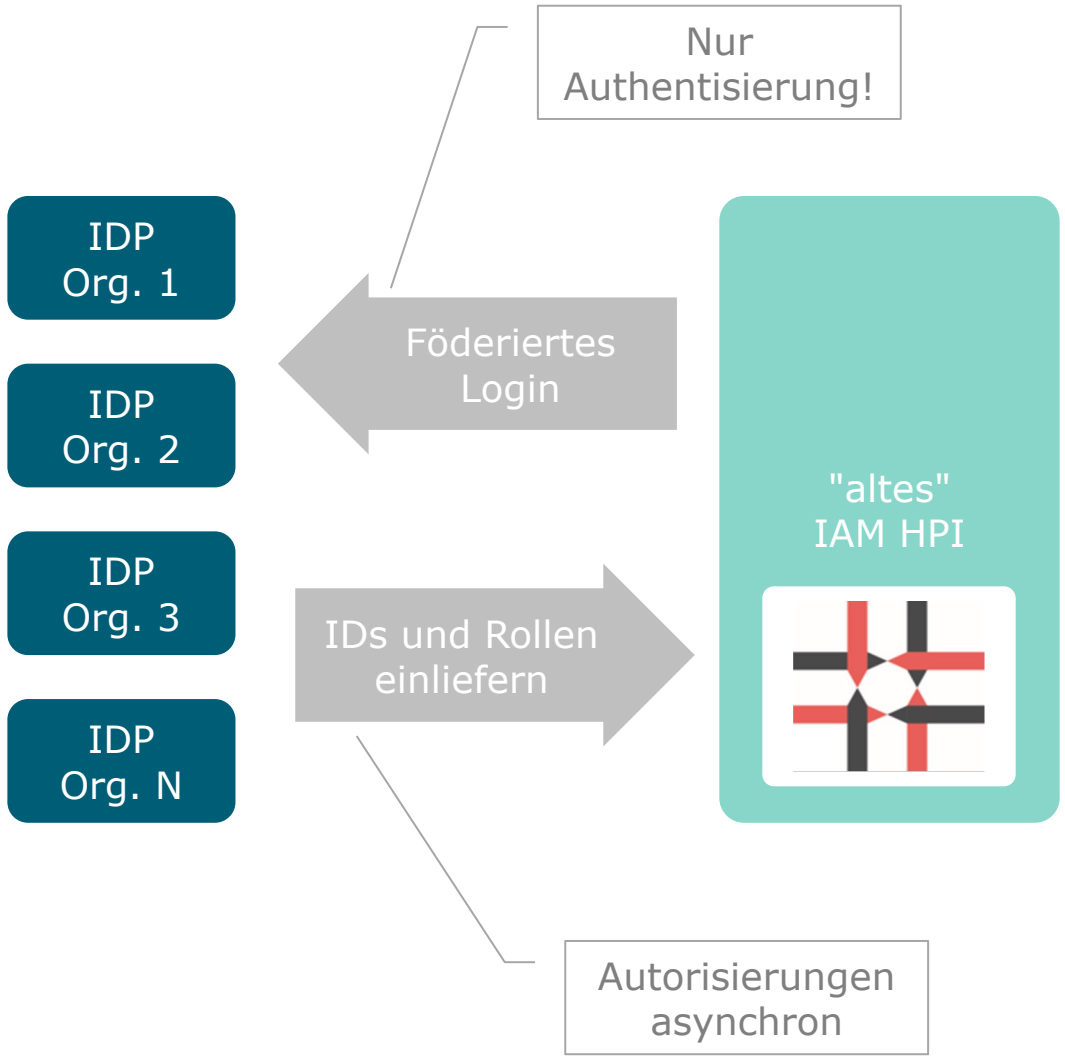
1. Was ist der Nutzen vom IAM PTI?
2. Was war die Ausgangslage?
3. Zielbild: Was ist neu am IAM PTI?
4. Wie lief der Neuaufbau ab?
5. Was waren die Herausforderungen?
6. Wo stehen wir heute mit dem IAM PTI?
7. Fazit

Was ist der Nutzen von IAM PTI?

- Identity und Access Management PTI ist das **Fundament zur digitalen korpsübergreifenden Zusammenarbeit**
- Erlaubt es einfach Applikationen zwischen Korps zu teilen bei gleichbleibend **hoher Datensicherheit**
- Erlaubt einfachen, **sicheren und benutzerfreundlichen Zugang** zu Applikationen mittels Single Sign-On (SSO)



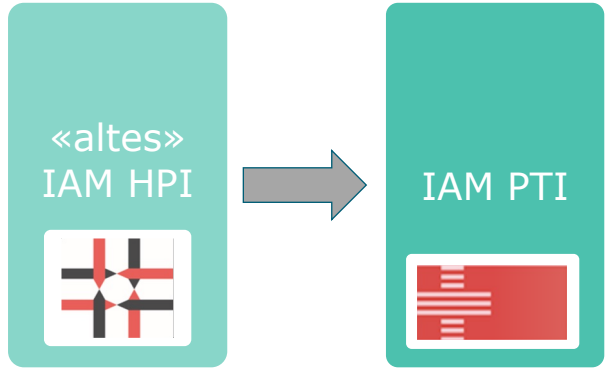
Was war die Ausgangslage?



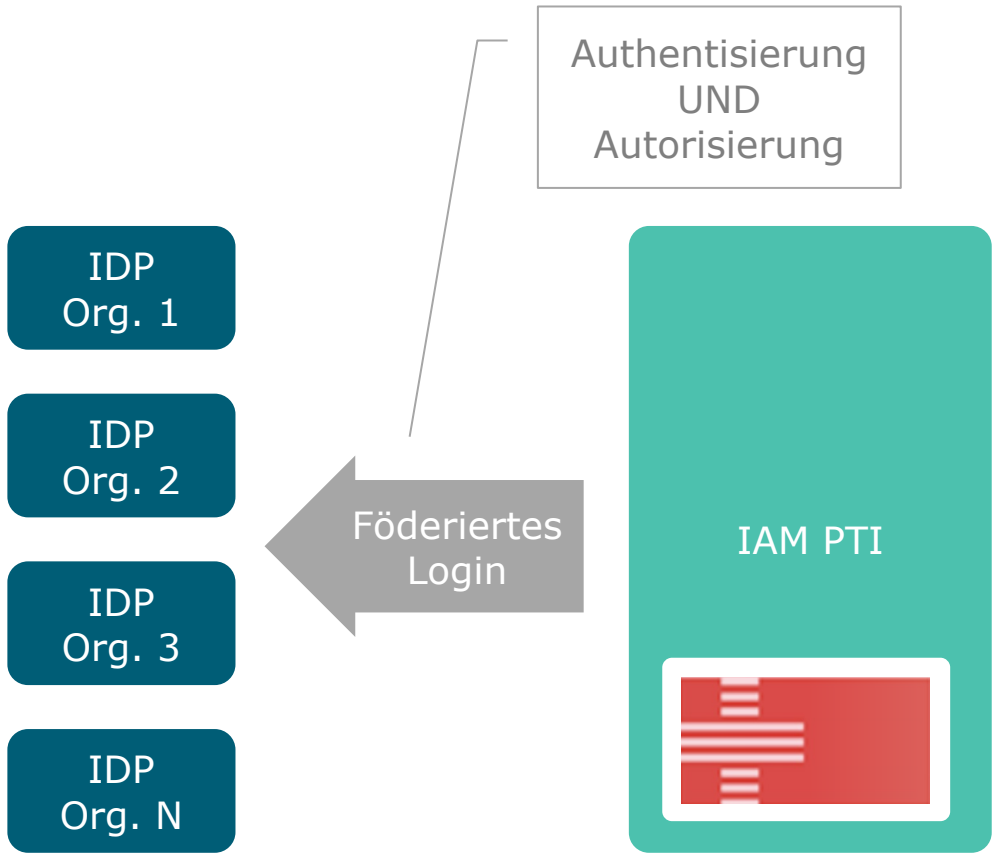
- IAM HPI entstand auf Basis eines Produktes, das bei der Kapo ZH bereits eingesetzt wurde.
- Authentisierung (Identitätsnachweis) wurde über föderiertes Login gemacht.
- Identitäten und Rollen auf Applikationen von Korps-Mitarbeiter mussten **via Sedex ins IAM HPI eingeliefert** werden.
- Nicht föderierte Organisationen konnten ihre Identitäten selbst verwalten,
- Bis Ende 2024 gab es das «alte» IAM HPI noch.

Motivation für das IAM PTI NextGen

- Für die Einlieferung der Identitäten und deren Rollen entstanden **Aufwände** bei den Korps, teilweise mussten Daten von verschiedenen Source-Systemen zusammengezogen werden.
- Aufrechterhaltung der Datenaktualität und der **Datenqualität** für Identitäts- und Berechtigungsdaten war herausfordernd und fehleranfällig.
- **Verwaltungsoberfläche** für Identitäten gehörte nicht zum Standardprodukt, war nicht optimal, war komplex und generierte dadurch Supportaufwände.
- Gewählte **Architektur** verhinderte effizientes Wachstum hinsichtlich neuer Anbindungen von Applikationen und IDPs.
- IAM HPI war **nicht wirtschaftlich skalierbar.**

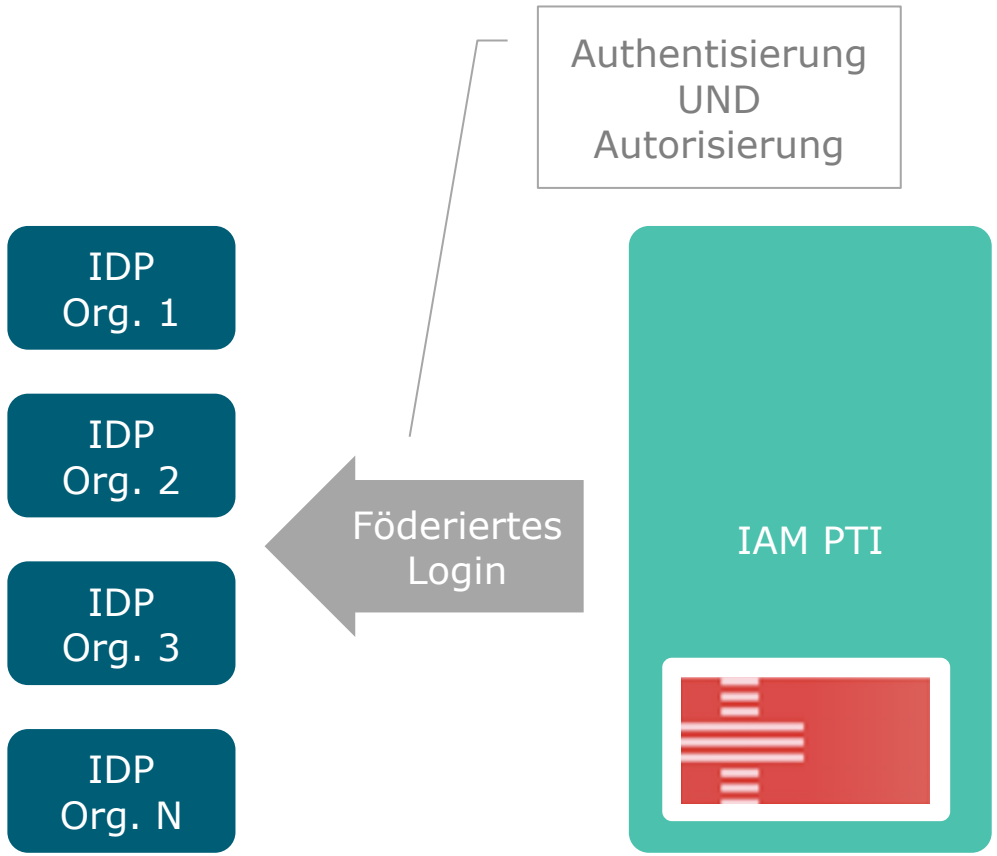


Zielbild: Was ist neu am IAM PTI?



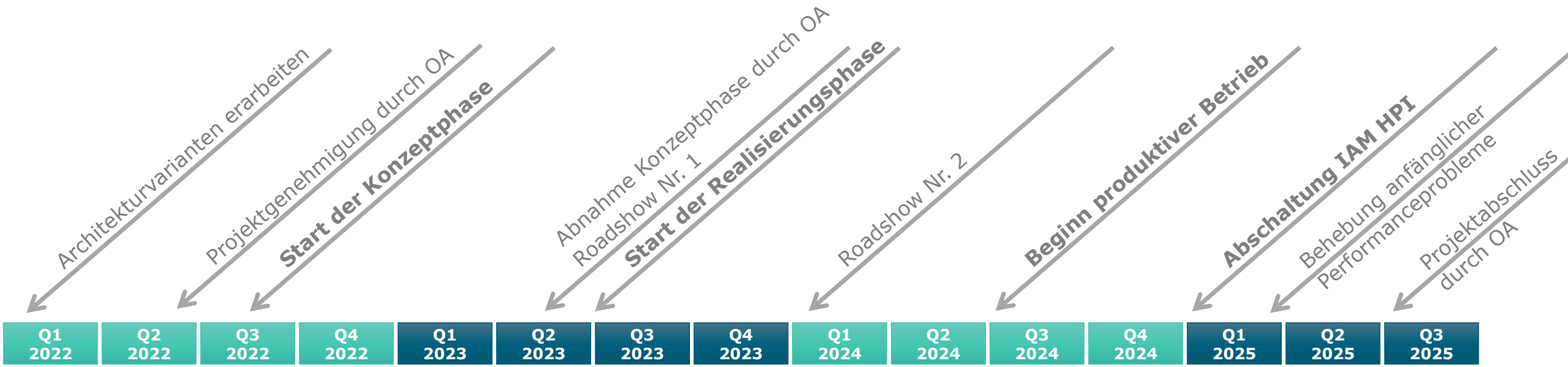
- IAM PTI föderiert (benutzt) das **Login von den Korps**, somit wird Authentisierung (Identitätsnachweis) und Autorisierung (Berechtigungen) übernommen.
- Somit werden Identitätsdaten und Rollen beim Login in **«Echtzeit»** übermittelt - sind somit immer aktuell!
- **Rollen auf Applikationen** können über etablierte Prozesse direkt auf den Korps IDP verwaltet werden.
- Identitäten und Rollen können über das Benutzerinterface eingesehen werden.
- **Starker 2. Faktor** für lokale Logins

Zielbild: Was ist neu am IAM PTI?



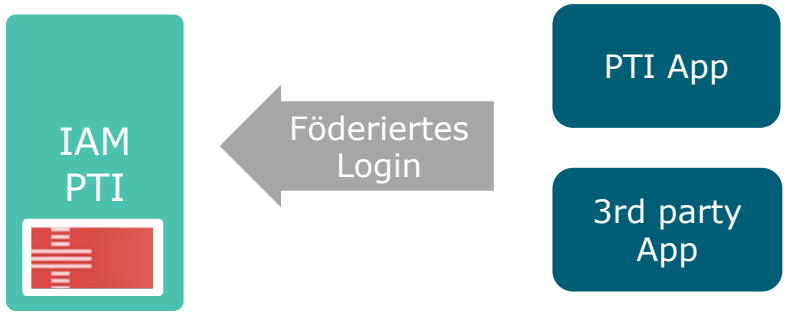
- Einsatz von etablierten **IAM- und WAF-Services der Abraxas** sowie Betrieb im KDC (KAPO Zürich Datacenter)
- Fokus auf **«neue» Protokolle** (OpenID Connect) bei der Anbindung von Applikationen und Identitäts-Providern
- Klar **definierte Blueprints** für die Applikationsanbindung
- Intuitives **Benutzer-Interface** zur Verwaltung von Identitäten für nicht föderierter Organisationen
- Transparentes und faires **Preismodell**

Wie lief der Neuaufbau des IAM PTI ab?

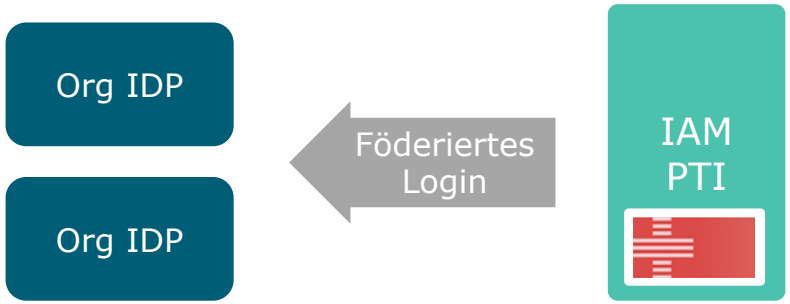


Was waren die Herausforderungen?

Applikationsanbindung



IDP-Anbindung



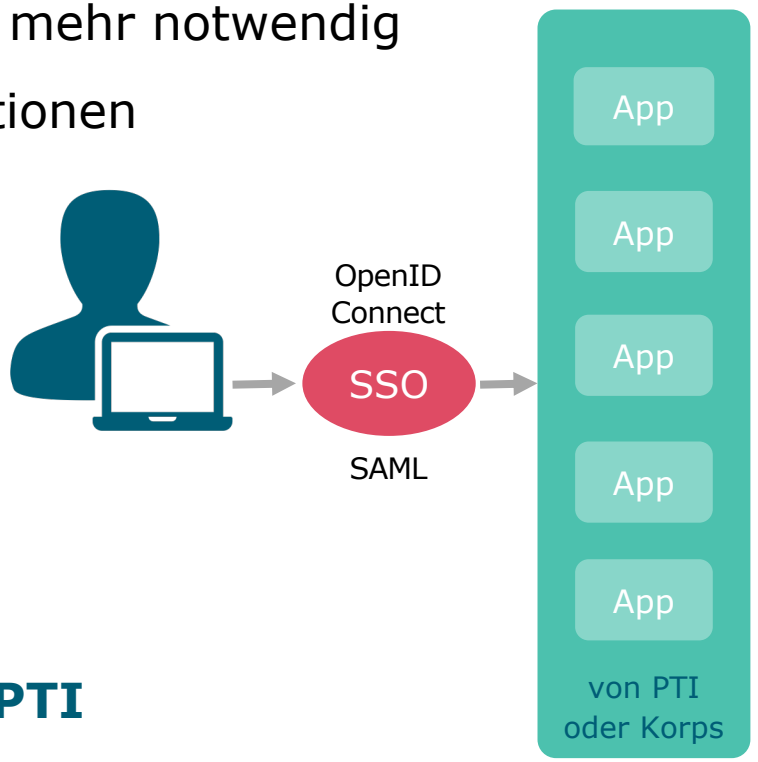
- **KDC** als Service Provider für Dritte war eine Herausforderung.
- **Applikationsanbindungen** dauerten länger als eingeplant:
  - Aufgabenteilung nicht von Anfang an klar IAM, WAF
  - Komplexität und Aufwand unterschätzt
  - Fehlendes Know-How auf Applikationsseite
  - Optimierung von Prozesse und Dokumentationen
- Wechsel von **Netzwerkadressen** für IAM PTI und PTI-Applikationen im KDC -> Schwierigkeiten mit Erreichbarkeit (KomBV/KTV) von verschiedenen Geräten verschiedener Korps
- Identitäts-Provider wurden alle mit **OpenID Connect** angebunden, was Herausforderungen mit der Erreichbarkeit der Organisations-IDP nach sich zog.
- Einige Korps brauchten bei der Umsetzung **Unterstützung**, um neben der Identität auch Rollen im Token mitliefern zu können.

Wo stehen wir heute mit dem IAM PTI?

- Zielbild wurde wie spezifiziert umgesetzt
- **68** geführte **Organisationen** im IAM PTI
- **27 föderierte Organisationen** -> im Projekt konnten neue föderiert und bestehende teilweise gleich auf Entra ID migriert werden
- **13 PTI-Applikationen** (inkl. AFV über eIAM, eOBV, MEF)
- **10 Korps-Applikationen**
- Bundesorganisationen mittels Föderation anzuschliessen in Arbeit

Fazit: Wo liegt der entscheidende Vorteil?

- **Voll föderative Lösung**: Keine Provisionierung der Benutzer mehr notwendig
- **IM-as-a-Service** oder **Full Service PTI**, für kleine Organisationen
- **Moderne technische Standards**
  (OIDC und SAML, JSON Web Token) für die Föderations- und Applikationsanbindungen
- Sichere Authentisierung mit
  Mobile Access App als zweiten Faktor
- **Besseres Benutzererlebnis** für Nutzer und Administratoren
  (bessere Login-Screen & Admin-GUI)
- Solide Grundlage für **dedizierte Mandanten-URL und SSO PTI**
  => Lösungen wie ILB



Wir sind ready für weitere Korps-Applikationen!

KKPKS CCPCS
PTI TIP
2026: 5 Jahre PTI - 5 ans TIP

Fragen & Anmerkungen

Vielen Dank