

# **IAM TIP**

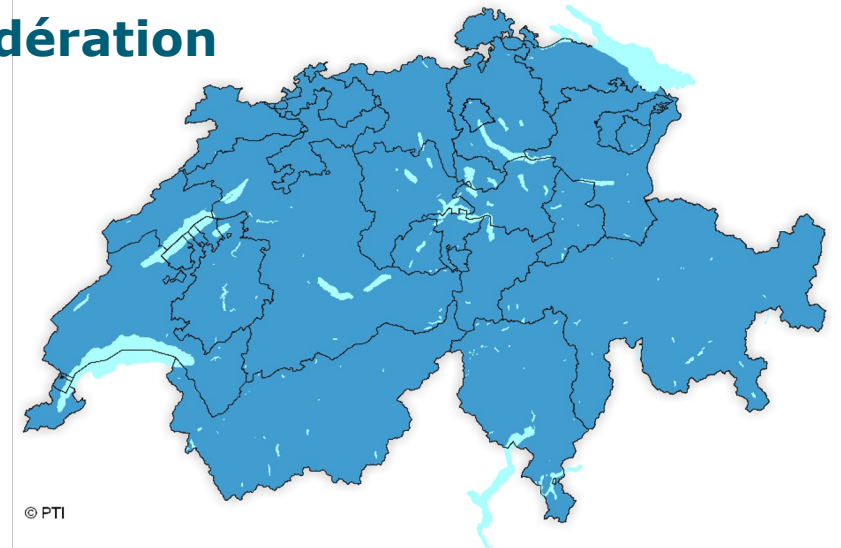
**Identity and Access Management : la clé d'une collaboration sûre entre les Corps de police**

Silvano Fari | 17.03.26 | public

# Rétrospective

## Origine IAM HIP/TIP

- **2017** : lancement du projet *IAM HIP/TIP* (CCDJP)
- **Objectifs**
  - Éviter les gestions redondantes et manuelles des utilisateurs
  - Introduction d'un **Single Sign-On (SSO)**
  - **Participation de tous les Corps, y compris la Confédération**
- **Approche de mise en œuvre : trois phases**
- **Mise en production 2018**
  - Avec connexion des applications IMP et OAWR
  - Suivi d'autres applications

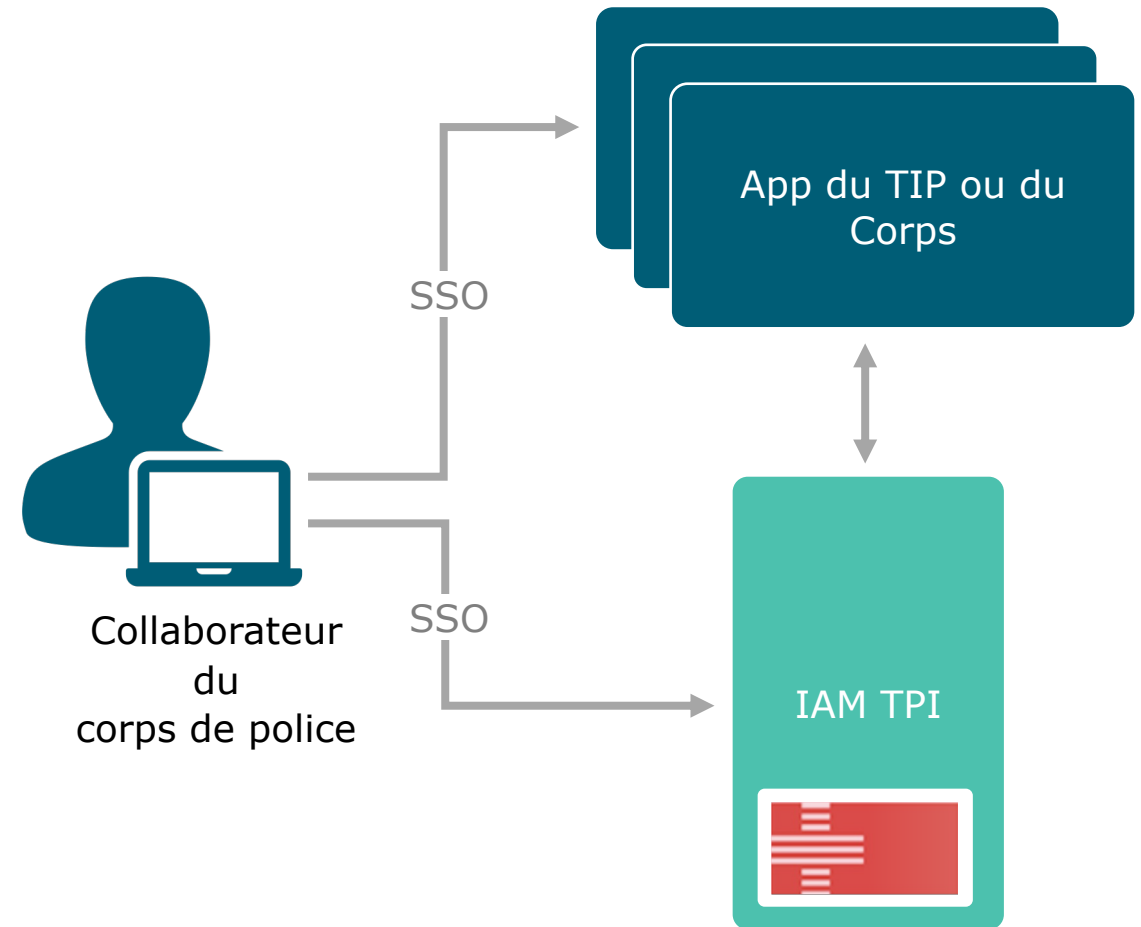


# Ordre du jour

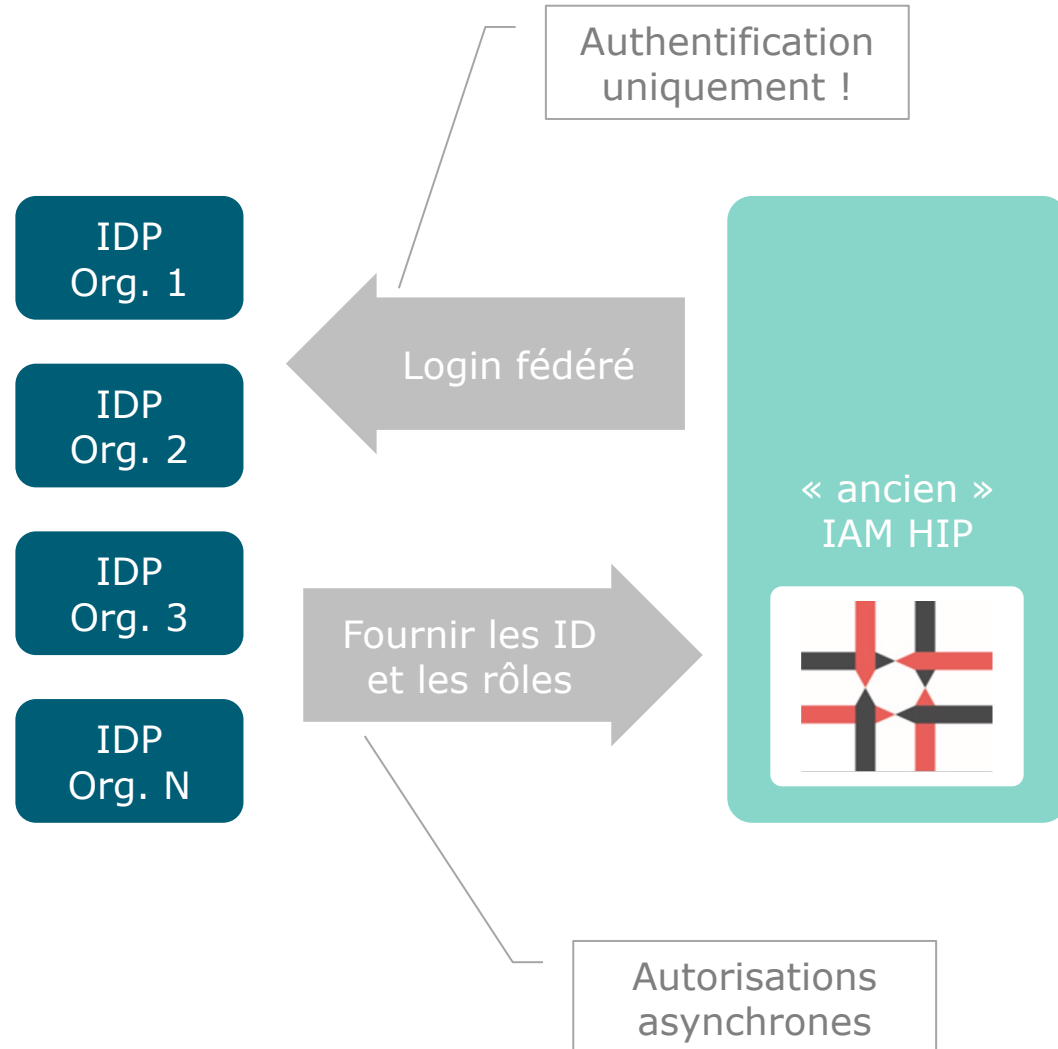
- 
1. Quels sont les avantages de l'IAM TIP ?
  2. Quelle était la situation de départ ?
  3. Objectif : quelles sont les nouveautés de l'IAM TIP ?
  4. Comment s'est déroulée la mise en place de la nouvelle structure ?
  5. Quels ont été les défis à relever ?
  6. Où en sommes-nous aujourd'hui avec l'IAM TIP ?
  7. Conclusion
-

# Quels sont les avantages de l'IAM TIP ?

- › L'Identity and Access Management TIP est le **fondement de la collaboration numérique entre les Corps**
- › Il permet de partager facilement des applications entre les Corps tout en assurant une **sécurité élevée et constante des données**
- › Il permet un **accès simple, sûr et convivial** aux applications via Single Sign-On (SSO)



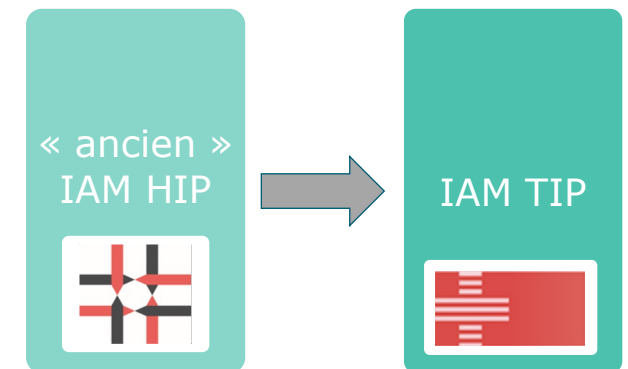
# Quelle était la situation de départ ?



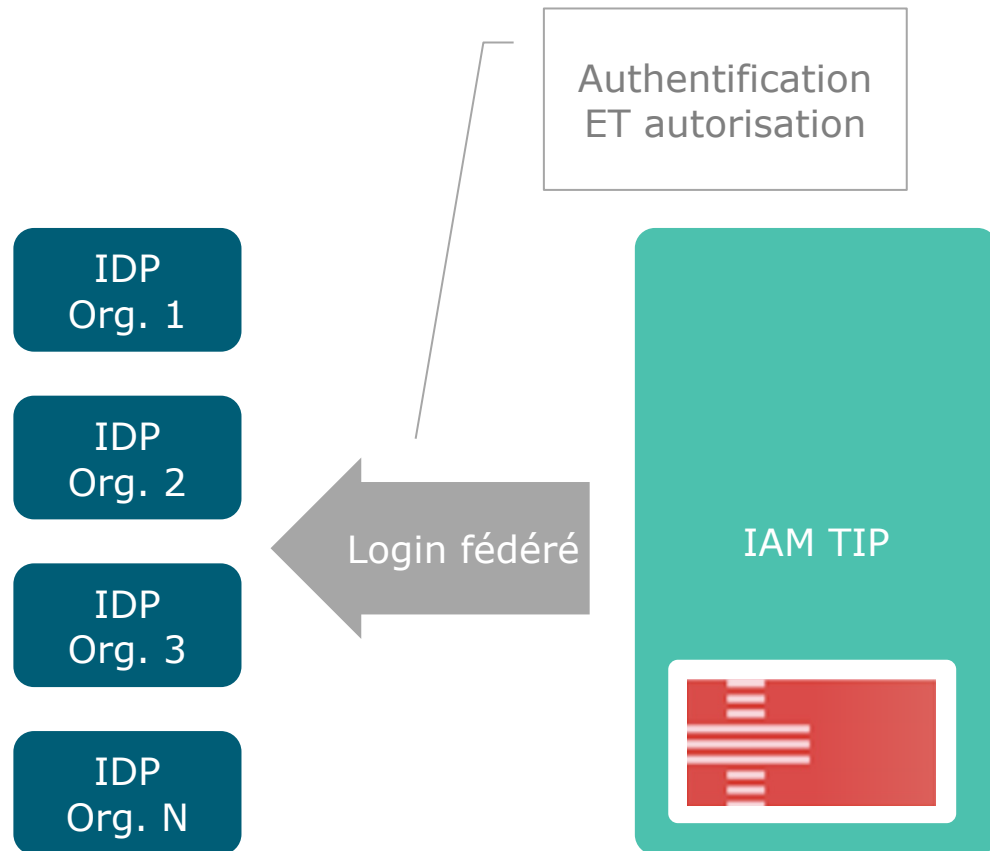
- › Ce processus a été élaboré sur la base d'un produit déjà utilisé par la police cantonale de Zurich.
- › L'authentification (certificat d'identité) était effectuée via le login fédéré.
- › Les identités et les rôles sur les applications des collaborateurs du Corps devaient être **livrés via Sedex dans IAM HIP**.
- › Les organisations non fédérées pouvaient gérer elles-mêmes leurs identités.
- › L'« ancien » IAM HIP existait encore jusqu'à fin 2024.

# Motivation pour l'IAM TIP NextGen

- › La transmission des identités et de leurs rôles a engendré **un travail considérable** pour les Corps, et il a parfois fallu rassembler des données de différents systèmes sources.
- › Le maintien de l'actualité et de la **qualité des données** pour les données d'identité et d'autorisation a été difficile et source d'erreurs.
- › L'**interface de gestion** des identités ne faisait pas partie du produit standard, n'était pas optimale, était complexe et générait de ce fait un travail de support.
- › L'**architecture** choisie a empêché une croissance efficiente concernant les nouvelles connexions d'applications et d'IDP.
- › IAM HIP n'était **pas économiquement évolutif**.

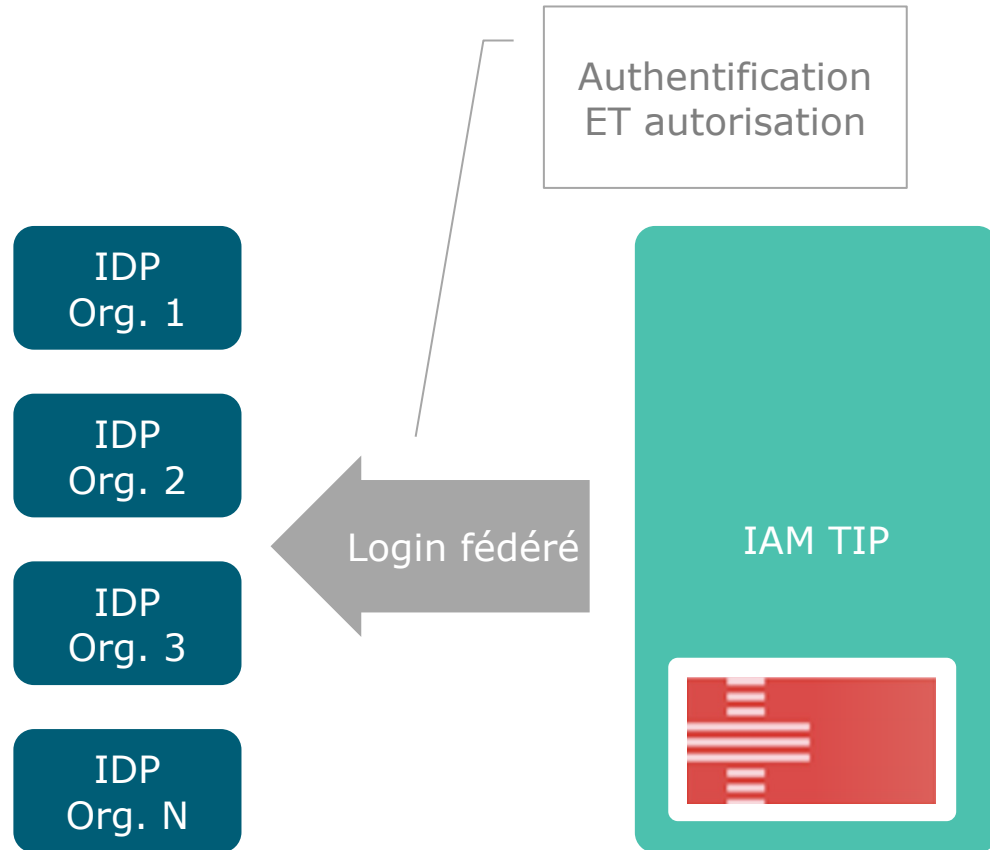


# Objectif : quelles sont les nouveautés de l'IAM TIP ?



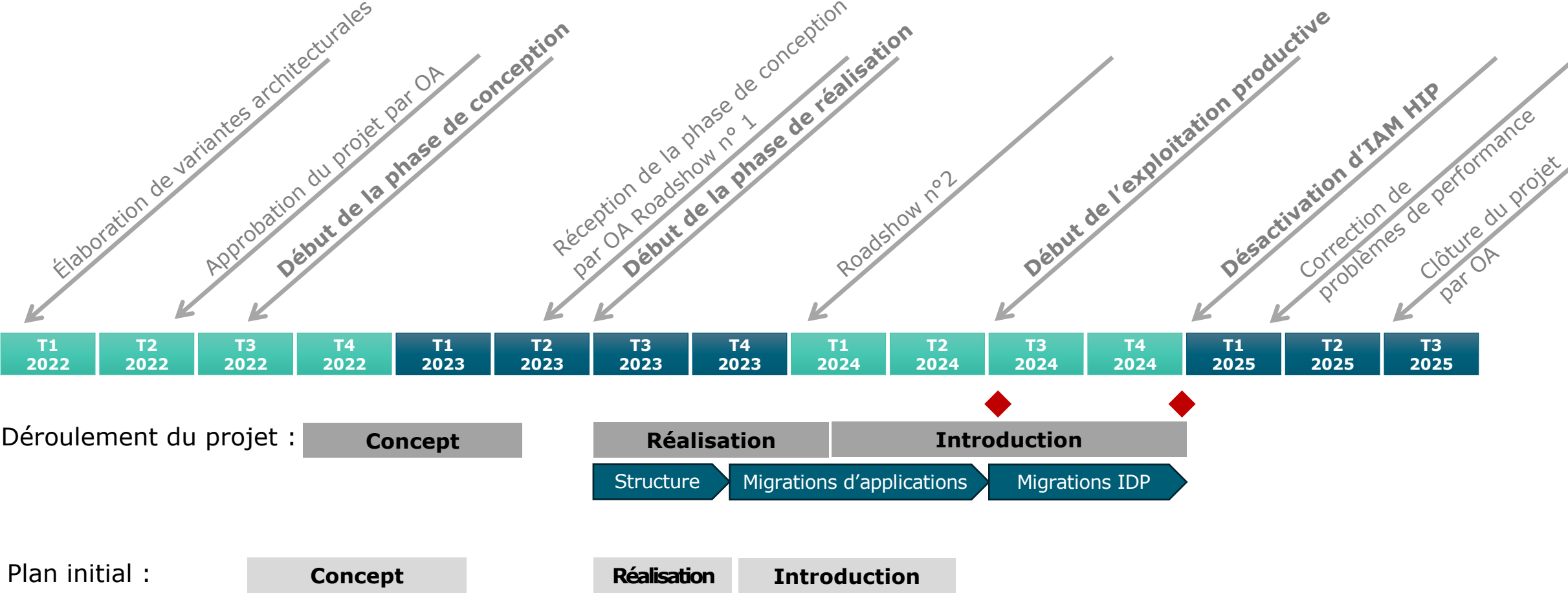
- > L'IAM TIP fédère (utilise) le **login des Corps**, de sorte que l'authentification (preuve d'identité) et l'autorisation (droits d'accès) sont reprises.
- > Ainsi, les données d'identité et les rôles sont transmis en « **temps réel** » lors de la connexion – ils sont donc toujours à jour !
- > Les **rôles sur les applications** peuvent être gérés directement sur l'IDP Corps via des processus établis.
- > Les identités et les rôles peuvent être consultés dans l'IAM via l'interface utilisateur.
- > **2<sup>e</sup> facteur fort** pour logins locaux

# Objectif : quelles sont les nouveautés de l'IAM TIP ?



- > Utilisation des **services IAM et WAF** établis d'**Abraxas** et exploitation au centre clientèle (PoCa Zurich Datacenter)
- > Focalisation sur les « **nouveaux** » **protocoles** (OpenID Connect) lors de la connexion d'applications et de fournisseurs d'identité
- > **Blueprints clairement définis** pour la connexion des applications
- > **Interface utilisateur** intuitive pour la gestion des identités pour les organisations non fédérées
- > **Modèle de prix** transparent et juste

# Comment s'est déroulée la mise en place de la nouvelle structure IAM TIP ?

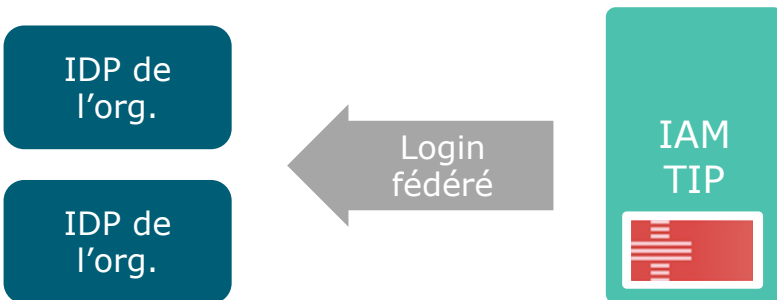


# Quels ont été les défis à relever ?

## Connexion d'applications



## Connexion IDP



- > **KDC** comme prestataire de services pour des tiers a constitué un défi.
- > Les **connexions d'applications** ont duré plus longtemps que prévu :
  - la répartition des tâches n'est pas claire d'emblée IAM, WAF
  - complexité et charge de travail sous-estimées
  - manque de savoir-faire du côté des applications
  - optimisation des processus et de la documentation
- > Changement d'**adresses réseau** pour IAM TIP et applications TIP au centre clientèle -> difficultés d'accessibilité (RCCom/CTV) de différents appareils de différents Corps
- > Les fournisseurs d'identité ont tous été connectés à **OpenID Connect**, ce qui a entraîné des difficultés en termes d'accessibilité de l'IDP de l'organisation.
- > Certains Corps avaient besoin d'**aide** pour la mise en œuvre afin de pouvoir fournir non seulement l'identité, mais aussi des rôles dans le token.

# Où en sommes-nous aujourd'hui avec l'IAM TIP ?

- › L'objectif a été mis en œuvre comme spécifié
- › **68 organisations** gérées dans l'IAM TIP
- › **27 organisations fédérées** -> dans le cadre du projet, de nouvelles organisations fédérées et certaines organisations existantes ont pu être migrées directement vers Entra ID
- › **13 applications TIP** (y compris AFV via eIAM, eOBV, MEF)
- › **10 applications Corps**
- › Affiliation d'organisations fédérales par le biais de la fédération en cours

KKPKS CCPCS  
PTI TIP

Anmelden

Bitte melden Sie sich mit Ihrem Identitätsanbieter an

AGK AIK ARK BEK BLK BSK  
FRK GEK GLK GRK HUK JUK  
LUK NEK NWK OWK POLICE SGK  
GEM SAS SHK SOK SRZ SZK  
TSK TIK URK VDK VSK ZGK  
ZHK ZHS ZHW

oder anmelden mit

Benutzername

Passwort

☐ Angemeldet bleiben

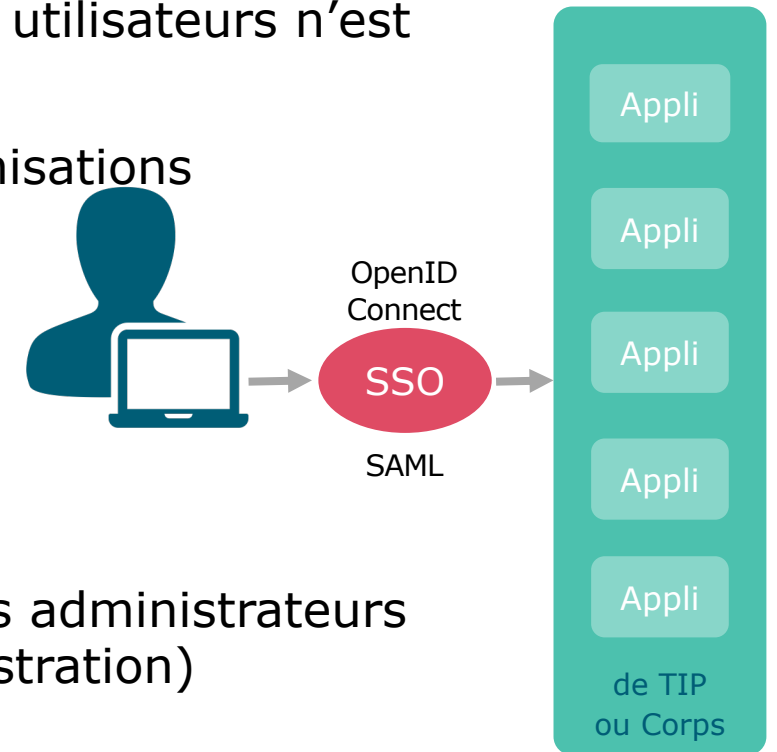
[Passwort vergessen?](#)

Weiter

[Deutsch](#) [English](#) [Français](#) [Italiano](#)

# Conclusion : quel est le principal avantage ?

- › **Solution entièrement fédérative** : le provisionnement des utilisateurs n'est plus nécessaire
- › **IM-as-a-Service** ou **Full Service TIP** pour les petites organisations
- › **Normes techniques modernes** (OIDC et SAML, JSON Web Token) pour les connexions de fédérations et d'applications
- › Authentification sécurisée avec **App Mobile Access comme deuxième facteur**
- › **Meilleure expérience utilisateur** pour les utilisateurs et les administrateurs (meilleur écran de connexion et interface graphique d'administration)
- › Base solide pour **URL dédiée aux mandants et SSO TIP**  
=> Solutions comme ILB



Nous sommes prêts pour d'autres applications Corps !

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

# Questions et remarques



**Merci beaucoup**