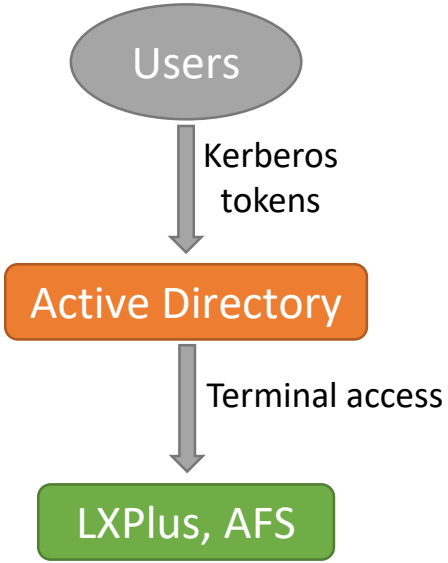

CERN

The new CERN Authentication and Authorization

Paolo Tedesco
Emmanuel Ormancey
Hannah Short
Tim Smith

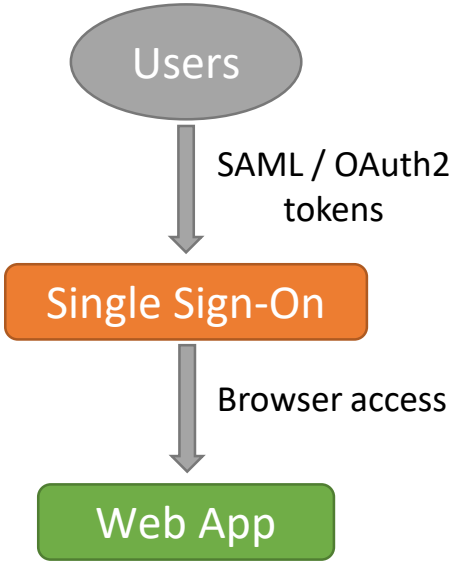
Current situation

Kerberos authentication



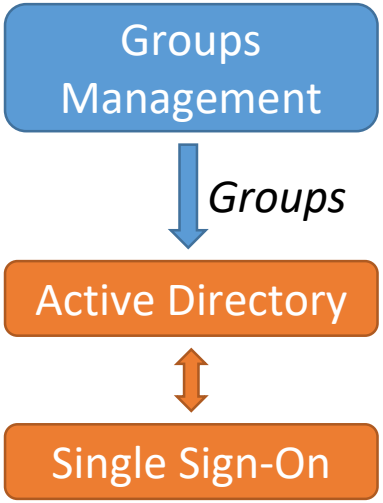
- Desktop/terminal login
- Console-based core services
- Local credentials
  - No federation support
  - "Guest" CERN accounts required
- No Multi-Factor Authentication (MFA) support

Single Sign-On authentication



- Support for Multi-Factor Authentication
- Support for federation
- Focused on (restricted to) web applications

Authorization



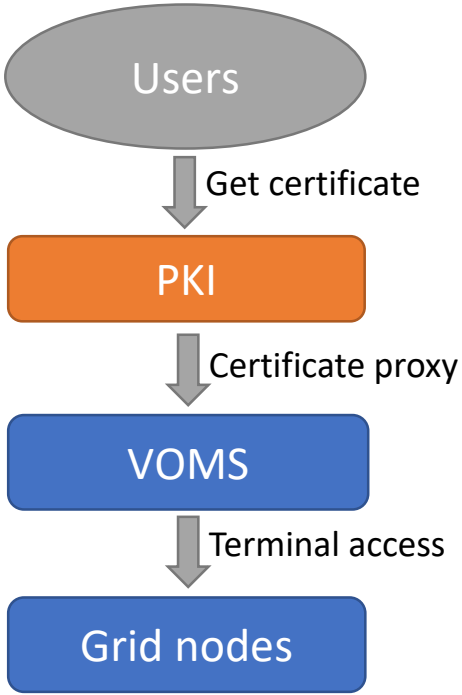
Based on groups

- Local accounts required
- Policies limited to CERN users

Applications can use:

- LDAP / KRB (privacy concerns)
- SSO token (technical problems)

WLCG authentication



'Federation like' X509 certificates

- Circles of trust (EUGridPMA, IGTF)
- Difficult user experience

Emerging alternatives & projects, based on

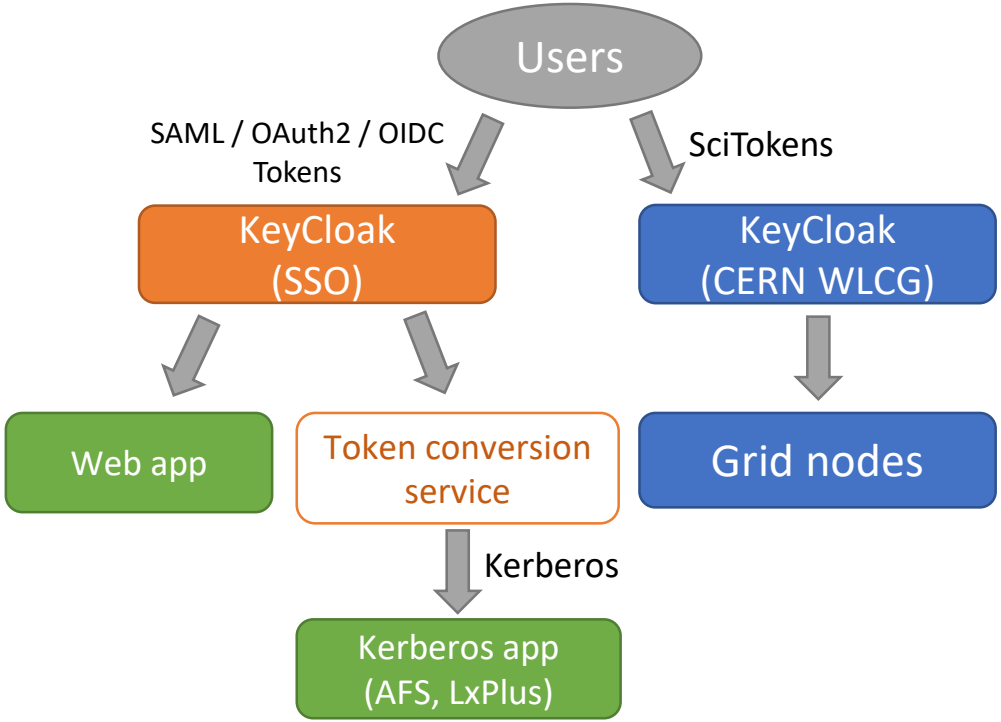
- SAML (e.g EduGain)
- OIDC (e.g. ORCID)
- OAuth2 (SciTokens, INDIGO-IAM)

Future plans

Opportunity for improvement

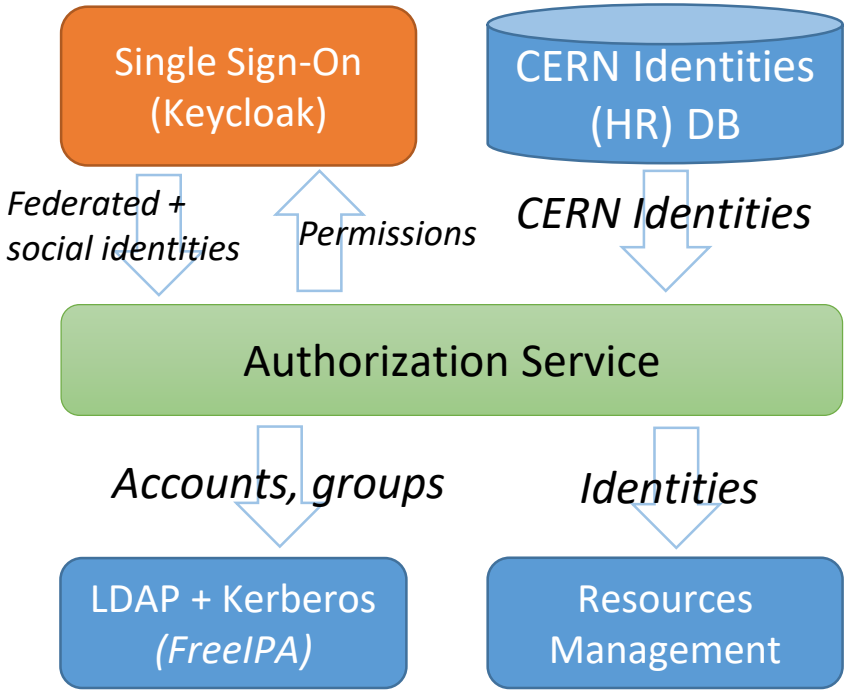
- Designing the next generation of CERN authentication and authorization services
- Provide uniform access schemes and user experience
- Similar architecture for CERN and HEP usage

New authentication



- Tokens at the heart
  - WLCG alignment
- Single Sign-On for all
- Token conversion service

New authorization



Full federation support

Identities management

- Map account(s) to an identity

Application-specific roles

- Levels of Assurance, MFA
- Reduce privacy impact

Resources lifecycle and policies

Extend to non CERN accounts

- Support federated identities
- More Flexible policies
- Better granularity of allocation
- Federated identity ownership

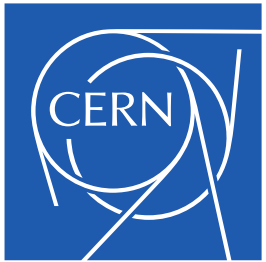
Changes ahead

- Changes and upgrades required in all services and applications
- Occasion for services to evolve
  - Align to token based authentication
  - Widen their user scope
- Fall-back solutions for legacy services
  - Token conversion

Links

The Road to the new CERN Authentication (whitepaper)

CERN Authentication and Authorization Infrastructure Design (informal architecture overview)


CERN