

CERN Authentication and Authorization

Paolo Tedesco
Hannah Short

Recap

- Next generation CERN authentication & authorization
 - Presented at HEPiX Autumn/Fall 2018
- Authentication
 - Uniform scheme for all use-cases (web, desktop...)
 - WLCG alignment
- Authorization
 - Full federation support
 - Identities over accounts
 - Roles over groups
- Resources lifecycle
 - Accounts and other resources
 - Federation support
- LDAP migration

Authentication

- Single Sign-On
 - Fully operational
 - ~3.000 applications / ~15.000 total
- Based on **Keycloak**
 - *More later*
- Support for
 - CERN accounts
 - eduGAIN users
 - Social logins (Linkedin, Github, Google, Facebook)
 - Guest accounts (mail and password)

Authorization

- Groups portal
 - Grouping: fully functional
 - Limited communication
- Groups contain *identities*
- Identities
 - Mapped to one or more accounts (CERN, Edugain...)
 - People, services, applications
- Application owners define *roles*
 - Mapped to groups
 - Restrict by Level of Assurance and Multifactor
 - User token is populated with roles
 - Using groups possible (privacy issues)

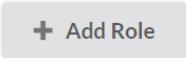
Applications portal: defining roles

> Applications > My Application

 Application: demo app

Application details SSO Registration **Roles** Group memberships

Name	Role Identifier	Description	Required?	Multifactor?	Apply to all users?	
Default Allowed Users	default-role	Users must be from CERN or eduGAIN to have access	✓		✓	 
Demo Administrators	demo-admins	Admins of the demo application		✓		  

 + Add Role

Resources lifecycle

- Lifecycle for computing resources
- Lifecycle rules based on *roles* transitions, e.g.:
 - “Storage users” role, mapped to several groups
 - Identities in users role can create workspaces
 - When identity leaves role, reassign resources
- Work in progress
 - Implementation completed
 - Migrations needed

LDAP Migration

- New LDAP/Kerberos service based on FreeIPA
- Pilot phase
- Users and groups synchronized from production
- Services migration strategy defined
- Next steps: proof of concept service on FreeIPA
 - Grid Batch

Keycloak deployment

- Keycloak 11
 - Some preview features enabled, e.g. Token Exchange
- Multiple realms, to allow:
 - “Optional” MFA (to be rediscussed)
 - “Optional” one-click authentication
 - Edugain
 - Social and Guest access

Login screen

CERN Single Sign-On

Log in with your CERN account

Username ⓘ

Password

[Forgot Password?](#)

Log In

Reminder: you have agreed to comply with the [CERN Computing Rules](#), in particular OC5. CERN implements the measures necessary to ensure compliance.

Two-factor authentication ⓘ

 Log in with Two-factor

One-click authentication ⓘ

 Log in with Kerberos

Authenticate through your home institute ⓘ

 eduGAIN

Log in with your social account ⓘ

Some social account providers, e.g. Facebook, may use knowledge about your access to CERN for purposes such as profiling.

Log in with your email ⓘ

 Guest access

eduGAIN integration

- Authentication to CERN using home institute credentials
 - CERN must register a Service Provider (SP) proxy in eduGAIN (done)
- Authentication to eduGAIN SPs using CERN credentials
 - CERN must register an Identity Provider (IdP) in eduGAIN (in progress)
- Must consume a trusted subset of the eduGAIN metadata (> 4000 members)

Additional software used

- [Satosha](#) (SAML-to-SAML): token translation proxy
 - Impose restrictions
 - Add authorisation
- [PyFF](#) (Python Federation Feeder)
 - Discovery service
 - Metadata Query provider
 - Avoids registering over 4000 entities in Satosa or Keycloak

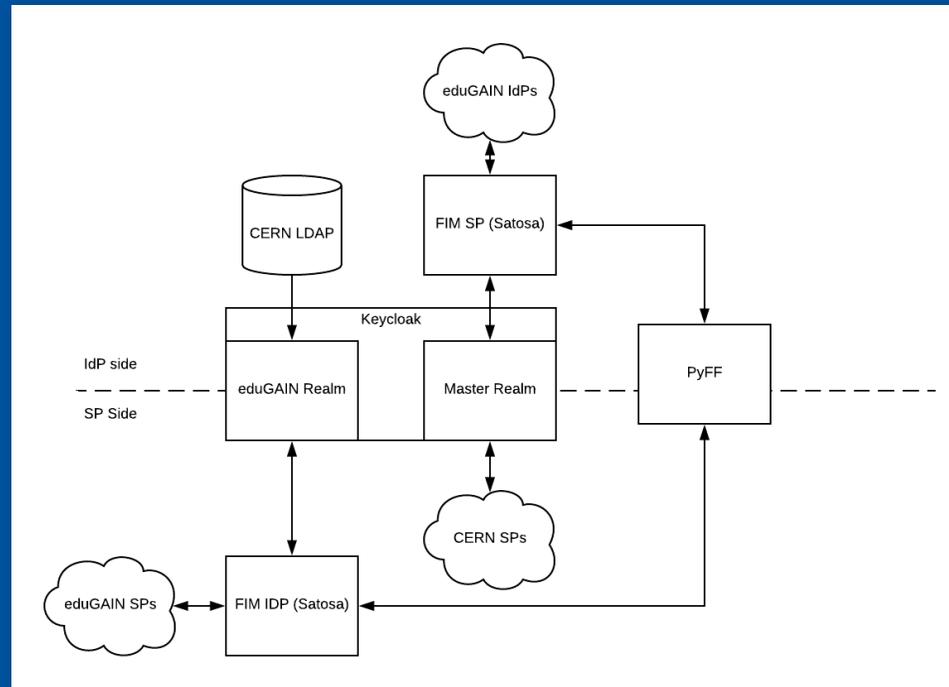
eduGAIN login to CERN

- eduGAIN IdP configured in main CERN realm
- IdP is a Satosa instance handling:
 - Registration of the eduGAIN IdPs
 - Their discovery (through PyFF)
- Satosa rewrites the incoming (from external IdP) token
 - Standardizes attributes in token that goes to Keycloak

CERN login to eduGAIN

- Dedicated eduGAIN realm in Keycloak
- Enable only CERN users
 - LDAP is the only IdP in the realm
- Add a client with eduGAIN attribute mappers configured
- Client is a Satosa instance handling:
 - Registration of eduGAIN SPs

eduGAIN integration overview



Why this design?

- Satosa is the service that interacts with eduGAIN
 - Maintained by the eduGAIN community
- Single point of login where users enter passwords
 - Keycloak if CERN
 - Federated users' home organisation
- We don't have to register clients in Keycloak
- Layer over Keycloak
 - We can change SSO transparently
- Improvements from the previous solution
 - Cleaner design
 - Higher interoperability with the wider community

Additional Keycloak customizations

- Service Provider Interfaces (SPI)
- Custom mappers integrated in the login flow
- Query Authorization Service DB to populate user token
 - Application-specific roles
 - Groups

