The new (and improved!) CERN Single-Sign-On

A. Ahmad, A. Aguado Corman, M. Fava, M. Georgiou, J. Rische, C. Schuszter, H. Short, P. Tedesco

Presented by M. Georgiou, vCHEP 2021

1. Introduction
2. Architecture Overview
3. SSO Authorization
4. Recent Progress - SSO
5. Recent Progress - LDAP and Kerberos Migration
6. Recent Progress - Account Management
7. Community Engagement
8. Next Steps

Introduction

- Current authentication stack is not longer suitable for the CERN community
  - Insufficient support of modern protocols (e.g., OIDC, multifactor)
  - Cost impact due to Microsoft licenses (Malt Project)
- Alternative Open-Source system under development
- Currently operating two systems in parallel, Microsoft stack and Open-Source stack
- Aim is to complete transition and improve the service offering

SSO - Authorization

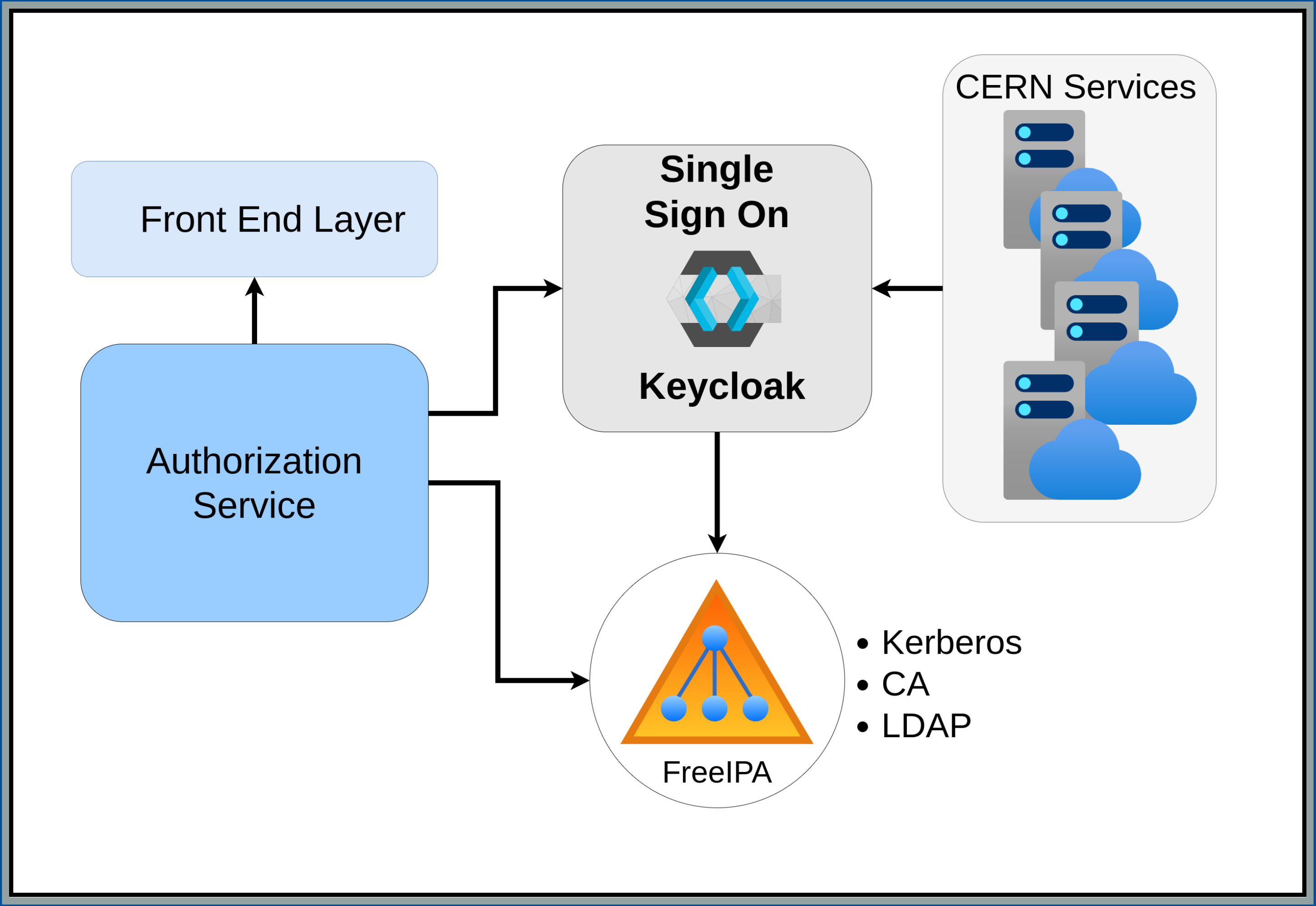
Old SSO	New SSO

Numbers

- > 60.000 user accounts
- > 60.000 user groups
- > 3.000.000 group memberships
- > 15.000 services registered in the old Single Sign On (SSO)

  > 3.700 services are already registered in the new SSO

Overview of new infrastructure



Front End Layer

Authorization Service

Single Sign On

Keycloak

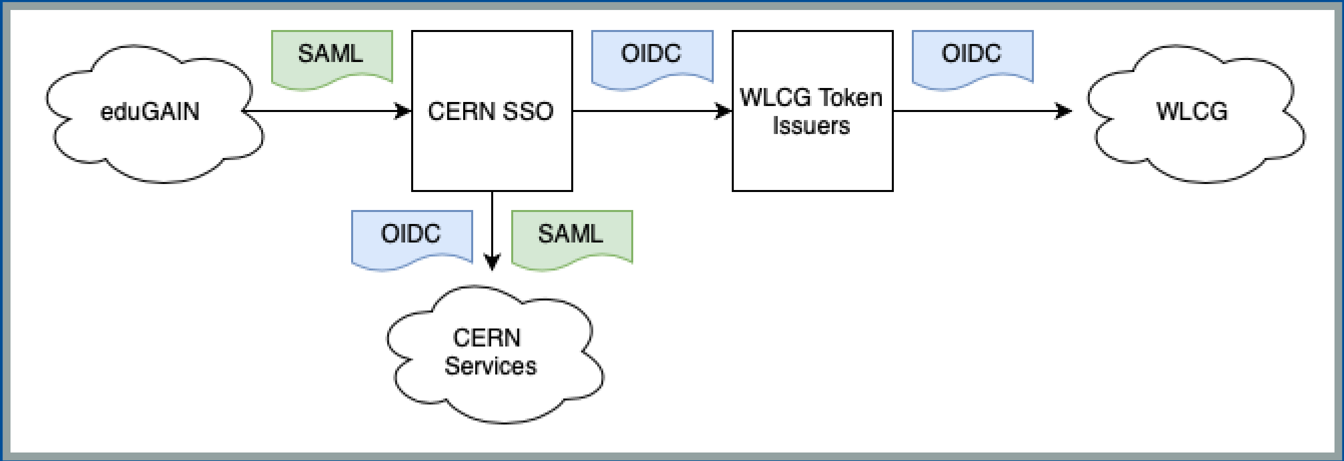
CERN Services

FreeIPA

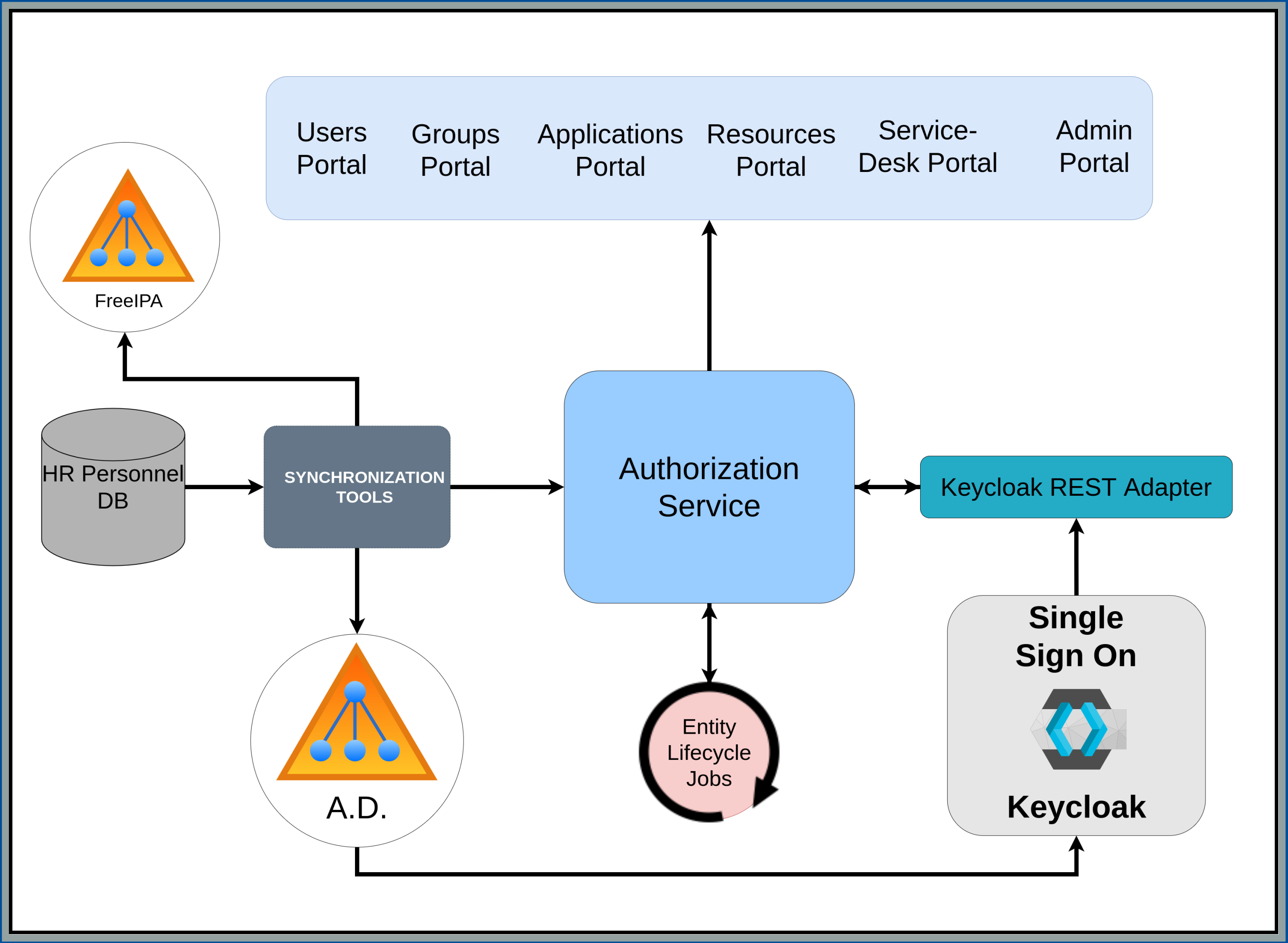
- Kerberos
- CA
- LDAP

Why these choices?

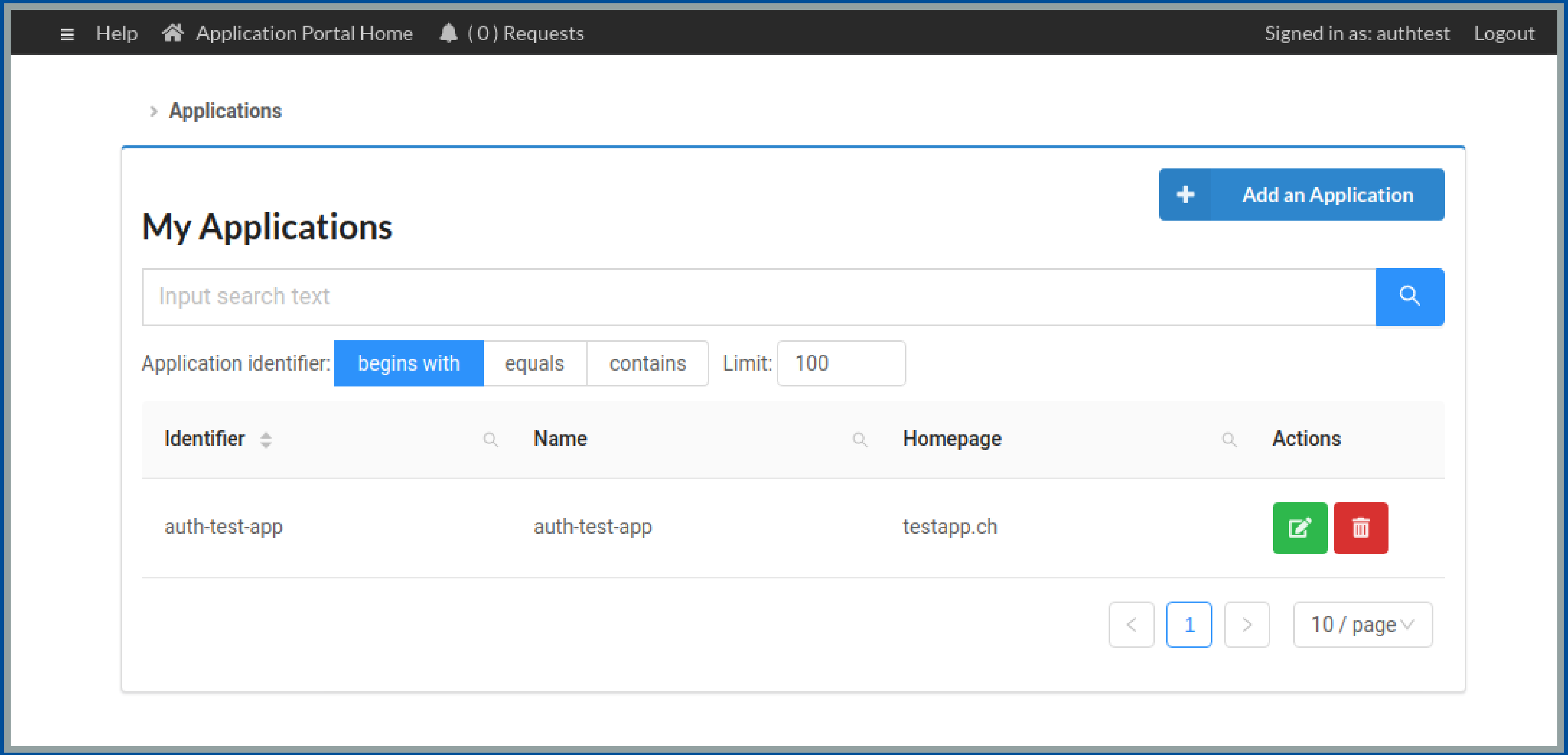
- In line with CERN requirments while following standards
- Vendor independent (as much as possible)
- In line with efforts to move HEP towards Token based authorisation (no more certificates)
- Working with the wider community to ensure interoperability



Mid-Transition Infrastructure



Application Portal



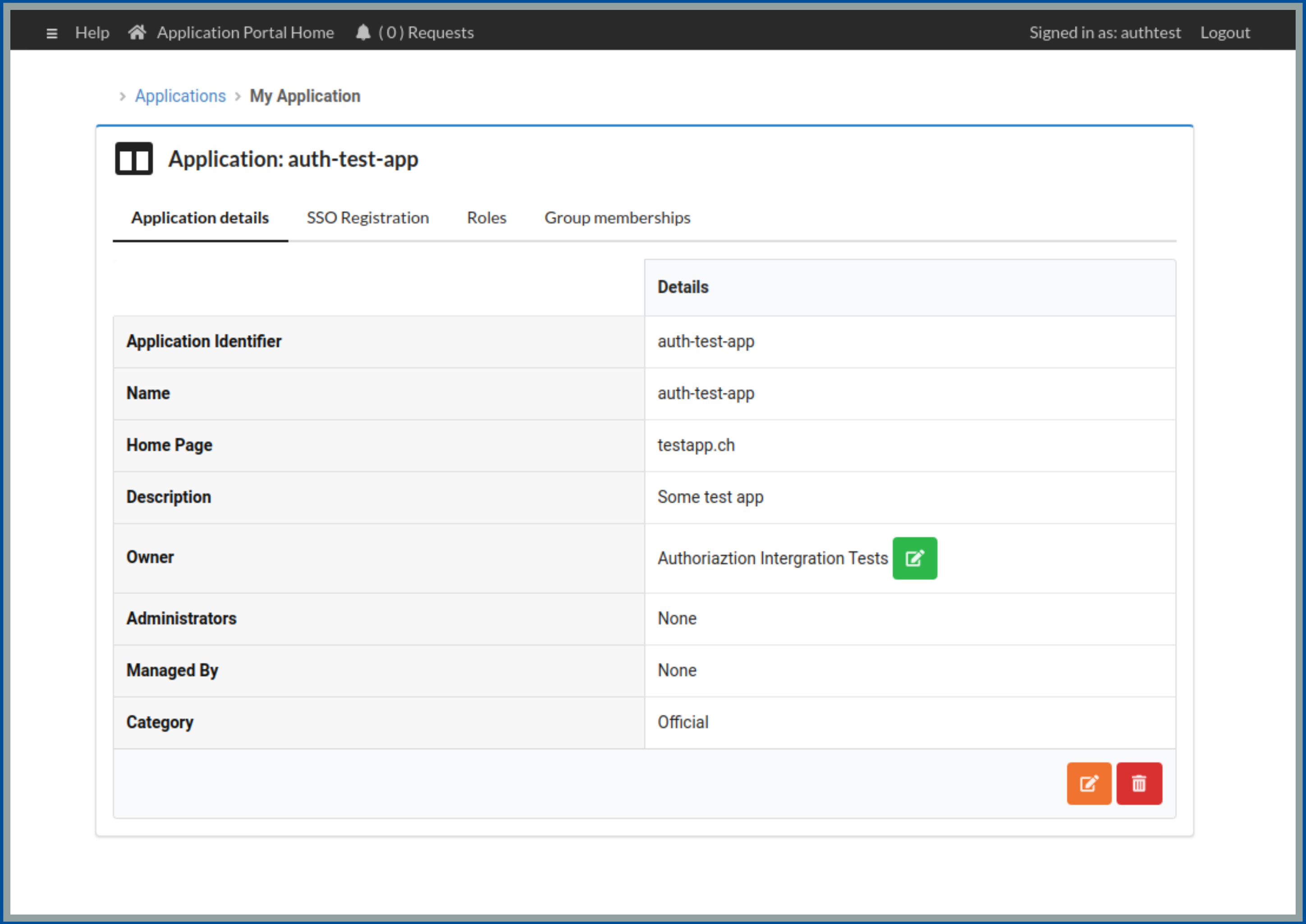
My Applications

Input search text

Application identifier: [✓ begins with] equals contains Limit: 100

Identifier	Name	Homepage	Actions
auth-test-app	auth-test-app	testapp.ch	

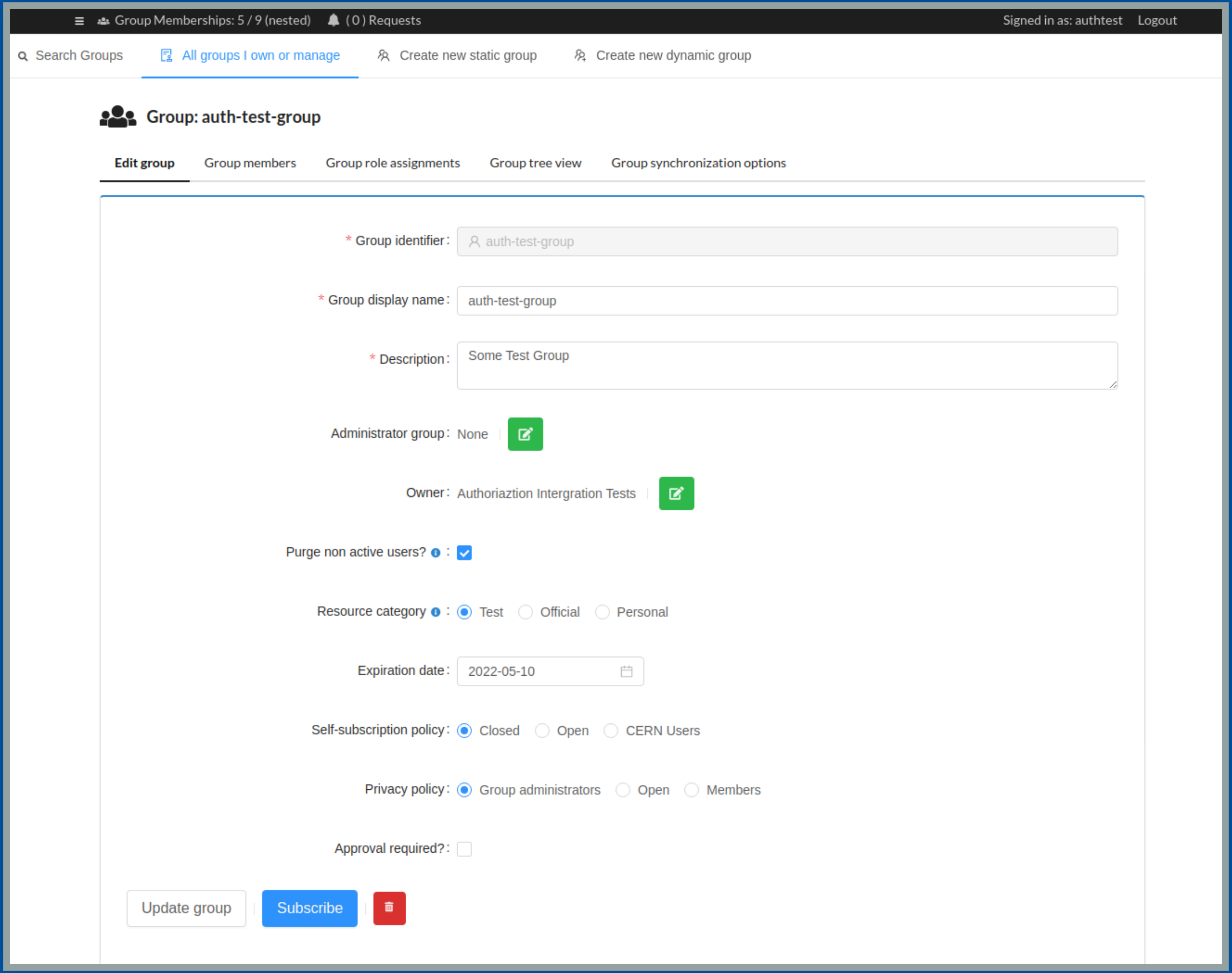
Application Portal



Application: auth-test-app

	Details
Application Identifier	auth-test-app
Name	auth-test-app
Home Page	testapp.ch
Description	Some test app
Owner	Authoriaztion Intergration Tests
Administrators	None
Managed By	None
Category	Official

Groups Portal



Group: auth-test-group

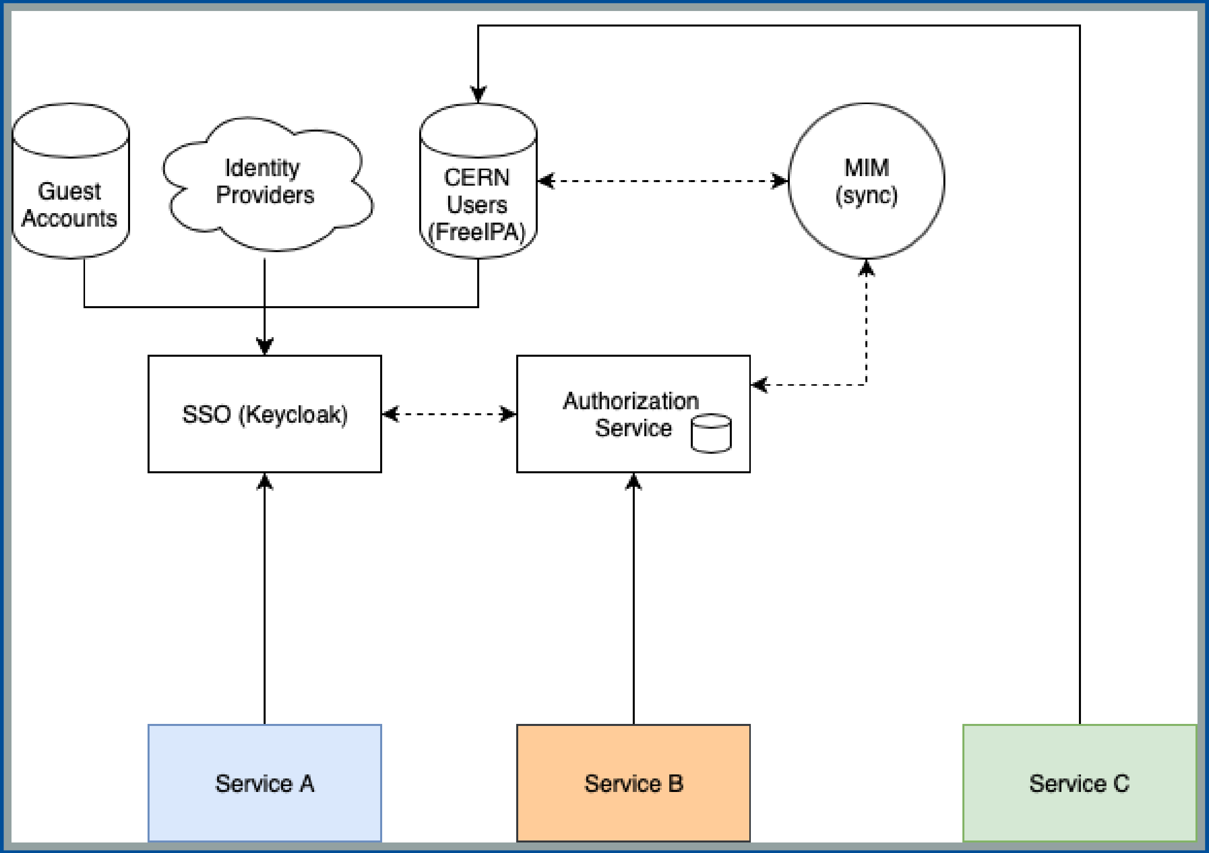
* Group identifier :	auth-test-group
* Group display name :	auth-test-group
* Description :	Some Test Group
Administrator group :	None
Owner :	Authoriaztion Intergration Tests
Purge non active users? :	☑
Resource category :	● Test ○ Official ○ Personal
Expiration date :	2022-05-10
Self-subscription policy :	● Closed ○ Open ○ CERN Users
Privacy policy :	● Group administrators ○ Open ○ Members
Approval required? :	□

1. Introduction
2. Architecture Overview

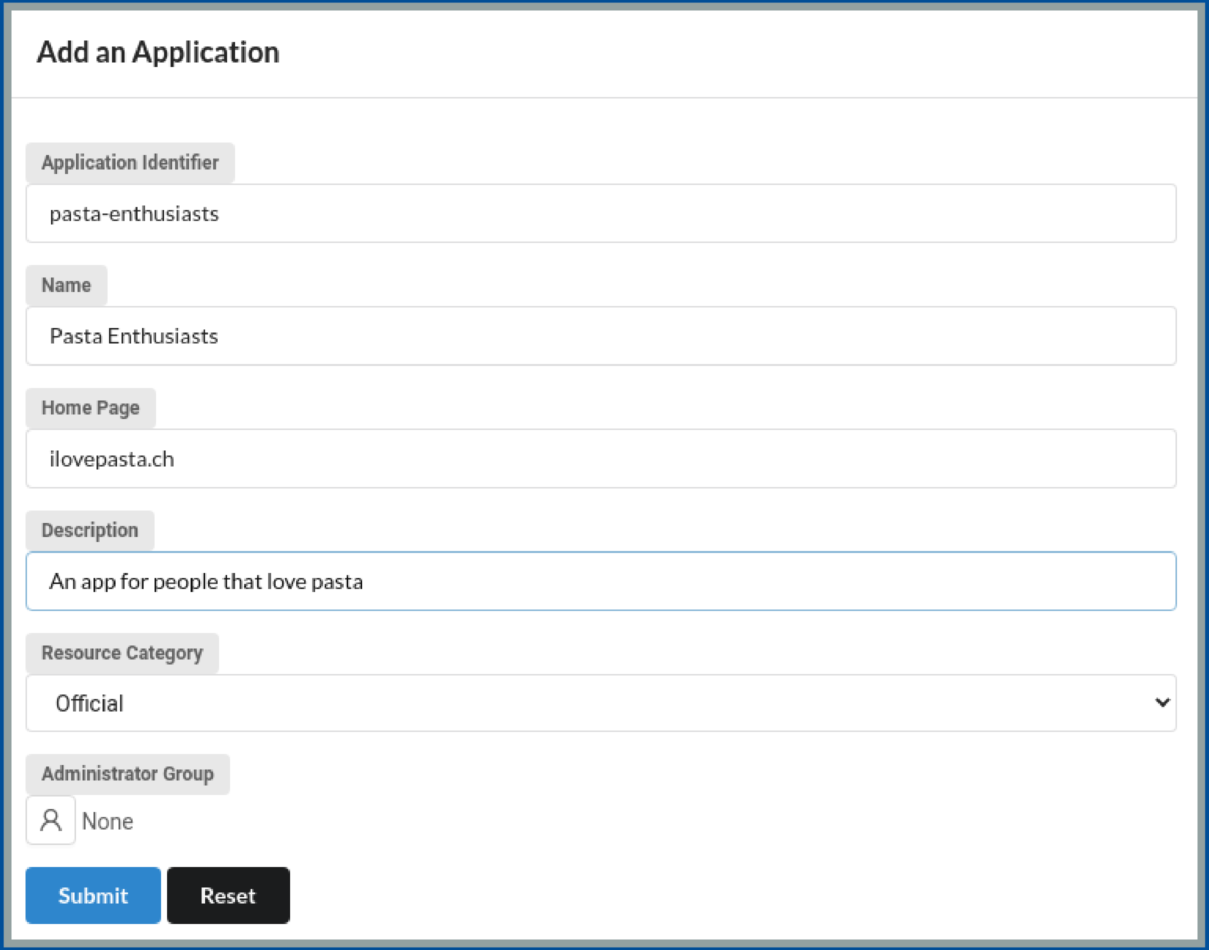
4. SSO Authorization

3. Recent Progress - SSO
4. Recent Progress - LDAP and Kerberos Migration
5. Recent Progress - Account Management
6. Community Engagement
7. Next Steps

SSO - Authorization



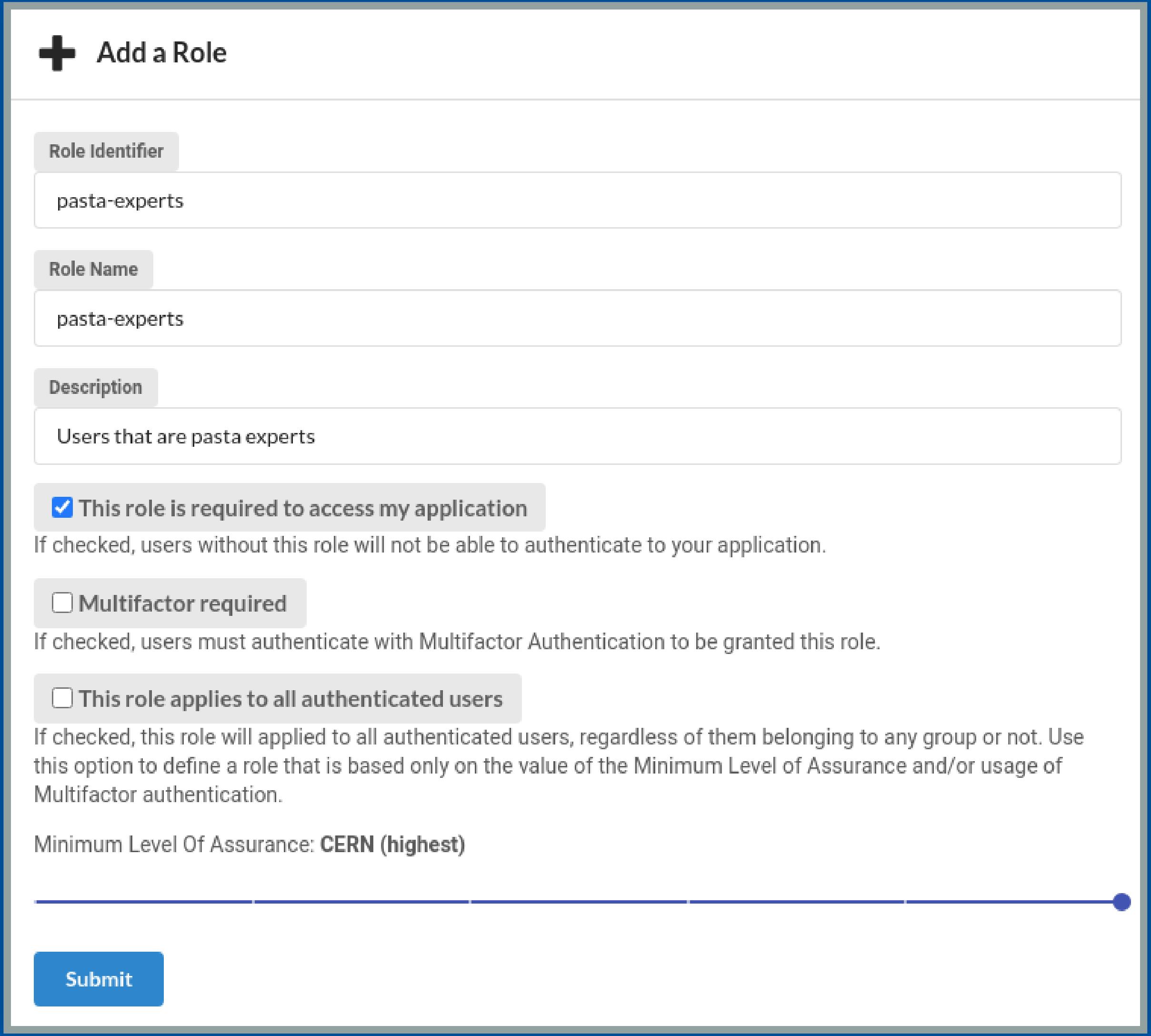
SSO - Authorization



Add an Application

Application Identifier	pasta-enthusiasts
Name	Pasta Enthusiasts
Home Page	ilovepasta.ch
Description	An app for people that love pasta
Resource Category	Official
Administrator Group	None

SSO - Authorization



✚ Add a Role

Role Identifier

pasta-experts

Role Name

pasta-experts

Description

Users that are pasta experts

☑ This role is required to access my application

If checked, users without this role will not be able to authenticate to your application.

☐ Multifactor required

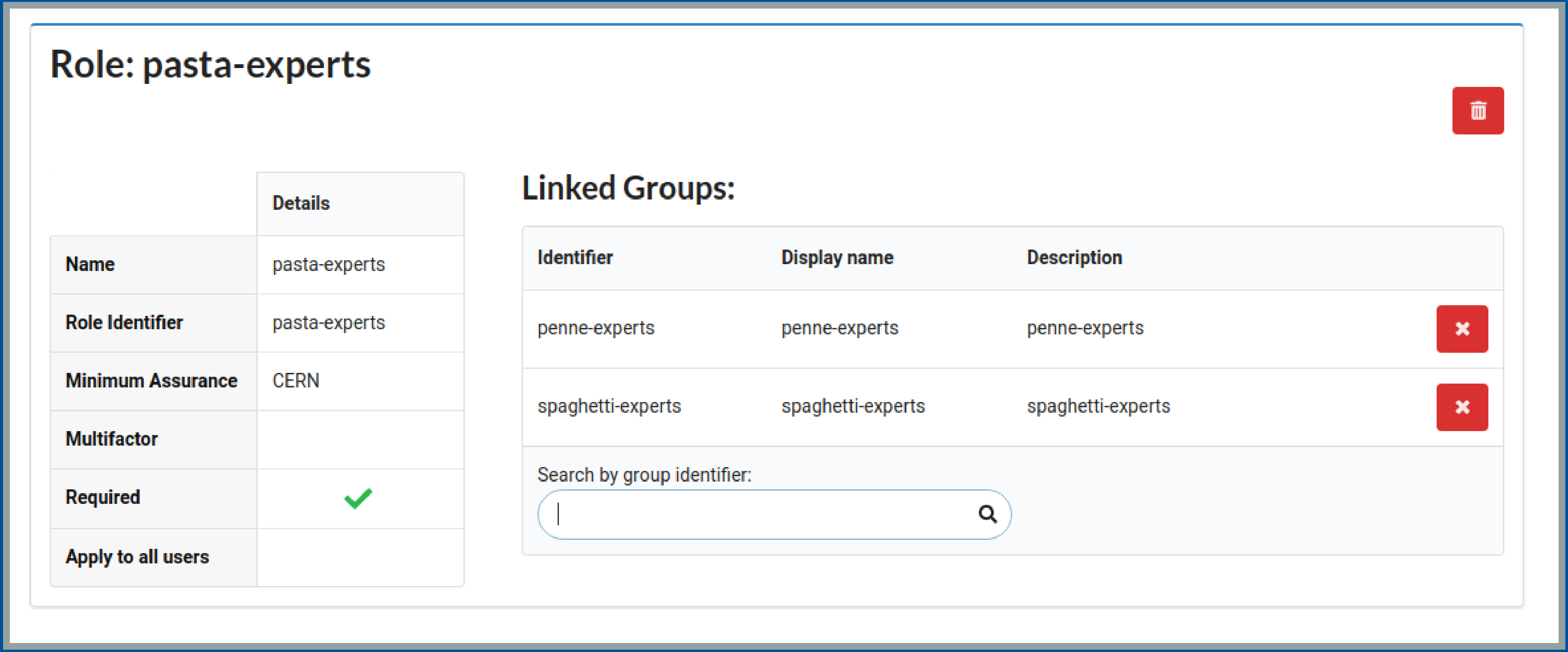
If checked, users must authenticate with Multifactor Authentication to be granted this role.

☐ This role applies to all authenticated users

If checked, this role will applied to all authenticated users, regardless of them belonging to any group or not. Use this option to define a role that is based only on the value of the Minimum Level of Assurance and/or usage of Multifactor authentication.

Minimum Level Of Assurance: **CERN (highest)**

SSO - Authorization



Role: pasta-experts

	Details
Name	pasta-experts
Role Identifier	pasta-experts
Minimum Assurance	CERN
Multifactor	
Required	✓
Apply to all users	

Linked Groups:

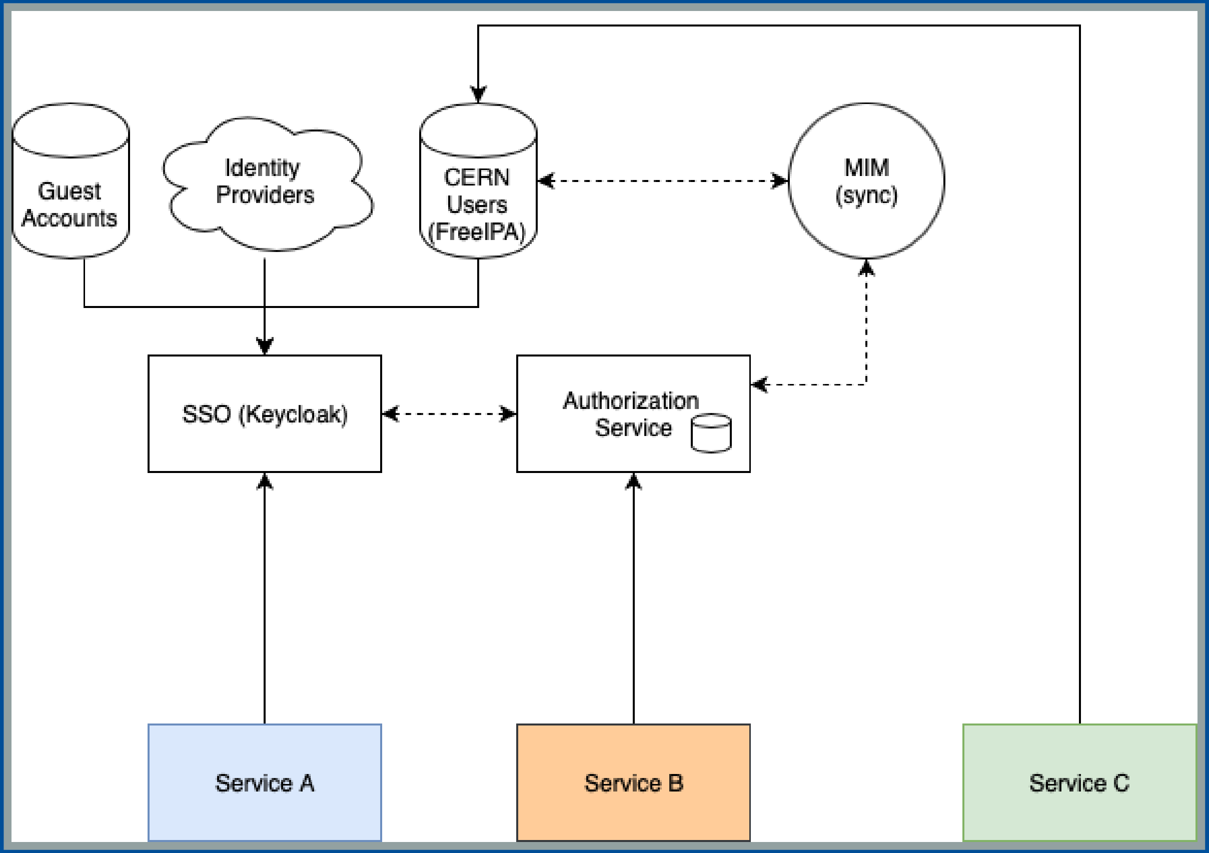
Identifier	Display name	Description	
penne-experts	penne-experts	penne-experts	✖
spaghetti-experts	spaghetti-experts	spaghetti-experts	✖

Search by group identifier:

SSO - Authorization

```
"resource_access": {
    "pasta-enthusiasts": {
      "roles": [
        "spaghetti-experts"
      ]
    }
  },
  "cern_roles_missing_mfa": [
    "mfarole"
  ],
```

SSO - Authorization



SSO - Authorization

- Only CERN accounts will be stored in CERN's LDAP (FreeIPA)
- Any service that requires authorization information for Guest Accounts should use the SSO
- Groups:
    - In the old system they were used for both authorization and for mailing lists
    - In the new system these use cases will be decoupled with existing groups to be imported as both authorization groups and mailing lists

1. Introduction
2. Architecture Overview
3. SSO Authorization
    4. Recent Progress - SSO
    5. Recent Progress - LDAP and Kerberos Migration
    6. Recent Progress - Account Management
4. Community Engagement
5. Next Steps

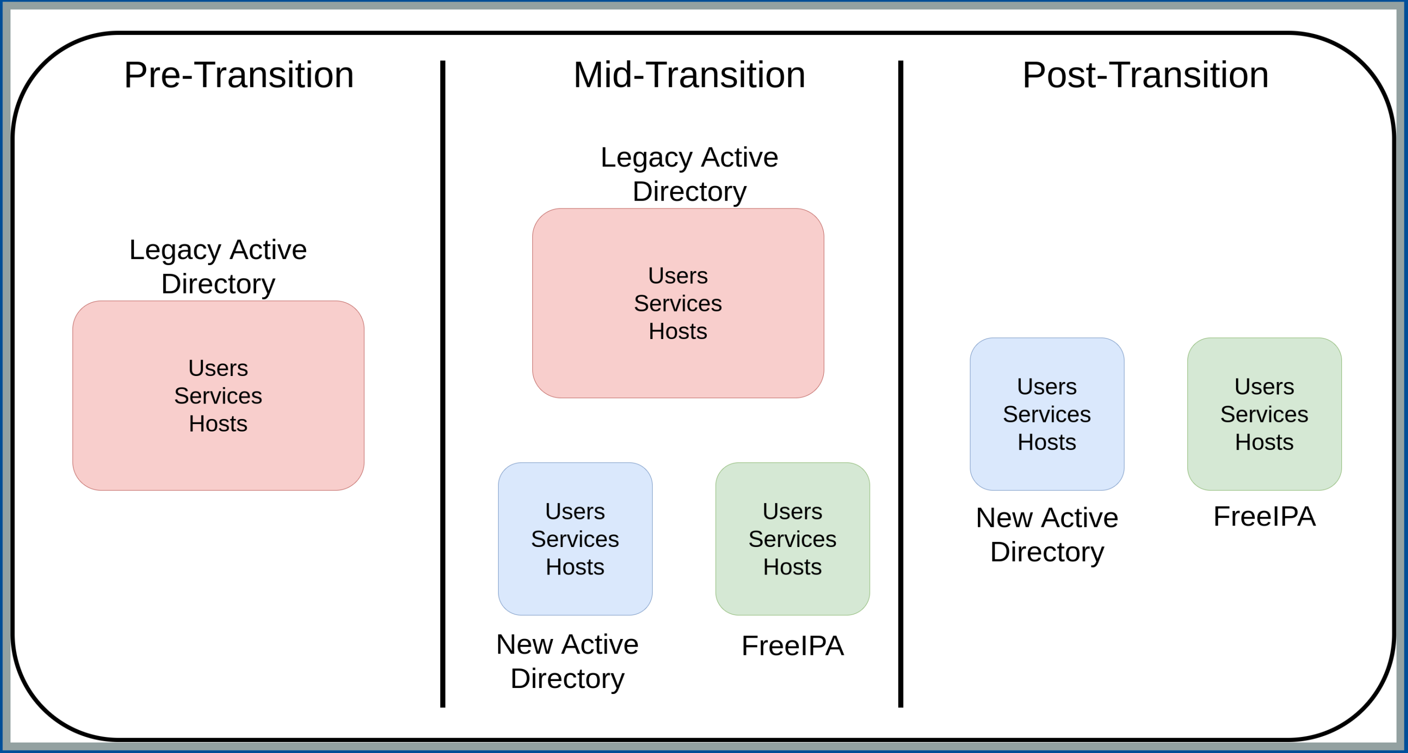
Recent Progress - SSO

- System scale-up to cope with the amount of applications registered on it
- Users can choose between 2 options as second factor authentication (2FA) methods:
    - One Time Passwords (OTP)
    - WebAuthN hardware tokens (Yubikey)
- More options for visiting users

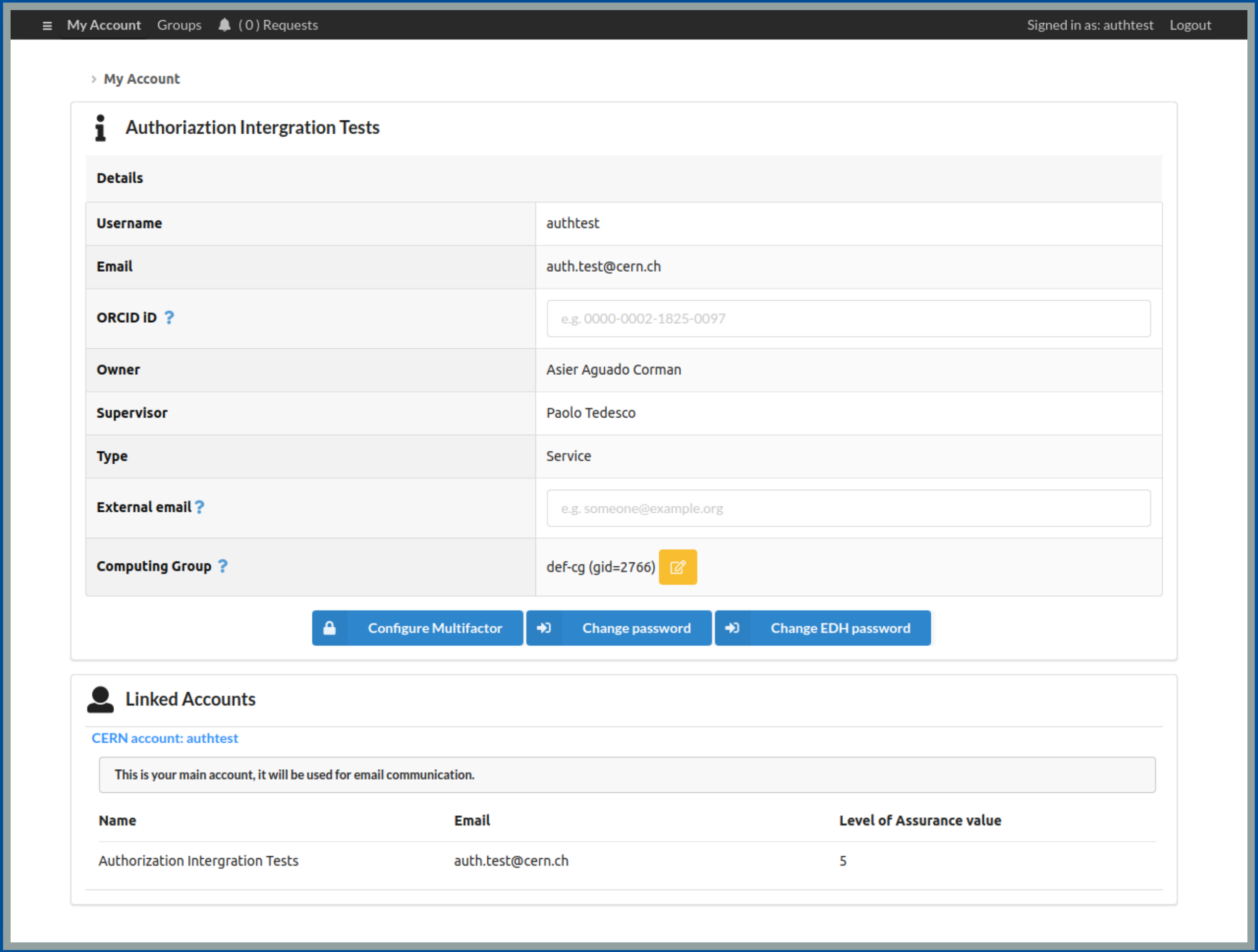
Recent Progress - LDAP and Kerberos Migration

- FreeIPA QA environment for service managers to test
- Complex migration of services is unavoidable
- Critical to automate service discovery to minimise disruption to the CERN Community
- H1 2021 focusing on proof of concept for grid batch workflows on FreeIPA

LDAP and Kerberos Migration



Recent Progress - Account Management


≡ My Account Groups (0) Requests
Signed in as: authtest Logout

› My Account

Authoriaztion Intergration Tests

Details

Username	authtest
Email	auth.test@cern.ch
ORCID iD ?	e.g. 0000-0002-1825-0097
Owner	Asier Aguado Corman
Supervisor	Paolo Tedesco
Type	Service
External email ?	e.g. someone@example.org
Computing Group ?	def-cg (gid=2766)

Configure Multifactor
Change password
Change EDH password

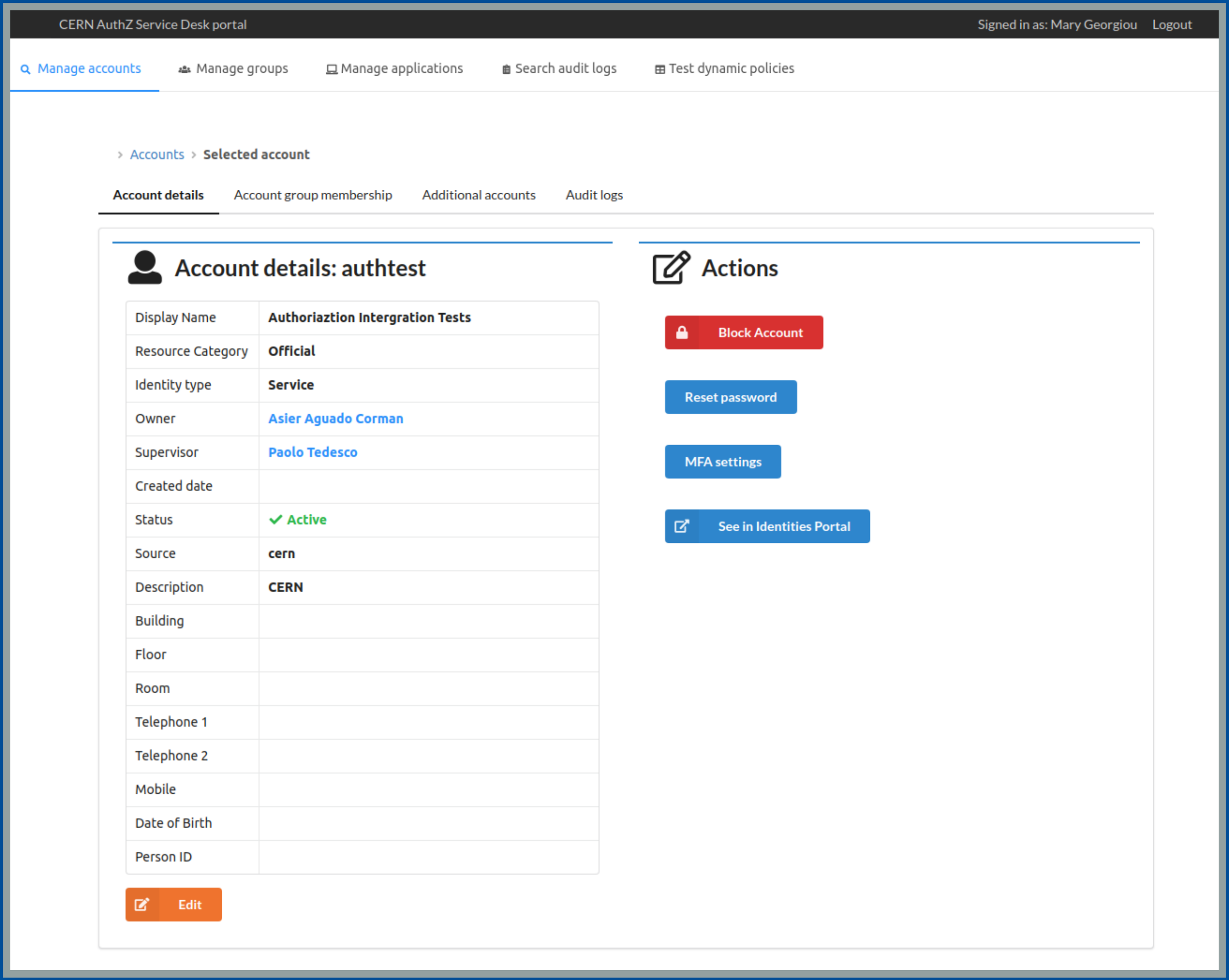
Linked Accounts

CERN account: authtest

This is your main account, it will be used for email communication.

Name	Email	Level of Assurance value
Authorization Intergration Tests	auth.test@cern.ch	5

Recent Progress - Account Management



Account details: authtest

Display Name	Authoriaztion Intergration Tests
Resource Category	Official
Identity type	Service
Owner	Asier Aguado Corman
Supervisor	Paolo Tedesco
Created date	
Status	✓ Active
Source	cern
Description	CERN
Building	
Floor	
Room	
Telephone 1	
Telephone 2	
Mobile	
Date of Birth	
Person ID	

Recent Progress - Account Management

- Currently transitioning all account management to new system, which has much improved lifecycle management
- Password management already migrated with improved features:
  - Password hashes are checked against a DB of leaked password hashes
  - Password rules more user friendly

1. Introduction
2. Architecture Overview
3. SSO Authorization
4. Recent Progress - SSO
5. Recent Progress - LDAP and Kerberos Migration
6. Recent Progress - Account Management
7. **Community Engagement**
8. **Next Steps**

Community Engagement

- Huge challenge
- Lots and Diverse Teams = Multiple, diverse and complex requirements
- Some services are not actively supported and/or their mailboxes are not actively read
- Malt Active Directory Task Force established in late 2020 to engage with representatives from many technical sectors of CERN and experiments

Next Steps

- Focus on finalizing the account management in the new system
- Final decision on Active Directory to FreeIPA migration plan
- Resources management migration into the new system

Want more information?

- Visit https://auth.docs.cern.ch/