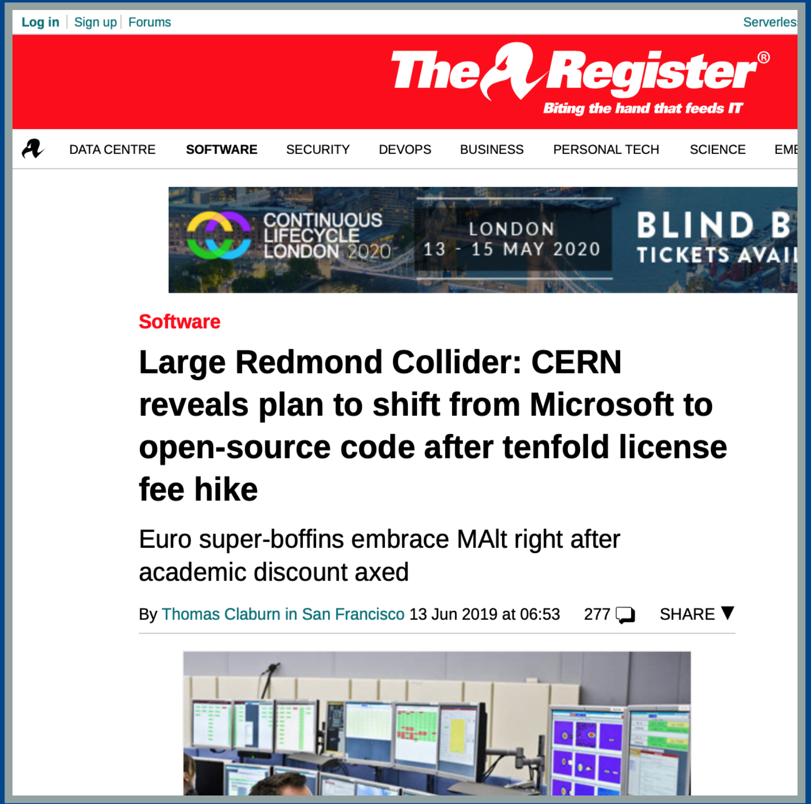
CERN’s Identity and Access Management

CHEP November 7th 2019, Adelaide

Presented by Hannah Short, CERN IT

Authored by the Malt AAI Project Team: P. Tedesco, A. Aguado Corman, D. Fernandez Rodriguez, M. Georgiou, J. Rische, C. Schuszter, H. Short

A Journey to Microsoft Alternatives



Software

Large Redmond Collider: CERN reveals plan to shift from Microsoft to open-source code after tenfold license fee hike

Euro super-boffins embrace MAlt right after academic discount axed

By Thomas Claburn in San Francisco 13 Jun 2019 at 06:53 277 SHARE ▼

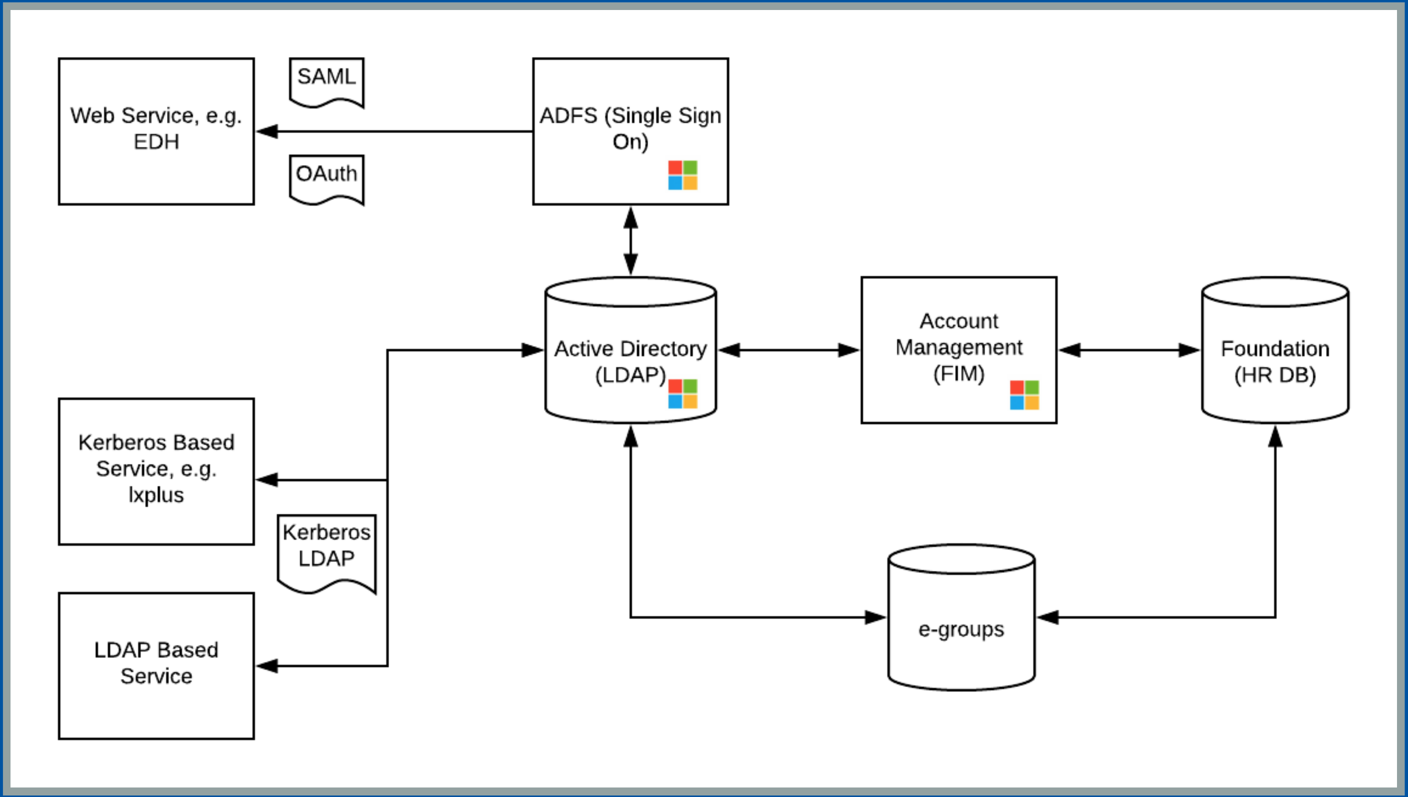
Why change?

- Microsoft based Identity Management stack strongly affected by **License Fee price increase**
- Opportunity to **harmonise** CERN and WLCG Authentication & Authorization
- Focus on Data **Privacy** requires new authorization model

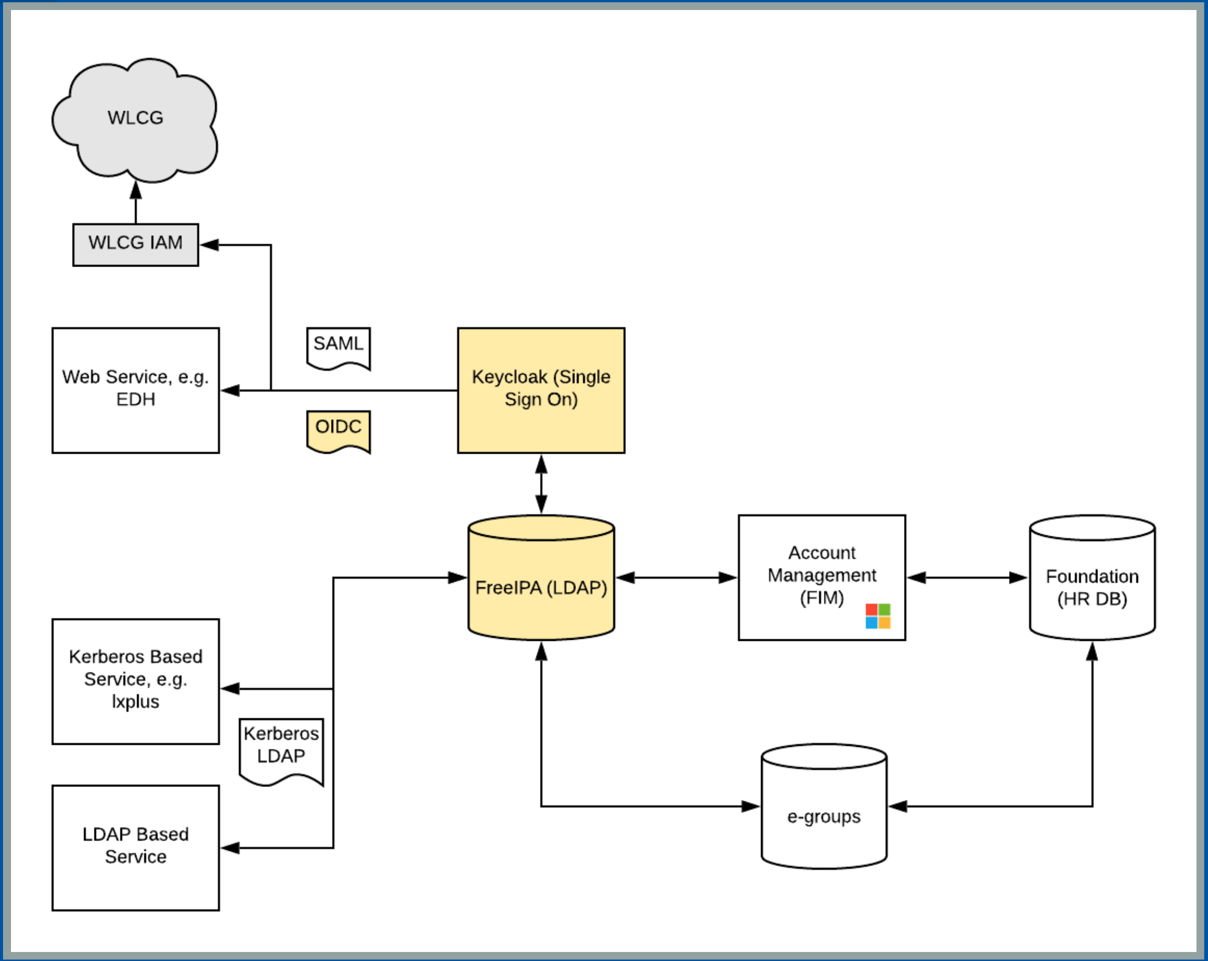
Principles of change

- Identify suitable **alternatives** based on use cases
- Prioritise **Free and Open Source software**
- Stick to **standards**
- Contribute back and share knowledge

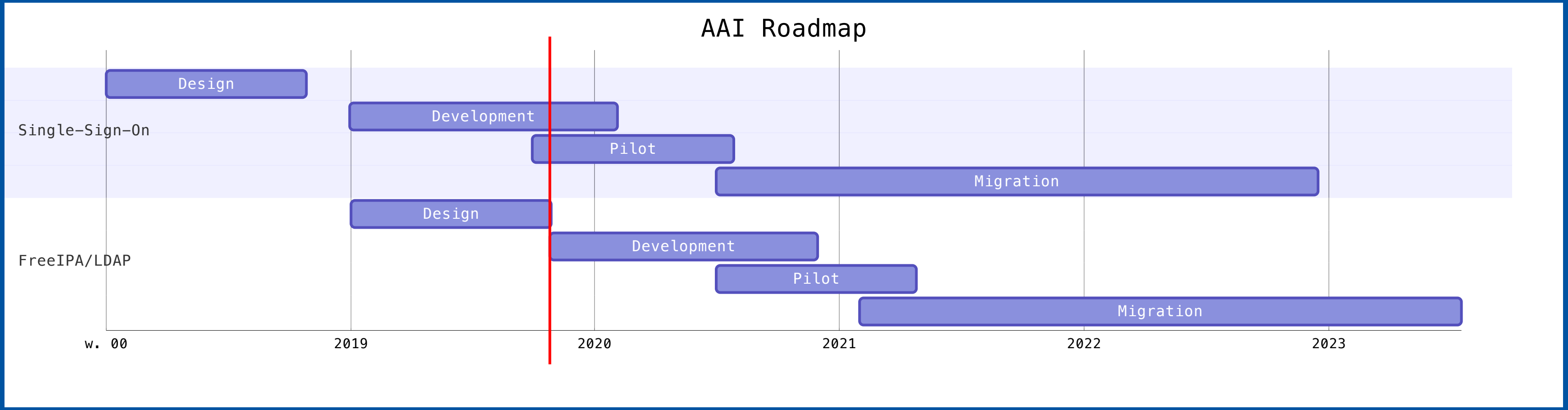
Before


Web Service, e.g. EDH
SAML
OAuth
ADFS (Single Sign On)
Active Directory (LDAP)
Account Management (FIM)
Foundation (HR DB)
Kerberos Based Service, e.g. lxplus
Kerberos
LDAP
LDAP Based Service
e-groups

After

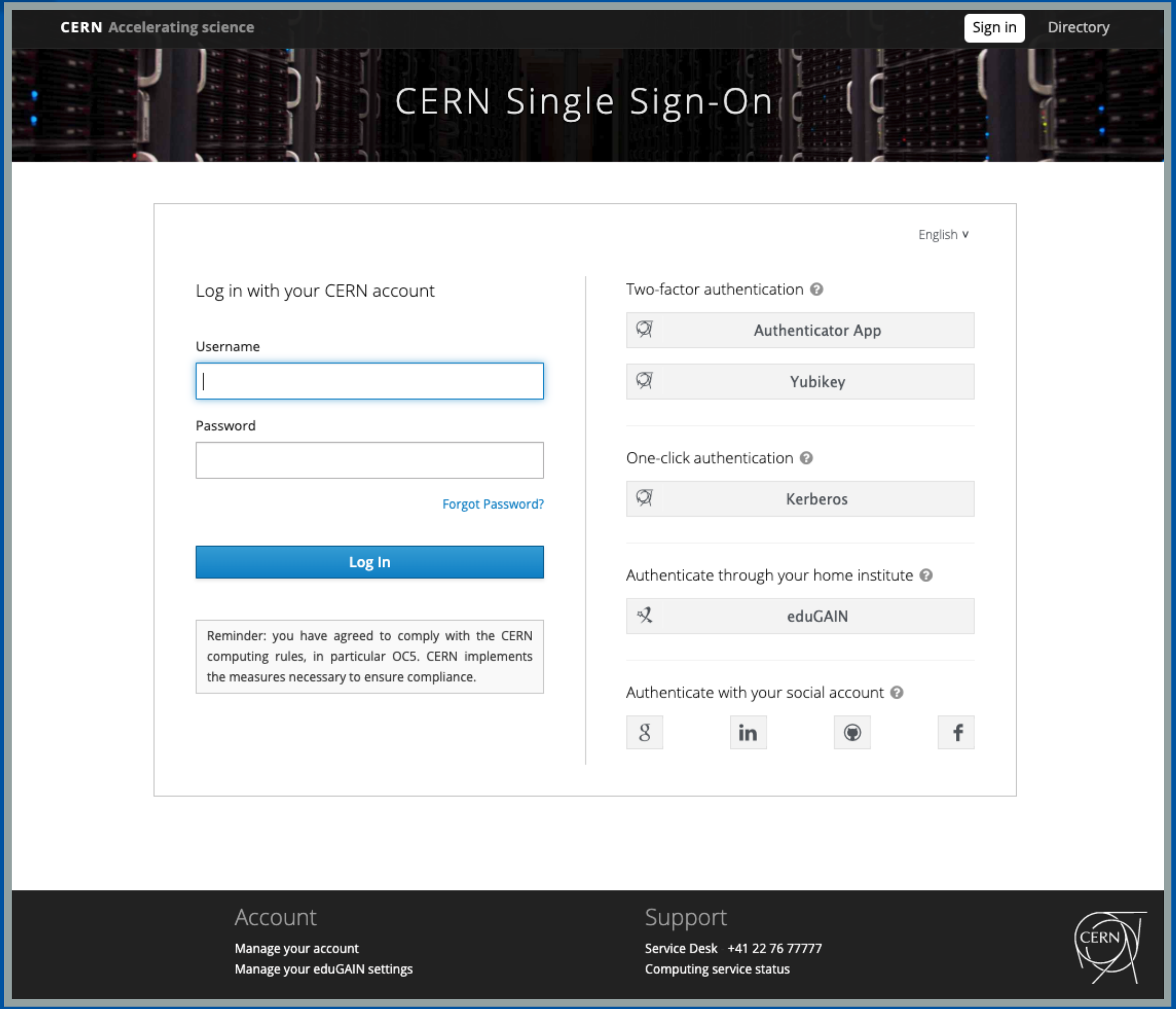

WLCG
WLCG IAM
Web Service, e.g. EDH
SAML
OIDC
Keycloak (Single Sign On)
FreeIPA (LDAP)
Account Management (FIM)
Foundation (HR DB)
Kerberos Based Service, e.g. lxplus
Kerberos LDAP
LDAP Based Service
e-groups

Timeline


AAI Roadmap
Single-Sign-On
Design
Development
Pilot
Migration
FreeIPA/LDAP
Design
Development
Pilot
Migration
w. 00
2019
2020
2021
2022
2023

What’s changing?

New Look



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

- Authenticator App
- Yubikey

One-click authentication

- Kerberos

Authenticate through your home institute

- eduGAIN

Authenticate with your social account

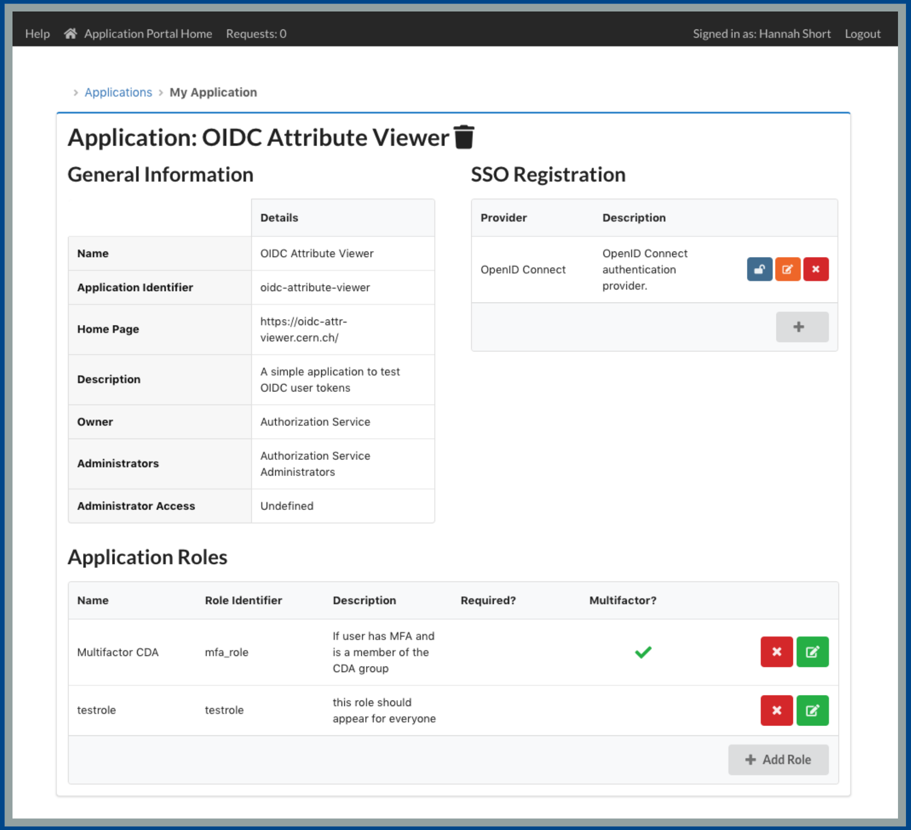
Account

Manage your account
Manage your eduGAIN settings

Support

Service Desk +41 22 76 77777
Computing service status

Roles



› Applications › My Application

Application: OIDC Attribute Viewer

General Information

	Details
Name	OIDC Attribute Viewer
Application Identifier	oidc-attribute-viewer
Home Page	https://oidc-attr-viewer.cern.ch/
Description	A simple application to test OIDC user tokens
Owner	Authorization Service
Administrators	Authorization Service Administrators
Administrator Access	Undefined

SSO Registration

Provider	Description
OpenID Connect	OpenID Connect authentication provider.

Application Roles

Name	Role Identifier	Description	Required?	Multifactor?
Multifactor CDA	mfa_role	If user has MFA and is a member of the CDA group		✓
testrole	testrole	this role should appear for everyone		

Application owners decide on roles for their application and map them to user groups

Tokens

OIDC support in addition to SAML

```
{
  "iss": "https://auth.cern.ch/auth/realms/cern",
  "aud": "oidc-attribute-viewer",
  "sub": "hshort",
  "typ": "ID",
  "cern_person_id": 777777,
  "name": "Hannah Short",
  "preferred_username": "hshort",
  "cern_roles": [
    "testrole",
    "mfa_role"
  ],
  "given_name": "Hannah",
  "cern_preferred_language": "EN",
  "family_name": "Short",
  "email": "hannah.short@cern.ch",
  "eduperson_orcid": "0000-0003-2187-0980",
  "cern_upn": "hshort"
}
```

Researcher Lifecycle Management

- Account linking
  - Retirees to maintain access without CERN accounts
- ORCID Researcher Identifiers

Get involved!

1. Become pilot users of the new Single-Sign-On
2. Enable OAuth2/OIDC for your use cases (web, grid)
3. Follow the Malt Project's progress