

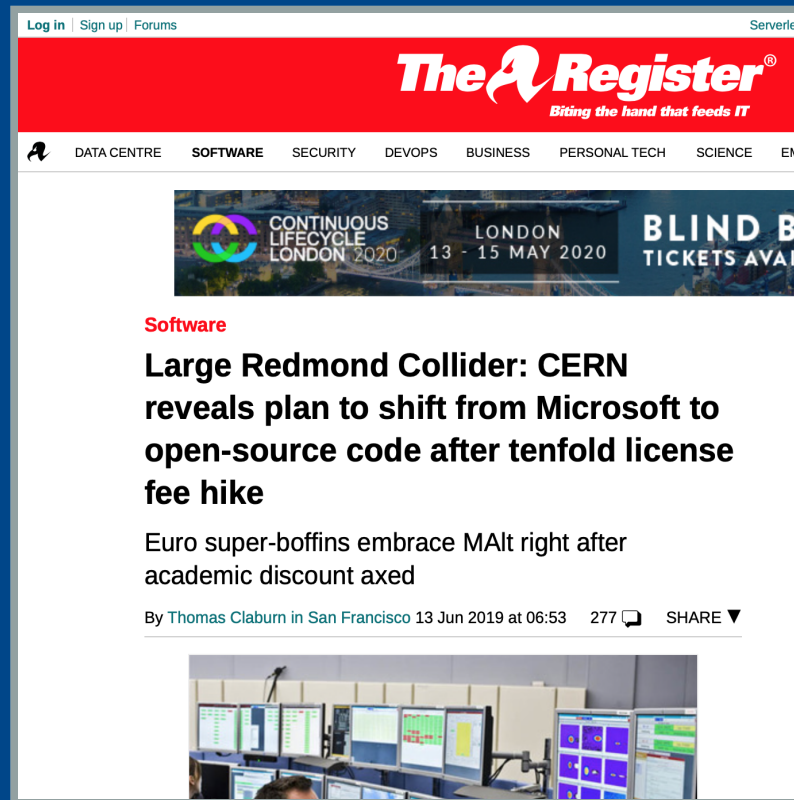
CERN's Identity and Access Management

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



The screenshot shows the homepage of The Register website. At the top, there is a navigation bar with links for "Log in", "Sign up", and "Forums". The main header features the "The Register" logo with the tagline "Biting the hand that feeds IT". Below the header is a secondary navigation bar with categories: "DATA CENTRE", "SOFTWARE", "SECURITY", "DEVOPS", "BUSINESS", "PERSONAL TECH", "SCIENCE", and "EMERGENCY". A banner for "CONTINUOUS LIFECYCLE LONDON 2020" is visible, with dates "13 - 15 MAY 2020" and "BLIND B TICKETS AVAIL". The main article is titled "Large Redmond Collider: CERN reveals plan to shift from Microsoft to open-source code after tenfold license fee hike". The author is "Thomas Claburn in San Francisco" and the date is "13 Jun 2019 at 06:53". The article has 277 comments and a share button. Below the text is a photo of a server room with multiple monitors displaying data.

Log in | Sign up | Forums Serverless

The Register[®]

Biting the hand that feeds IT



DATA CENTRE SOFTWARE SECURITY DEVOPS BUSINESS PERSONAL TECH SCIENCE EMERGENCY


CONTINUOUS LIFECYCLE LONDON 2020 13 - 15 MAY 2020 BLIND B TICKETS AVAIL

Software

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

Euro super-boffins embrace MAIt right after academic discount axed

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



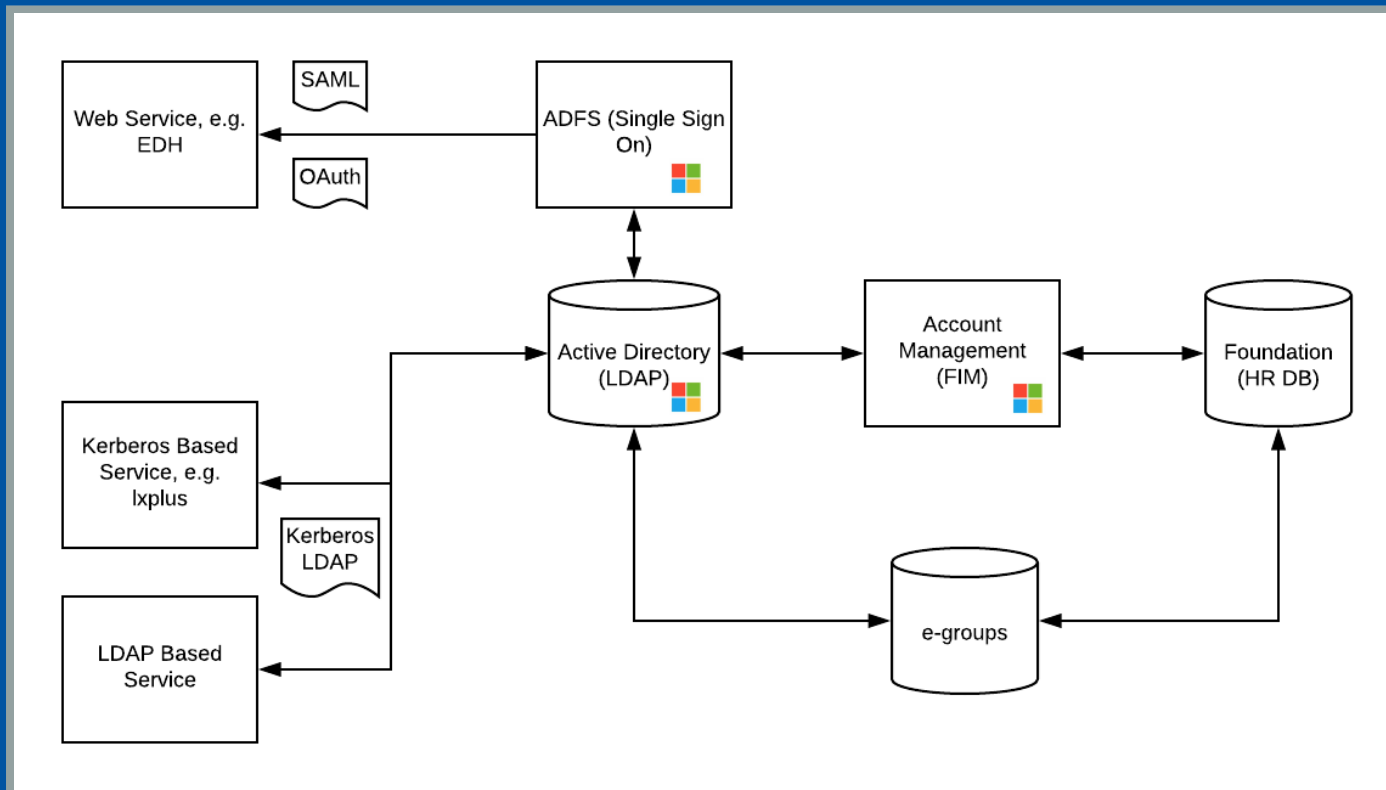
Why change?

- 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

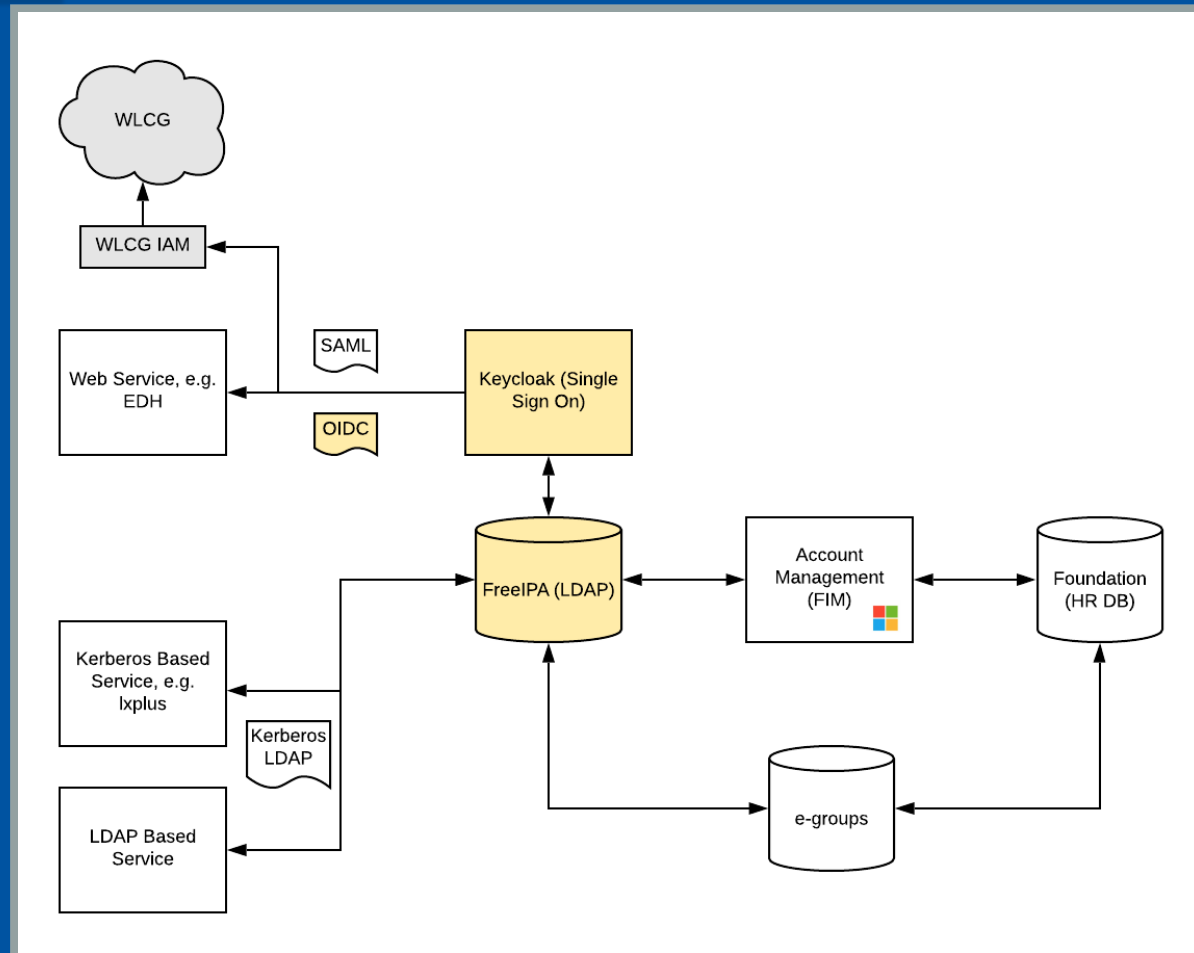
Principles of change

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

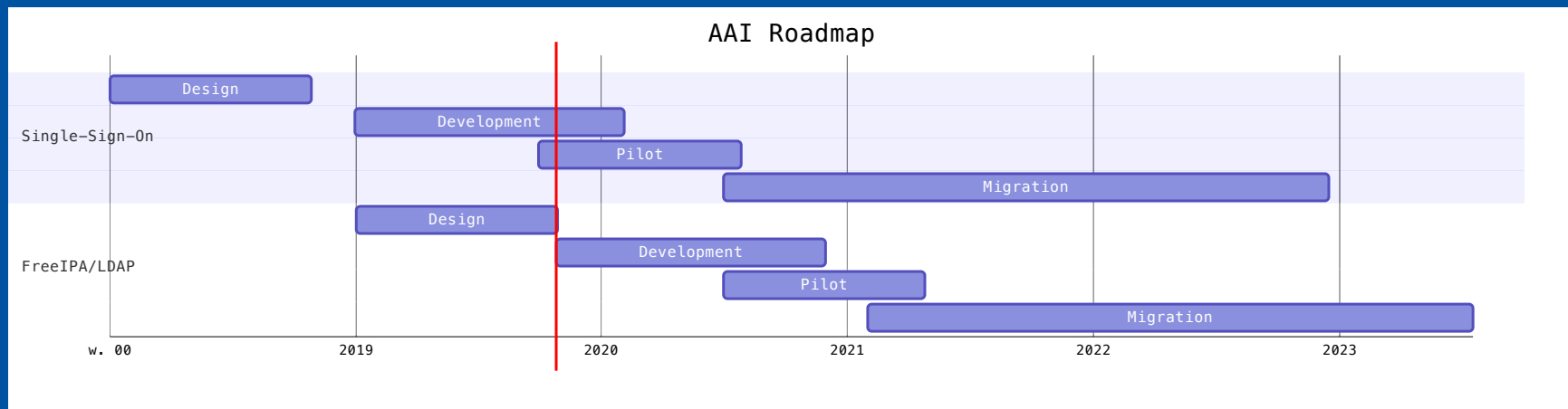
Before



After



Timeline



What's changing?

New Look

The screenshot displays the CERN Single Sign-On login interface. At the top left, it says "CERN Accelerating science". On the top right, there are "Sign in" and "Directory" links. The main header features a server rack background with the text "CERN Single Sign-On".

The login form is divided into two main sections:

- Log in with your CERN account:** Includes fields for "Username" and "Password", a "Forgot Password?" link, and a blue "Log In" button. A reminder box states: "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:** Includes buttons for "Authenticator App" and "Yubikey".
- One-click authentication:** Includes a button for "Kerberos".
- Authenticate through your home institute:** Includes a button for "eduGAIN".
- Authenticate with your social account:** Includes icons for Google, LinkedIn, and Facebook.

At the bottom, there are sections for "Account" (Manage your account, Manage your eduGAIN settings) and "Support" (Service Desk +41 22 76 7777, Computing service status). The CERN logo is in the bottom right corner.

Roles

The screenshot shows a web application management interface. At the top, there is a navigation bar with 'Help', 'Application Portal Home', 'Requests: 0', and 'Signed in as: Hannah Short Logout'. Below the navigation bar, the breadcrumb path is '> Applications > My Application'. The main content area is titled 'Application: OIDC Attribute Viewer' and is divided into two sections: 'General Information' and 'SSO Registration'. The 'General Information' section contains a table with the following data:

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

The 'SSO Registration' section contains a table with the following data:

Provider	Description
OpenID Connect	OpenID Connect authentication provider.

Below the 'SSO Registration' table is an '+ Add Role' button. The 'Application Roles' section contains a table with the following data:

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		

At the bottom of the 'Application Roles' table is an '+ Add Role' button.

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