MFA in Helmholtz AAI

and a small addition to OIDC and SCIM

Sander Apweiler

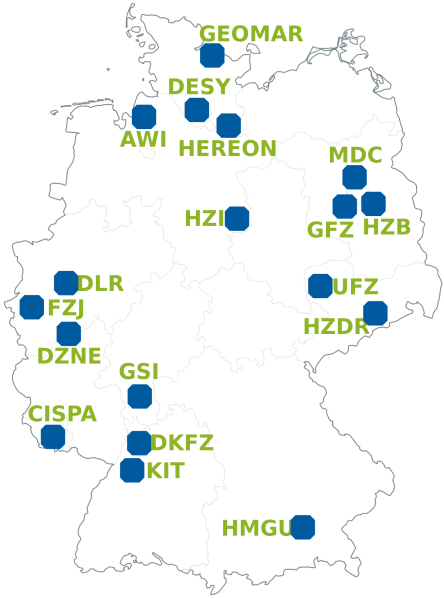
Forschungszentrum Jülich / 2023-05-15

Agenda

- Helmholtz AAI
- AARC
- OIDC
- SCIM
- MFA

Helmholtz AAI

Helmholtz AAI - Helmholtz Association



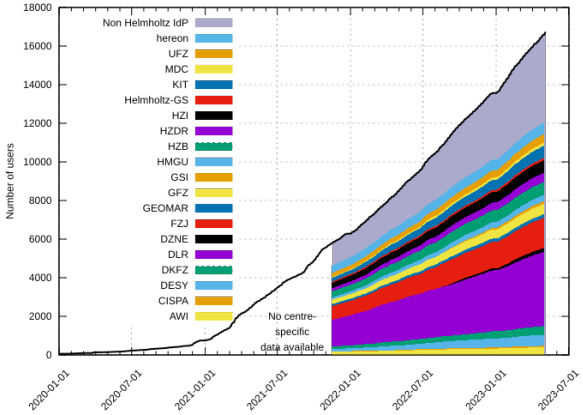
- Over 43.000 Employees
- 18 centres + head office
- 19 completely independent legal entities
- 19 data protection officers
- 19 employee representatives
- 19 information security officers

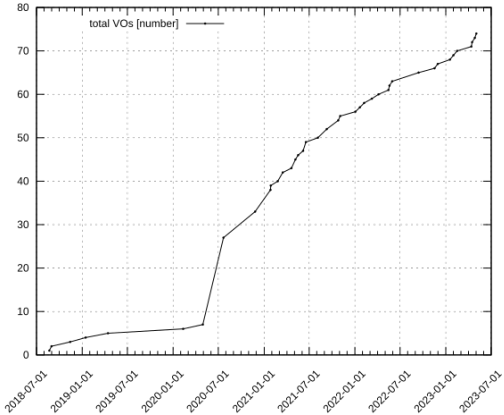
Helmholtz AAI - some numbers

- 2018 started as HDF AAI in Helmholtz Data Federation project
- 2019 co-used in HIFIS platform
- 2020 re-branded as Helmholtz AAI and first services online
- Since 2021 fully funded by HIFIS

Helmholtz AAI - some numbers

- More than 16.000 user
- 147 services from 2/3 of the Helmholtz centres
- Supporting 74 research groups / projects





Helmholtz AAI - features

- Operates as SP-IdP-Proxy following the AARC Blueprint
- Translates between different authentication protocols
- Offers group management
- Enabling MFA
- Preparing automated deprovisioning flow of users
- Compliant to EOSC guidelines for easy exchange with other infrastructures

AARC

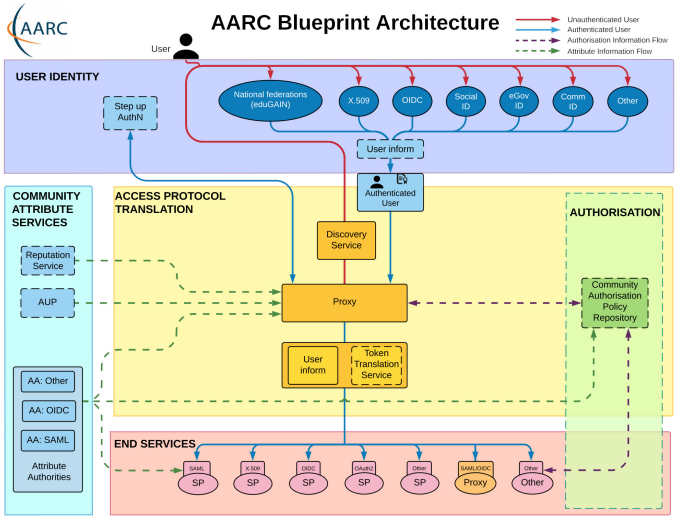
AARC - about

- Authentication and Authorisation for Research and Collaboration
- Launched in May 2015 as EU-funded project to address need for federated access and authentication & authorisation mechanisms from research and e-infrastructures
- Created guidelines, policies and blueprint architecture in this area
- Since 2019 work is ongoing without funding
- Validation of outcomes by AEGIS (AARC Engagement Group for Infrastructures)
  - Members from Europe and America
  - Observers from Europe and Asia
- AARC BPA and guidelines are basis of EOSC

AARC - important guidelines

- AARC-G002/G069: exchange of group membership and role information
- AARC-G027: exchange of resource capability information
- AARC-G045: Blueprint Architecture
- Policy Development Kit

AARC Blueprint Architecture



source: AARC

OIDC

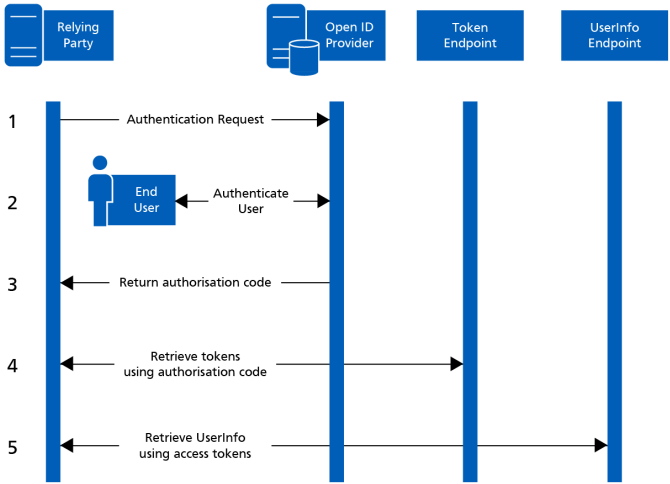
OIDC - key terms

- **OpenID Provider (OP)**: authentication server, like SAML IdP
- **Relying Party (RP)**: service which requests user authentication, like SAML SP
- **Claim**: a piece of information about an entity
- **Scope**: a set of claims
- **ID Token**: JWT containing claims about authentication event and optionally about the user
- **Access Token**: credential used to access resources, representing specific scopes and validity
- **Refresh Token**: credential to request access tokens, if current access token becomes invalid; bound to a RP
- **Token Endpoint**: part of the OP, which releases the tokens to RP
- **Userinfo Endpoint:** part of the OP, which returns information about an user belonging to an access token

OIDC - grant types

- Implicit Flow
  - Required for applications having no ”‘back-end”’ logic
  - E.g. Javascript applications
  - Not recommended for other applications
- Authentication code
  - For web-server applications having an own back-end
  - Covers most uses-cases
- Device flow
  - Flow without own login UI
  - Designed to browserless applications, where the service is not able to capture user credentials securely, e.g. IoT
  - Outsources user authentication to en external device, e.g. smart phone
- Client Credentials
  - Used in machine to machine authorization.

OIDC - Authorisation code grant type



source: NHS Digital

OIDC - reasons to use

For service providers

- Easier to integrate and implement than SAML
- Can be used in a wider range than SAML, e.g. device flow
- Valid access tokens can be reused by other RPs, which allows service interconnections without additional credentials

For users

- Standard which is used in industry
- Can be used on mobile devices and REST APIs
- Valid access tokens can be reused by other RPs

SCIM

SCIM - in the Helmholtz AAI

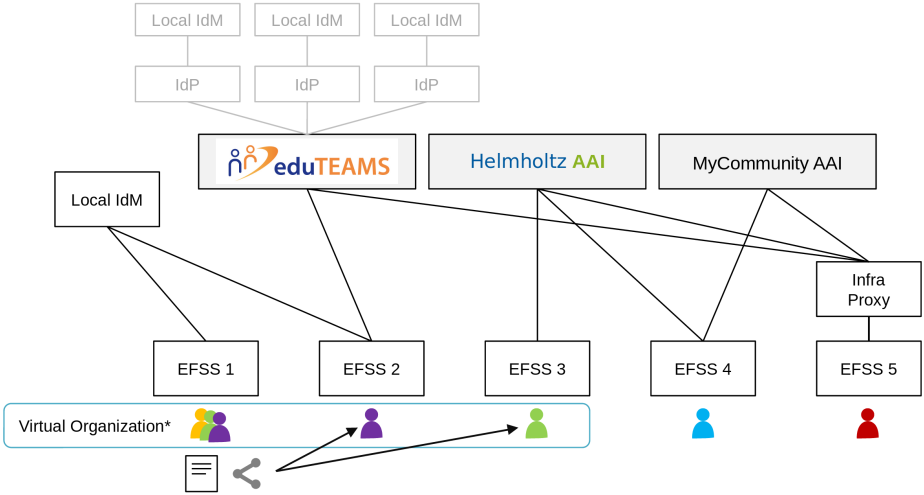
- Used as extension where information exchange via user authentication is not sufficient
- Pulling authorization information regularly
- E.g. updating group membership information even if the user does not login
- Authentication against the Helmholtz AAI with OIDC tokens of the user
- At the moment still in deployment

SCIM - usecase

Problem:

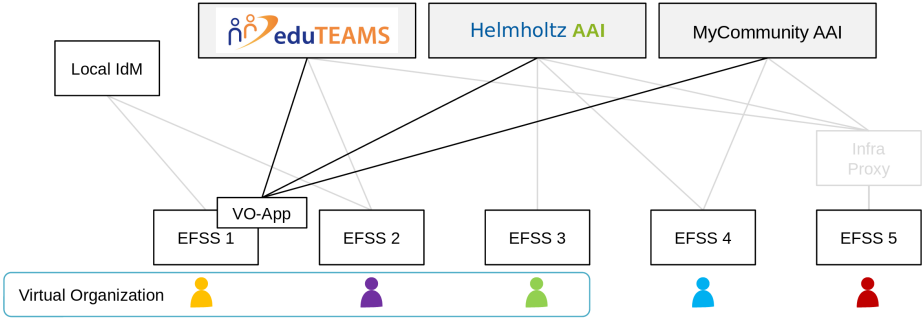
- Multiple research centres provide EFSS service
- Different instances are used in different projects
- Researchers are part of multiple projects and have multiple accounts
- Researchers need to search where the data was shared
- Providers need to buy more licenses than needed

SCIM - usecase

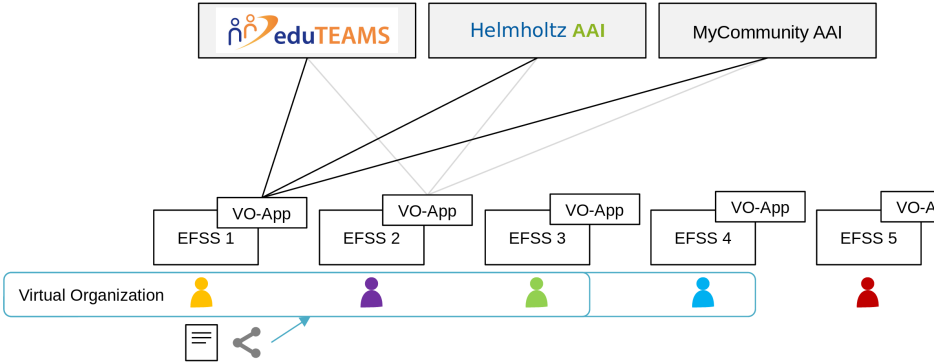


* a group of any size. It may just be two persons or a whole research center/community

SCIM - usecase



SCIM - usecase



MFA

MFA - basics

- User authentication should be secured/account hijacking avoided by providing multiple factors
- The factors are
  - Knowledge, e.g. password
  - Ownership, e.g. smartphone
  - Inherence, e.g. fingerprint
  - Location
- Using one factor multiple times, e.g. password and security questions does not secure the authentication in this sense
- Mainly used is 2 factor authentication (2FA) where two factors are combined

MFA - 2FA

- Most common in 2FA is using the password and a (time-based) onetime password (TOTP)
- Different ways for providing (T)OTPs
  - Authenticator apps, which are creating the TOTPs after registration at the services
  - OTPs via SMS/E-Mail
  - OTPs via proprietary apps of the service provider
- Fido/U2F uses a dedicated device as second factor which is verified by the service

MFA - 2FA problems

- (T)OTPs
  - Some authenticator apps, did not work that secured like they should do
  - Missing import and export functions makes it hard if the used device is changed
  - Reusing the password manager which stores already the password is not really a second factor
  - OTPs via SMS/E-Mail is prone to SMS-Spoofing and Man in the middle attacks
- Fido/U2F is not offered by all services who are offering 2FA

MFA - signalling

- Policy which allows only users that authenticated with MFA to access the service
- If no policy is in place the service needs to be informed if MFA was performed
- SAML: set `AuthnContextClassRef` to `https://refeds.org/profile/mfa`
- OIDC: set `acr` claim to `https://refeds.org/profile/mfa`

`https://refeds.org/profile/mfa` criteria:

- User's current session used a combination of at least two of the four distinct types of factors
- The factors used are independent, in that access to one factor does not by itself grant access to other factors.
- The combination of the factors mitigates single-factor only risks related to non-real-time attacks such as phishing, offline cracking, online guessing and theft of a (single) factor.

MFA - What about AARC

- Not yet a guideline in place
- But a guideline for step-up authentication (G029) is in place
- Containing the information from previous page
- MFA from (home-)IdP is preferred to third-party services
  - They are close to the user
  - Benefit for the user having less 2nd factors

MFA - Helmholtz AAI

- Start enforcing if in beginning of 2023 using TOTP
- At the moment only for administrators
- Next steps are enforcing it on OIDC RPs (to change their configuration) and group managers
- Optional for users in summer
- If MFA was performed by the home IdP, Helmholtz AAI should not repeat it but transfer information to services
- Investigate and test support of FIDO additional to TOTP end of the year

Time for questions