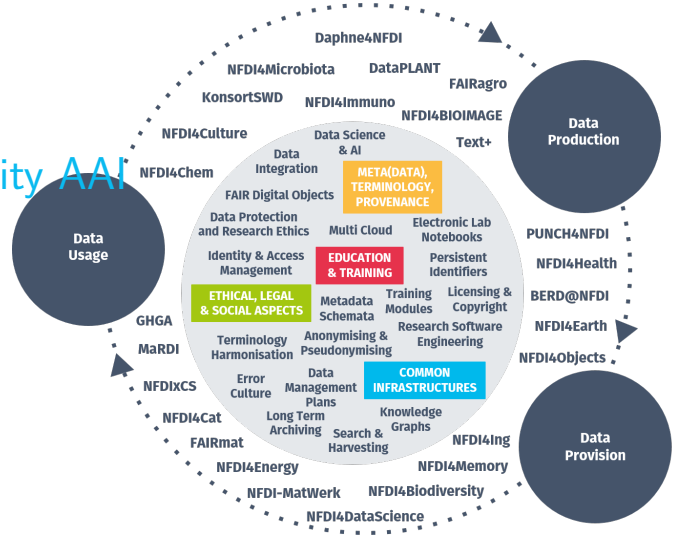
base4nfdi Basic Services for NFDI

# Unity-IdM as Community AAI

## IAM4NFDI workshop

18.01.24

Sander Apweiler, Laura Hofer




base4nfdi Funded by **DFG** as part of **NFDI**.
Grant Numbers: 521453681, 521460392, 521462155, 521463400, 521466146, 521471126, 521473512, 521474032, 521475185, 521476232

# Agenda

- Basics
- User authentication
- Group management
- Client registration
- Policy management
- Attribute management
- Other
- WIP/Outlook

# Basics

Development of unity:

- Unity-IdM started in 2013, under open source license
- Since 2016 BixBit offers paid support and feature requests
- 2021 BixBit launched Authvisor trademark for public commercial support

The software itself:

- Java based
- All-in-one software solution
- Configuration via files or web UI
- Supports most common authentication protocols
- Several pre-configured upstream IdPs

Features:

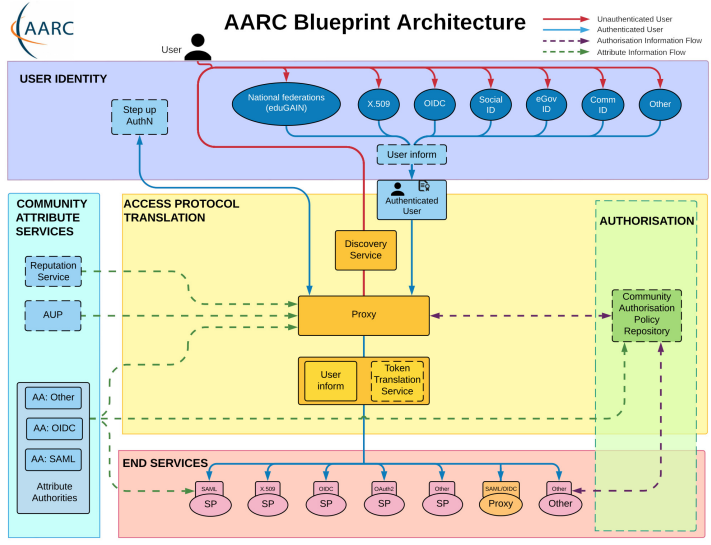
- Tree-based user directory
- Policy management
- Group management (delegation)
- Dynamic attribute creation
- Multi-factor authentication (MFA)
- Separated web interfaces for system administrators and group managers
- Extendable by third party applications due to different REST APIs
- Account linking

Features:

- Multi protocol identity management
  - OAuth2
  - OIDC
  - SAML2 single IdP
  - SAML2 Federation
  - LDAP authentication

# Basics

Unity fulfils AARC BPA and contains the Access protocol translation layer, parts of authorisation and community attribute services



Who uses unity?

- EUDAT CDI

  Collaborative EUDAT Data Infrastructure
  Data shared and preserved across borders and disciplines

- HELMHOLTZ / HIFIS

  HELMHOLTZ RESEARCH FOR GRAND CHALLENGES

  HIFIS HELMHOLTZ FEDERATED IT SERVICES

- FENIX

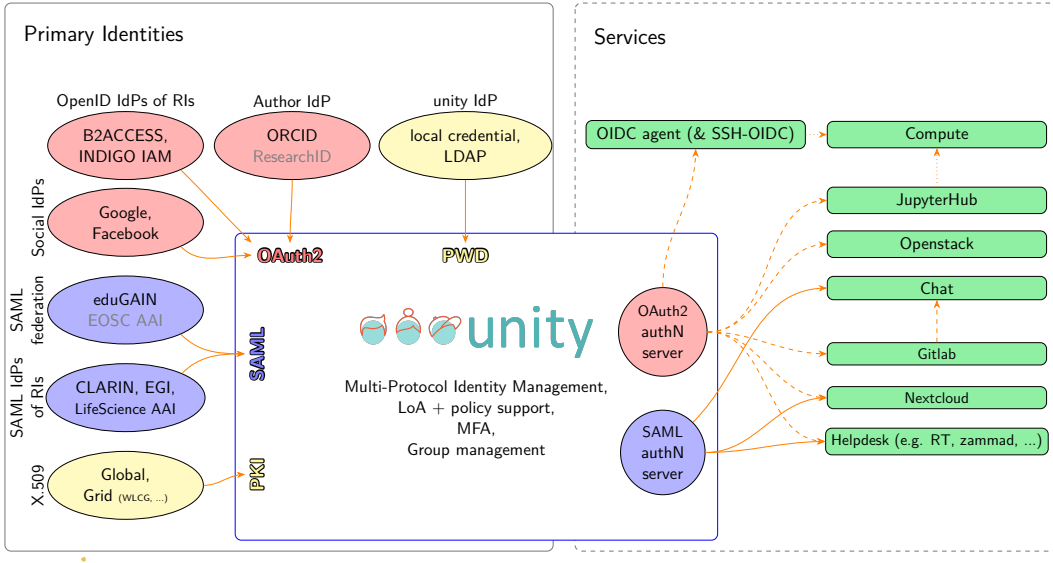
  FENIX RESEARCH INFRASTRUCTURE

- PUNCH4NFDI (early adopter in NFDI and role model for other consortia)

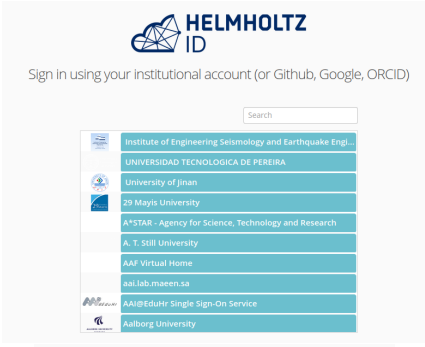
  Particles, Universe, NuClei and Hadrons for the NFDI
  A consortium in the NFDI

# User authentication

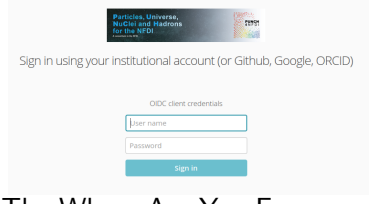
# User authentication - overview

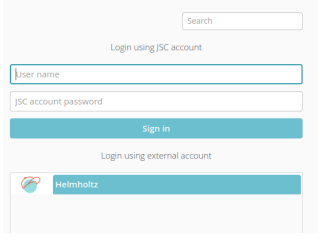


# User authentication - customisable WAYF





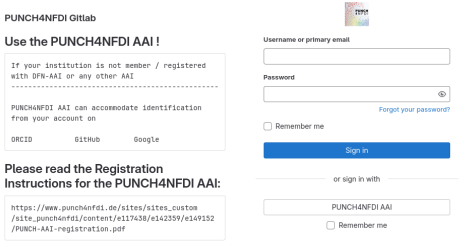


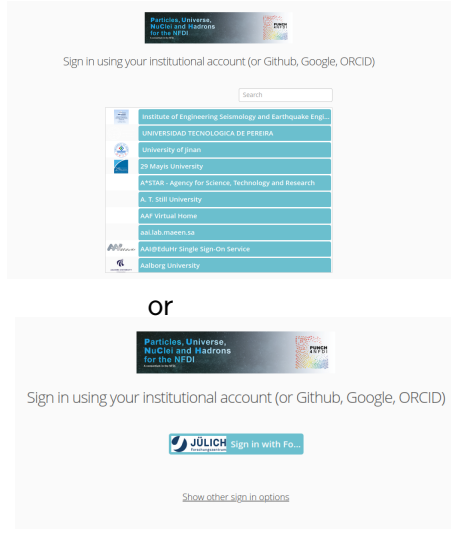




The Where-Are-You-From service can be customized to limit or highlight the connected authentication services

base4 nfdi

# User authentication - flow example with PUNCH Gitlab

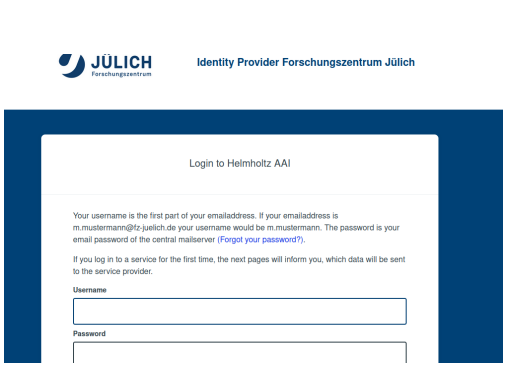


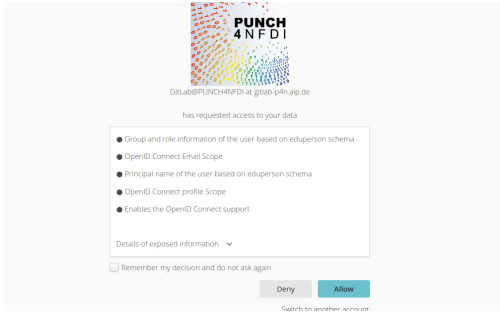

Press on PUNCH4NFDI button to start authentication

Select your institute or other for authentication; your last choice might be preselected

# User authentication - flow example with PUNCH Gitlab



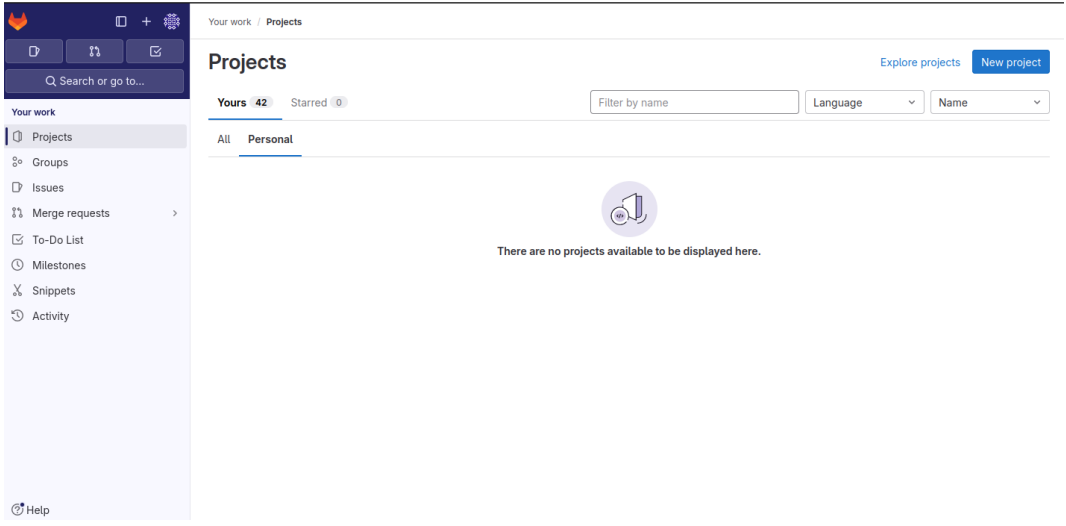

Login screen of the home organisation




Released attributes from unity to the service can be reviewed and the decision stored for the next time. In this case the window is not shown again

base4 nfdi

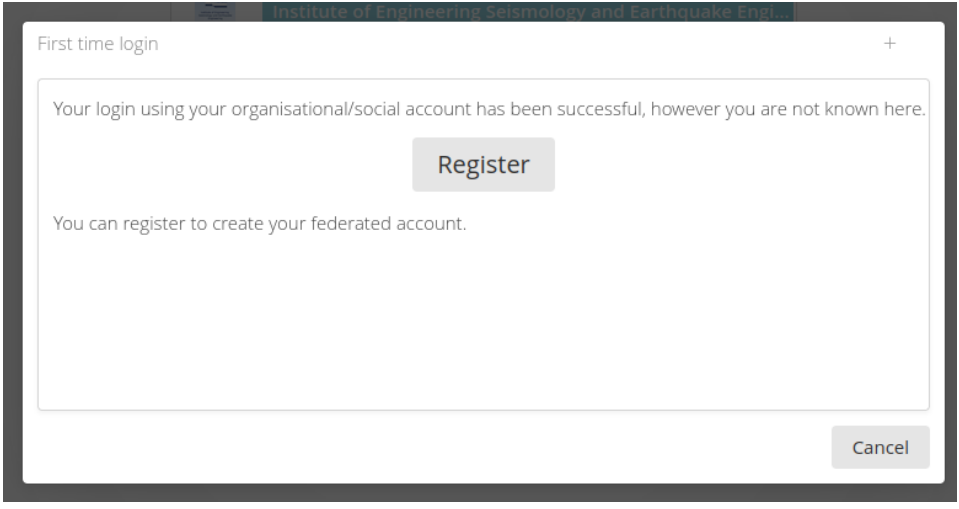
# User authentication - flow example with PUNCH Gitlab




Successfully logged into PUNCH Gitlab

base4 nfdi

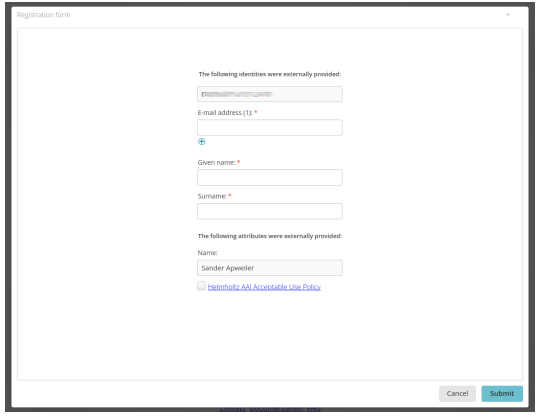
# User authentication - new users




If users appear for the first time with the chosen account, they need to register (or link to an existing account, if supported by the instance)

# User authentication - new users


If the external account provides all information, users must accept policies




Otherwise they need to enter mandatory information as well

base4 nfdi

# User authentication - new user

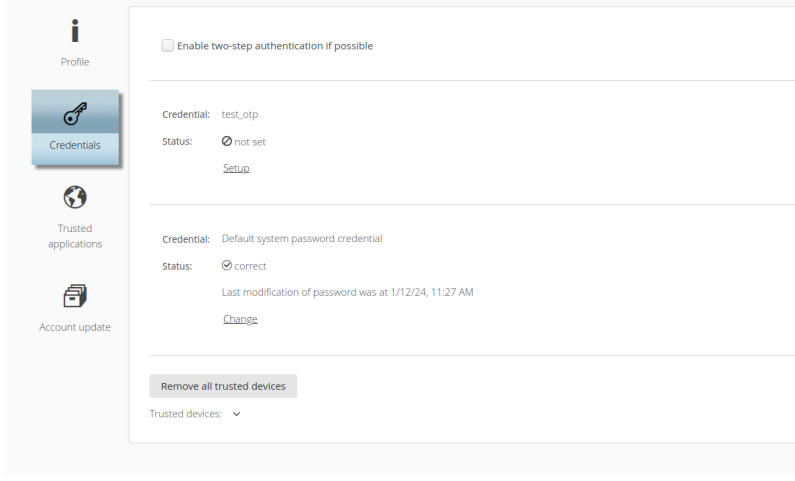
- The set of provided attributes differs, especially for social IdPs
- User may need to confirm their email, before the account is finally created
- Multiple policies may be displayed

## User authentication - multi-factor authentication

- Unity supports TOTP or FIDO for MFA
- At the moment just TOTP tested
- Can be optional or enforced
- Improvements in area of MFA are ongoing, see WIP/Outlook section

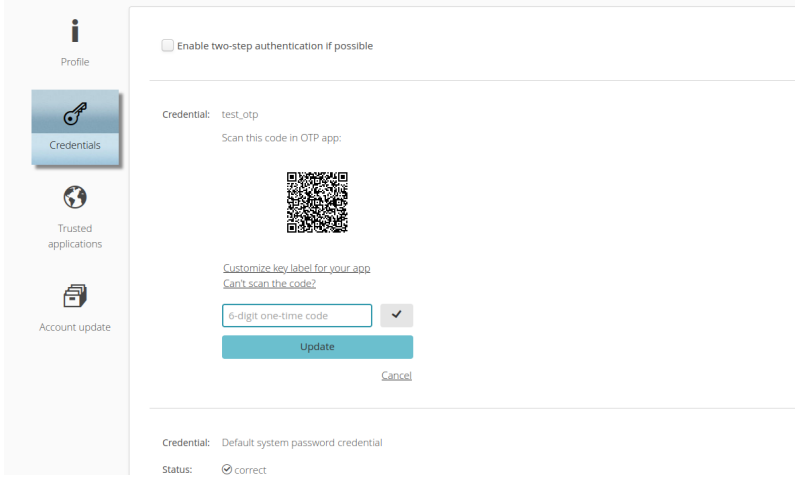
# User authentication - multi-factor authentication

User set MFA usage in credentials tab of home endpoint



# User authentication - multi-factor authentication

Common setup for TOTP sync between service and device



# Group management

# Group management

- Unity has it's own endpoint for group management
- Group managers can
  - Invite people by email
  - Manage requests
  - Create group structure
  - Grant/revoke management permissions to/of other members
  - Delegate management of sub-groups
- Group management must be prepared by the unity administrators
- Groups can be
  - free for all without further validations
  - free for all on request with validation of group managers
  - closed, by invitation only
- Unity labels a group as a project

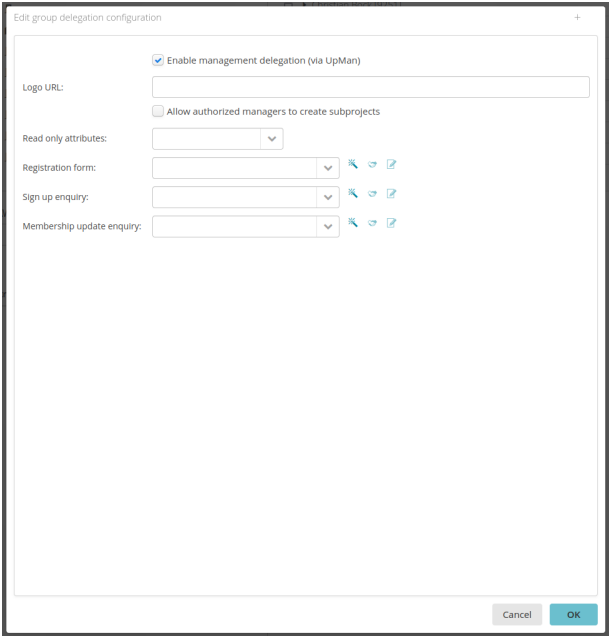
# Group management - creating new groups

New groups are created and prepared by the unity administrators via web-UI or API

- Create new sub-group in unity's user directory
- Enable delegation configuration
  - Create registration and enquiry forms
  - Set logo, if desired
  - Allow delegation of further sub-groups, if desired
- Add a manager to the group and grant group management permissions

# Group management - creating new groups

Forms can be created automatically, using the wand symbol in the UI and fine-tuned afterwards



## Group management - creating new groups

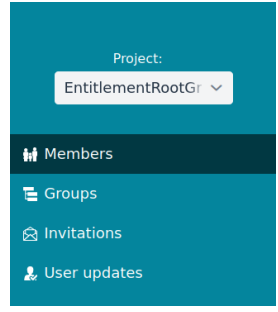
Semi-Automated groups are possible as well

- Instead of enabling the delegation configuration
- Users are added automatically by some defined condition to a group, e.g. remote authentication
- But users are not removed, if the condition is not met at the next login
- Adding a rule in input translation profile for this

```
{
    "condition":{
        "conditionValue":"idp == 'https://idp.its.fz-juelich.de/idp/shibboleth'"
    },
    "action":
    {
        "name":"mapGroup",
        "parameters":["'/FZJ'","REQUIRE_EXISTING_GROUP"]
    }
}
```

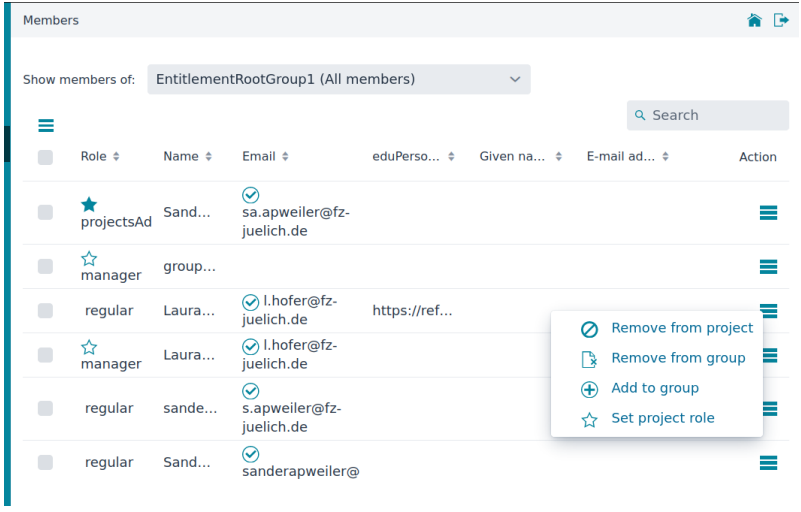
# Group management - group management endpoint

- Drop-down list shows manageable groups
- Members tab: management of the group members
- Groups tab: creating and adjusting the group structure
- Invitations tab: invite new users
- User updates tab: review user requests



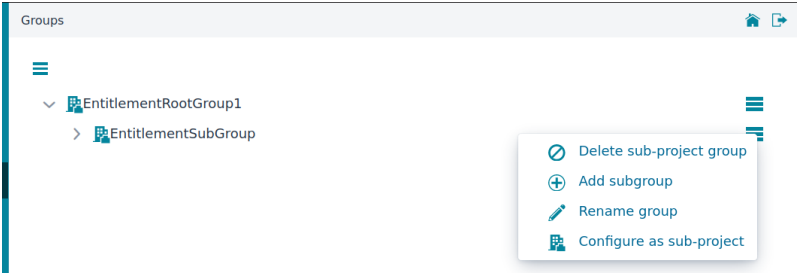
# Group management - member management tab

- Delete members from project (whole group)
- Delete members from current (sub-)group
- Add user to another sub-group
- Set role of a member



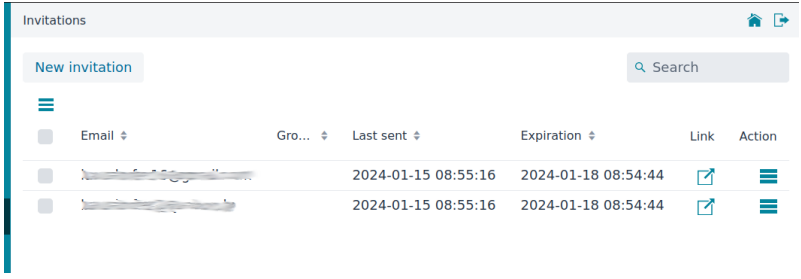
# Group management - group management tab

- Add or delete sub-groups
- Rename a group
- Configure a sub-group to delegate the management



# Group management - invitation tab

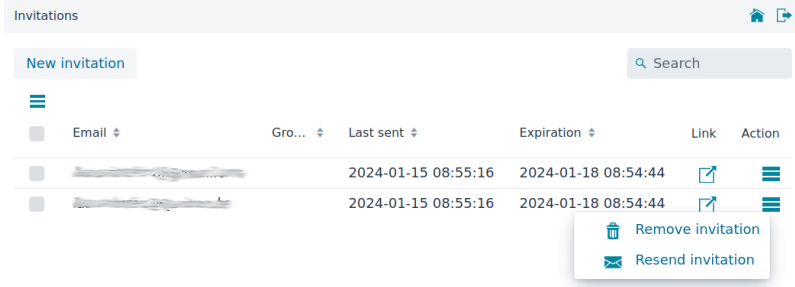
- Review all invitations
- Create new invitations



# Group management - invitation tab

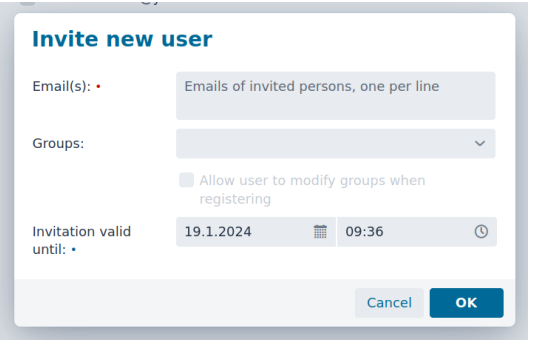
Not expired invitations can be

- resent
- revoked



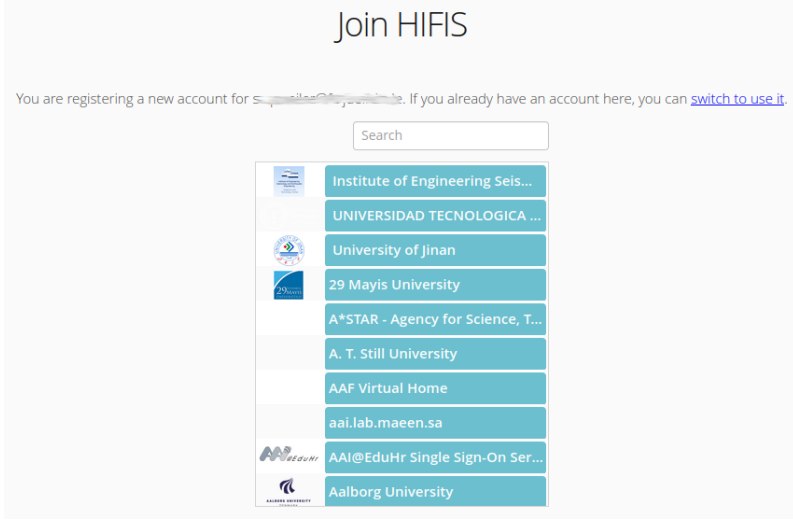
# Group management - invite user

- Add the email addresses of the users (one per line)
- Optional subgroups can be added
- Validity of the invitation can be adjusted
- Invitee receives an email with link to join the group
- The invitation is sent to the provided email address, but not bound to it



# Group management - accept invitation

User can create a new account or switch to sign into an existing one



# Client registration

# Client registration - OAuth2/OIDC

- OAuth2/OIDC clients are accounts in unity itself
- Therefore they are not bound to any user
- Can be created by the service operator directly, using registration forms
- Adding a rule in input translation profile for this
- Automated or manual acceptance by the unity administrators

# Client registration - OAuth2/OIDC

Different level of attributes during the registration

- Technical mandatory
  - Username/password, aka Client ID and secret
  - Return or redirect URL of the client
- Optional for enhancement of the login flow to the users
  - Client name
  - Logo
- Mandatory, due to policy or law, e.g.
  - Contact
  - Link to service data privacy statement

# Client registration - SPA & public clients

The client credentials of Single Page Applications (SPA) or non web application might not be kept on the web-server and the authentication is handled at the computer of the user. For those scenarios public clients can be used.

- Application must use Proof Key for Code Exchange (PKCE)
- Return URL must still match
- User can not save their consent

# Client registration - SAML2

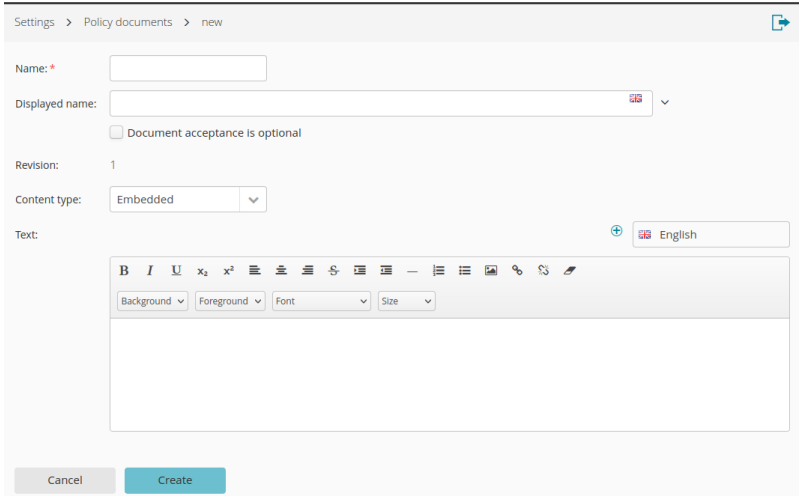
- SAML trusted applications are added by the unity administrators
- In configuration files or web UI, depending on the operation model
- Technical mandatory information
  - entityID of the client
  - URL of the assertion consumer service (return URL)
- Optional information to enhance user experience
  - Client name
  - Logo

# Policy management

# Policy management - accept invitation

Policy document

- Is formatted text or link to external URI
- Is mandatory or optional
- Has a version number



# Policy management

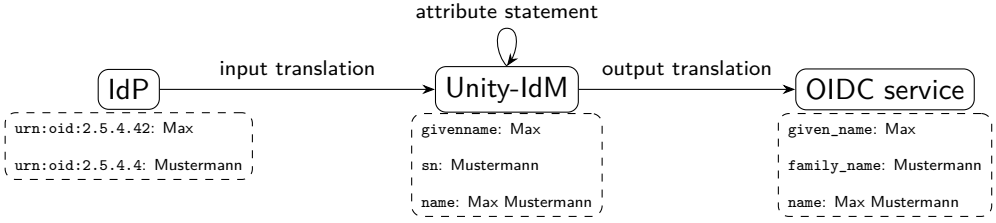
- The policy documents are created by the unity administrators
- Updates can be silent or create a new version
- New versions are shown to users at the next login
- Policy documents are part of the user registration or user update
- Accepted policies are stored with date and version in an internal attribute

# Attribute management

# Attribute management

- Attributes can be configured quite flexibly
  - 13 different types (common and special types)
  - Single or multi-valued (limited or unlimited)
  - Unique values in multi-value attributes
  - Self modifiable
- Some attributes are already pre-defined

# Attribute management - attribute translation




- Attributes from IdP are translated in input translation profile to local format
- Attributes from unity are translated in output translation profile to expected format of services
- Attribute statements can create new attributes based on existing information

## Attribute management - attribute translation

- Translation profiles are converting attributes between protocol specific names and an internal database
- Translation profiles are configured as JSON files or in web UI
- Multiple attributes can be combined to a single one within the translation profiles
- Attribute statements create new attributes based on information from internal database
- Attribute statements can be simple, like combine existing attributes or copy information into another group, or complex, like expressing group structure and membership information into an attribute
- Each group has it's own attribute statements
- Attribute statements are configured in web UI using MVEL

# Attribute management - attribute translation

- In some cases additional information, beside the information from the IdP, are required
- Unity can query an LDAP for additional information, during the login

# Others

## Others - IdP hinting

- Some services want to recommend an IdP for sign in
- Those clients can use IdP hinting
- The client need to add `uy_select_authn=` as query parameter and add the internal IdP ID
- The AARC guidelines are not supported, but this is in discussion with BixBit

## Others - attributes in OIDC claims

- Some services require user attributes within the token
- PUNCH4NFDI compute workflows are the first service, which required this and made a feature request for it
- The client needs to add `claims_in_tokens` as query parameter to the authorization URL call
- The returned token contains all attributes, which can be fetched from the user info endpoint as well

# WIP/Outlook

# WIP/Outlook

WIP: already implemented in unity but not yet (fully) configured
Outlook: needs implementation in unity and is in discussion with BixBit

WIP:

- Deprovisioning
- SCIM API
- Step-up AuthN
- FIDO

Outlook:

- MFA enhancement

# WIP/Outlook - deprovisioning

- Handled by external app
- Workflow with check at home organisation, if possible
- Fail-over with email to users
- Already working
- Extend logging of account deletion and notifications to connected services

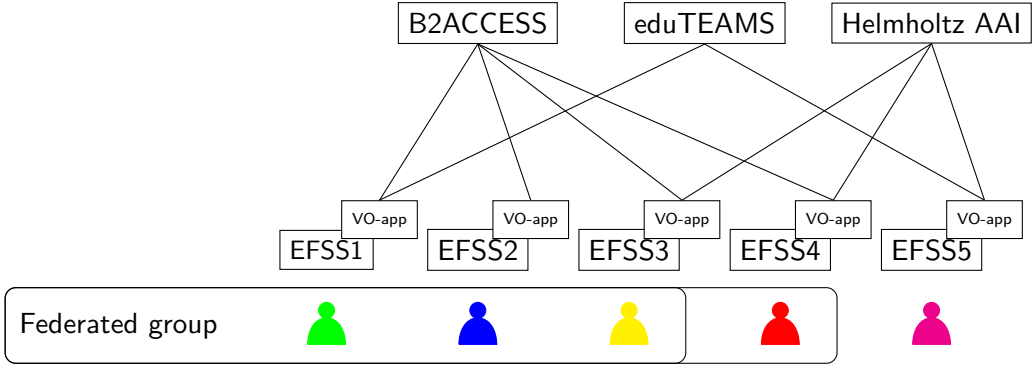
# WIP/Outlook - SCIM API

- Requesting information of a user or members of a group
- Schema are prepared
- Already successful tested with administrator account
- Working on queries with OAuth token

# WIP/Outlook - SCIM API - use-case

- Designed by HIFIS
- Map group membership information from different Identity providers, into EFSS, without offering authentication by them
- Periodical update of group membership information without user login using SCIM and OIDC
  - New members get access to data without re-sharing
  - Former member loses access to the data

# WIP/Outlook - SCIM API - use-case



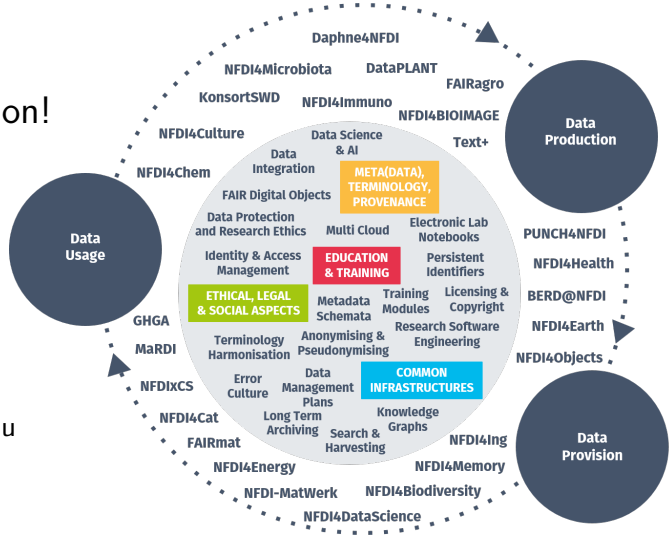
# WIP/Outlook - MFA enhancement

- Honor MFA from remote IdP and do not ask for second factor itself
- Inform services about MFA usage via protocol standards
- Support MFA requests from services

Thank you for your attention!

Questions?

Contact: aai-kernteam@lists.kit.edu




base4nfdi
Funded by **DFG** as part of **NFDI**.
Grant Numbers: 521453681, 521460392, 521462155, 521463400, 521466146, 521471126, 521473512, 521474032, 521475185, 521476232