



UNITY

within Helmholtz Data Federation AAI

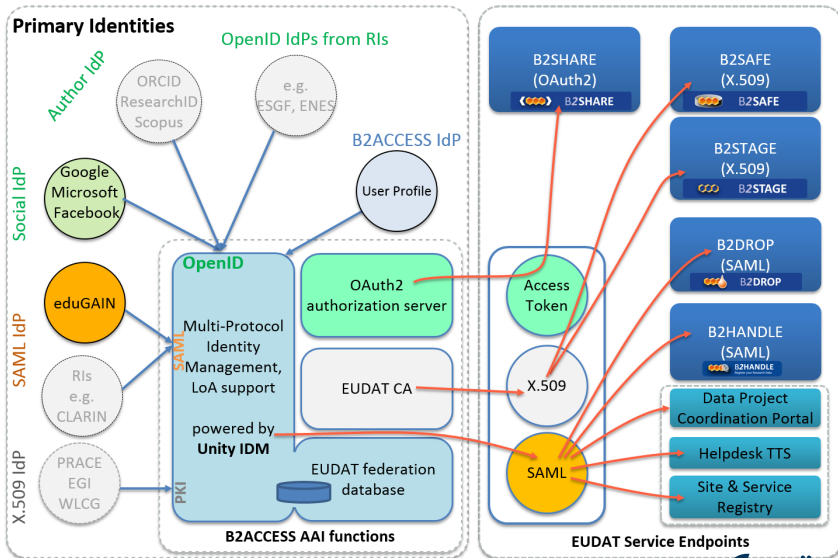
30. August 2018 | Sander Apweiler | JSC

1. Application description
2. Service integration
3. Group management
4. User management
5. Open issues/enhancements

Application description

- Proxy IdP with protocol translation
- Can be used as IdP without the proxy part
- Has multiple endpoints (SP Gateways)
 - Multiple SPs can use the same endpoint
 - SPs can use dedicated endpoints
- Offers multiple authenticators
 - An authenticator can be used for multiple endpoints
 - An authenticator can be dedicated for one endpoint

PROTOCOL TRANSLATION





Profile



Credentials
management



Preferences



OAuth Tokens

Displayed name: Sander Apweiler

Credentials status: sys:password: not set
Certificate credential: correct

Groups membership: /

Anonymous Identifier : 063ae90a-e7e1-4b47-b0c4-818a7af851bd


Identifier: sa.apweiler@fz-juelich.de


Name: Sander Apweiler

E-mail address: sa.apweiler@fz-juelich.de [confirmed at 8/20/18 2:55 PM]

eduPersonPrincipalName: sa.apweiler@fz-juelich.de

eduPersonScopedAffiliation: staff@fz-juelich.de


Preferred username: 

Public SSH key: 

 Save

 Refresh

Associate another account...

 Remove account

[Data Privacy Statement](#) [Services](#) [AUP](#)



Profile



Credentials
management





Preferences



OAuth Tokens

Credentials status:

-  Password credential
-  Certificate credential

Credential to be updated:

Password credential 

Description: Default system password credential

Current status: not set

New value

New password: *

Repeat the password: *

Update



Profile



Credentials
management



Preferences



OAuth Tokens

UNICORE

OAuth preferences

SAML Authentication

 Save

 Reset

 Refresh

Relying service provider (SP) ^



Profile



Credentials
management



Preferences



OAuth Tokens

 Refresh

 Remove

<input type="checkbox"/>	Type ^	Value	Client	Issued	Expires	Scopes	Refresh token	

ADMIN UI

HDF dev AAI administration interface

Logged as: Sander Apweiler



Contents management

Registration & enquiry

Schema management

Server management

Groups



- ▼ Root (/)
- ▶ GSI user group (/GsiUserGroup)
- ▶ AAI Administrators (/aai-admin)
- ▶ FEUDAL Test (/feudal-test-group)
- ▶ hdfdev (/hdfdev)
- ▶ myExampleColab (/myExampleColab)

Group details

! No group is selected

Group members

! No group is selected

Attributes

! No entity is selected

[Data Privacy Statement](#) [Services](#) [AUP](#)

ADMIN UI

Divided in four sections

- Contents management
 - Add, delete and edit groups
 - Manage user attributes
 - Edit group membership
 - Disable and remove user
- Registration & enquiry
 - Manage registration and enquiry forms
 - Accept, create, delete or reject registration requests
 - Create invitations

ADMIN UI

- Schema management
 - Manage attribute definitions
 - Manage credential types and definition
 - Manage identity definitions
- Server management
 - Configuration of the system itself
 - Manage authenticators, endpoints and translation profile
 - Edit message templates
 - Create or restore database backups

Service integration

SERVICE INTEGRATION

Services can be connected via

- SAML
 - Must be added in configuration files
 - Done by metadata file, like DFN AAI
 - Static configuration for whole IdP
 - URL
 - Entity ID
 - Certificate
 - ...
- OAuth2/OIDC
 - Done by self-service
 - Administrator of SP registers the OAuth2/OIDC client
 - The administrator must not be signed in to create the request
 - During the registration all necessary information are provided
 - Manually acceptance of the client request as last validation

OAuth2/OIDC REGISTRATION

Login to HDF dev AAI user's account

[Register a new account](#)



Username:

Password:

Authenticate

Select your preferred authentication option

Search:

Log in with your HDF dev AAI ID

[Password](#)

Log in with your social ID



Log in with your organisational ID



Academy of fine arts Dresden

Academy of Fine Arts Leipzig



Albert-Ludwigs-Universität Freiburg



Alphardt-Siemeringen University of Applied Sciences

[Data Privacy Statement](#) [Services](#) [AUP](#)

OAuth2/OIDC REGISTRATION

Registration form

+

Oauth2/OIDC client Registration

Please provide necessary information below to register your OAuth 2.0 Client. Your request will be sent to HDF AAI administrator.

Password requirements:

- minimum eight characters long
- minimum three character classes (numbers, lower- and upper cases, special signs)
- do not use your last two passwords
- do not use an easy to guess sequence

Identities

User name: *

Credentials

Group management

GROUP STRUCTURE

Groups



- ▼ Root (/)
 - ▶ GSI user group (/GsiUserGroup)
 - ▶ AAI Administrators (/aai-admin)
 - ▶ FEUDAL Test (/feudal-test-group)
 - ▶ hdfdev (/hdfdev)
 - ▶ myExampleColab (/myExampleColab)
 - ▶ /oauth-clients

- Hierarchical groups
- Membership in multiple groups is supported
- Roles and attributes may be different in each group

ATTRIBUTE STATEMENTS

Attribute statements

Assign eduPersonPrincipalName = expr(eattrs['eduPersonPrincipalName']) if 'eattrs contains 'eduPersonPrincipalName' is true

Assign eduPersonScopedAffiliation = expr(eattrs['eduPersonScopedAffiliation']) if 'eattrs contains 'eduPersonScopedAffiliation' is true

Assign givenName = expr(eattrs['givenName']) if 'eattrs contains 'givenName' is true

Assign sn = expr(eattrs['sn']) if 'eattrs contains 'sn' is true

Assign role = expr(eattrs['role']) if 'eattrs contains 'role' is true

- Create attributes within the specific group
- Copy attributes from another group, e.g. root group
- Create attributes, depending on attributes from another group

User management

Groups



▼ Root (/)

► GSI user group (/GsiUserGroup)

► AAI Administrators (/aai-admin)

► FEUDAL Test (/feudal-test-group)

Group /aai-admin details

Group's attributes classes



Attribute statements



Assign eduPersonPrincipalName =



Group /aai-admin members

☐ Group by entities ☐ Show targeted identities

Search:    

Remove entity

<input type="checkbox"/>	Entity	Identity type	Identity	
<input checked="" type="checkbox"/>	Sander Apweiler [2]	userName	sapweiler	
<input type="checkbox"/>	Sander Apweiler [2]	persistent	89b91130-8a11-4cef-9f51-ff5308fd8261	

Attributes of entity Sander Apweiler [2] in group /aai-admin

☒ Effective ☐ Internal **Required in bol**

<input type="checkbox"/>	Attributes	
<input checked="" type="checkbox"/>	givenName	
<input type="checkbox"/>	role	
<input type="checkbox"/>	sn	



Information

Effective

Created at 8/20/18 4:04 PM updated at 8/20/18 4:04 PM

Values

Sander

[Data Privacy Statement](#) [Services](#) [AUP](#)

USER MANAGEMENT

- Attributes of a selected user can be
 - Reviewed
 - Edited
 - Added
 - Deleted
- Users must be member of the parent group, before they can be added to a subgroup
- User can be added to a subgroup by
 - Drag & Drop
 - REST API

Open issues/enhancements

OPEN ISSUES

- expires_in
 - Part of Bearer token
 - Released as exp
 - Not defined in RFC 6750, but used within the example
 - Some clients expect „expires_in“ as key
- external_authn
 - Not yet supported
 - Pass Information from „first level“ IdP down to SP
 - Maybe tricky because of the data minimisation in the GDPR
 - Deleted

ENHANCEMENT

- Group management
 - Have a „Add to group“ button in user context menu, especially if multiple users should be added to a group
 - Have a dedicated and simplified interface for the group management
 - Only users with Content manager role will see this interface
 - The group administrators will only see their own groups and the parent groups
 - No attribute management within this interface
 - Users can request group membership and administrators can grant or reject it
 - Administrators can invite users and external people to their groups