
● Field report: RDMO integration



Workshop: IAM Basics #2

August 24th, 2023

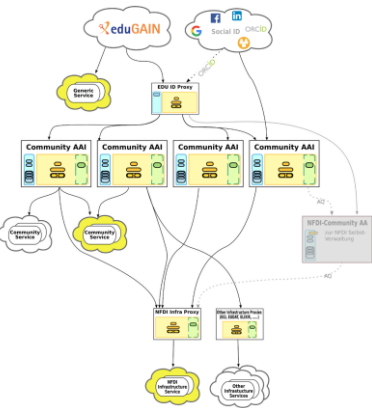
David Wallace

david.wallace@tu-darmstadt.de

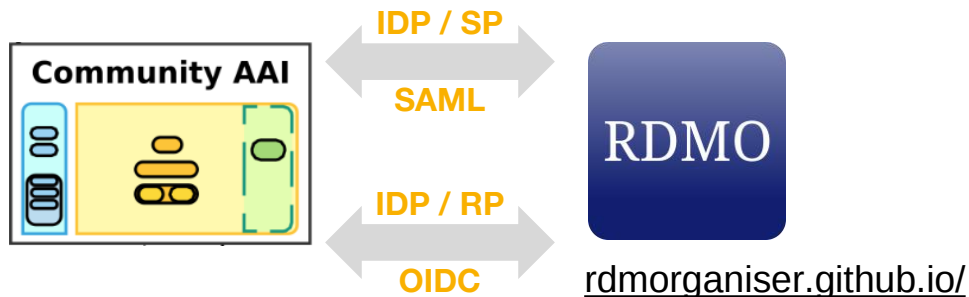
Recap: Workshop IAM Basic #1

Community AAls would solve our problem to support both SAML and OIDC users

- Implementation in RDMO would be straightforward because of OIDC
- Looking forward to authentication via a Community AAI (CAAI) !



<https://doc.nfdi-aai.de>



Web service

RDMO NFDi4ing test instance

Welcome to RDMO

The tool enables researchers of engineering to create a data management plan (DMP) for their research project. After logging in with and one time activation of your DFN account you can choose from several templates that guide you through the different aspects of a DMP.

We appreciate your feedback

rdmo@nfdi4ing.de

Maintenance window

Tuesday 6:30 am - 8:30 am



**Authentication with a
Community AAI**

Contact

rdmo@nfdi4ing.de

Based on software RDMO funded by DFG.



This service is provided by University and
State Library Darmstadt

[Imprint](#) / [Privacy Policy](#) /
[Nutzungsbedingungen](#)



NFDi4ing



Gefördert durch

DFG Deutsche
Forschungsgemeinschaft

NFDi4ing is supported by DFG under
project number 442146713

Also currently in-use in the productive instance rdmo.nfdi4ing.de/



Overview of how-to connect a service with a Community AAI

Starting point: doc.nfdi-aai.de/

Information:

- Ideally, there are docs provided by the specific CAAI providers.

Registration, Policy and Security Contacts:

- Registration of the service
- Provide the required legal documents and/or references
 - the service needs a valid Data Privacy Statement (!)
- Provide admin and security contacts

Technical implementation:

- Re-use an existing OIDC/SAML solution that is compatible with your service?
- Consider the user authentication and sign-up flow
- Existing user accounts?
- Staging and production instances



Implementation: registration

Register your service as an OIDC client in the CAAI

Information:

- This example is for the CAAI type Unity provided by the Helmholtz AAI
- Docs: hifis.net/doc/helmholtz-aaai/howto-services/

Registration, Policy and Security :

- Self-registration, submit a request to register a new client.
 - Organizational: Name, description, contact, Data Privacy Statement, logo
 - Technical: **client ID** and **secret** (username/pass), redirect URLs
- Request will be reviewed by the CAAI admins.
- Client can be used when the request is accepted.

Take-away for your service:

- the **client ID** and **secret** will be used by your service
 - store them in a secure place! (eg. password manager)
- redirect URLs, one could add localhost for local debugging



Implementation: technical aspects in general

Technical implementation depends on software framework of the service

Information:

- Look for existing solutions?
 - OIDC certified libraries: openid.net/certified-open-id-developer-tools/
 - or uncertified: uncertified-openid-connect-implementations/
 - Via web search “OIDC client” or “social authentication” for your framework

Configuration:

- **client ID** and **secret**, deploy with environment variables?
- **server URL**, one URL of the CAAI can be used to build the required OIDC endpoints
 - URL to the metadata of the OP configuration
- **scope**, defines the sets of user attributes that the service requests from the OP
 - Important for which attributes your service requires
 - doc.nfdi-aai.de/attributes/, emails are verified



RDMO implementation: Django web framework



The Django allauth library supports any OIDC compatible provider

Information:

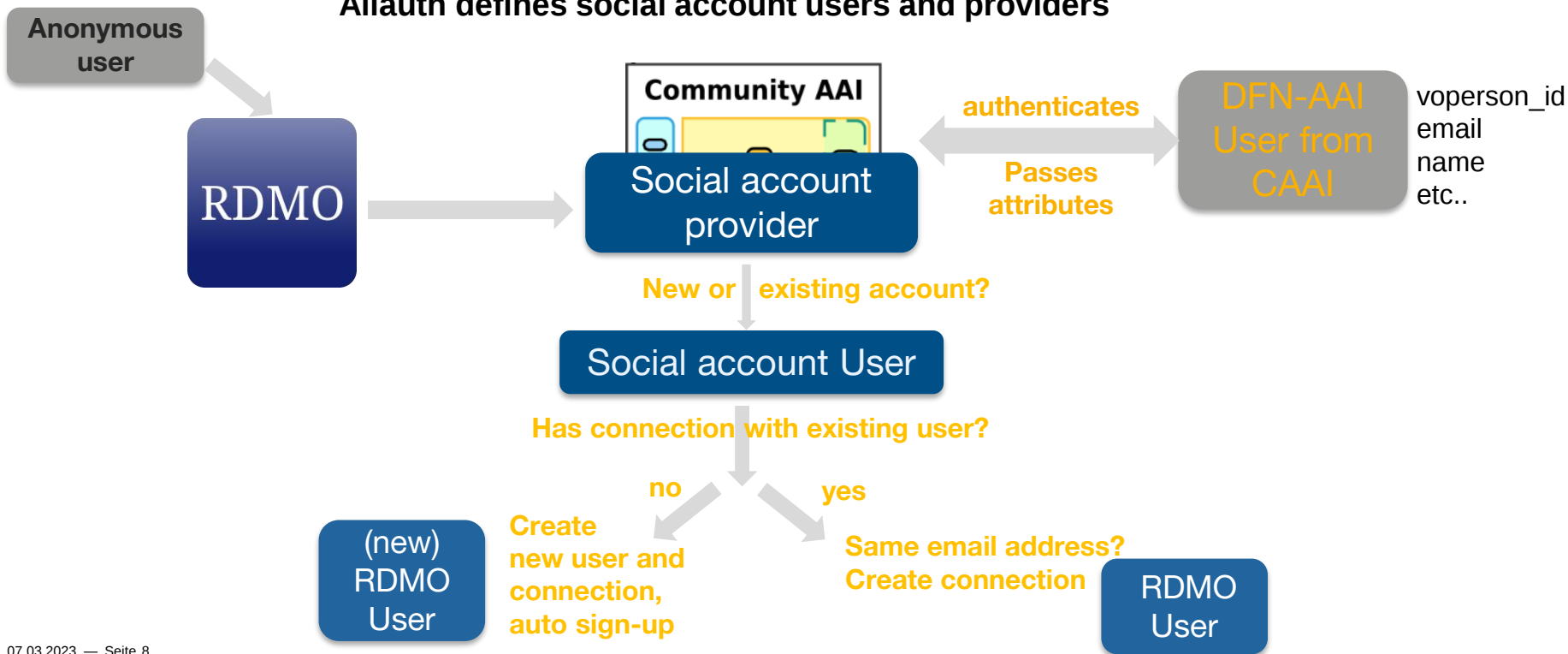
- Widely used and long-lived Django app, django-allauth.readthedocs.io/
- Supports any OIDC compatible provider, as well as many OAuth 1.0/2.0 and SAML 2.0, [providers/](#)
- Integrated with User Model, configurable authentication flows

Configuration:

- Implementing of the CAAL requires minimal adaption (if at all) of existing code.
- In the latest version, new OIDC providers can be added directly via the web admin UI without any codebase adaptation.
- Extraction or mapping of attributes
 - uid as voperson_id, take only verified emails

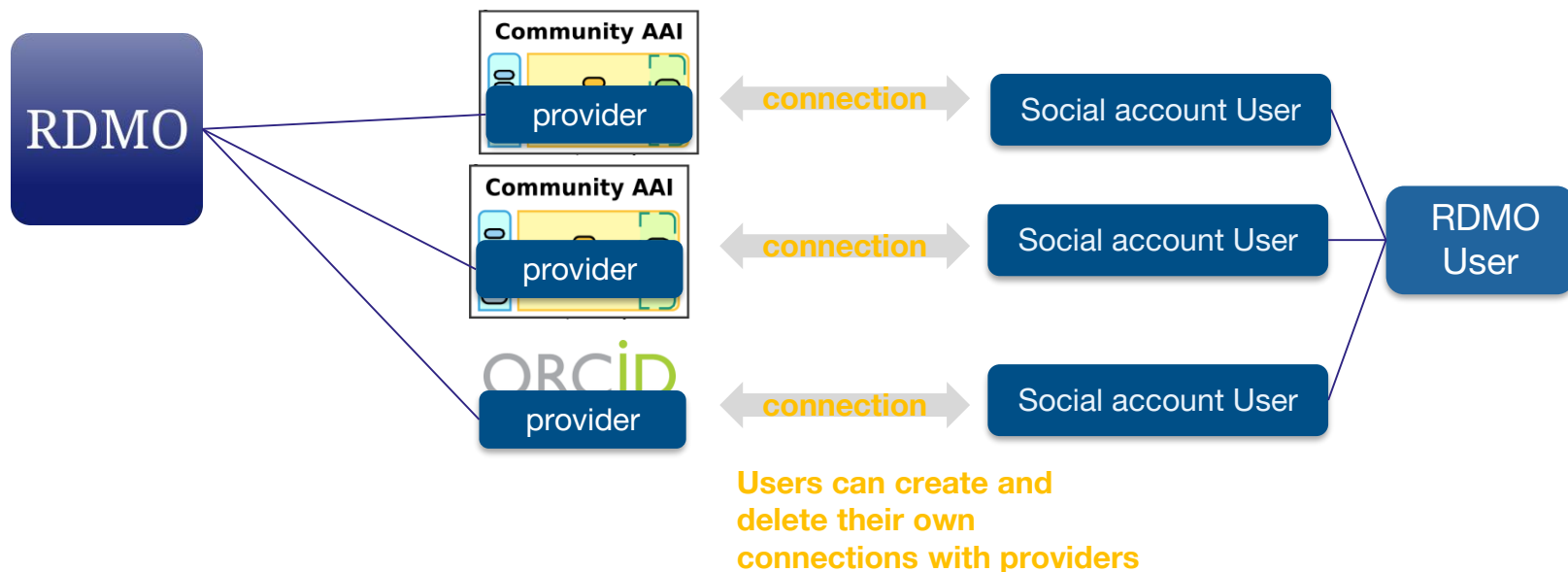
RDMO implementation: allauth and user flow

Allauth defines social account users and providers



RDMO implementation: multiple providers

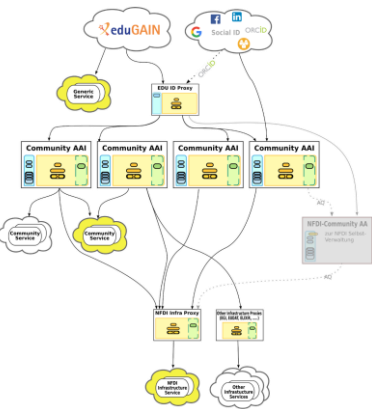
Allauth allows for the use of multiple providers in parallel



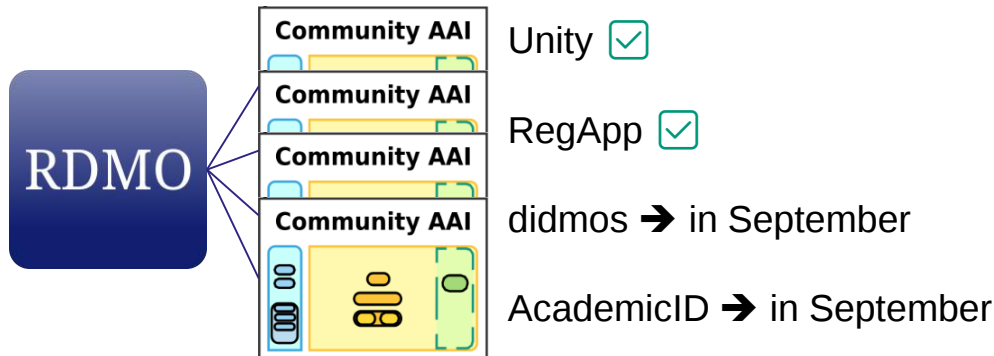
Conclusion of field report and outlook

Community AAls provide a straightforward authentication service

- ☒ documentation available for the service provider
- ☒ service registration via online form
- ☒ support for OIDC and SAML
- ☒ uniform user attributes, email verification
- ☒ user profile self service in CAAI
- Button logos like shibboleth?



<https://doc.nfdi-aa1.de>



Thank you for your kind attention!

Welcome to RDMO

The tool enables researchers of engineering to create a data management plan (DMP) for their research project. After logging in with and one time activation of your DFN account you can choose from several templates that guide you through the different aspects of a DMP.

We appreciate your feedback

rdmo@nfdi4ing.de

Maintenance window

Tuesday 6:30 am - 8:30 am

NFDI AAI with Unity

NFDI AAI with Reg-APP

SIGN IN with ORCID 

Contact

rdmo@nfdi4ing.de

Based on software RDMO funded by DFG.



This service is provided by University and
State Library Darmstadt

[Imprint](#) / [Privacy Policy](#) /
[Nutzungsbedingungen](#)



Gefördert durch

DFG Deutsche
Forschungsgemeinschaft

NFDI4ing is supported by DFG under
project number 442146713

David Wallace
Forschungsdaten-Services
ULB Darmstadt
david.wallace@tu-darmstadt.de