didmos as a Community AAI solution

Workshop on Community AAIs | 2024/01/25

David Hübner
DAASI International GmbH

didmos

DAASI International

Identity

Management with/as

Open

Source

didmos

- A standardised IAM system
  - so flexible that it is able to address all customer needs no matter how specific
- The current version is „didmos2“ which is being developed since 2019 and is based on modern frameworks, libraries and architectures
- Successfully implemented for >20 customers in projects with >250k users
- didmos consists of several modules for different tasks
- didmos also allows for plugin interfaces in many places to allow for extensions
- Each IAM project is different. We can pick the right modules and extensions based on the requirements
- didmos by its modularity is also easily combinable with other open source IAM components

DAASI International

didmos

- Open source and open standards
  - didmos is fully open source (except very specific functionality for customers)
  - didmos uses established open source software such as OpenLDAP, RabbitMQ and SATOSA
  - didmos relies on open standards for interoperability, such as LDAP, SAML, OIDC, SCIM and SPML
- Available as Docker images

DAASI International

didmos in NFDI

Central instance for NFDI

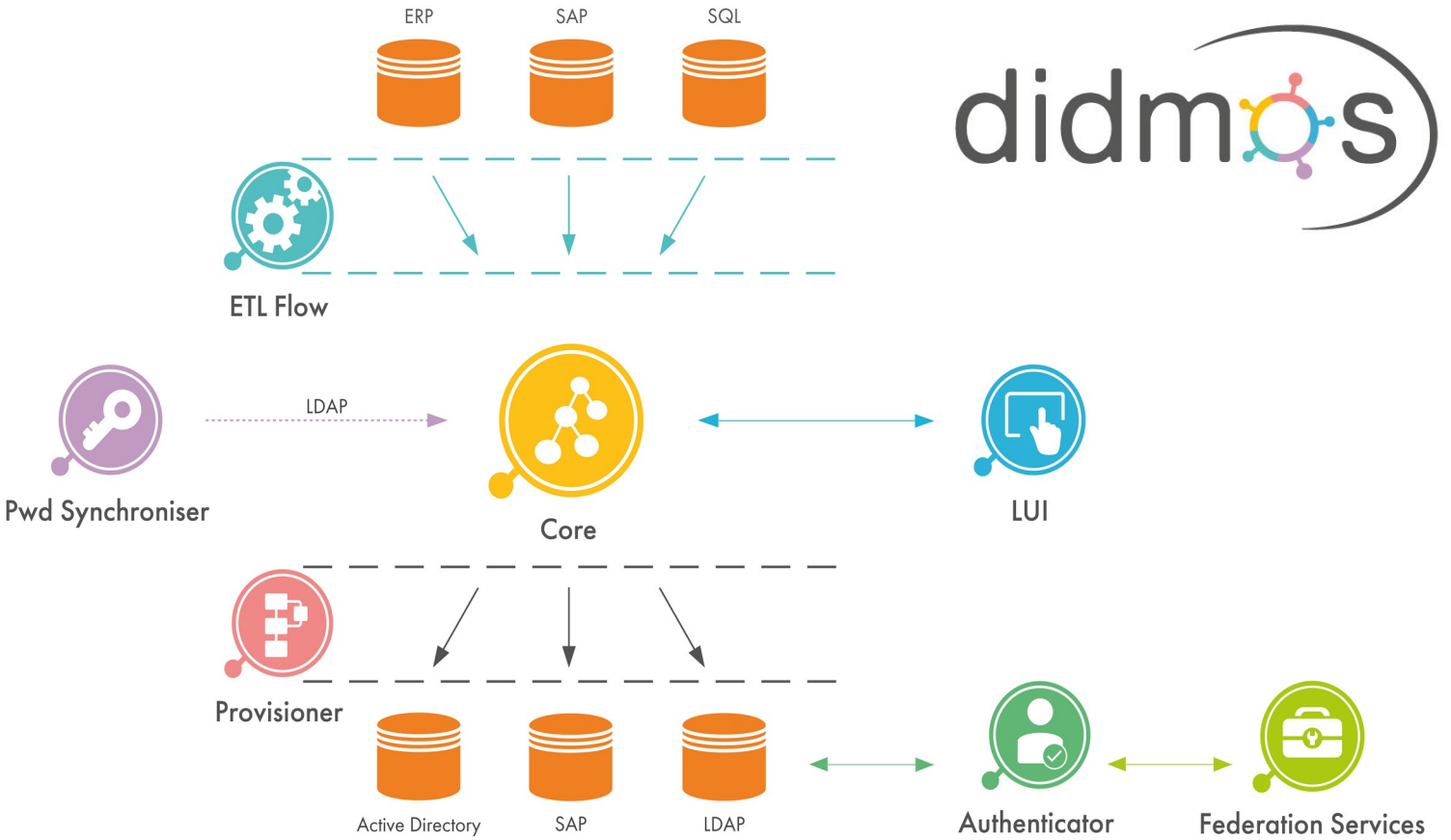
- https://portal.didmos.nfdi-aai.de
- Operated by DAASI with „best effort“ SLAs
- **Free of charge for NFDI Consortia**
- Multi-tenancy (a NFDI Consortium is a tenant) with isolated user and group management
- Limited options for customization
- Will be updated over the course of the NFDI project with additional features

Dedicated productive instance

- Developed and operated by DAASI for a NFDI Consortium
- A project for setup and managed service **contract for operations between DAASI and the NFDI Consortium is required**
- Same base software, but full customization and individual features are possible
- Based on project requirements, additional modules that are not part of the central instance, can be added
- Higher SLA for operations and dedicated environment

DAASI International

didmos - Overview



didmos in NFDI

Central instance for NFDI

- Contains the modules Core, LUI and Auth
- Use case:
  - didmos is the main CAAI
  - Users can login via Edu-ID, eduGAIN, ORCID or social IDs. Local users are also possible
  - A consortium assigns a number of Consortium admins that have extended permissions in didmos mainly for management of group memberships within the Consortium
  - Services can be connected via SAML or OIDC either globally or only for one Consortium by DAASI International

Dedicated productive instance

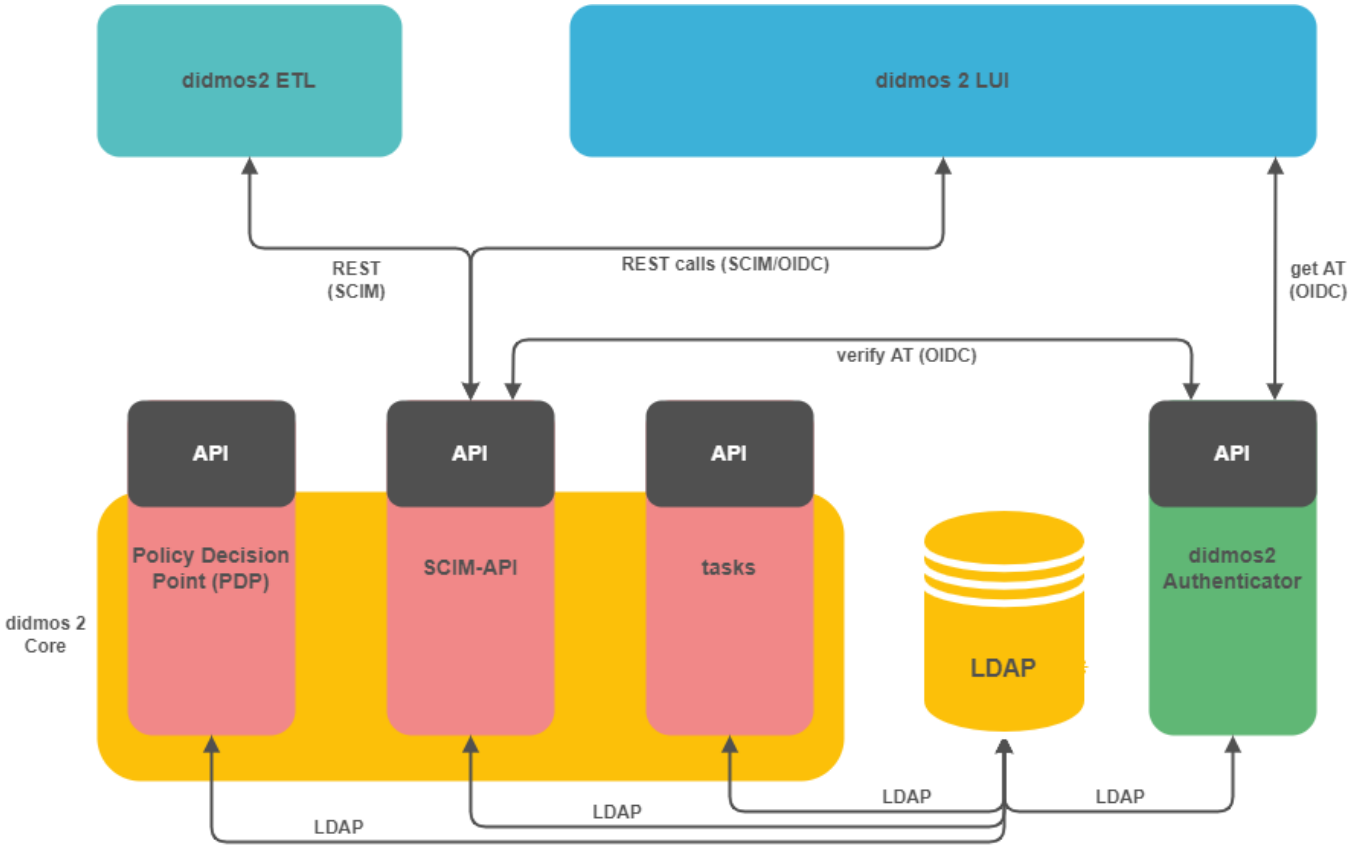
- Can contain additional modules, such as:
  - ETL for synchronization with existing user stores
  - Provisioner to connect applications with non-SSO-protocols or possibly real-time deprovisioning
- Can be used for more advanced use cases since the instance can be fully customized and setup according to requirements in the Consortium

DAASI International

didmos Core

- Core consists of two components:
  - OpenLDAP server as metadirectory
  - API server for data access and background processes (based on Django/Python)
- The API server consists of several modules (called “apps” in Django), which respectively provide a modern REST API via which data can be shared as JSON.
- Following APIs are ready to use:
  - Access to IdM via SCIM
  - Workflow management
  - Policy Decision Point (PDP) / RBAC
  - MFA token management with privacyIDEA
- Multi tenant capable both in LDAP and API server

didmos Core


didmos2 ETL
didmos 2 LUI
REST
(SCIM)
REST calls (SCIM/OIDC)
get AT
(OIDC)
verify AT (OIDC)
API
API
API
API
Policy Decision
Point (PDP)
SCIM-API
tasks
didmos2
Authenticator
didmos 2
Core
LDAP
LDAP
LDAP
LDAP
LDAP

didmos LUI

Frontend entirely based on JavaScript (Angular)

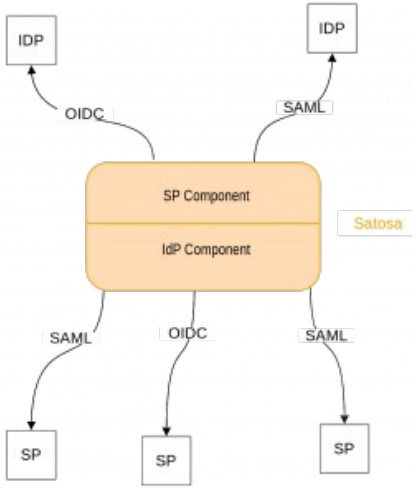
- Responsive Single-page application
- Mobile app (PWA) capable
- Authentication with OIDC
- Adjustable, both for layout and functionality (we have various standard modules in a shared library and can create custom frontends)
- Both for selfservice and admin functionality

Extensive usage of SCIM

- Only Core is responsible for the manipulation of LDAP objects
- SCIM calls protected by OAuth2 bearer tokens
- Menu items can be controlled via permission assignment from Core to LUI

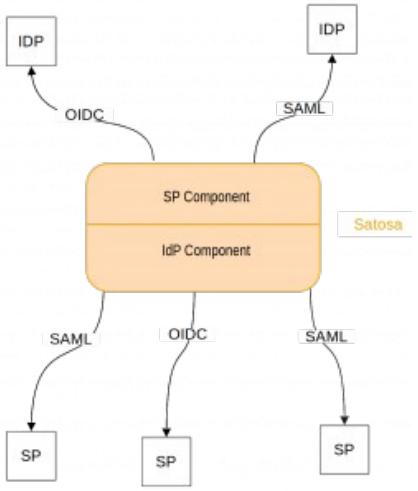
didmos Authenticator

- Acts as an SSO proxy and supports multiple protocols by default
  - IdP/OP for SAML2 and OIDC
  - SP/Client for various protocols/services such as OIDC, SAML2, Social IdPs, Orcid, etc.
- Queries additional attributes, such as entitlements from didmos Core via SCIM API
- Therefore, also can act as a full IdP
- Various optional microservices for functionality such as MFA, Consent, Restricting access at the IdP etc.
- Users with external accounts are created in didmos as „Shadow accounts“ without passwords and can be managed in the VO, especially added and deleted from priviledge groups
- Due to using open standards, the IdP/proxy is interchangeable. E.g. we also have modules to use Shibboleth IdP with didmos, which can make sense for use cases where e.g. AQ for deprovisioning or „global“ SLO are needed



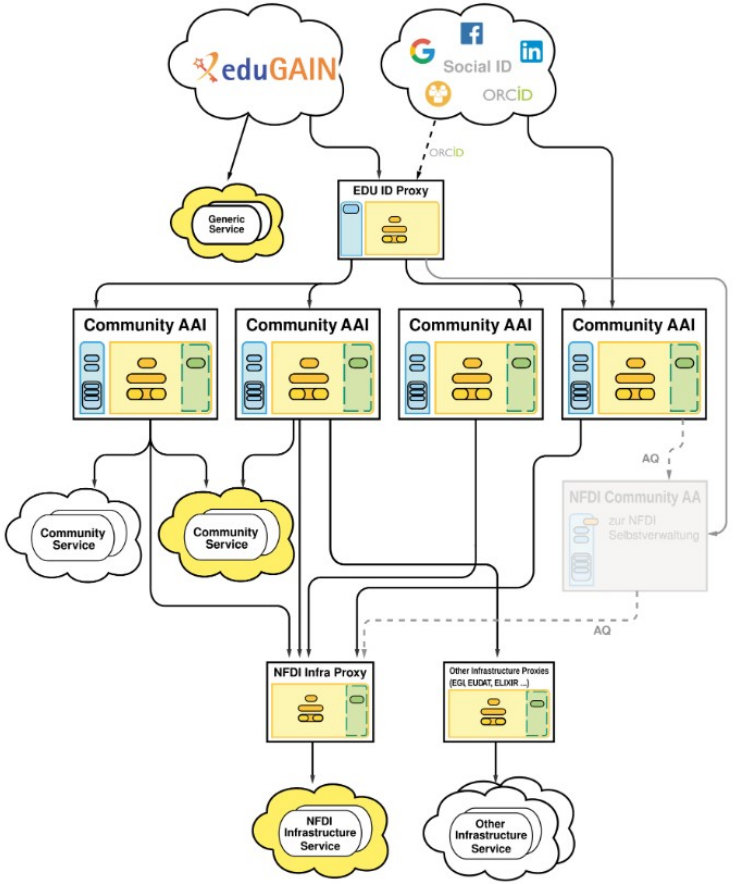
didmos Authenticator

- Due to using open standards, the IdP/proxy is interchangeable. E.g. we also have modules to use Shibboleth IdP with didmos
- This can make sense for use cases where e.g.:
  - SAML attribute queries (AQ) are needed for deprovisioning
  - SLO propagation across „proxy boundaries“ are needed



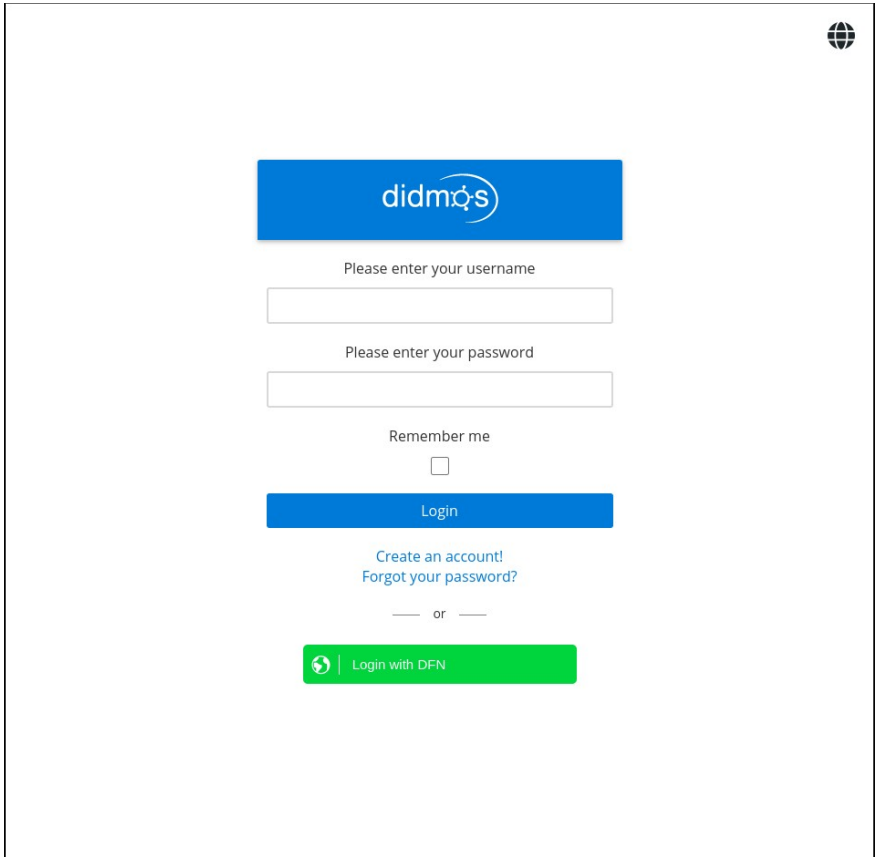
Integration into NFDI Architecture

- Community services can be connected via SAML or OIDC
- Once the NFDI Infra Proxy exists, it will be connected to didmos as an SP so that NFDI infrastructure services can be used
- NFDI attribute profiles (see https://doc.nfdi-aai.de/attributes/) are supported with the attributes coming from either eduGAIN or didmos
- We forward assurance information for federated users. Assurance information for local users can be configured globally.
- Services can be either connected globally (all tenants) or tenant-specific



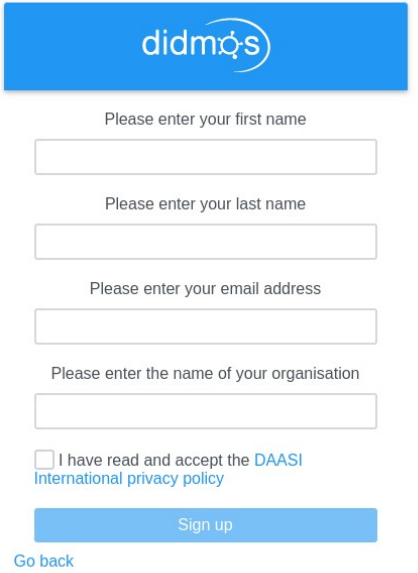
Login and registration

- Authentication either with local accounts (password managed in didmos) or federated
- Supported protocols for federated login: SAML2 and OAuth2/OIDC
- Possible integrations: eduGAIN, individual IdPs, Social IDs
  - In this case: connected to DFN-AAI and eduGAIN
- Local accounts can be disabled if only federated login should be supported
- Federated accounts are created based on attributes from the home organization IdP
  - Some attributes (unique identifier, name, ideally mail) are required. We hope that the DFN Edu-ID proxy will make sure that we always receive the attributes



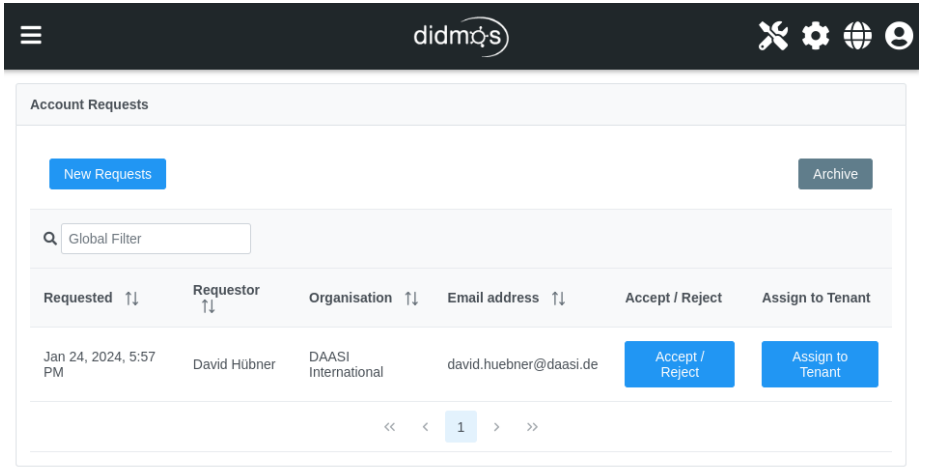
Login and registration

- Optionally, account registration can be supported to support a „homeless IdP“
- This is currently enabled in the central instance



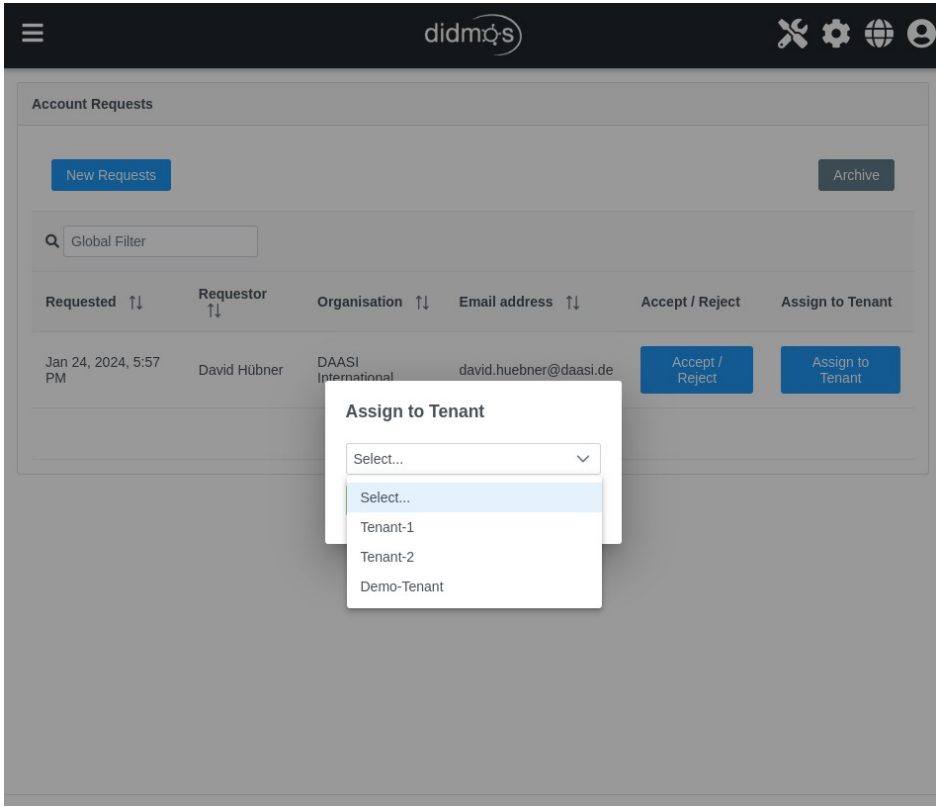
Login and registration

- Optionally, account registration can be supported to support a „homeless IdP“
- This is currently enabled in the central instance
- The result of an account registration is an account request, that must be approved by the admin
- In the central NFDI instance the request must first be assigned to a tenant/consortium so that the tenant administrator can grant or deny the request
- This assignment can be done by a generic helpdesk role (superadmin)



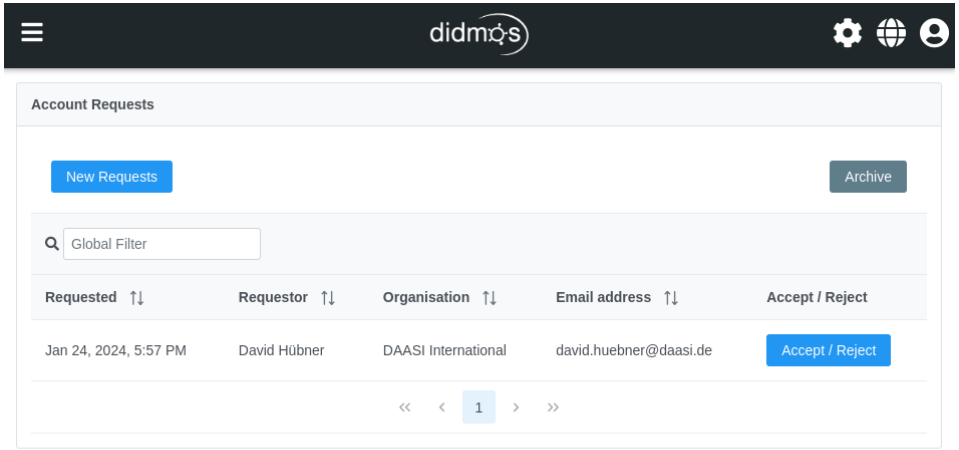
Login and registration

- Optionally, account registration can be supported to support a „homeless IdP“
- This is currently enabled in the central instance
- The result of an account registration is an account request, that must be approved by the admin
- In the central NFDI instance the request must first be assigned to a tenant/consortium so that the tenant administrator can grant or deny the request
- This assignment can be done by a generic helpdesk role (superadmin)



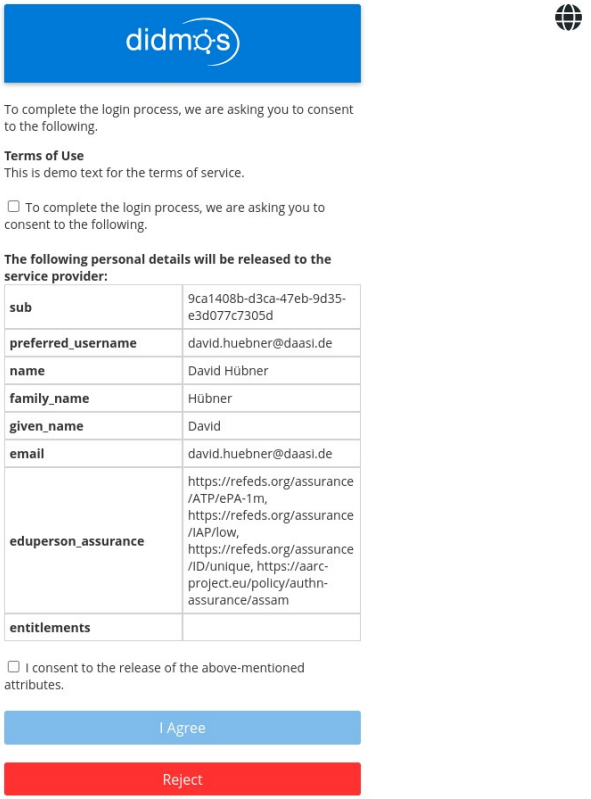
Login and registration

- Optionally, account registration can be supported to support a „homeless IdP“
- This is currently enabled in the central instance
- The result of an account registration is an account request, that must be approved by the admin
- In the central NFDI instance the request must first be assigned to a tenant/consortium so that the tenant administrator can grant or deny the request
- This assignment can be done by a generic helpdesk role (superadmin)
- Finally, the consortium admin can either accept or reject the account request
- The user will be notified via email about the decision and, if accepted, can set a password and activate the account



Login and registration

- A consent module can be configured for terms of use/AUP and attribute release consent
  - Terms of use consent / AUP are global and apply to all services
  - Attribute release consent is per service



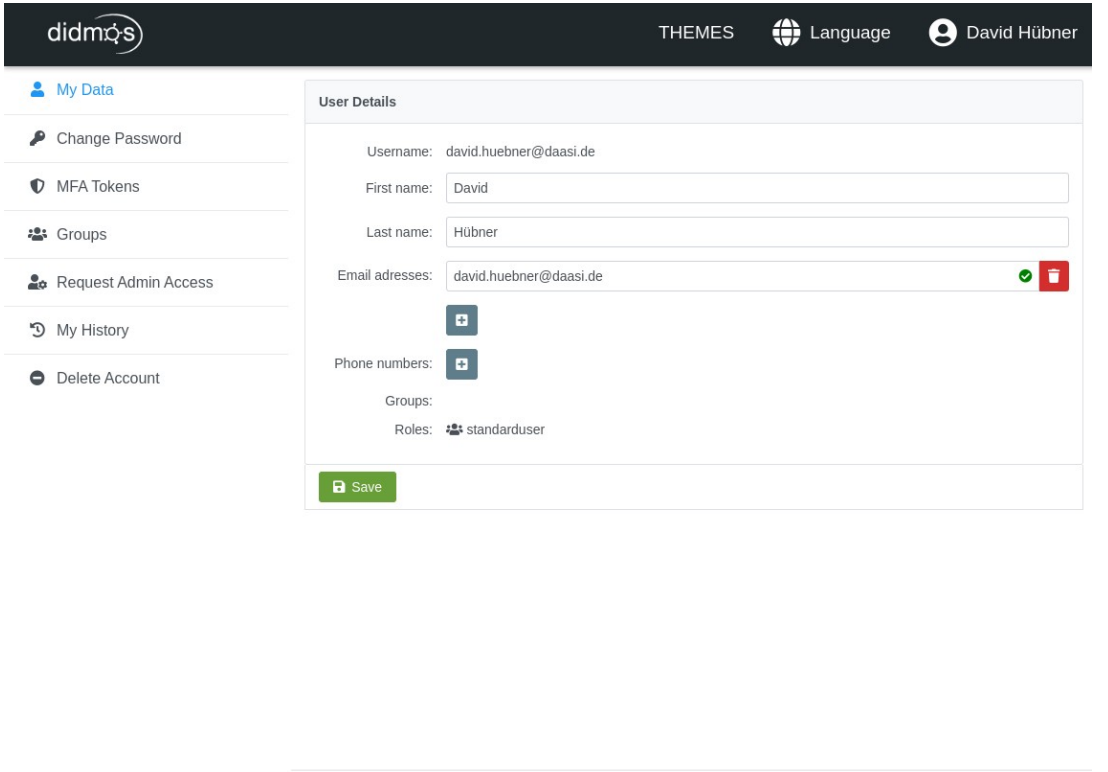
Login and registration - Roadmap

- We’re currently working on the following:
  1) Automatic assignment of tenant/consortium after registration (e.g. based on user selection or rule based)
  2) Account approval for new federated users. This would be a config option that requires an approval process similar to local accounts.
  3) Allow account linking of different federated accounts.

DAASI International

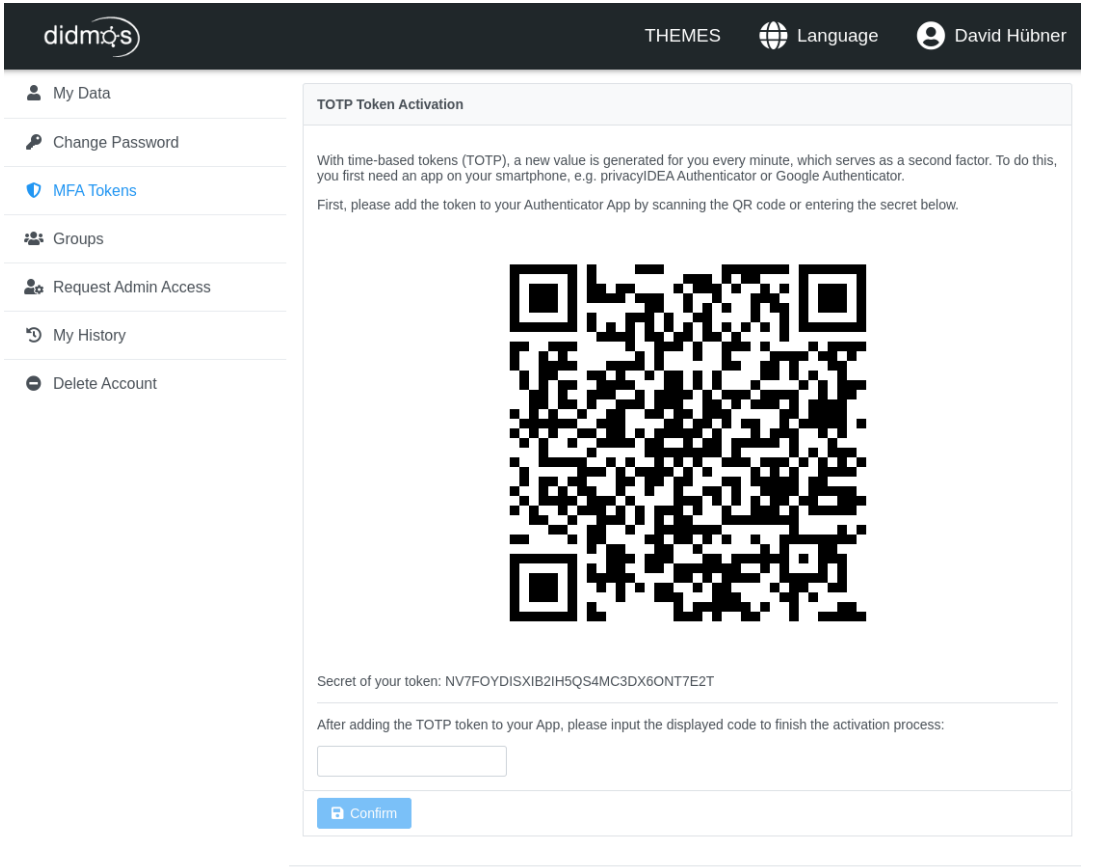
Self service portal

- Allows users to perform common self service functions, such as:
  - Modify user attributes and verify attributes
  - Change password (not for federated users)
  - MFA token management
  - View and apply for open groups
  - Request roles (can be disabled)
  - View activity log
  - Delete account (can be disabled or configured to require approval)
- Other functionality can be added as part of a dedicated instance



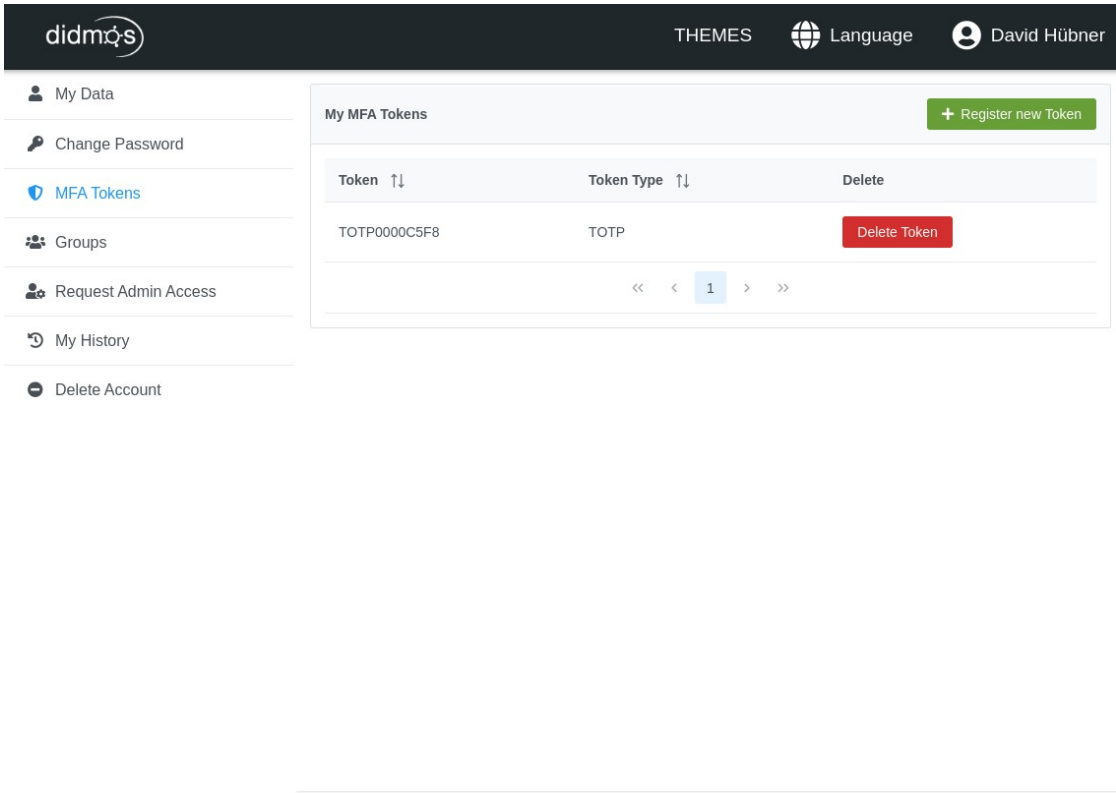
MFA token management

- The central NFDI instance supports TOTP and OTP per email
- We also have modules for OTP per SMS and PUSH Tokens
- TAN codes as recovery option are supported



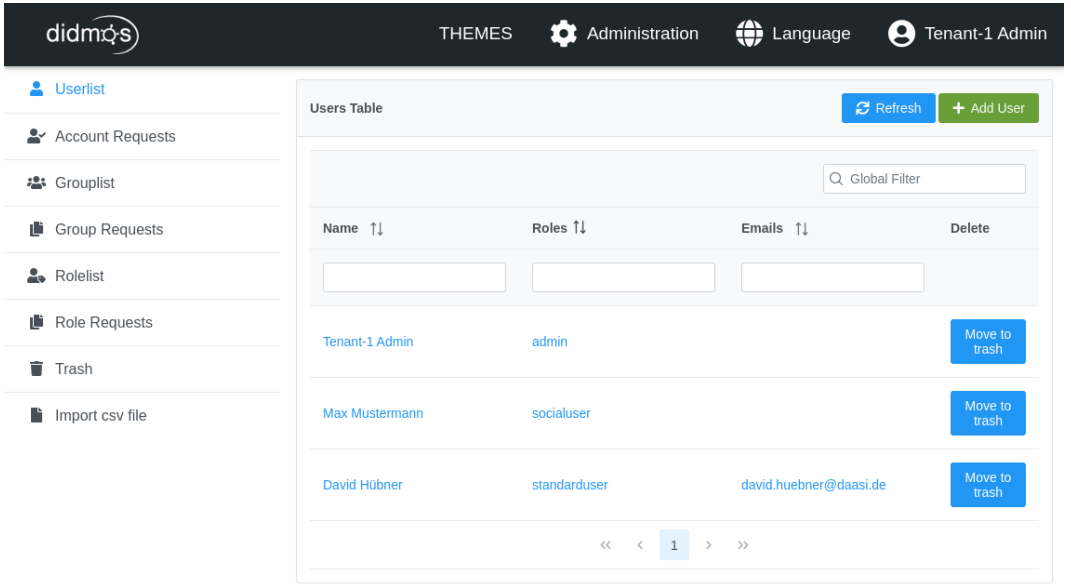
MFA token management

- The central NFDI instance supports TOTP and OTP per email
- We also have modules for OTP per SMS and PUSH Tokens
- TAN codes as recovery option are supported
- Users can manage their own tokens for additional account security.
- Scenarios for mandatory tokens are possible with a dedicated instance
- Once a user has registered MFA tokens, MFA is required for login to services and didmos, as well as operations such as password change and account deletion



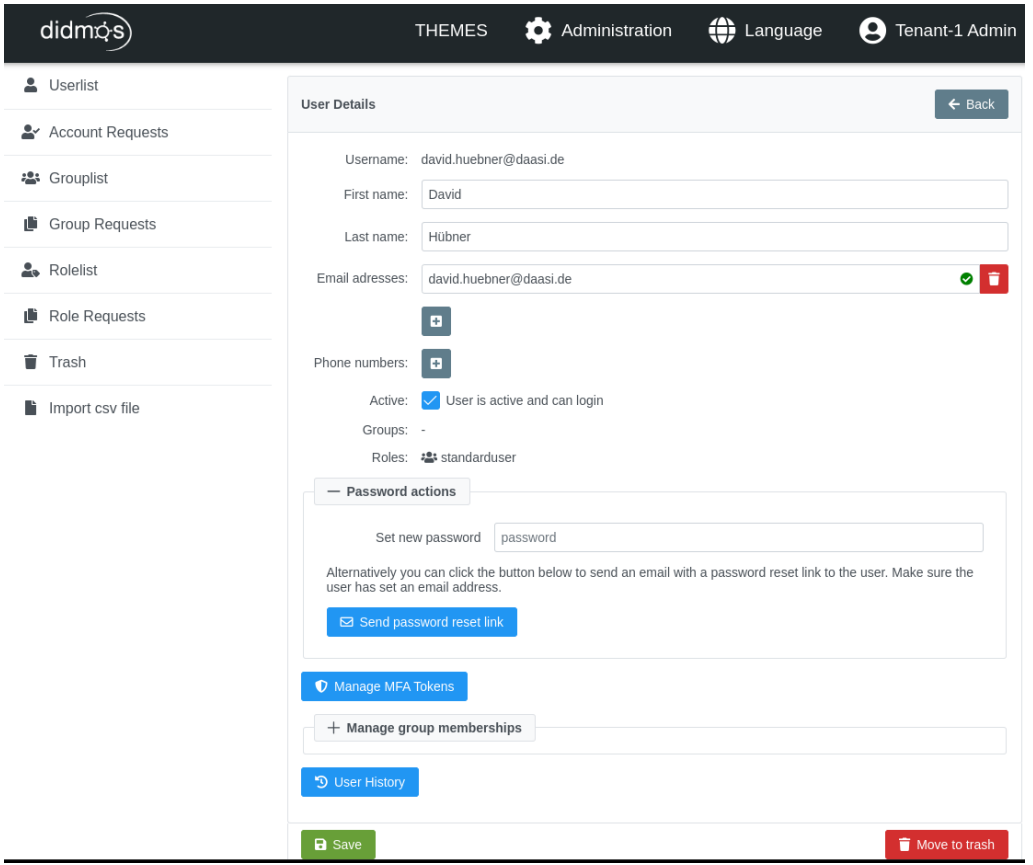
Admin portal

- Consortia can assign some users as admins with access to the admin portal
- This allows admins to perform actions such as:
  - User management in the consortium
  - Review account requests
  - Group management
  - Permission management
  - Bulk import of existing users
- Other functionality can be added as part of a dedicated instance



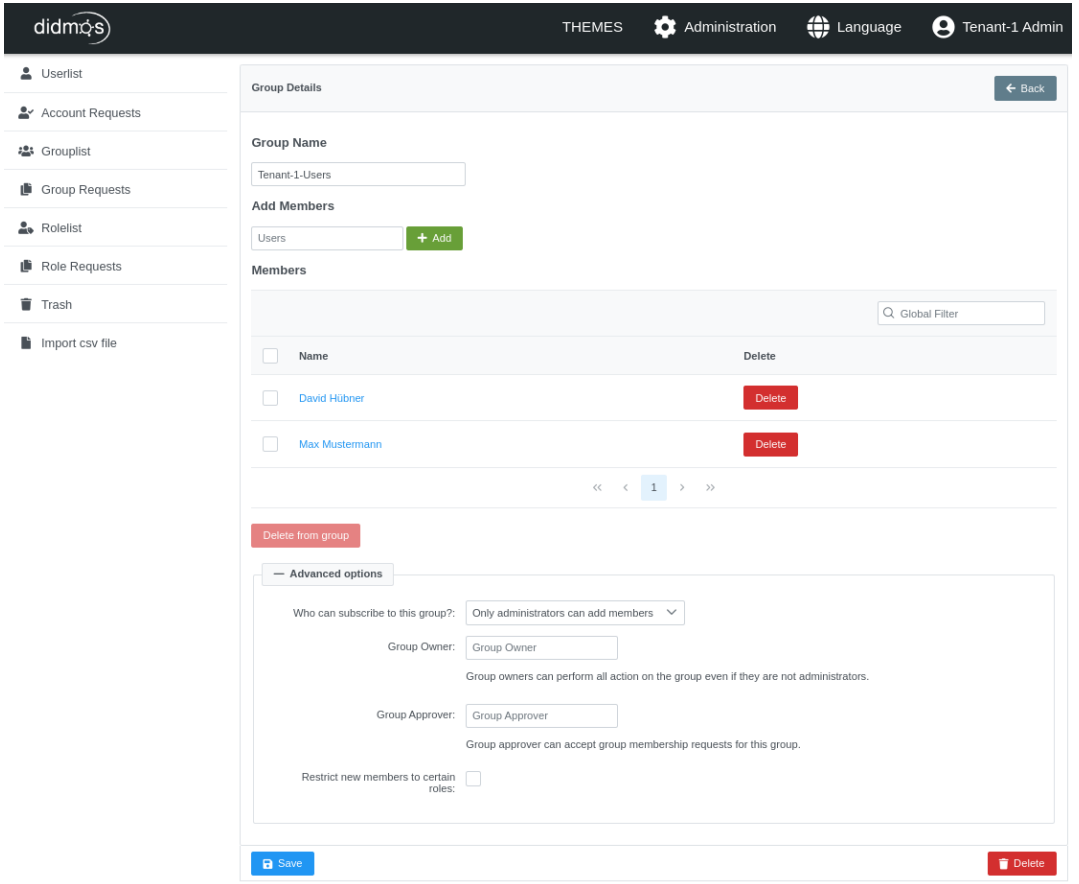
Admin portal

- Consortia can assign some users as admins with access to the admin portal
- This allows admins to perform actions such as:
  - User management in the consortium
  - Review account requests
  - Group management
  - Permission management
  - Bulk import of existing users
- Other functionality can be added as part of a dedicated instance



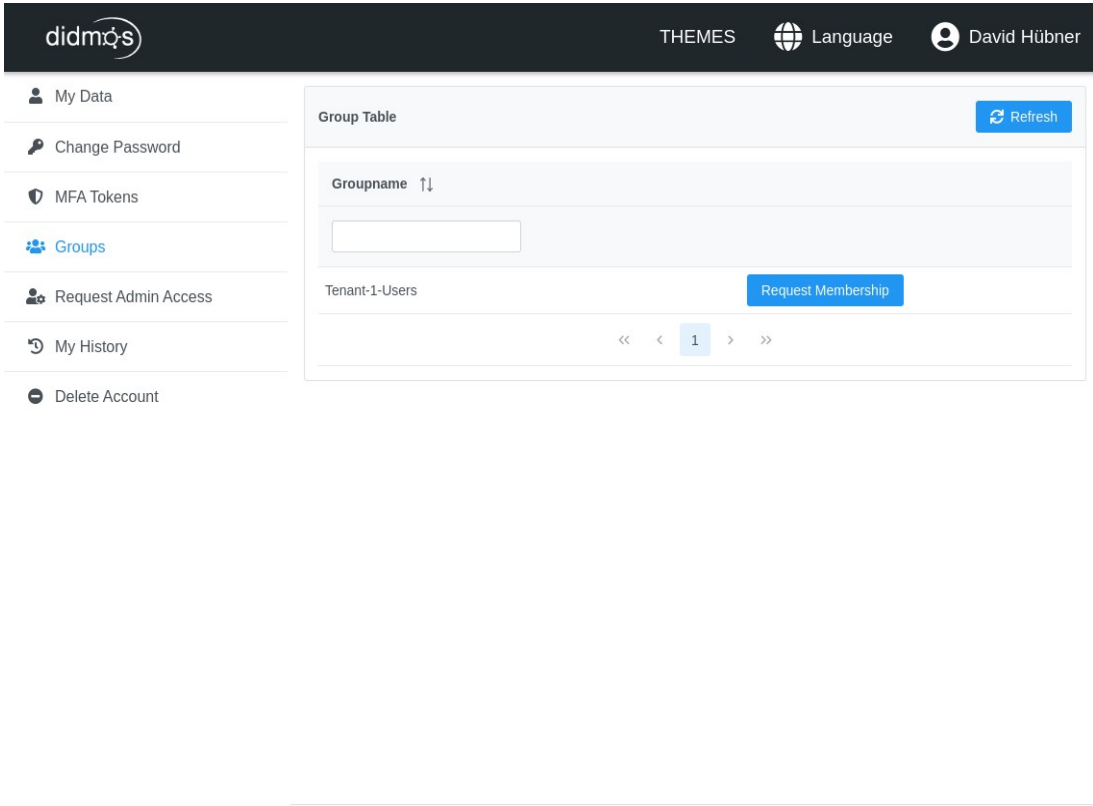
Group management

- Admins can create groups within the consortium and manage memberships of users in the consortium
- This is possible for both local users and federated users
- By default groups can only be added by admins
- Other options are:
  - Users can see the group in the self service portal and depending on the group type
    - Either request membership
    - Or freely join groups



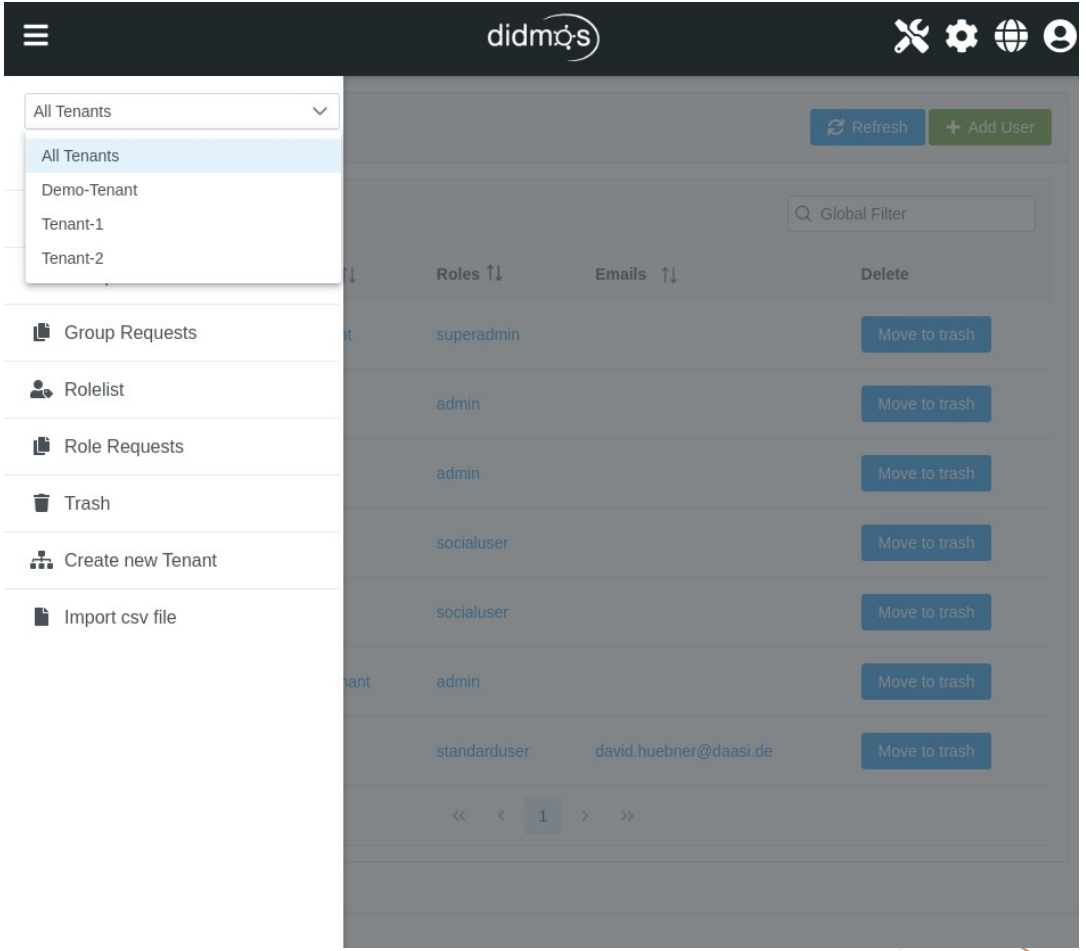
Group management

- It’s possible to delegate group management of a particular group to particular users without giving that user admin permissions. This is called „Group Owner“.
- Group memberships are sent to services AARC compliant as entitlement values for authorization
  e.g. urn:geant:dfn.de:nfdi.de:group:tenant-1-users#auth.didmos.nfdi-aai.de



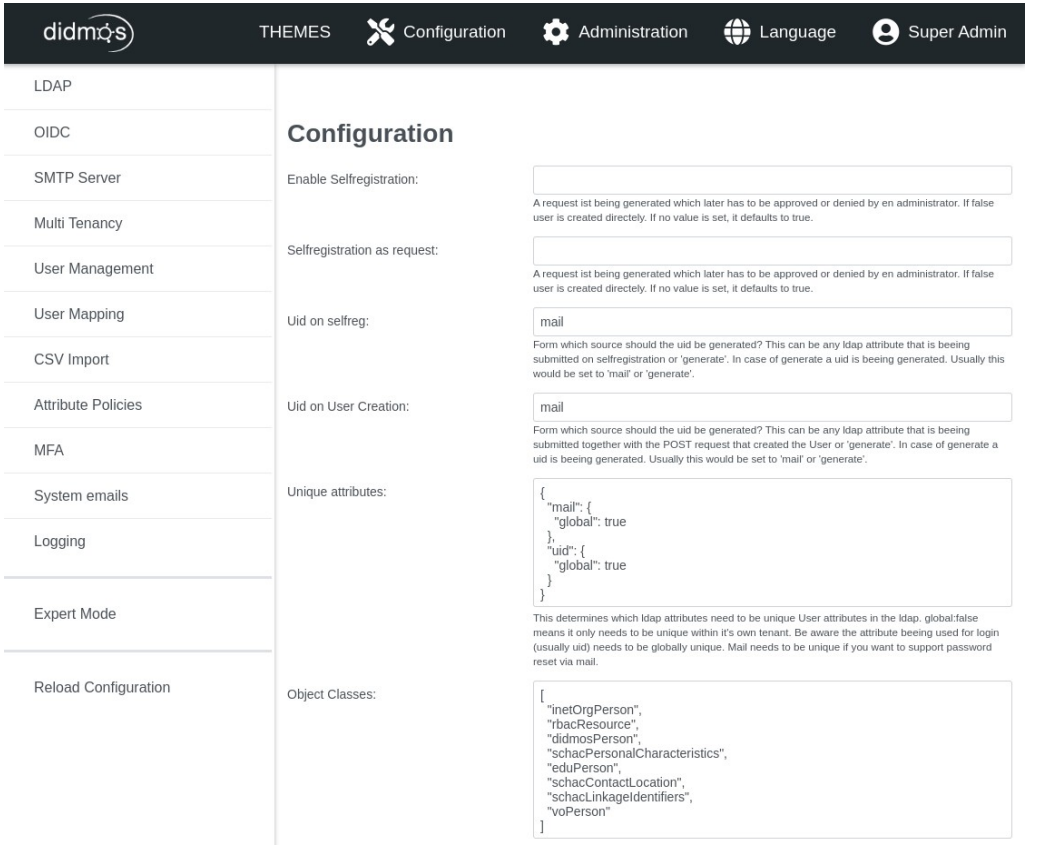
Global administration

- „superadmin“ is a permission above a tenant/consortium admin that can manage the system globally, such as:
  - Manage all tenants
  - Create new tenants
  - Assign account requests to tenants
  - Manage global configuration
- In the central NFDI instance, this role is limited to the Operator (DAASI)
- In dedicated instances multi tenancy is either disabled and every admin is „superadmin“ or the role can be managed by the consortium
- Another role such as „helpdesk“ that can assign account requests but not manage global config is possible



Global administration

- „superadmin“ is a permission above a tenant/consortium admin that can manage the system globally, such as:
  - Manage all tenants
  - Create new tenants
  - Assign account requests to tenants
  - Manage global config
- In the central NFDI instance, this role is limited to the Operator (DAASI)
- In dedicated instances multi tenancy is either disabled and every admin is „superadmin“ or the role can be managed by the consortium
- Another role such as „helpdesk“ that can assign account requests but not manage global config is possible



Self service and administration - Roadmap

- We are currently working on the following:
  1) Extend global configuration with more functionality such as management of SAML and OIDC services
  2) Extend global configuration to be tenant specific
  3) Policy management for NFDI that extends the Consent module during login
- We are open for further requirement, e.g. from the incubator projects

didmos ETL Flow

- **E**xtract **T**ransform **L**oad
- Typical flow (simplified):
  - Read and convert (multiple) data sources (e.g. ldapsearch, SQL dump etc.)
  - Identify against IdM
  - Merge identical data sets within one data source if necessary
  - Merge identities from multiple data sources
  - Automatically create roles or group memberships
  - Calculate diff against IdM
  - Install changes
- Typically used for either one-time data migration or regular synchronization of existing users
- The workflow is configured via LDAP objects (=configuration)

DAASI International

didmos Provisioner

- Real-time transfer of identity information to connected target systems
  - Reads change information in the OpenLDAP accesslog
  - Architecture is inspired by SPML, however SCIM is implemented as well
- Changes are recorded in SCIM complient JSON documents which are inserted into the queuing system RabbitMQ
- A dedicated worker then installs them in the target system and reports back to didmos Core
- We have workers for
  - LDAP, Active Directory
  - SCIM2
  - Gluu
  - Nextcloud
  - etc.

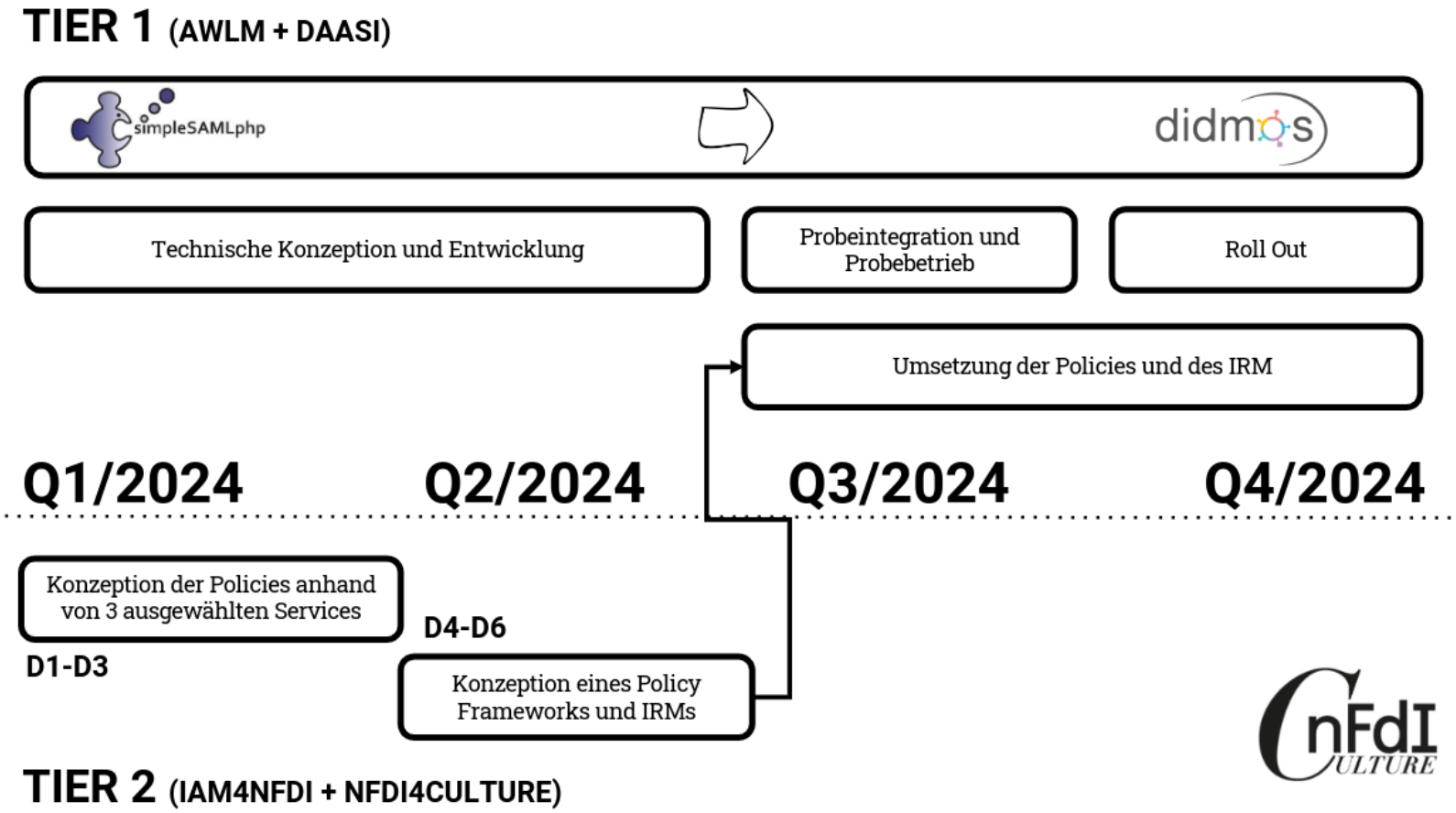
DAASI International

Example for dedicated instance: NFDI4Culture

- NFDI4Culture will use a dedicated didmos instance for as their CAAI
- Requirements:
  - Migration of existing data (user and services)
  - Customization
  - Extension for license management for protected resources as a special type of group memberships / entitlements
  - On-premise deployment
- IAM4NFDI will also do an Incubator with NFDI4Culture on policies and incident response, which will run in parallel to the didmos setup and migration project

DAASI International

Example for dedicated instance: NFDI4Culture



Next steps

Central instance for NFDI

- We can create a tenant for testing purposes for your Consortium and send you credentials for an admin account
- We're happy to test the integration of one of your services with you
- Our central NFDI instance can be used with real services and users, ***but some paperwork is required for that***

To get a tenant on the central NFDI instance or discuss a project for customization:

- **david.huebner@daasi.de**
- **p.gietz@daasi.de**

For general questions about didmos, also feel free to join the mailing list :-)

- **https://lists.daasi.de/listinfo/didmos-users**

DAASI International

Thank you for listening.

David Hübner

DAASI International

email: david.huebner@daasi.de