

didmos as a Community AAI solution

Workshop on Community AAls | 2024/01/25

David Hübner
DAASI International GmbH

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

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

didmos in NFDI

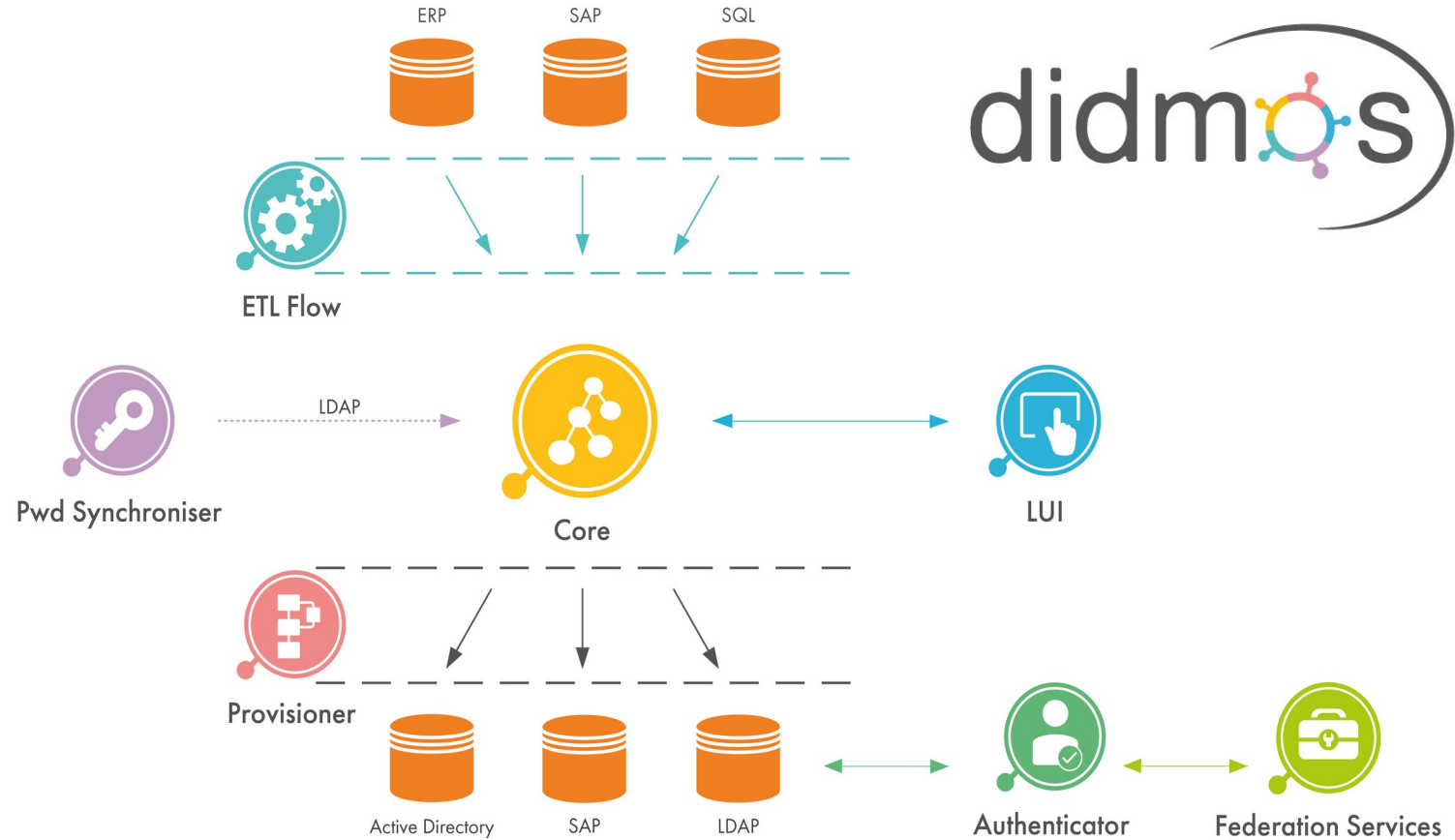
Central instance for NFDI

- <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

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

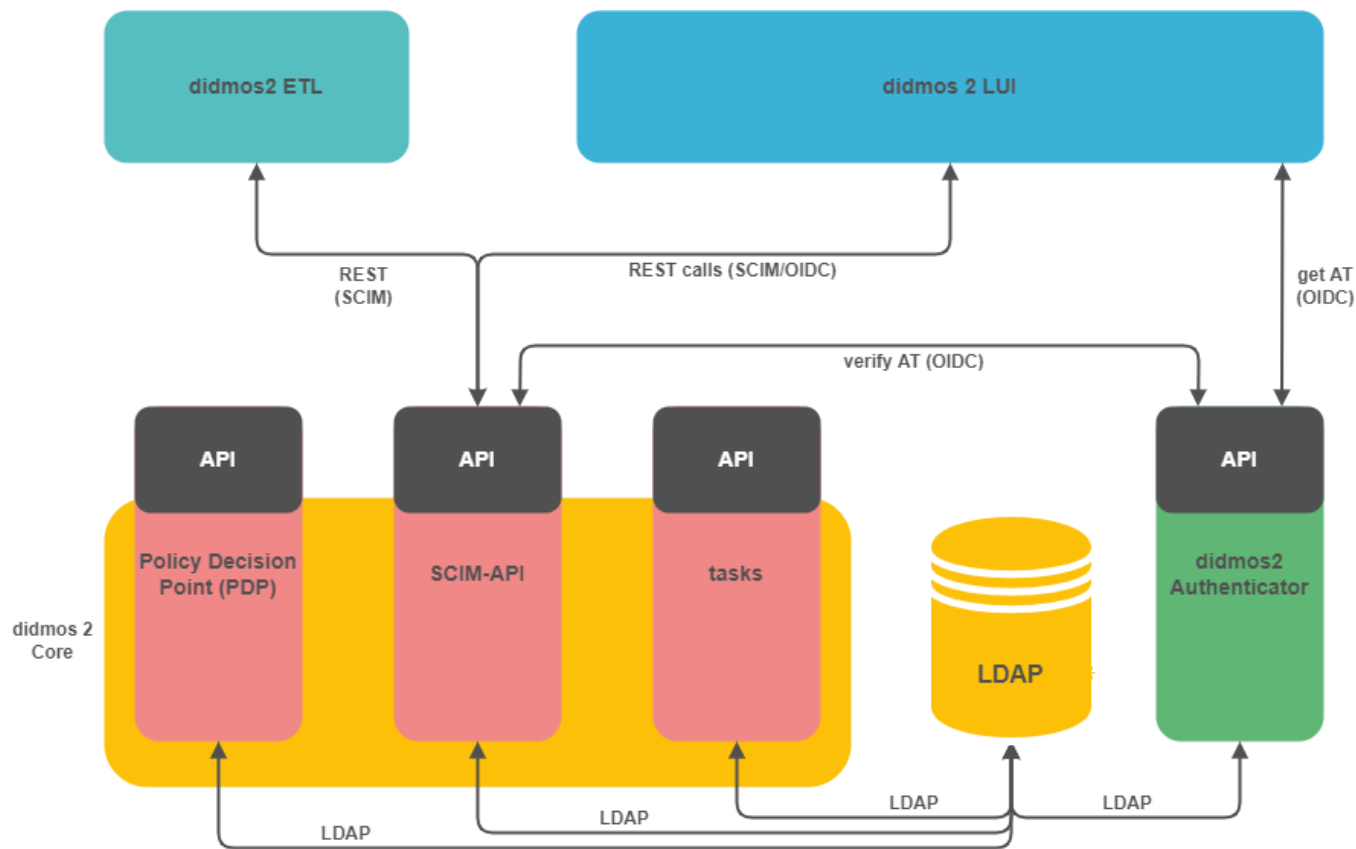
- Can contain additional modules, such as:
 - ETL for synchronization with existing user stores
 - Provisioner to connect applications with non-SSO-protocols or possibly real-time deprovisioning
- Can be used for more advanced use cases since the instance can be fully customized and setup according to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

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





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

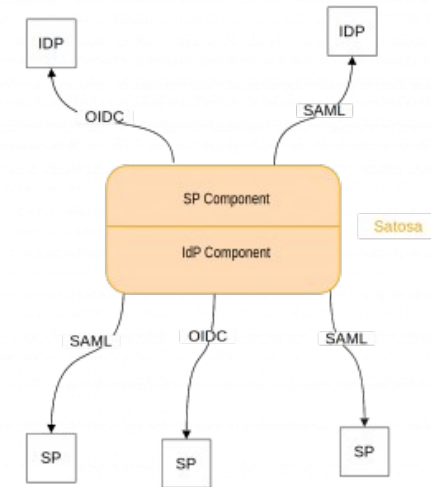
Extensive usage of SCIM

- 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



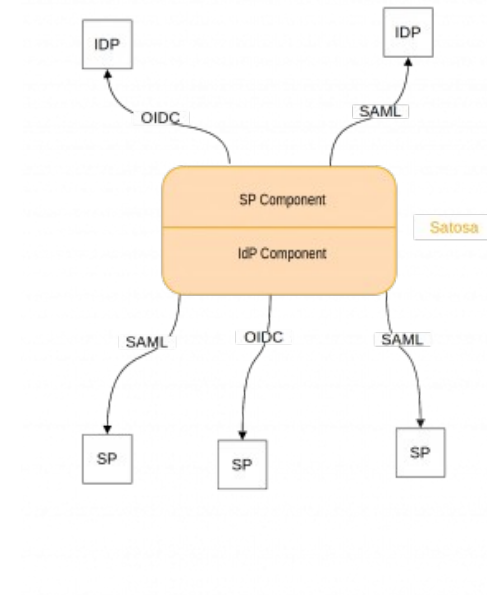
- Acts as an SSO proxy and supports multiple protocols by default
 - IdP/OP for SAML2 and OIDC
 - SP/Client for various protocols/services such as OIDC, SAML2, Social IdPs, Orcid, etc.
- Queries additional attributes, such as entitlements from didmos Core via SCIM API
- Therefore, also can act as a full 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 privilege 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

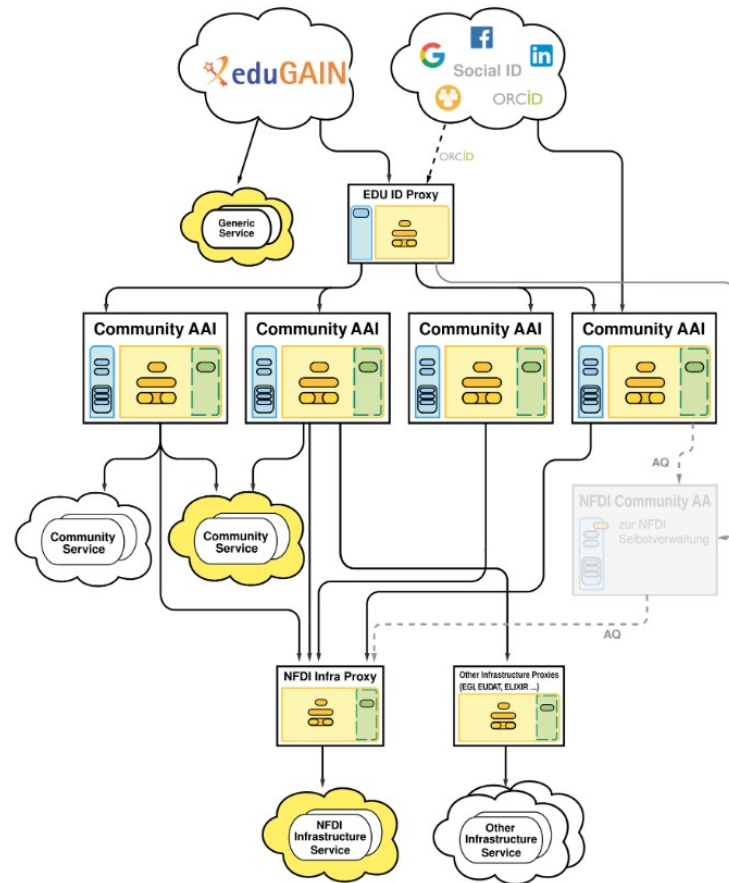


- Due to using open standards, the IdP/proxy is interchangeable. E.g. we also have modules to use Shibboleth IdP with didmos
- This can make sense for use cases where e.g.:
 - SAML attribute queries (AQ) are needed for deprovisioning
 - SLO propagation across „proxy boundaries“ are needed



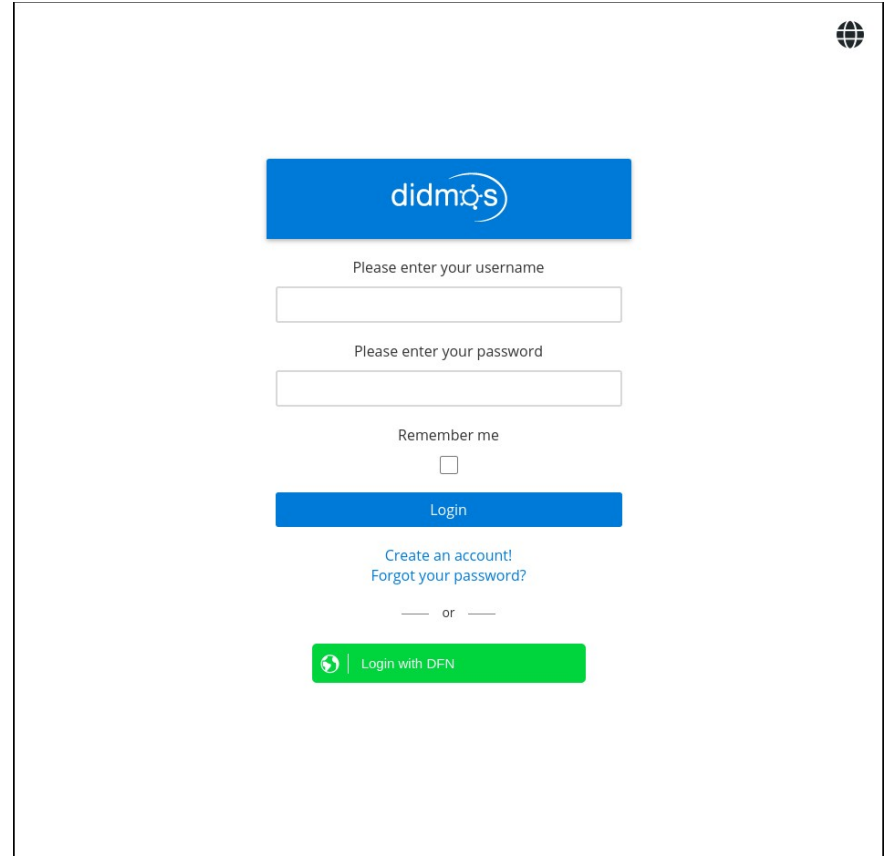
Integration into NFDI Architecture

- 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



The screenshot displays the didmos login and registration page. At the top right is a small globe icon. The main content area features a blue header with the 'didmos' logo. Below the header, there are two input fields: 'Please enter your username' and 'Please enter your password'. A 'Remember me' checkbox is located below the password field. A blue 'Login' button is positioned below the checkbox. Below the 'Login' button are two links: 'Create an account!' and 'Forgot your password?'. Below these links is a separator line with the text 'or'. At the bottom, there is a green button with a globe icon and the text 'Login with DFN'.

Login and registration



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



Please enter your first name

Please enter your last name

Please enter your email address

Please enter the name of your organisation

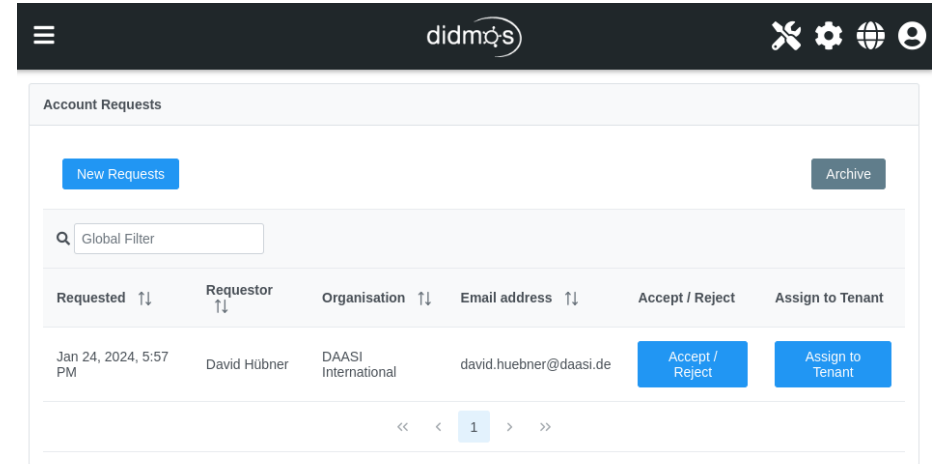
☐ I have read and accept the [DAASI International privacy policy](#)

[Sign up](#)

[Go back](#)

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)

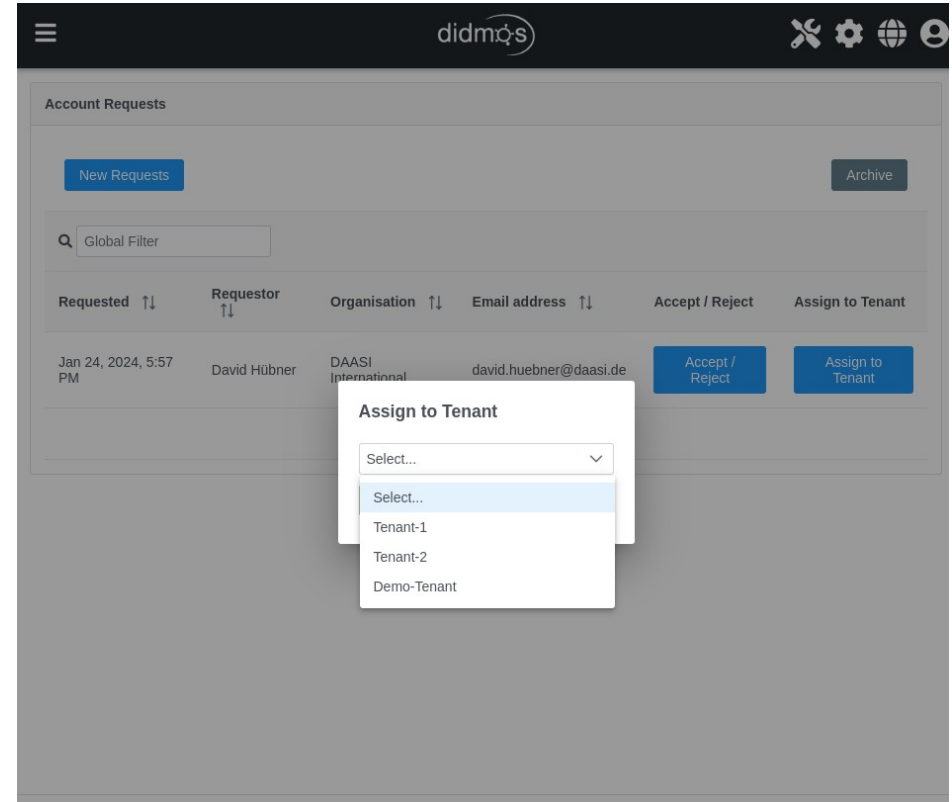


The screenshot shows the 'Account Requests' page in the didmos system. At the top, there is a dark header with the didmos logo, a menu icon, and icons for settings, a globe, and a user profile. Below the header, the page title 'Account Requests' is displayed. There are two buttons: 'New Requests' and 'Archive'. A search bar labeled 'Global Filter' is present. The main content is a table with columns: 'Requested' (with a sort icon), 'Requestor' (with a sort icon), 'Organisation' (with a sort icon), 'Email address' (with a sort icon), 'Accept / Reject', and 'Assign to Tenant'. The table contains one row of data: 'Jan 24, 2024, 5:57 PM', 'David Hübner', 'DAASI International', 'david.huebner@daasi.de'. To the right of the email address are two buttons: 'Accept / Reject' and 'Assign to Tenant'. At the bottom of the table, there is a pagination bar showing '<< < 1 > >>'.

Requested ↑↓	Requestor ↑↓	Organisation ↑↓	Email address ↑↓	Accept / Reject	Assign to Tenant
Jan 24, 2024, 5:57 PM	David Hübner	DAASI International	david.huebner@daasi.de	Accept / Reject	Assign to Tenant

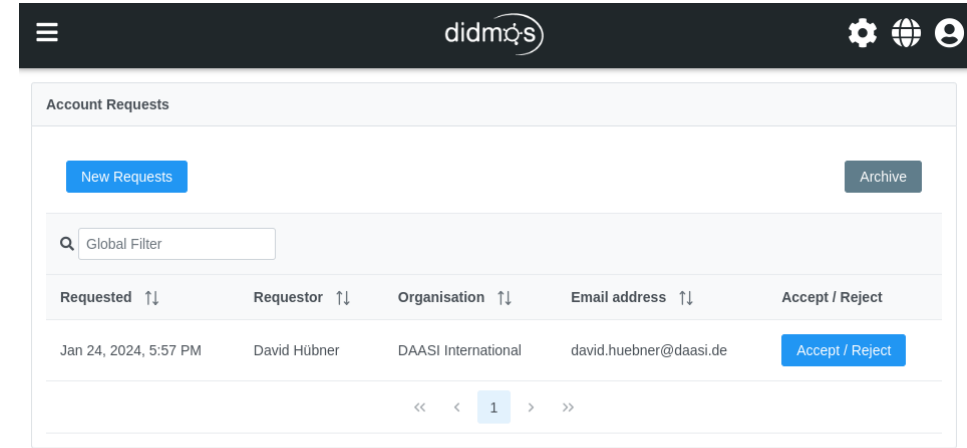
Login and registration

- 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



The screenshot shows the 'Account Requests' page in the didmos system. At the top, there is a dark header with a menu icon, the 'didmos' logo, and icons for settings, a globe, and a user profile. Below the header, the page title 'Account Requests' is displayed. There are two buttons: 'New Requests' on the left and 'Archive' on the right. A search bar labeled 'Global Filter' is present. The main content is a table with the following columns: 'Requested' (with a sort icon), 'Requestor' (with a sort icon), 'Organisation' (with a sort icon), 'Email address' (with a sort icon), and 'Accept / Reject'. The table contains one row with the following data: 'Jan 24, 2024, 5:57 PM', 'David Hübner', 'DAASI International', 'david.huebner@daasi.de', and an 'Accept / Reject' button. At the bottom of the table, there is a pagination bar showing '<< < 1 > >>'.

Requested ↑↓	Requestor ↑↓	Organisation ↑↓	Email address ↑↓	Accept / Reject
Jan 24, 2024, 5:57 PM	David Hübner	DAASI International	david.huebner@daasi.de	Accept / Reject

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



To complete the login process, we are asking you to consent to the following.

Terms of Use
This is demo text for the terms of service.

☐ To complete the login process, we are asking you to consent to the following.

The following personal details will be released to the service provider:

sub	9ca1408b-d3ca-47eb-9d35-e3d077c7305d
preferred_username	david.huebner@daasi.de
name	David Hübner
family_name	Hübner
given_name	David
email	david.huebner@daasi.de
eduperson_assurance	https://refeds.org/assurance/ATP/ePA-1m , https://refeds.org/assurance/IAP/low , https://refeds.org/assurance/ID/unique , https://aarc-project.eu/policy/authn-assurance/assam
entitlements	

☐ I consent to the release of the above-mentioned attributes.

I Agree

Reject



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.

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

The screenshot displays the 'didmos' self-service portal interface. The top navigation bar includes the 'didmos' logo, a 'THEMES' link, a 'Language' selector with a globe icon, and a user profile for 'David Hübner'. A left-hand sidebar lists navigation options: 'My Data' (selected), 'Change Password', 'MFA Tokens', 'Groups', 'Request Admin Access', 'My History', and 'Delete Account'. The main content area is titled 'User Details' and contains the following information:

- Username: david.huebner@daasi.de
- First name: David
- Last name: Hübner
- Email addresses: david.huebner@daasi.de (with a green checkmark and a red trash icon)
- Phone numbers: (with a plus icon)
- Groups: (empty)
- Roles: standarduser

A green 'Save' button is located at the bottom of the 'User Details' form.

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

didmos

THEMES

Language

David Hübner

My Data

Change Password

MFA Tokens

Groups

Request Admin Access

My History

Delete Account

TOTP Token Activation

With time-based tokens (TOTP), a new value is generated for you every minute, which serves as a second factor. To do this, you first need an app on your smartphone, e.g. privacyIDEA Authenticator or Google Authenticator.

First, please add the token to your Authenticator App by scanning the QR code or entering the secret below.



Secret of your token: NV7FOYDISXIB2IH5QS4MC3DX6ONT7E2T

After adding the TOTP token to your App, please input the displayed code to finish the activation process:

Confirm

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

The screenshot shows the 'didmos' user interface. At the top, there's a navigation bar with the 'didmos' logo, 'THEMES', 'Language', and a user profile 'David Hübner'. A left sidebar contains menu items: 'My Data', 'Change Password', 'MFA Tokens' (highlighted in blue), 'Groups', 'Request Admin Access', 'My History', and 'Delete Account'. The main content area is titled 'My MFA Tokens' and includes a '+ Register new Token' button. Below this is a table with columns 'Token ↑↓', 'Token Type ↑↓', and 'Delete'. The table contains one entry: 'TOTP0000C5F8' with type 'TOTP'. A red 'Delete Token' button is next to it. At the bottom of the table, there's a pagination bar showing '<< < 1 > >>'. The interface is clean and modern, using a dark header and light body colors.

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

The screenshot displays the Admin portal interface. The top navigation bar includes the 'didmos' logo, 'THEMES', 'Administration' (with a gear icon), 'Language' (with a globe icon), and 'Tenant-1 Admin' (with a user icon). The left sidebar menu contains the following items: 'Userlist' (selected, with a user icon), 'Account Requests' (with a person icon), 'Grouplist' (with a group icon), 'Group Requests' (with a document icon), 'Rolelist' (with a person icon), 'Role Requests' (with a document icon), 'Trash' (with a trash can icon), and 'Import csv file' (with a document icon). The main content area is titled 'Users Table' and features a 'Refresh' button and an 'Add User' button. Below the title is a 'Global Filter' search bar. The table has four columns: 'Name ↑↓', 'Roles ↑↓', 'Emails ↑↓', and 'Delete'. The table contains three rows of user data:

Name ↑↓	Roles ↑↓	Emails ↑↓	Delete
Tenant-1 Admin	admin		Move to trash
Max Mustermann	socialuser		Move to trash
David Hübner	standarduser	david.huebner@daasi.de	Move to trash

At the bottom of the table, there is a pagination control showing '1' as the current page, with navigation arrows for previous and next pages.

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

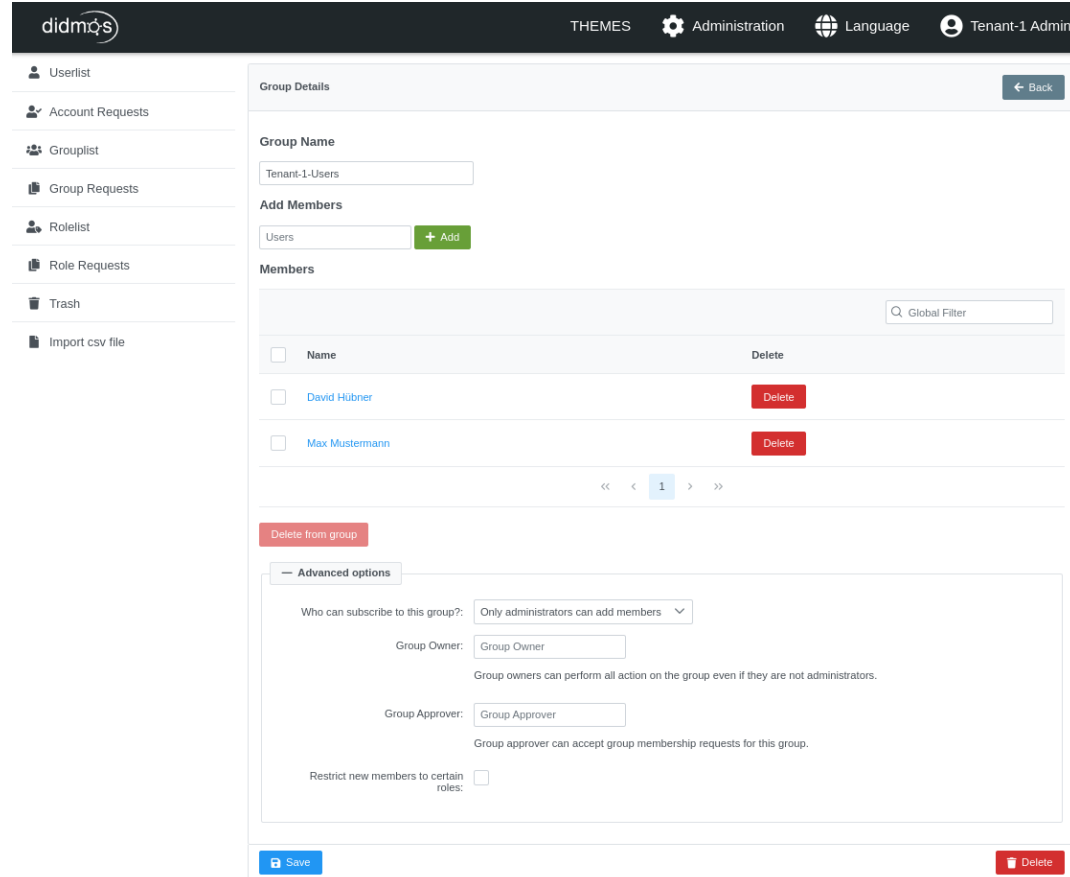
The screenshot displays the 'didmos' Admin portal interface. The top navigation bar includes the 'didmos' logo, 'THEMES', 'Administration' (with a gear icon), 'Language' (with a globe icon), and 'Tenant-1 Admin' (with a user icon). A left sidebar lists various management options: Userlist, Account Requests, Grouplist, Group Requests, Rolelist, Role Requests, Trash, and Import csv file. The main content area is titled 'User Details' and features a 'Back' button. It shows the following information for a user:

- Username: david.huebner@daasi.de
- First name: David
- Last name: Hübner
- Email addresses: david.huebner@daasi.de (with a green checkmark and a red trash icon)
- Phone numbers: (with a plus icon)
- Active: ☒ User is active and can login
- Groups: -
- Roles: standarduser

Below this information is a section for 'Password actions' with a 'Set new password' field containing the text 'password'. A note states: 'Alternatively you can click the button below to send an email with a password reset link to the user. Make sure the user has set an email address.' A blue button labeled 'Send password reset link' is provided. Further down are buttons for 'Manage MFA Tokens', '+ Manage group memberships', and 'User History'. At the bottom, there is a green 'Save' button and a red 'Move to trash' button.

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



The screenshot displays the 'didmos' Group management interface. The top navigation bar includes 'THEMES', 'Administration', 'Language', and 'Tenant-1 Admin'. A left sidebar lists navigation options: Userlist, Account Requests, Grouplist, Group Requests, Rolelist, Role Requests, Trash, and Import csv file. The main content area is titled 'Group Details' and features a 'Back' button. It shows the 'Group Name' as 'Tenant-1-Users' and an 'Add Members' section with a 'Users' input field and a '+ Add' button. Below this is a 'Members' table with columns for 'Name' and 'Delete'. The table lists two members: 'David Hübner' and 'Max Mustermann', each with a 'Delete' button. A 'Global Filter' search bar is present above the table. At the bottom of the members list, there is a 'Delete from group' button and an 'Advanced options' section. The 'Advanced options' section includes a dropdown for 'Who can subscribe to this group?' (set to 'Only administrators can add members'), input fields for 'Group Owner' and 'Group Approver', and a checkbox for 'Restrict new members to certain roles'.

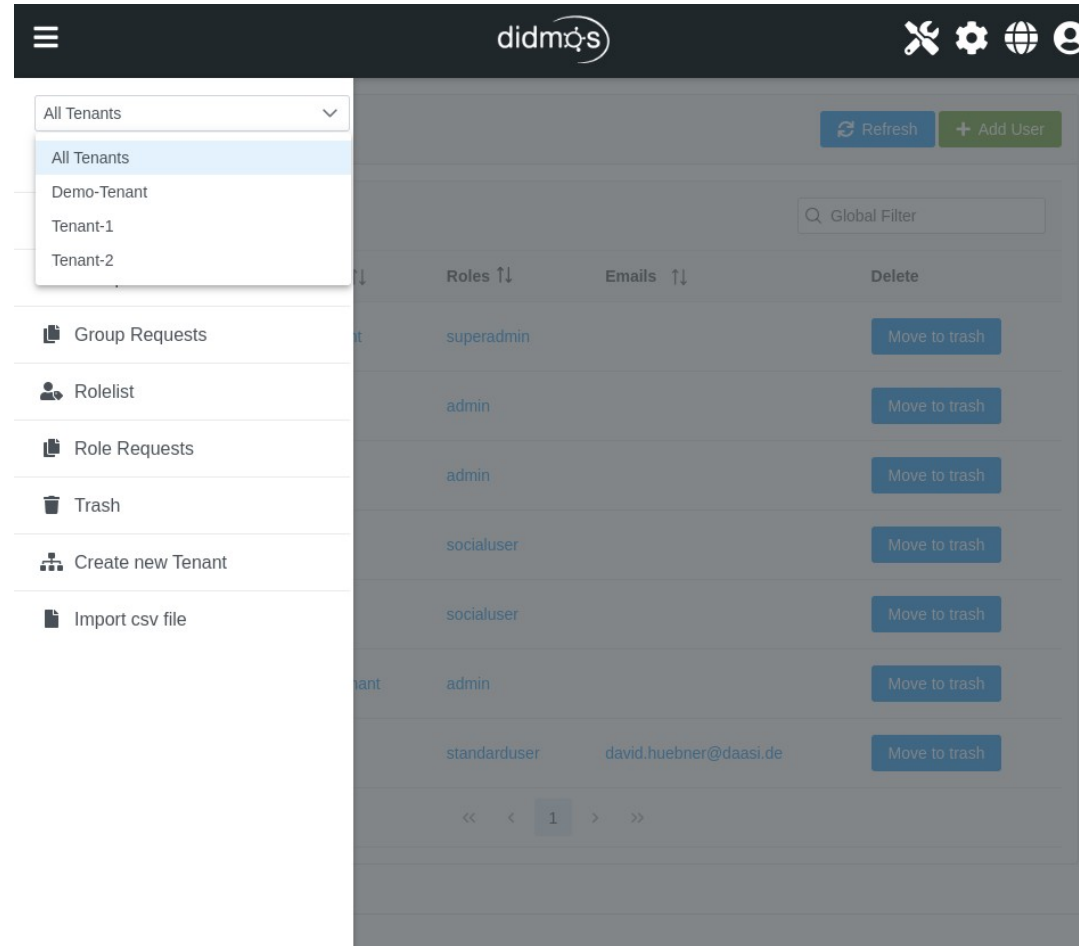
Group management

- 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

The screenshot displays the didmos web application interface. The top navigation bar includes the didmos logo, a 'THEMES' dropdown, a 'Language' selector with a globe icon, and a user profile for 'David Hübner'. A left sidebar contains a menu with options: 'My Data', 'Change Password', 'MFA Tokens', 'Groups' (highlighted in blue), 'Request Admin Access', 'My History', and 'Delete Account'. The main content area is titled 'Group Table' and features a 'Refresh' button. Below the title is a search bar labeled 'Groupname ↑↓'. A table below the search bar shows one entry, 'Tenant-1-Users', with a 'Request Membership' button to its right. At the bottom of the table, there is a pagination control showing '<< < 1 > >>'.

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

didmos

THEMES

Configuration

Administration

Language

Super Admin

LDAP

OIDC

SMTP Server

Multi Tenancy

User Management

User Mapping

CSV Import

Attribute Policies

MFA

System emails

Logging

Expert Mode

Reload Configuration

Configuration

Enable Selfregistration:

A request ist being generated which later has to be approved or denied by en administrator. If false user is created directly. If no value is set, it defaults to true.

Selfregistration as request:

A request ist being generated which later has to be approved or denied by en administrator. If false user is created directly. If no value is set, it defaults to true.

Uid on selfreg:

mail

Form which source should the uid be generated? This can be any ldap attribute that is beeing submitted together with the POST request that created the User or 'generate'. In case of generate a uid is beeing generated. Usually this would be set to 'mail' or 'generate'.

Uid on User Creation:

mail

Form which source should the uid be generated? This can be any ldap attribute that is beeing submitted together with the POST request that created the User or 'generate'. In case of generate a uid is beeing generated. Usually this would be set to 'mail' or 'generate'.

Unique attributes:

```
{  
  "mail": {  
    "global": true  
  },  
  "uid": {  
    "global": true  
  }  
}
```

This determines which ldap attributes need to be unique User attributes in the ldap. global:false means it only needs to be unique within it's own tenant. Be aware the attribute beeing used for login (usually uid) needs to be globally unique. Mail needs to be unique if you want to support password reset via mail.

Object Classes:

```
[  
  "inetOrgPerson",  
  "rbacResource",  
  "didmosPerson",  
  "schacPersonalCharacteristics",  
  "eduPerson",  
  "schacContactLocation",  
  "schacLinkageIdentifiers",  
  "voPerson"  
]
```

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



- **Extract Transform Load**
- 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)

didmos Provisioner



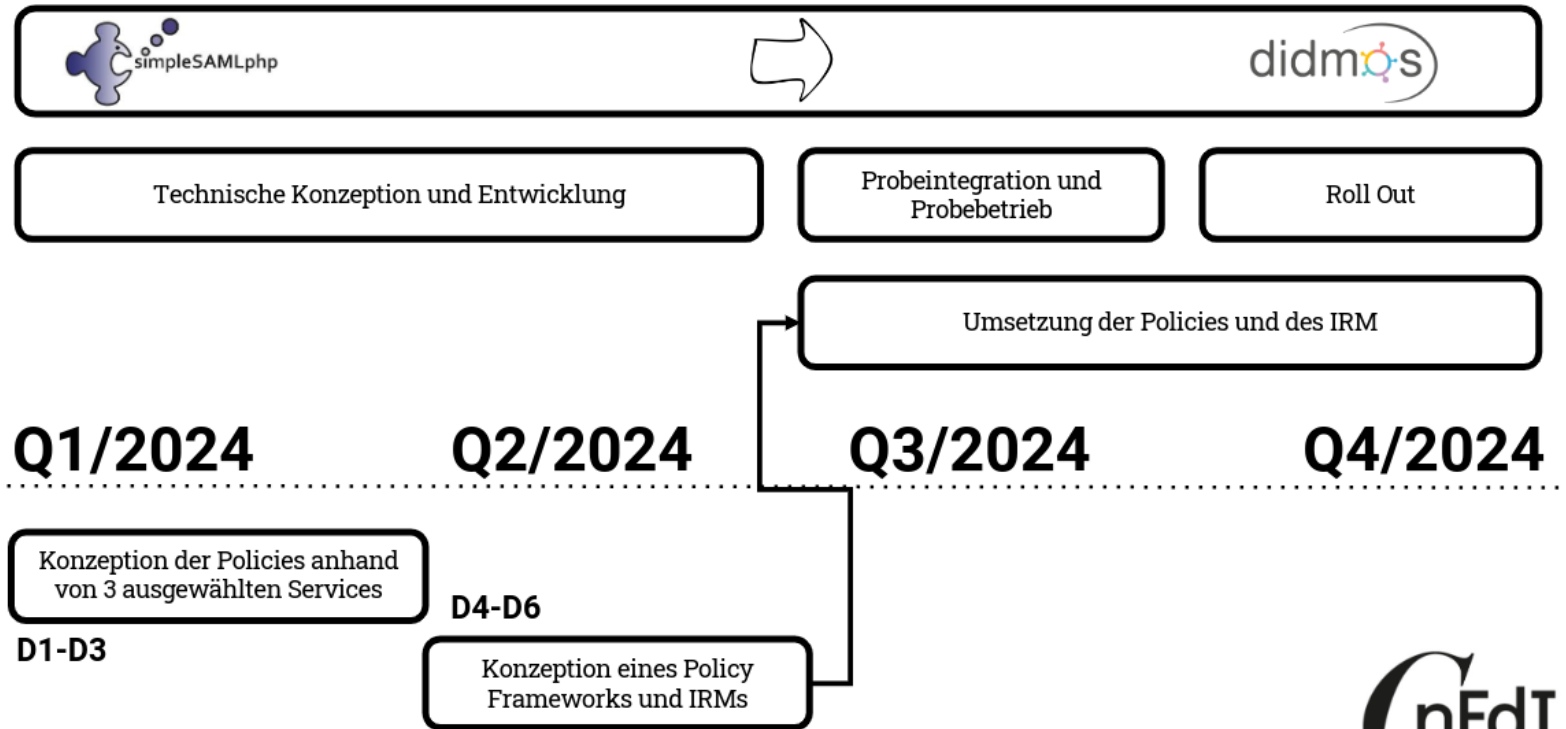
- Real-time transfer of identity information to connected target systems
 - Reads change information in the OpenLDAP accesslog
 - Architecture is inspired by SPML, however SCIM is implemented as well
- Changes are recorded in SCIM compliant JSON documents which are inserted into the queuing system RabbitMQ
- 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.

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

Example for dedicated instance: NFDI4Culture

TIER 1 (AWLM + DAASI)



TIER 2 (IAM4NFDI + 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>

Thank you for listening.

David Hübner

DAASI International

email: `david.huebner@daasi.de`