didmos as a Community AAI solution

Basic Service Identity & Access Management: Workshop IAM Basics #3

David Hübner, Peter Gietz
DAASI International GmbH

DAASI International

didmos

DAASI International

Identity

Management with

Open

Source

didmos

- A standardised IAM system so flexible it is able to address all customer needs no matter how specific
- Successfully implemented for >10 customers in projects with >100k users
- didmos consists of several flexibly configurable modules for different tasks
  - We can pick the right modules and extensions based on the requirements
- didmos also allows for plugin interfaces in many places to allow for extensions

DAASI International

didmos

- Open source and open standards
  - didmos is 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 SAML, OIDC, SCIM
- Available as Docker images and also runs under Kubernetes

DAASI International

didmos in NFDI

Central instance for NFDI

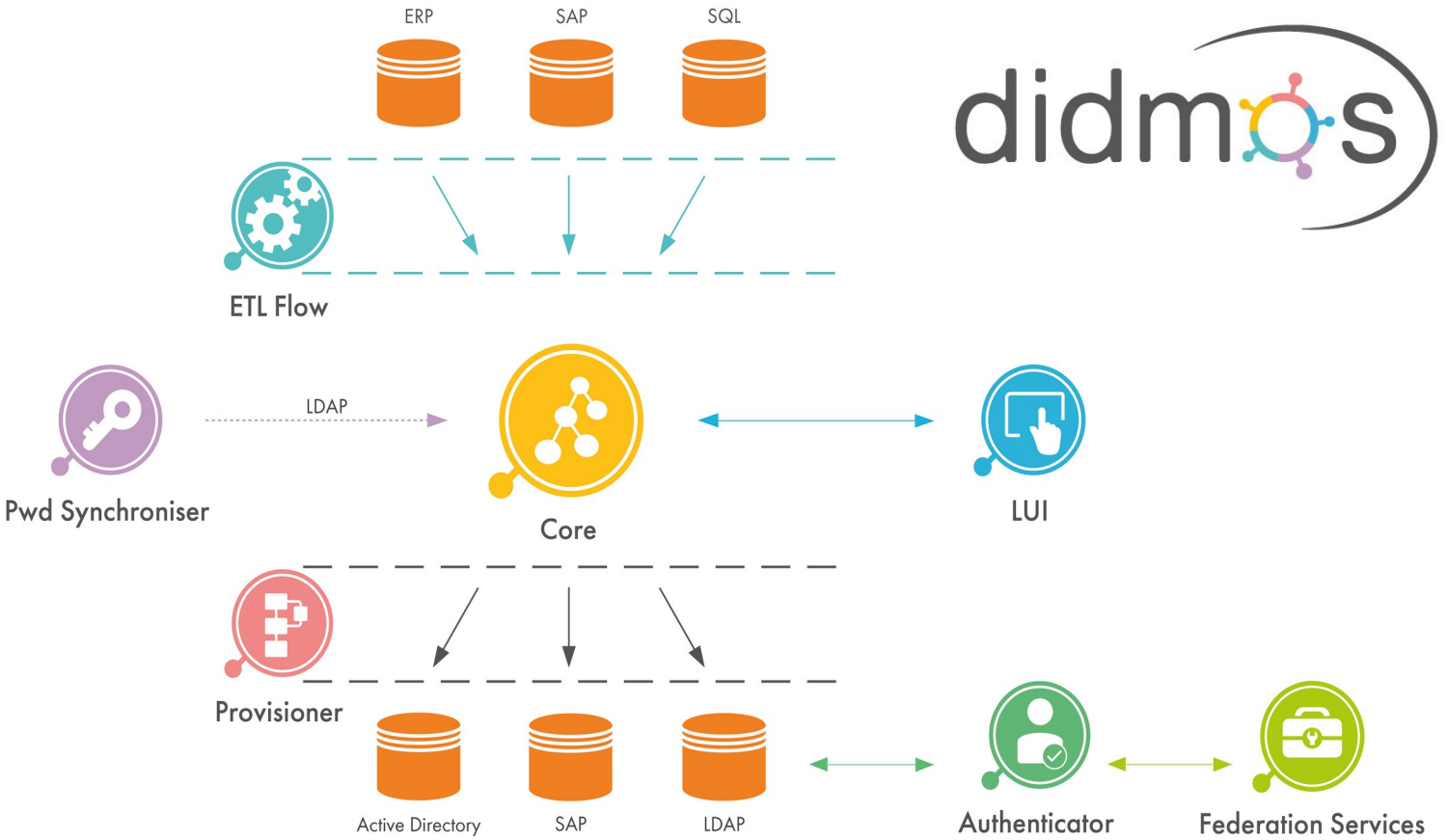
- https://portal.didmos.nfdi-aai.de
- Operated by DAASI with „best effort“ SLAs
- Free of charge for NFDI Consortia
- Multi-tenancy (a NFDI Consortium is a tenant) with isolated user and group management
- Limited options for customization
- Is being updated over the course of the NFDI project with additional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

Dedicated 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



DAASI International

didmos in NFDI

Central instance for NFDI

- Contains the modules Core, LUI and Auth
- Use case:
  - didmos is the main CAAI
  - Majority of the users can login via Edu-ID, eduGAIN or social IDs. Local users are also possible
  - A consortium assigns a number of Consortium admins that have extended permissions in didmos 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

Dedicated instance

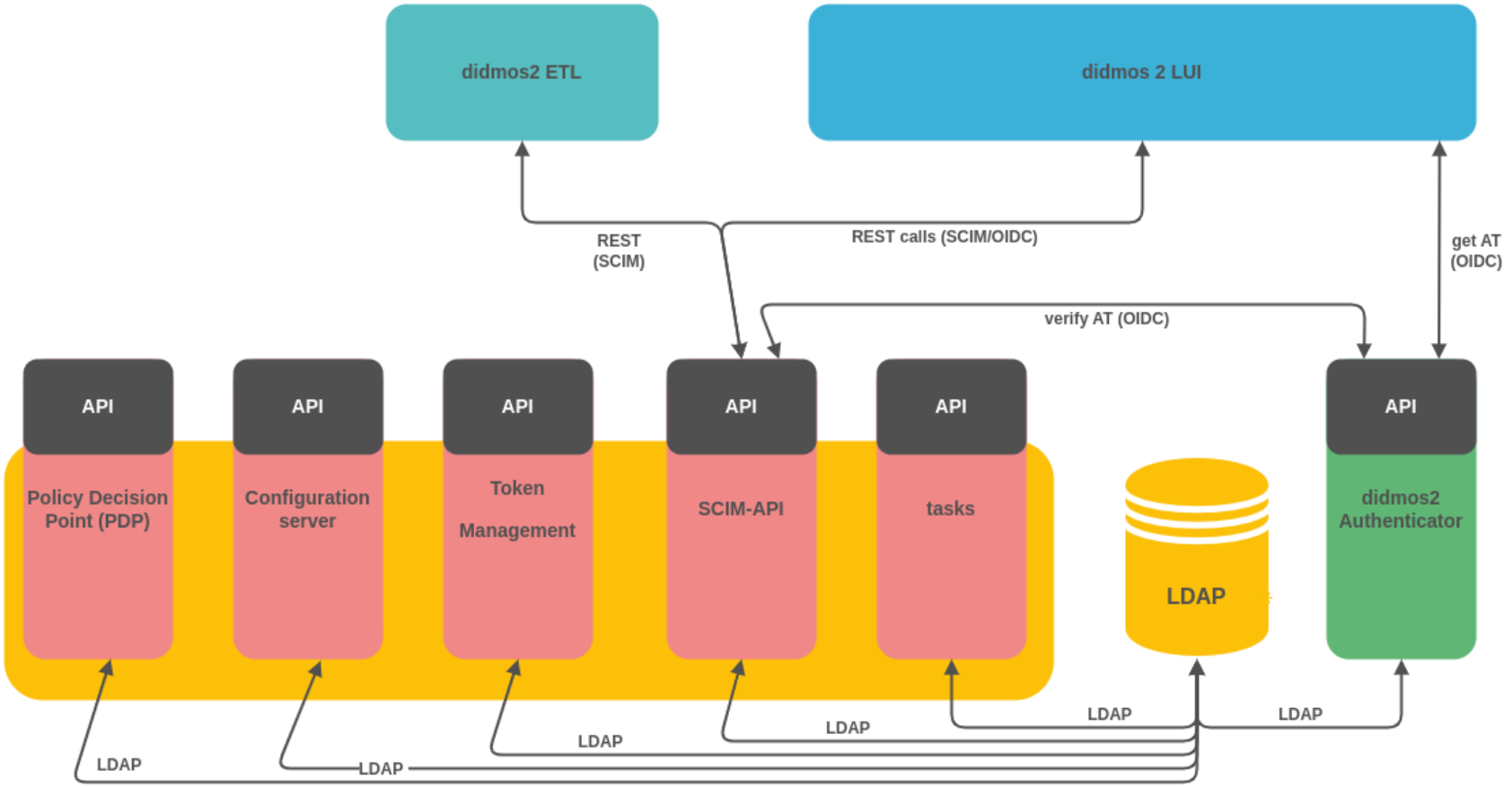
- Can contain additional modules, such as:
  - ETL for synchronization with existing user stores
  - Provisioner to connect applications with non-SSO-protocols or possibly real-time deprovisioning
- Can be used for more advanced use cases and as basis for individual feature development

DAASI International

didmos Core

- Core consists of two components:
  - OpenLDAP server as metadirectory
  - Backend/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
  - 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 and standards



didmos LUI

Frontend entirely based on JavaScript (Angular)

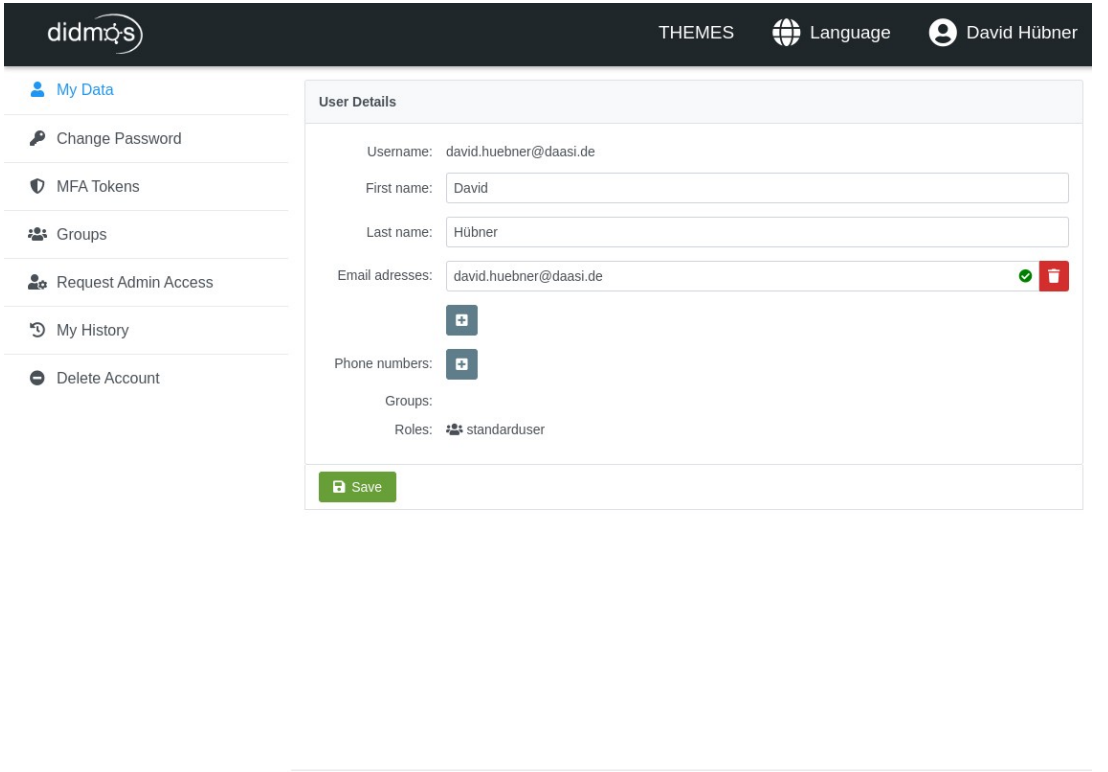
- Responsive Single-page application
- Mobile app (PWA) capable
- Authentication with OIDC
- Adjustable, both for layout and functionality (we have various standard modules in a shared library and can create custom modules)
- Both for selfservice and admin functionality

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

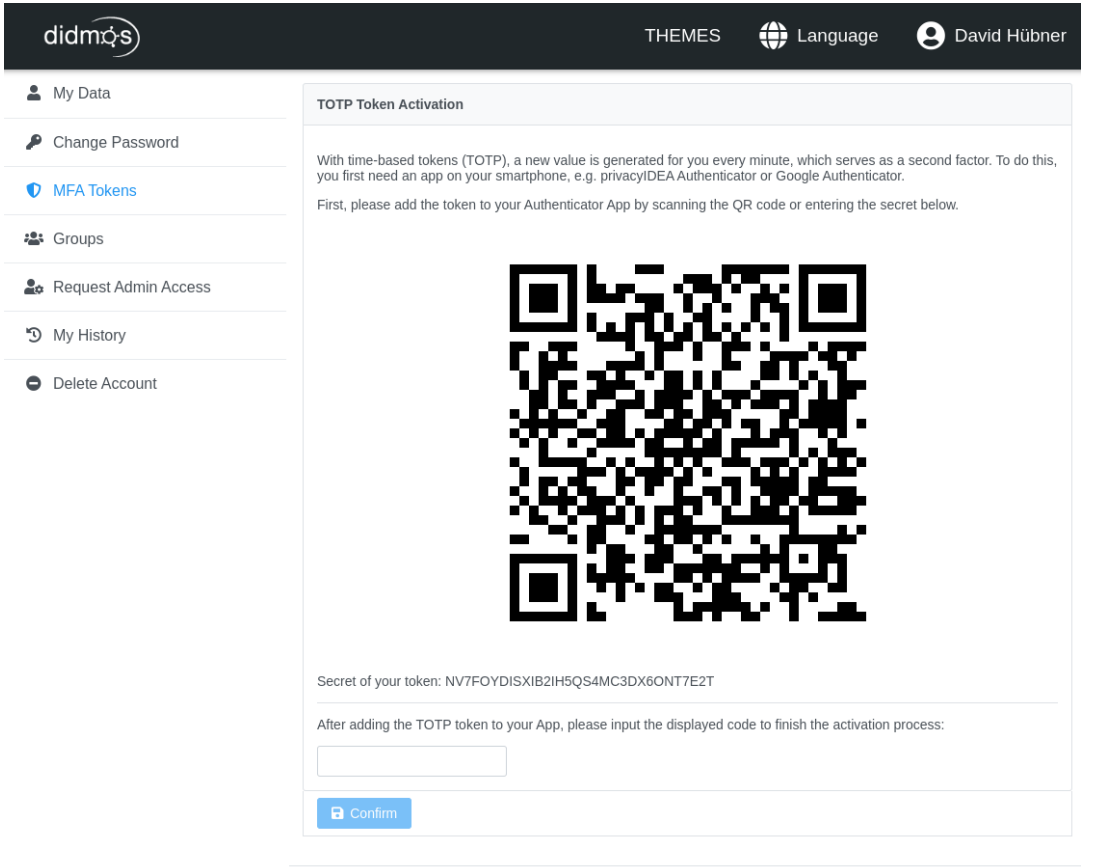
Self service portal

- 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



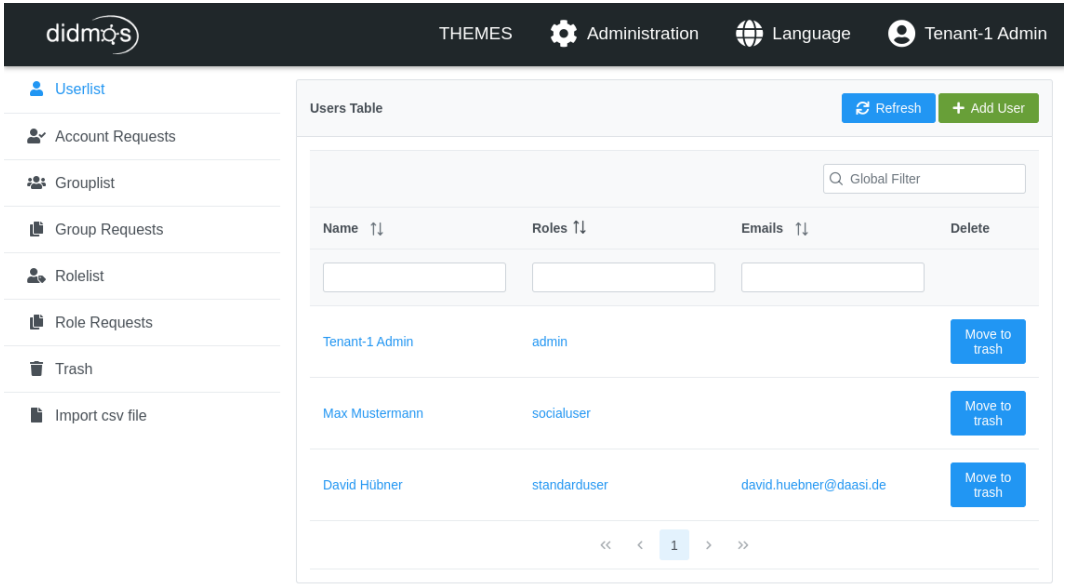
MFA token management

- 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
- 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 and operations such as password change and account deletion



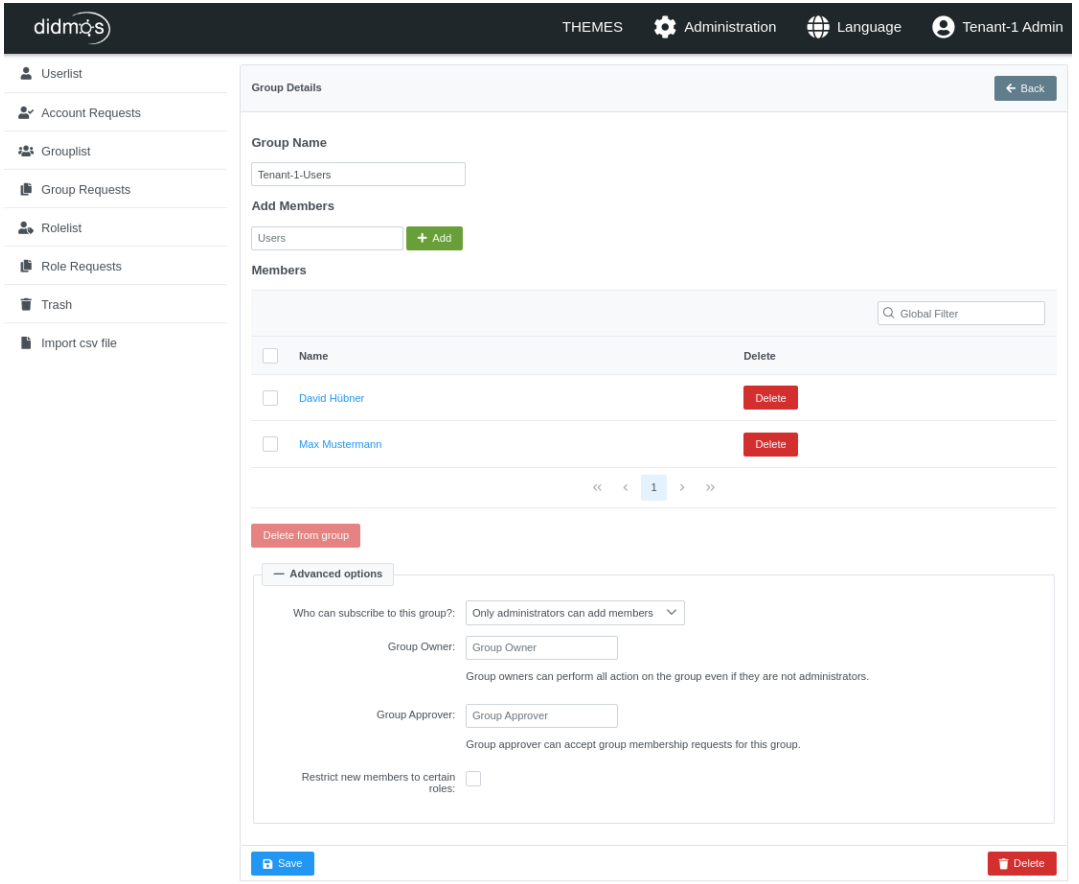
Admin portal

- 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



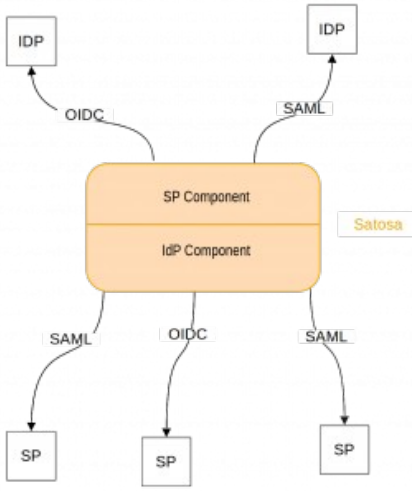
Group management

- 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 request membership
  - Users can freely join groups



didmos Authenticator

- Acts as an SSO proxy and supports multiple protocols by default
  - Acts as an IdP/OP for SAML2 and OIDC
  - Acts an an 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
- Various optional microservices for functionality such as MFA, Consent, etc.
- Users with external accounts are created in didmos as „Shadow accounts“ without passwords and can be managed in the VO
- Also support authentication with local accounts (i.e. users with passwords in didmos)



didmos ETL Flow

- **E**xtract **T**ransform **L**oad
- Typical flow (simplified):
  - Read and convert (multiple) data sources (e.g. ldapsearch)
  - Identify against IdM
  - Merge identical data sets within one data source if necessary
  - Merge multiple data sources
  - Calcluate diff against IdM
  - Install changes
- Typically used for either one-time data migration or regular synchronization from source systems
- The workflow is configured via LDAP objects (=configuration)

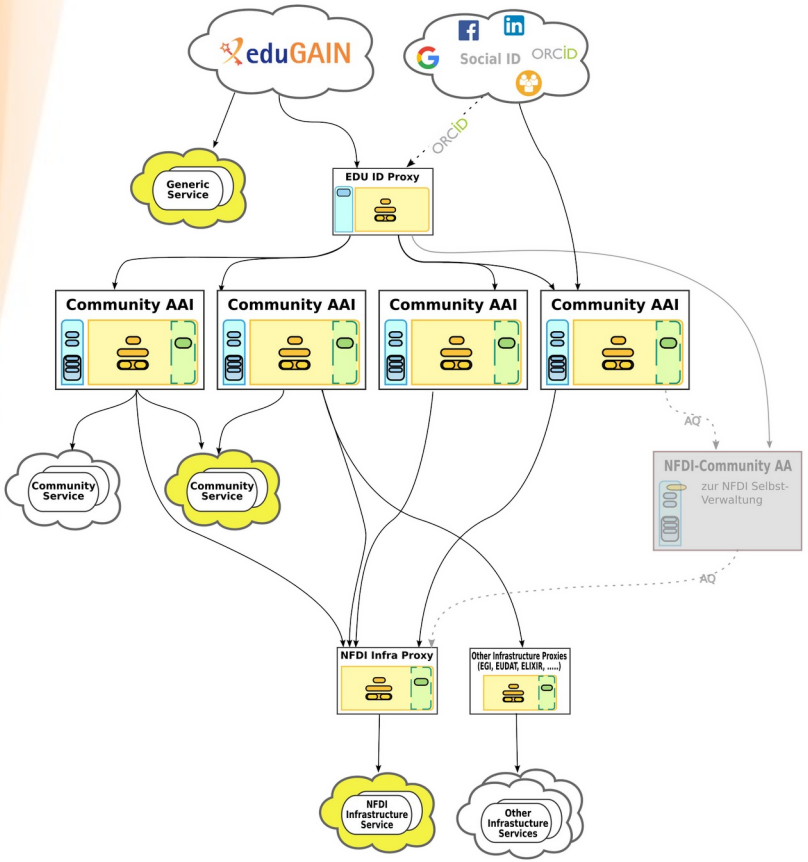
DAASI International

didmos Provisioner

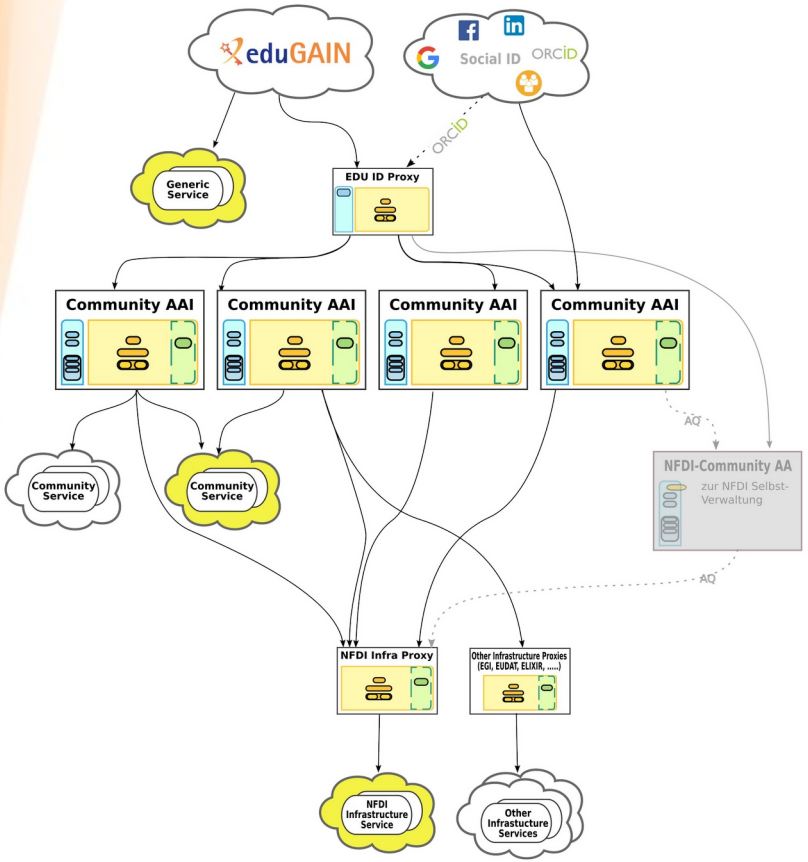
- Real-time transfer of identity information to connected target systems
  - Reads change information in the OpenLDAP accesslog
  - Architecture is inspired by SPML, however it can implement SCIM as well
- Changes are recorded in JSON documents which are inserted into the queuing system RabbitMQ
- A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

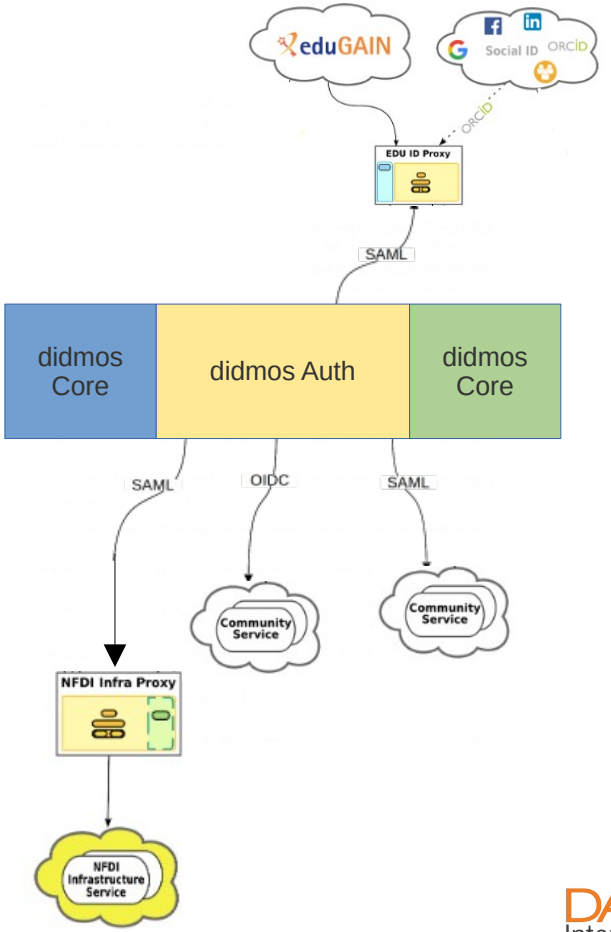
DAASI International

NFDI integration



NFDI integration





NFDI-Work

- NFDI attribute model integrated into our default config and refining our CI/CD processes
- A central instance is set up
  - that consists of our main components to implement the integration scenario shown on the previous page
  - didmos Core, didmos LUI and didmos Auth
  - Already evaluated by different NFDI consortia
- The multi tenancy capabilities of didmos can be used to onboard different consortia
- Once the Edu ID system is available, we will connect to that. For now we integrate eduGAIN directly
- We can create and deploy individual deployments for more complex projects, either on-premise or as a SaaS solution
  - In such projects we can also add didmos ETL Flow to sync existing user data and didmos Provisioner for systems that do not support SSO ...
  - ... or to support push (de)provisioning in addition to SSO

DAASI International

Thank you for listening.

David Hübner, Peter Gietz

DAASI International, www.daasi.de

email: david.huebner@daasi.de

p.gietz@daasi.de