

didmos as a Community AAI solution

Basic Service Identity & Access Management: Workshop IAM Basics #2

**David Hübner
DAASI International GmbH**

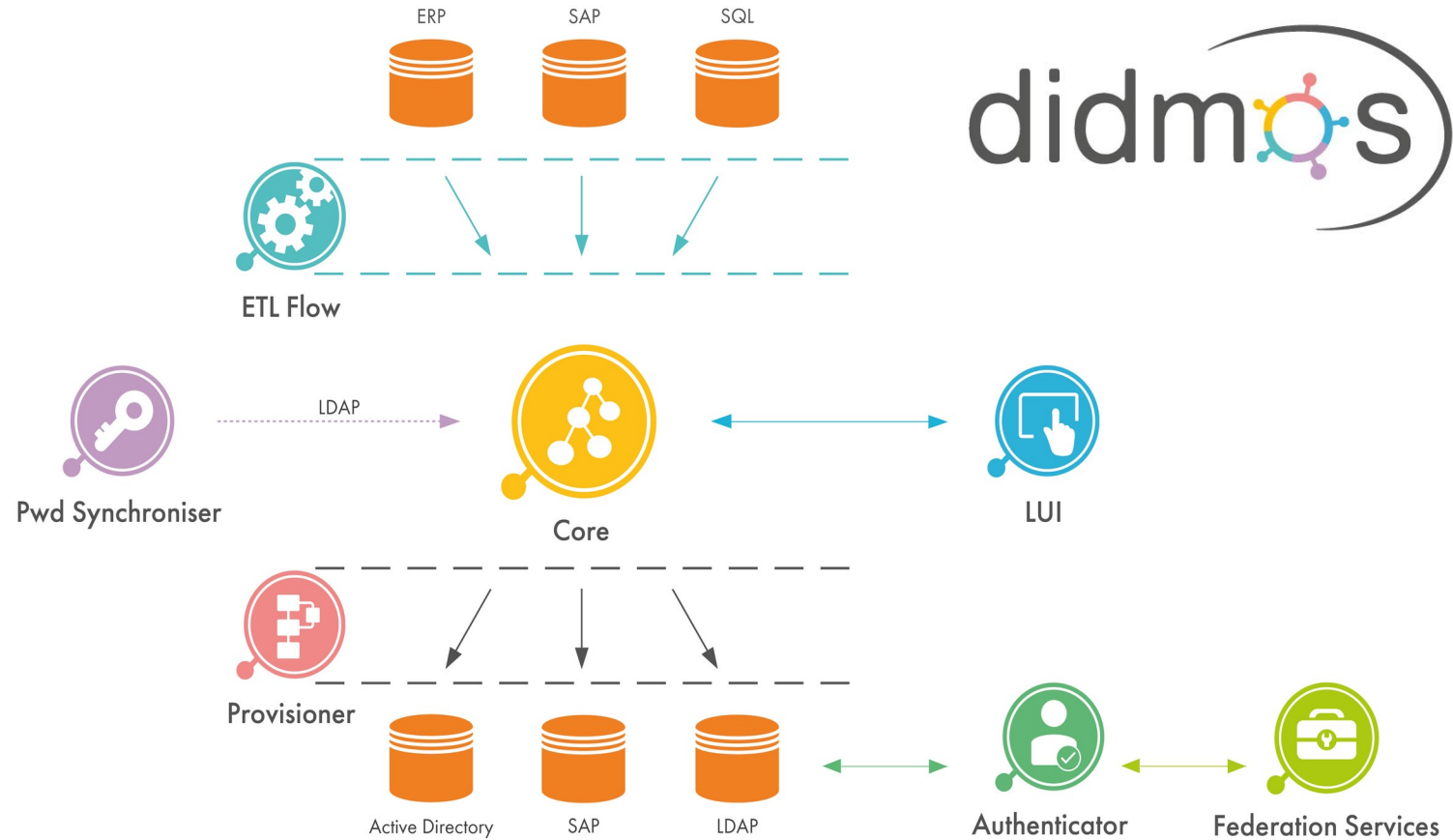
didmos

- A standardised IAM system so flexible it is able to address all customer needs no matter how specific
- Successfully implemented for more than nine customers
- It is very difficult to develop a software which meets all requirements. Hence, didmos consists of several modules for different tasks.
- didmos also allows for plugin interfaces in many places to allow for extensions
- The development of didmos relied on well-established open source products such as OpenLDAP, RabbitMQ, SATOSA, and many more
- Available as Docker Images

DAASI International Identity Management with Open Source



didmos - Overview



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



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

didmos LUI

- Self-Service – User Information



THEMES    Super Admin

 My Data

 Change Password

 Groups

 Request Admin Access

 My History

 Delete Account

User Details

Username: superadmin

First name:

Last name:

Email address:

Phone numbers: 

Groups:

Roles:

 standarduser

 superadmin

 Save

didmos2 - LUI

Developed by 

didmos LUI

- Customer – Edit Groups



THEMES    Super Admin

 My Data

 Change Password

 **Groups**

 Request Admin Access

 My History

 Delete Account

Group Table  Refresh

Groupname 	
grupppe3-open	Subscribe
gruppe2-requestable	Request Membership
gruppe4-isAssignable	Subscribe

  **1**  

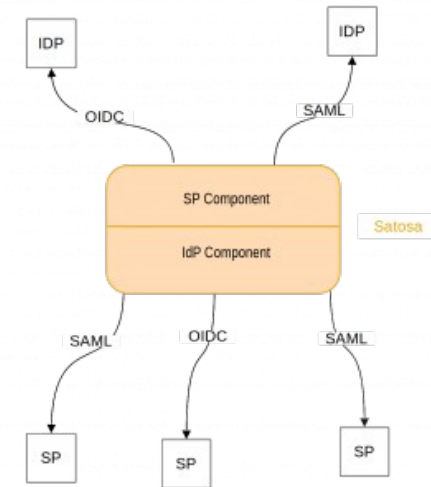
didmos2 - LUI

Developed by


didmos Authenticator



- Acts as an SSO proxy and supports multiple protocols by default
 - Acts as an IdP/OP for SAML2 and OIDC
 - Acts as 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



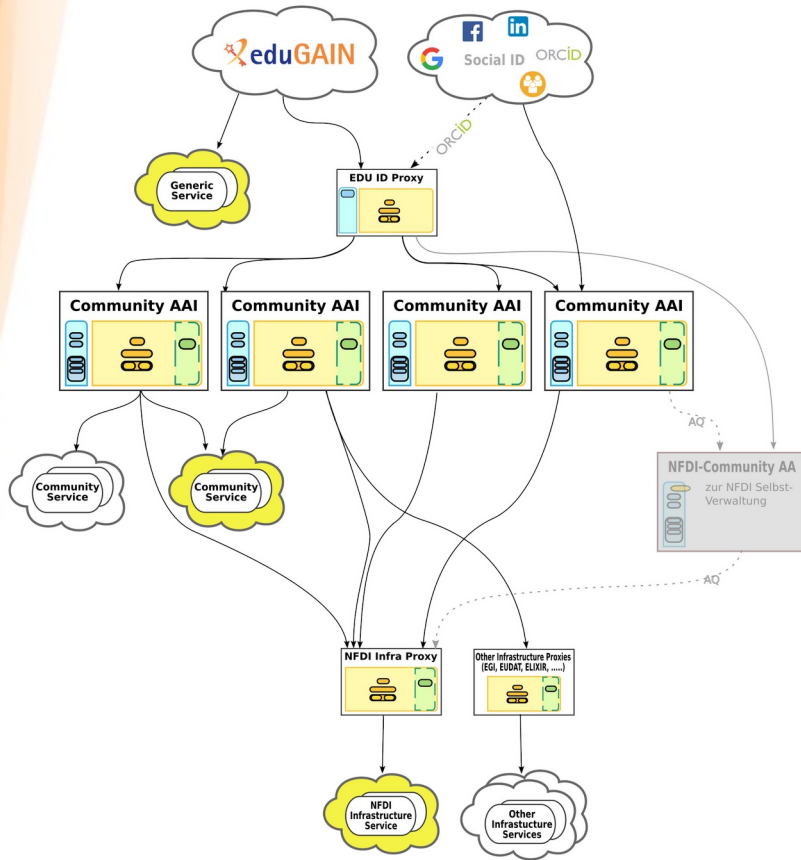
- **Extract Transform Load**
- Typical flow (simplified):
 - Read and convert (multiple) data sources (e.g. ldapsearch)
 - Identify against IdM
 - Merge identical data sets within one data source if necessary
 - Merge multiple data sources
 - Calculate diff against IdM
 - Install changes
- Typically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

didmos Provisioner

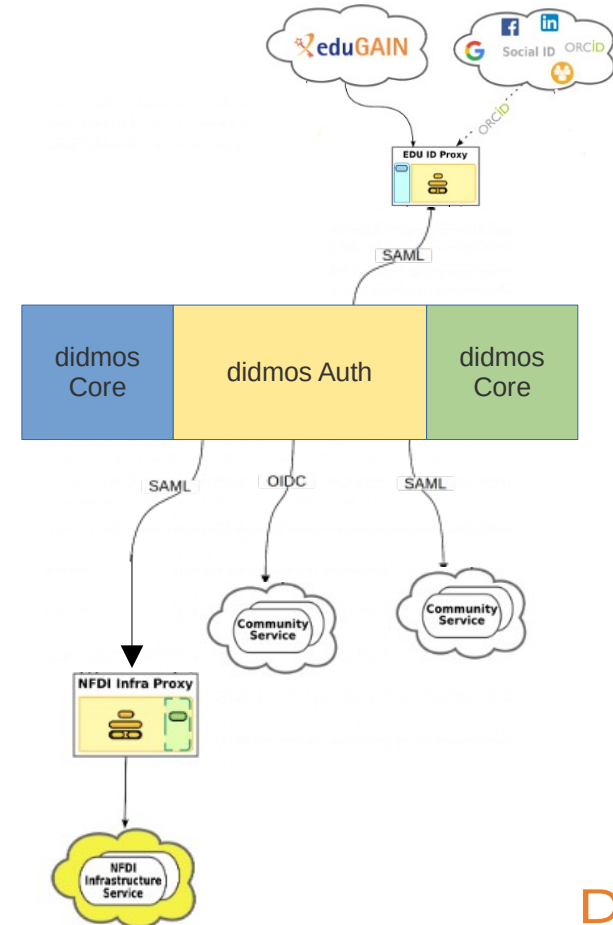
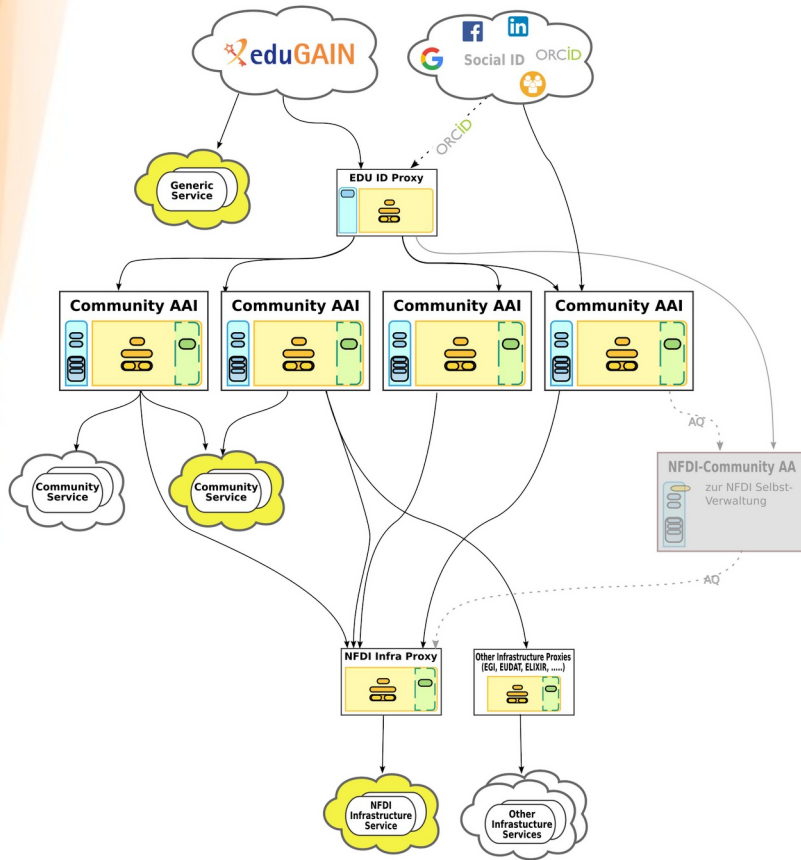


- Real-time transfer of identity information to connected target systems
 - Reads change information in the OpenLDAP accesslog
 - Architecture is inspired by SPML, however it can implement SCIM as well
- Changes are recorded in JSON documents which are inserted into the queuing system RabbitMQ
- A dedicated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

NFDI integration



NFDI integration



What we're working on

- We're currently implementing the NFDI attribute model into our default config and refining our CI/CD processes
- We're setting up a demonstrator that consists of our main components to implement the integration scenario shown on the previous page
 - didmos Core, didmos LUI and didmos Auth
- The multi tenancy capabilities of didmos can be used to onboard different communities
- 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

Thank you for listening.

David Hübner

DAASI International

email: david.huebner@daasi.de