

AcademicID

NFDI
Community AAI &
IAM Solution

IAM4NFDI – Workshop Community AAls

Ralph Krimmel – ralph.krimmel@gwdg.de

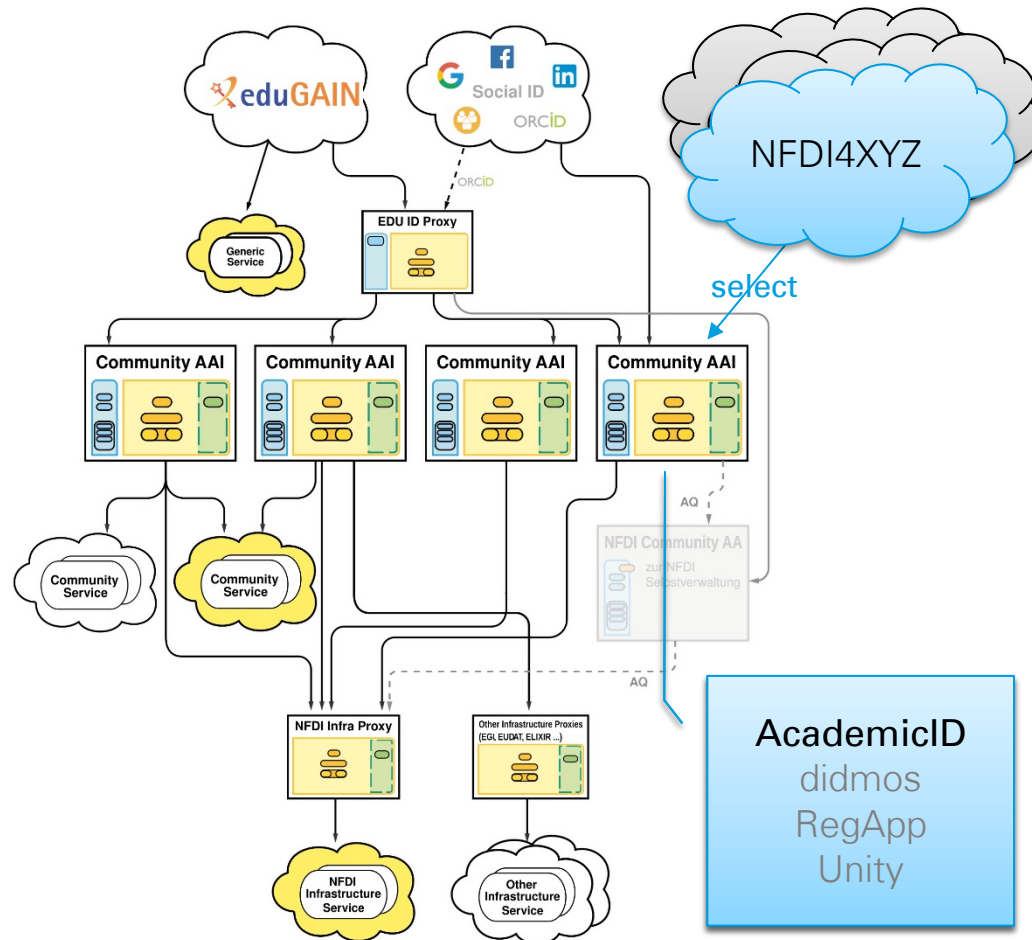
Sascha Krull – sascha.krull@gwdg.de

Christopher Menke – christopher.menke@gwdg.de

Christof Pohl – christof.pohl@gwdg.de

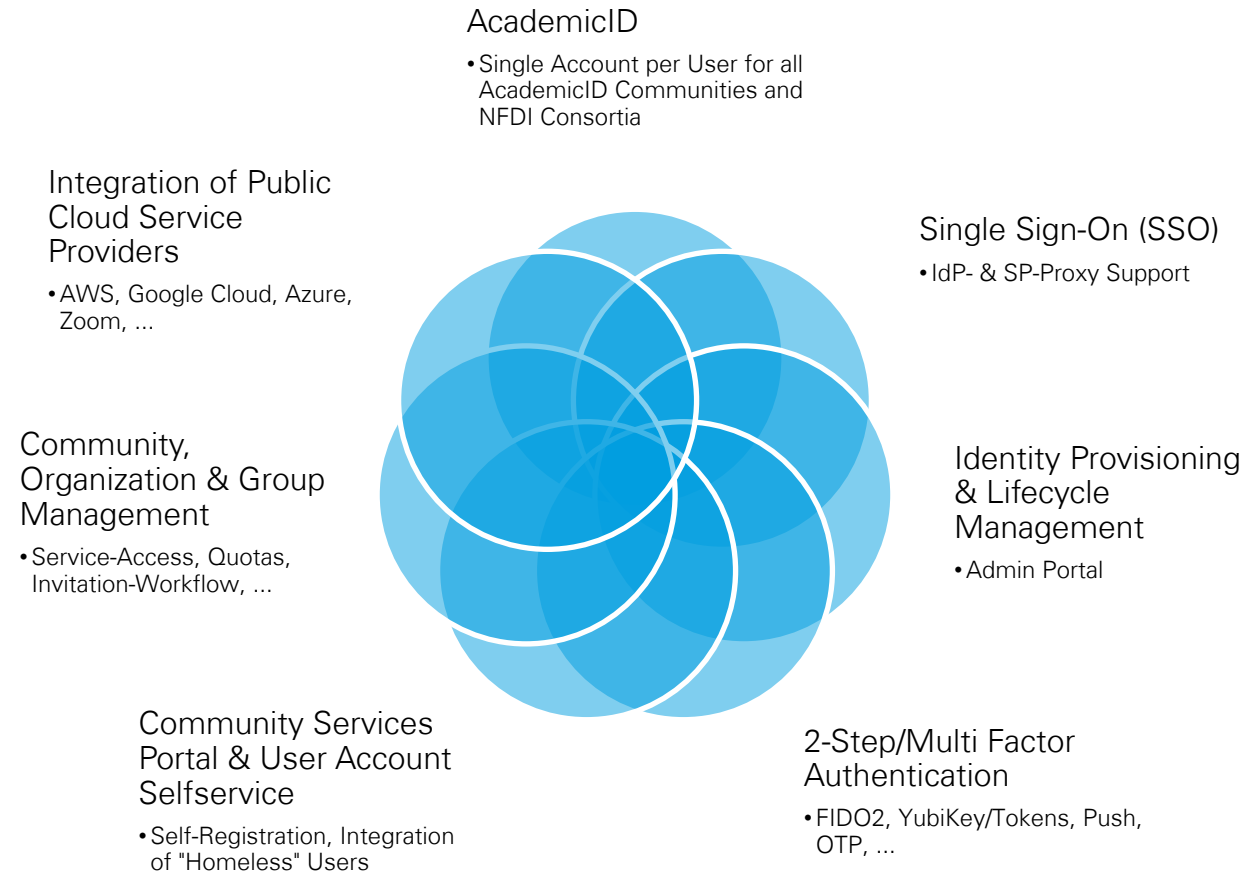


The Big Picture: NFDI-AAI Architecture



- Based on the AARC Blueprint Architecture and AARC-BPA-2019.
- Each NFDI consortium is expected to select one of the four NFDI CAAI solutions.
 - AcademicID, didmos, RegApp, Unity
- For the duration of the IAM4NFDI project, all partners will provide their CAAI solutions and additional AAI services to all NFDI consortia.

AcademicID CAAI Solution



Key Features

- Tenant-based operating model – NFDI consortia do not need to deploy and operate their own CAAI instance.
- New and improved features of AcademicID are immediately available to all communities using AcademicID.
- Open source products for most components – no vendor lock-in, lower total cost of ownership and high compatibility with common standards.
- Easy integration with external communities and AAls (e.g. DFN-AAI, eduGain).
- A single identity per user for all AcademicID communities.



Agenda



General Information



User-facing Features



Administrative Features



Further Information

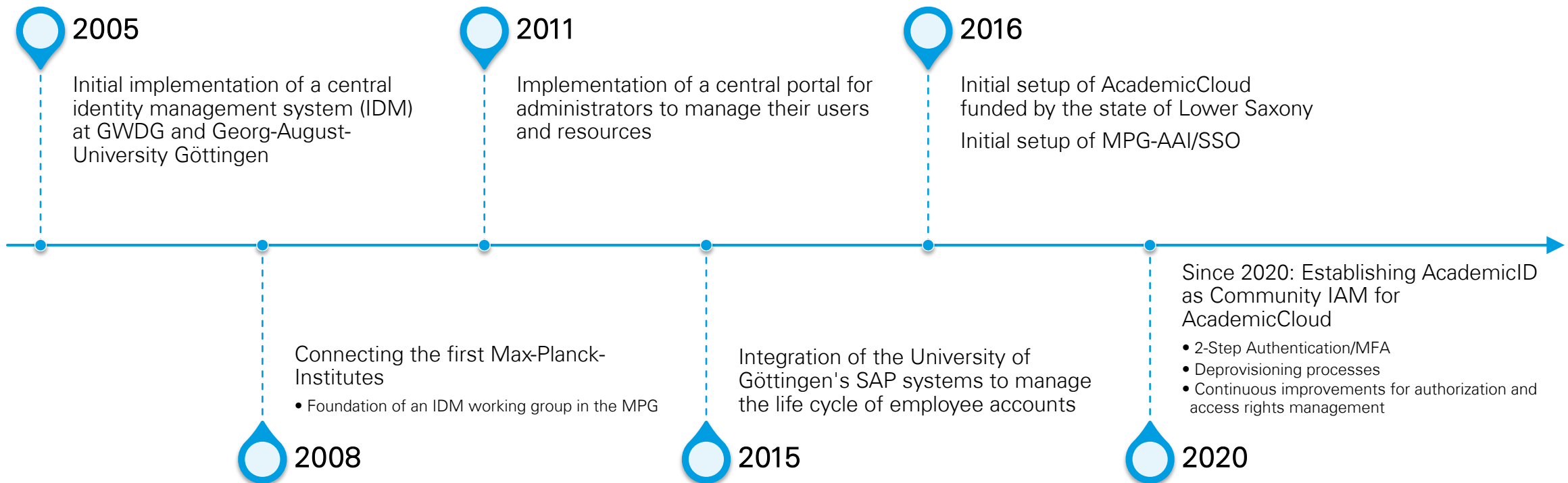


Your Questions, Comments and Suggestions

AcademicID NFDI Community AAI

General Information

History



~180.000 User
Accounts

~13.000 Groups

Over 160 connected
systems (LDAP, AD,
SQL, API,
LoopBack)

14 native SSO
Identity Providers
(IdP) for institutions
in AcademicID

Selected Services Connected to AcademicID

- Cloud Storage: OwnCloud, NextCloud,
- Collaboration: Sharepoint, Gitlab, Filesender, ShareLaTeX/Overleaf, HedgeDoc
- Mail Service: Exchange, Open-Xchange
- Cloud Server: VMware, OpenStack
- Research Data Management & Analysis: Jupyter, Data Repository & Archive
- Access to HPC resources operated by GWDG
- Videoconferencing: Big Blue Button, Zoom
- Chat: Rocket.Chat, Matrix
- Project Management: OpenProject

AcademicID User Testimonials

- Georg-August-University Göttingen, Universitätsmedizin Göttingen (UMG)
 - Lifecycle management via SAP/HIS
- Max Planck Society
 - Over 60 connected institutes
- LANIT: AcademicCloud
 - Universities in Lower Saxony
- Max Weber Stiftung
 - 11 connected institutes
- Forschungsverbund MWW
- Research Infrastructures: DARIAH, GFBio
- Plattform für internationale Studienmobilität (PIM)



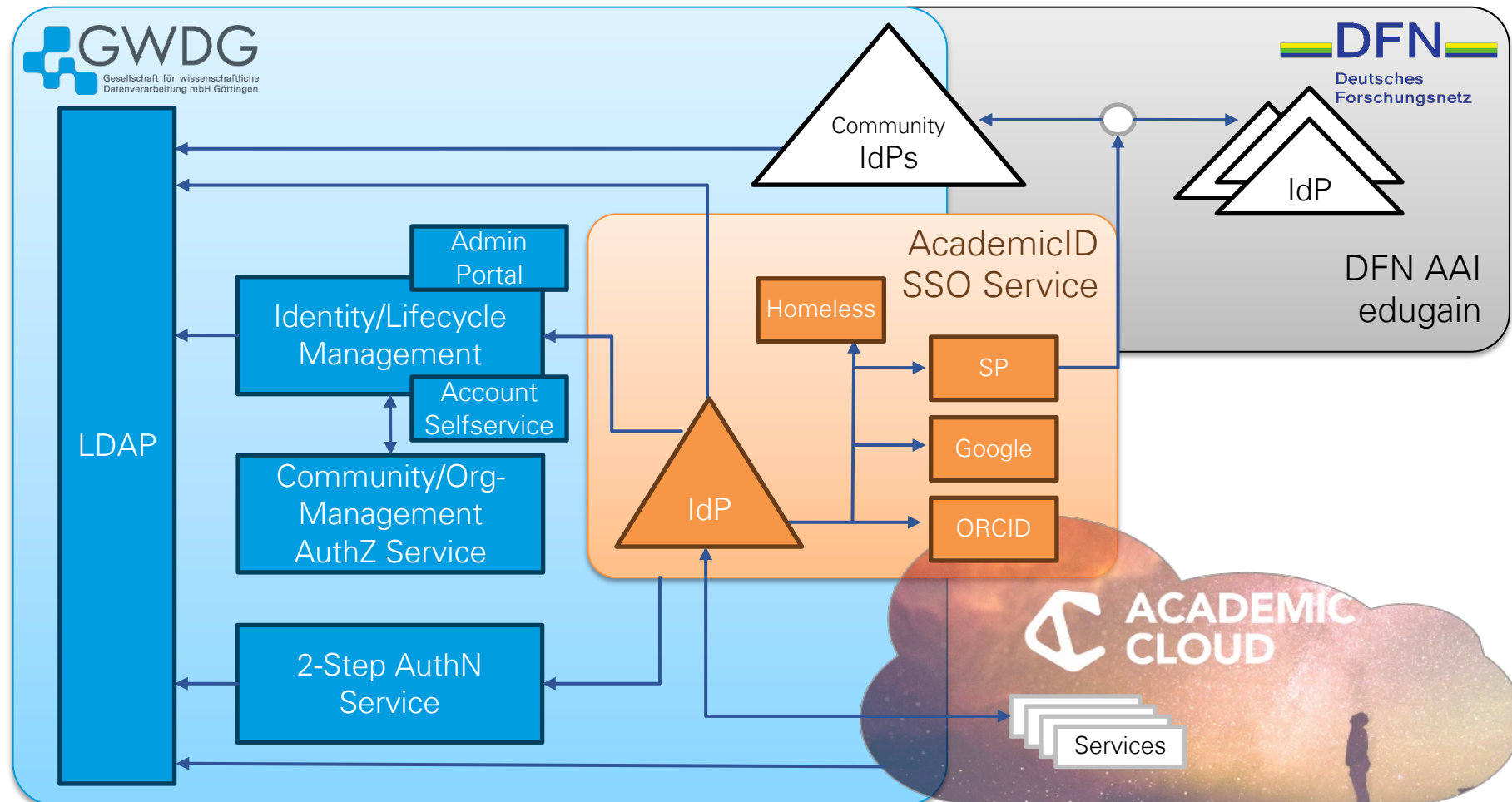
Deutsche
Geisteswissenschaftliche
Institute im Ausland



Identity & Access Management Staff

- Identity Management
 - 3 core IDM developers
 - 1 core AcademicID Admin Portal developer
- Access Management/AAI/SSO
 - 4 core SSO developers
- IAM 2nd level support
 - 1 dedicated IAM support specialist
- 12 general software development positions (including 5 trainees)
 - Support IAM development team with web technologies, web and UX design

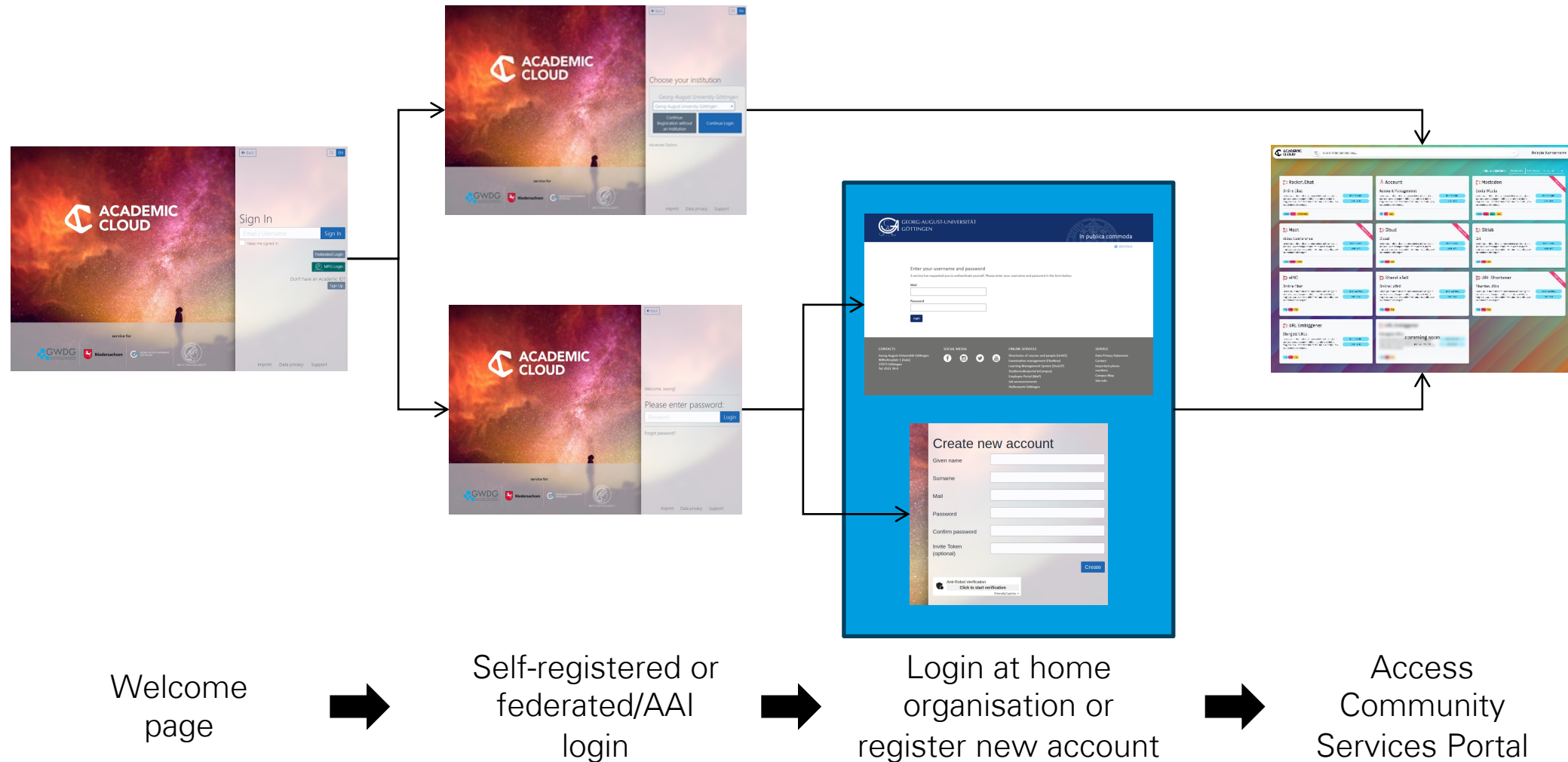
AcademicID Component Architecture



AcademicID NFDI Community AAI

User-facing Features

Login Flow

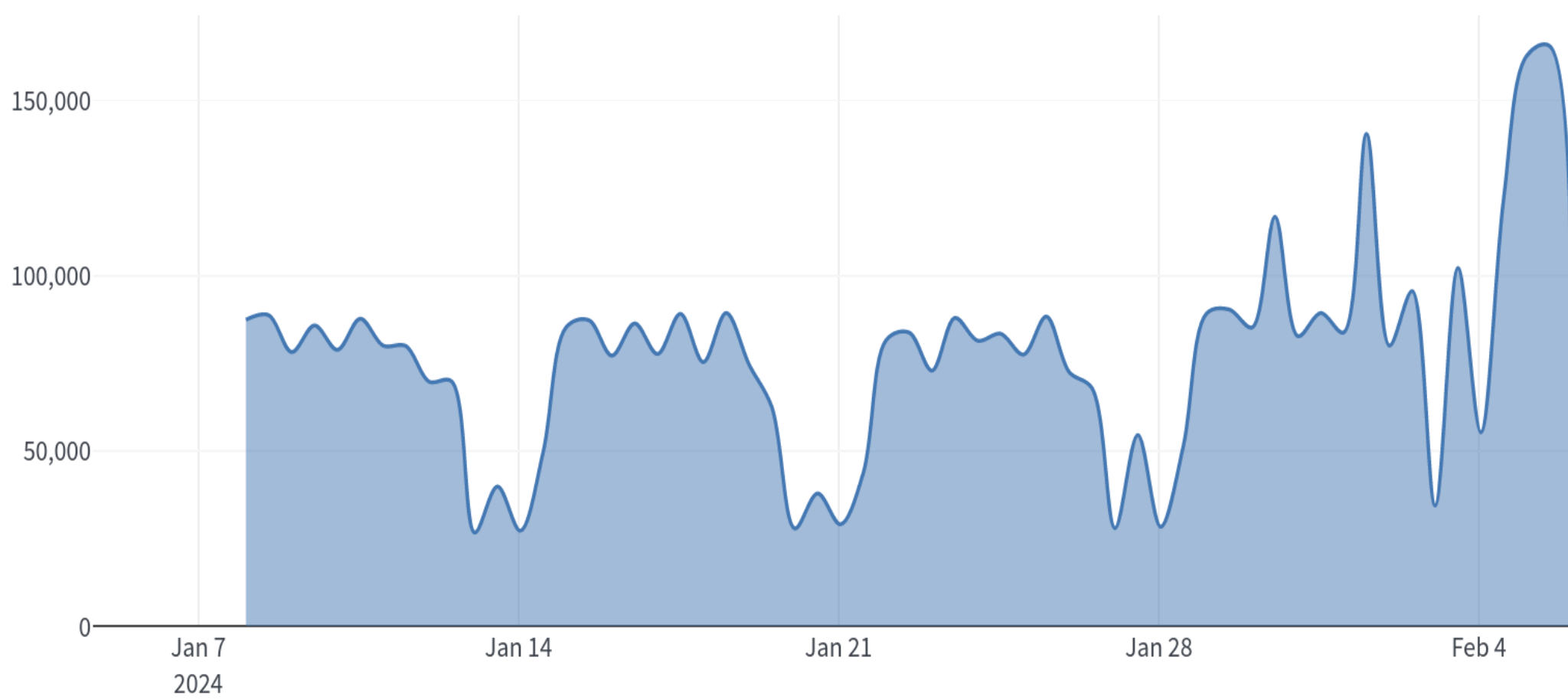


SSO Service Features

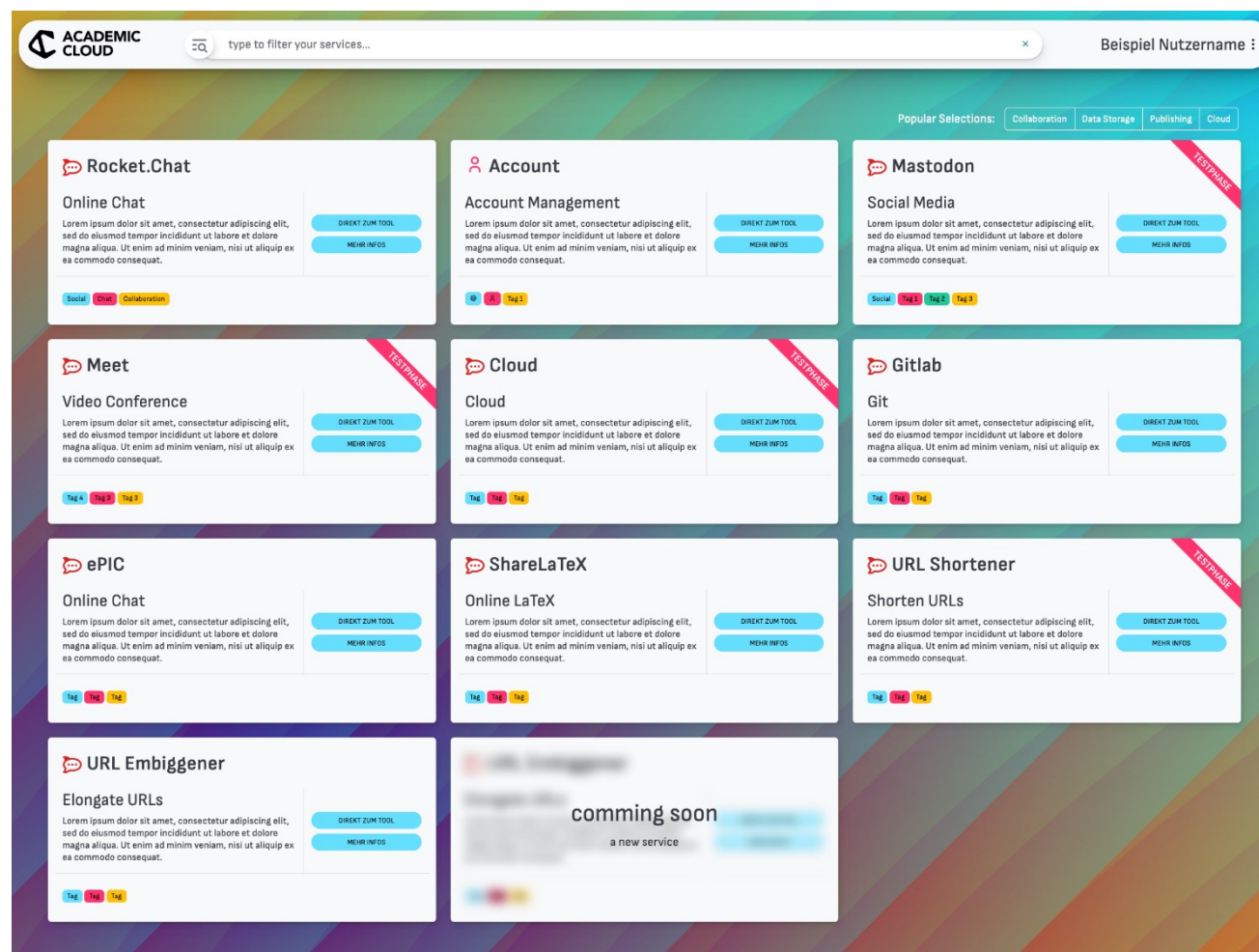
- Flexible authorization mechanism
 - Access to services can be granted depending on group/organization membership or individually
- Allows for individual terms of use/policy/privacy statements for each accessed service
- 2-Step/Multi-Factor Authentication
- Automatic update of attributes transmitted by external ID provider



Logins Counter (~ last 30 days)



Community Services Portal: Service Overview



The screenshot displays the Academic Cloud Community Services Portal. At the top, there is a search bar with the placeholder text "type to filter your services..." and a user profile section labeled "Beispiel Nutzername :". Below the search bar, a "Popular Selections:" section lists categories: Collaboration, Data Storage, Publishing, and Cloud. The main content area is a grid of service cards, each featuring a service icon, name, description, and buttons for "DIREKT ZUM TOOL" and "MEHR INFOS". The services shown are:

- Rocket.Chat**: Online Chat. Tags: Social, Chat, Collaboration.
- Account**: Account Management. Tag: Account.
- Mastodon**: Social Media. Tags: Social, Tag 1, Tag 2, Tag 3. A red "TESTPHASE" banner is visible.
- Meet**: Video Conference. Tag: Tag 4. A red "TESTPHASE" banner is visible.
- Cloud**: Cloud. Tag: Tag 1. A red "TESTPHASE" banner is visible.
- Gitlab**: Git. Tag: Tag 1.
- ePIC**: Online Chat. Tag: Tag 1.
- ShareLaTeX**: Online LaTeX. Tag: Tag 1.
- URL Shortener**: Shorten URLs. Tag: Tag 1. A red "TESTPHASE" banner is visible.
- URL Embiggener**: Elongate URLs. Tag: Tag 1.

A placeholder card at the bottom right indicates a service "coming soon".

Community Services Portal: Service Details


ACADEMIC CLOUD

SERVICES HELP

Beispiel Nutzername :

Online Chat

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Integer feugiat scelerisque varius morbi enim nunc faucibus a. Egestas pretium aenean pharetra magna. At in tellus integer feugiat scelerisque varius morbi. Suspendisse sed nisi lacus sed viverra tellus in hac. Nulla pellentesque dignissim enim sit amet venenatis urna cursus. Tristique et egestas quis ipsum suspendisse ultrices gravida.

Lorem Ipsum!

A lacus vestibulum sed arcu non odio euismod. Massa id neque aliquam vestibulum morbi blandit cursus. Senectus et netus et malesuada fames. Risus in hendrerit gravida rutrum. Tempus urna et pharetra pharetra massa massa. Amet est placerat in egestas erat imperdiet sed euismod. Dui id ornare arcu odio ut sem. Adipiscing elit pellentesque habitant morbi tristique senectus. Nibh tellus molestie nunc non blandit massa enim. Auctor augue mauris augue neque. Neque aliquam vestibulum morbi blandit cursus. Mauris pharetra et ultrices neque ornare aenean.

Ultrices dui sapien eget mi proin sed libero enim sed. Dui nunc mattis enim ut. Arcu risus quis varius quam quisque id. Eu consequat ac felis donec et. Sit amet commodo nulla facilisi nullam vehicula ipsum a. Enim sit amet venenatis urna cursus. Ornare arcu odio ut sem nulla pharetra. Elit pellentesque habitant morbi tristique senectus et netus et. A diam sollicitudin tempor id eu. Neque ornare aenean euismod elementum nisi. Ac tincidunt vitae semper quis lectus nulla at. Eget sit amet tellus cras adipiscing enim eu.

Lorem Ipsum?

Odio tempor orci dapibus ultrices in. Tempus iaculis urna id volutpat lacus laoreet. Venenatis cras sed felis eget velit.



Rocket.Chat

Materialien

Weiterführende Materialien
herunterladen:

FILE DOWNLOAD 

Social Chat Collaboration

Provider

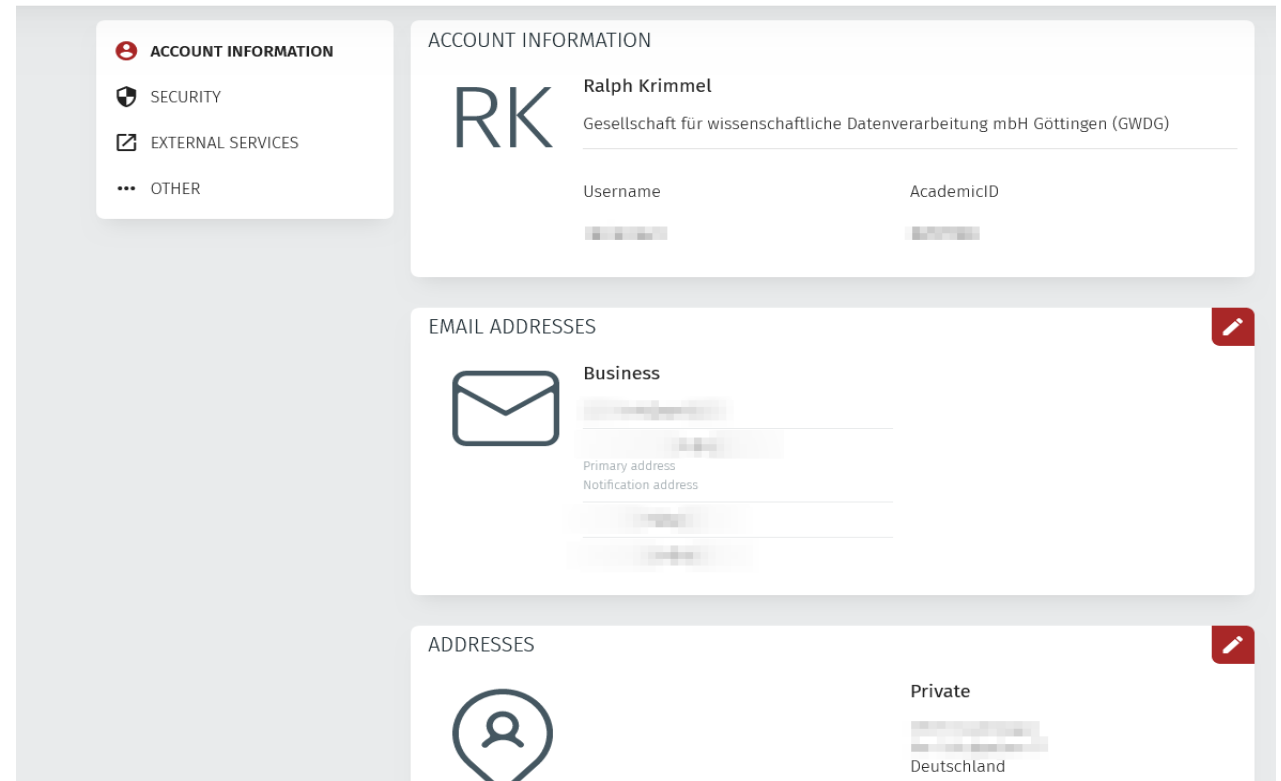


DIREKT ZUM TOOL

TESTPHASE

Account Portal: My AcademicID

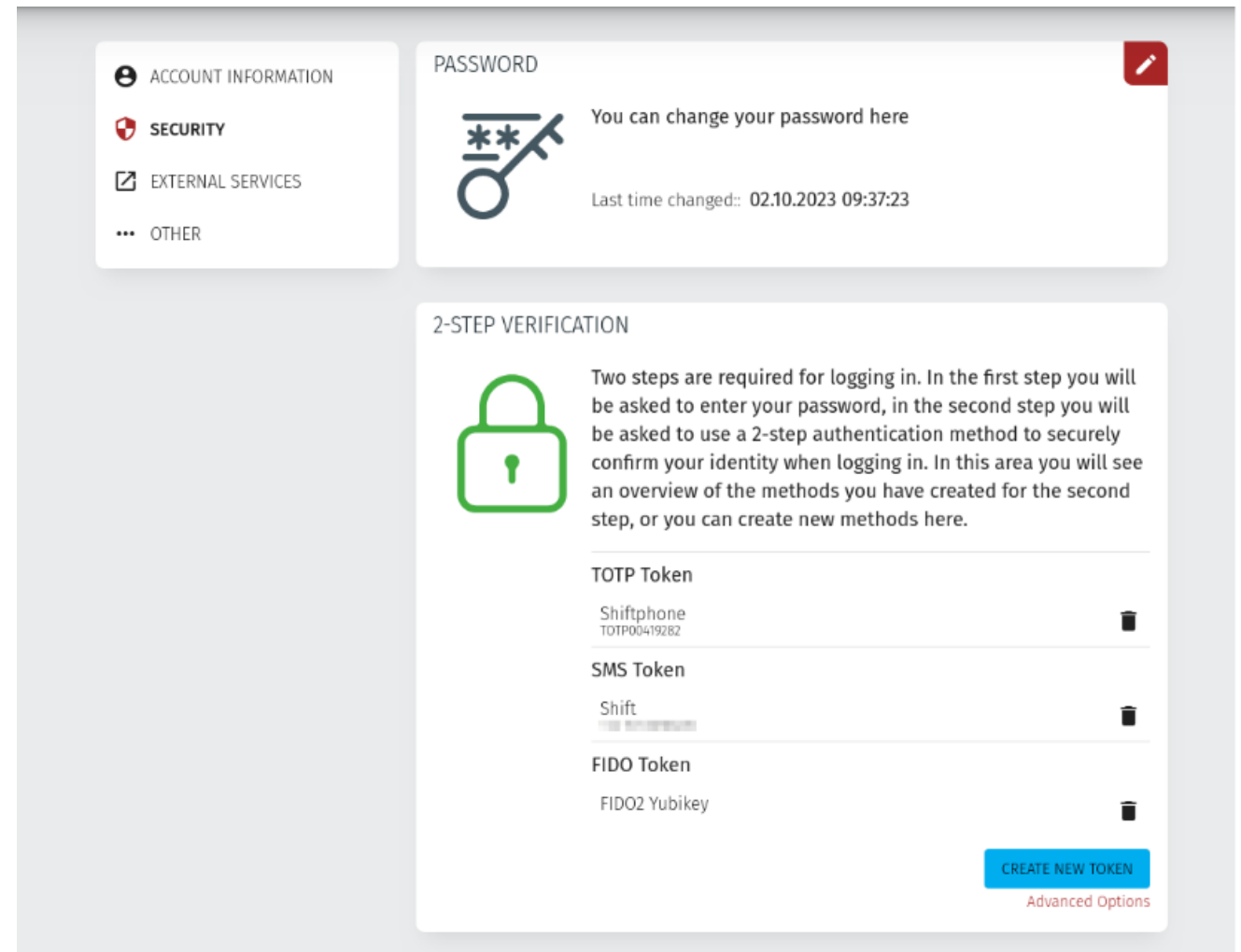
- User centric selfservice for basic account features
 - Email and contact information management
 - Registration and management of multiple factors for 2-step authentication



The screenshot displays the 'My AcademicID' account portal interface. On the left is a sidebar menu with four options: 'ACCOUNT INFORMATION' (selected), 'SECURITY', 'EXTERNAL SERVICES', and 'OTHER'. The main content area is divided into three sections: 1. 'ACCOUNT INFORMATION' showing the user's initials 'RK', name 'Ralph Krimmel', affiliation 'Gesellschaft für wissenschaftliche Datenverarbeitung mbH Göttingen (GWDG)', and fields for 'Username' and 'AcademicID'. 2. 'EMAIL ADDRESSES' with a 'Business' tab, an email icon, and fields for 'Primary address' and 'Notification address'. 3. 'ADDRESSES' with a 'Private' tab, a location pin icon, and a field for 'Deutschland'. Each of the three main sections has a red edit icon in its top right corner.

2-Step Authentication

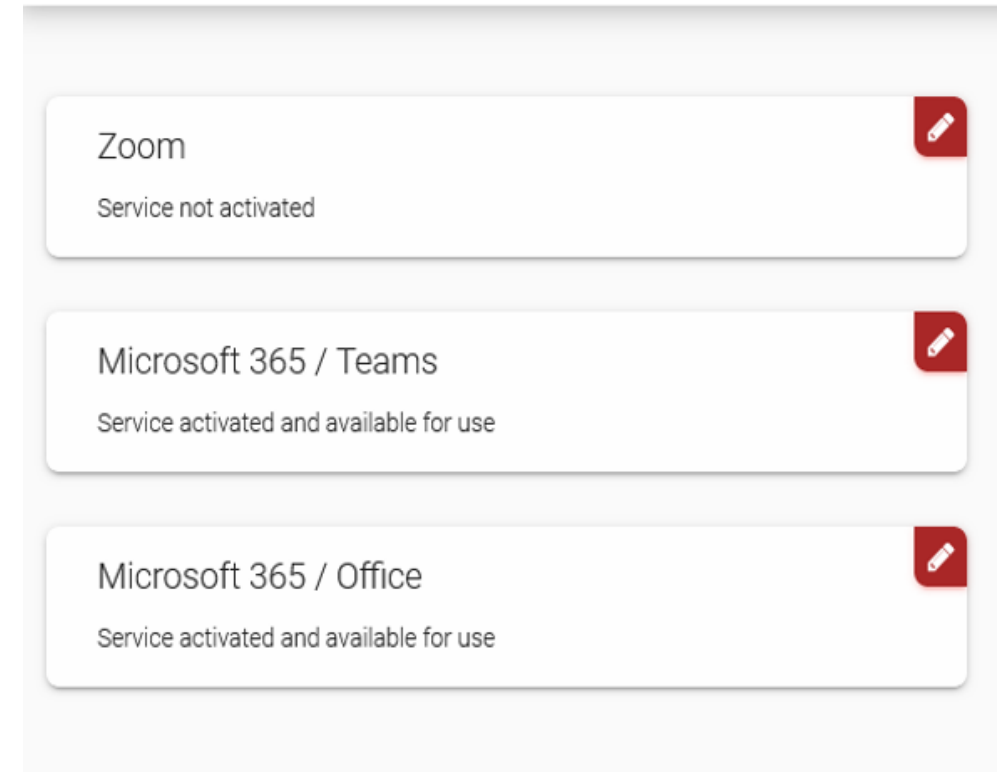
- Supported mechanisms for 2-Step authentication
 - FIDO2/Passkey
 - Hardware tokens (e.g. YubiKey)
 - Push (Android and iOS)
 - Time based tokens (TOTP)
 - SMS



Account Portal: Integration with Public Clouds

- Connect your AcademicID account to Public Cloud Services:
 - Amazon Web Services
 - Google Cloud
 - Microsoft Azure & Office 365
 - Zoom
 - ...

 My AcademicID



Service	Status
Zoom	Service not activated
Microsoft 365 / Teams	Service activated and available for use
Microsoft 365 / Office	Service activated and available for use

AcademicID NFDI Community AAI

Administrative Features

AcademicID Admin Portal (1/3)

- Administrative management of
 - Identities/Accounts
 - Edit user information (e.g. surname)
 - Password recovery
 - Change status of the account (e.g. disable, delete)
 - Groups
 - Assign email address – email distribution group
 - Delegation of group management
 - e.g. team leader could manage group for his/her team
 - Group members can also be generated dynamically
 - Based on a member filter
 - Invite to group (see next slides)



AcademicID Admin Portal (2/3)

PrivacyIDEA Token					
Serial number	Description	Tokentype	Active	Failcount	Action
██████████	Handy PUSH	push	True	0	<button>Delete</button>
██████████	SMS	sms	True	0	<button>Delete</button>
██████████	Yubikey Short Touch	yubikey	True	0	<button>Delete</button>

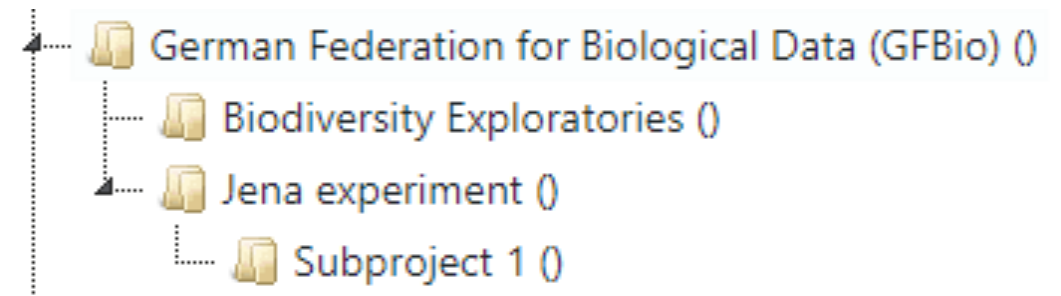
- Administrators can view and manage 2-Step authentication settings of community users
 - Overview per account
 - Delete tokens
 - e.g. Person loses device or key

AcademicID Admin Portal (3/3)

- Organisation management
 - Create and manage organisational units (OU)
 - Individual settings per OU and account:
 - Permissions and quotas of accounts
 - Roles (e.g. Community admin, invitation approver, member, ...)
- Other functions
 - Persistent audit log for all objects (accounts, groups, ...)
 - Individual password policy per community
 - Individual password recovery PDF document per community
 - Object creation templates (account, group, ...)
 - Application and approval processes
 - Apply for objects (account, group, ...)
 - Individual approver per org unit

Organizations, Projects & Groups (1/5)

- In AcademicID, organizations represent NFDI consortia (also known as “communities”, e.g. NFDI4XYZ).
 - How to assign members to a community?
 - Based on a membership token during login or account registration
 - Direct creation or application of account via IdM admin portal
 - Option: Connection to a directory service (e.g. LDAP) containing community members
 - Option: Identified by a community identity provider during login/registration
- Projects and subprojects of an NFDI consortium administrated via IdM Admin-Portal
- Nested projects possible



Organizations, Projects & Groups (2/5)

- How to invite new members to groups/projects?
 - Group/project administrator can create invitation token
 - Invitation link could be sent by email or could be distributed manually (e.g. via chat)
 - Invitee becomes a member of the group (after registration)

Overview							
Show 10 entries		Search:					
Token ▲	Description ▴	Maximum number of usages ▴	Already redeemed ▴	Expiration date ▴	Inviting person ▴	Status ▴	Action ▴
	NFDI Meeting 08.02.2024	5	0	2024-02-28		Open	Copy  Withdraw
Showing 1 to 1 of 1 entries						Previous	1 Next

Organizations, Projects & Groups (3/5)

- How to use groups/projects?
 - Grant access to services (e.g. Confluence)
 - Membership will be passed to SAML Assertion (SSO)
 - Query AcademicID API
 - Query AcademicID LDAP directory
 - Grant quota for services (e.g. storage in OwnCloud or computation time on HPC cluster)



Organizations, Projects & Groups (4/5)

- Membership management for groups/projects
 - Example 1:
 - Conference organizer creates a group via IdM Admin Portal
 - Approver of community NFDI4XYZ approves group
 - Conference organizer creates a voucher for the group and distributes it e.g. in relevant research communities
 - Event participants can join group
 - Group can then be used e.g. in OwnCloud to share documents
 - Conference organizer may assign an email address to group
 - Emails to this email address will be forwarded to all conference participants



Organizations, Projects & Groups (5/5)

- Membership management for groups/projects
 - Example 2:
 - IdM administrator of NFDI4XYZ community creates group for “Göttingen” team and delegate the administration to them
 - “Göttingen” team defines member filter on group so that all accounts of the NFDI4XYZ community will be added dynamically
 - Collaboration software (e.g. Confluence) reads all groups and memberships from LDAP so that access to “Göttingen” area can be assigned to this group



AcademicID NFDI Community AAI

Further Information

AcademicID Admin FAQ

- “Does each NFDI consortium need to appoint a CAAI admin or will the IAM4NFDI project (or GWDDG) take care of this?”
 - Each NFDI Consortium should appoint one or more CAAI admins to handle simple 1st level user requests. The 1st level support is not covered by IAM4NFDI or the GWDDG.
- “What happens if a request overwhelms me or a technical problem arises?”
 - IAM4NFDI partners (GWDDG in the case of AcademicID) provide fast and competent 2nd level support for their CAAI solutions.
- “Is it a difficult task to be the AcademicID admin for my NFDI consortium?”
 - The AcademicID Admin Portal is an easy-to-use web application that allows you to perform all common IAM tasks with just a few mouse clicks.
- “Will this cost me a lot of time (in the long run)?”
 - Usually not. Most processes are automated as self-service and designed to require minimal administrative interaction.

High Quality & Secure Operations (1/2)

- GWDG holds ISO 27001 and ISO 9001 certifications:
 - ISO 27001: Information Security: focuses on confidentiality, integrity, and availability of services and data.
 - ISO 9001: Quality Management: focuses on meeting customer expectations and continual improvement of services.
- AcademicID Community IAM is in the scope of both certificates.
- AcademicID Community IAM is also covered by regular KRITIS audits of University Medical Center Göttingen (UMG)
 - KRITIS: focuses on security and availability aspects in the area of critical medical infrastructures.



High Quality & Secure Operations (2/2)

- GWDG employees are regularly sensitized to important information security and quality management issues.
- Up-to-date and standard-compliant documentation
- Ongoing efforts to improve the quality and security of AcademicID software components and administrative activities, as well as operation of systems and infrastructure.
- Frequent quality checks & yearly re-certifications



Roadmap (Selection)

- Support for account linking
- AI supported detection of account doublets
- Extended invite and voucher features for community memberships and service access
- Establishment of a Security Operations Center (SOC) for the MPG, the University of Göttingen and the GWDDG



How to get AcademicID?

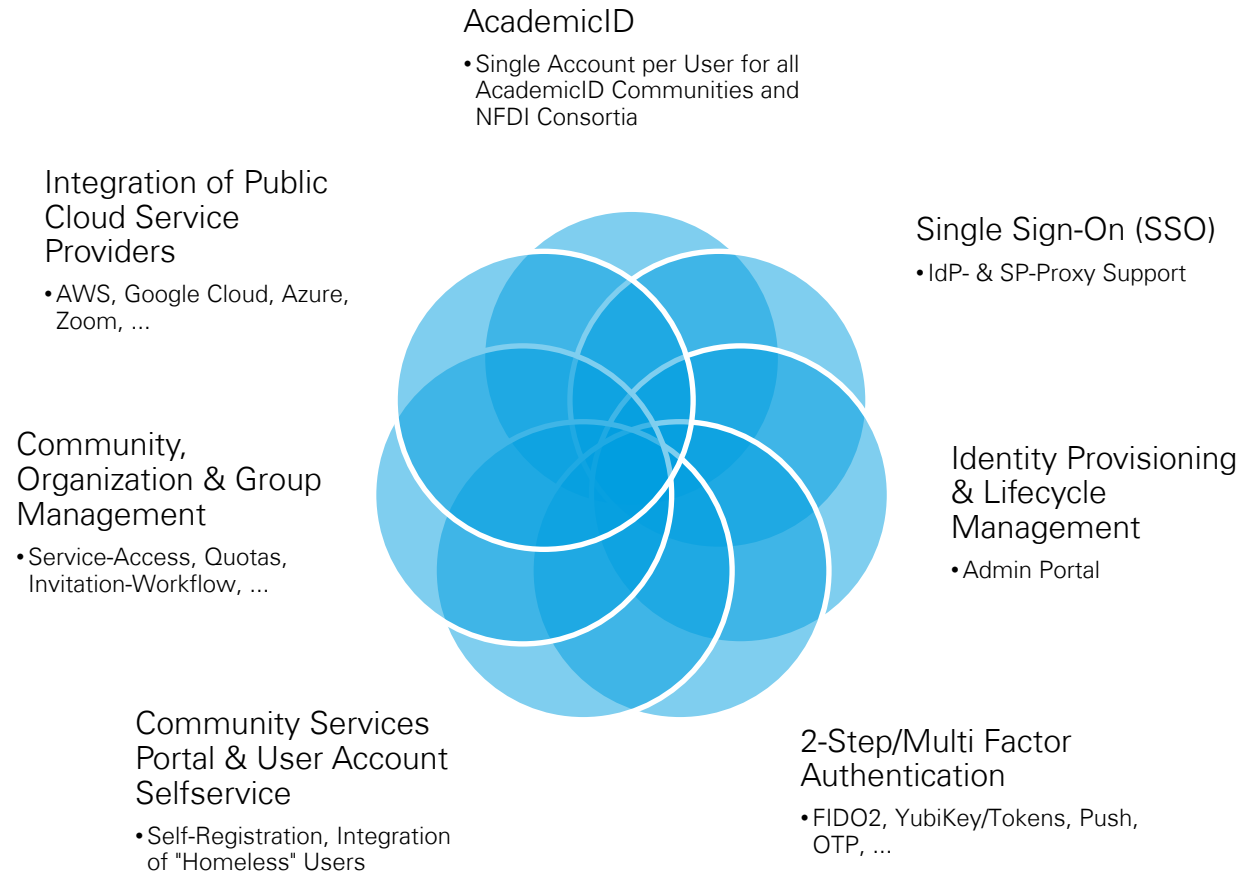
- Contact us
 - support@gwdg.de
- “Get in Touch” appointment
 - We answer your questions, offer consulting and requirements analysis.
 - If AcademicID is on the short list for your NFDI, we will work together with you to develop an onboarding roadmap.
- Your NFDI: “We want you, AcademicID!”
 - We will closely coordinate all steps for onboarding your NFDI consortium with you.
 - You can follow up progress via a project management system and are always up-to-date.
- Best of all: it’s free for you (funded by Base4NFDI via the IAM4NFDI project)!

And Then?

- We continue to take care of you, even when onboarding has finished.
 - We provide 2nd level support, secure operations and are always ready to listen to your questions, ideas or problems.
 - And yes, that's also free for you (funded by Base4NFDI).

- Optional: Fly to the moon (solutions for your very special NFDI consortium's requirements)
 - IAM4NFDI Incubators (funded by Base4NFDI)
 - We (GWDDG) offer paid IAM expert consulting and development services for AcademicID.
 - New features in AcademicID, whether developed on behalf of NFDI, University of Göttingen, MPG, GWDDG or others, will always be available to all our clients and NFDI consortia for free!

Your Questions, Comments and Suggestions



Contact:
support@gwdg.de

Powered by

 **GWDG**
Gesellschaft für wissenschaftliche
Datenverarbeitung mbH Göttingen