

# AcademicID

NFDI  
Community AAI &  
IAM Solution

**IAM4NFDI – Workshop Community AAls**

Ralph Krimmel – [ralph.krimmel@gwdg.de](mailto:ralph.krimmel@gwdg.de)

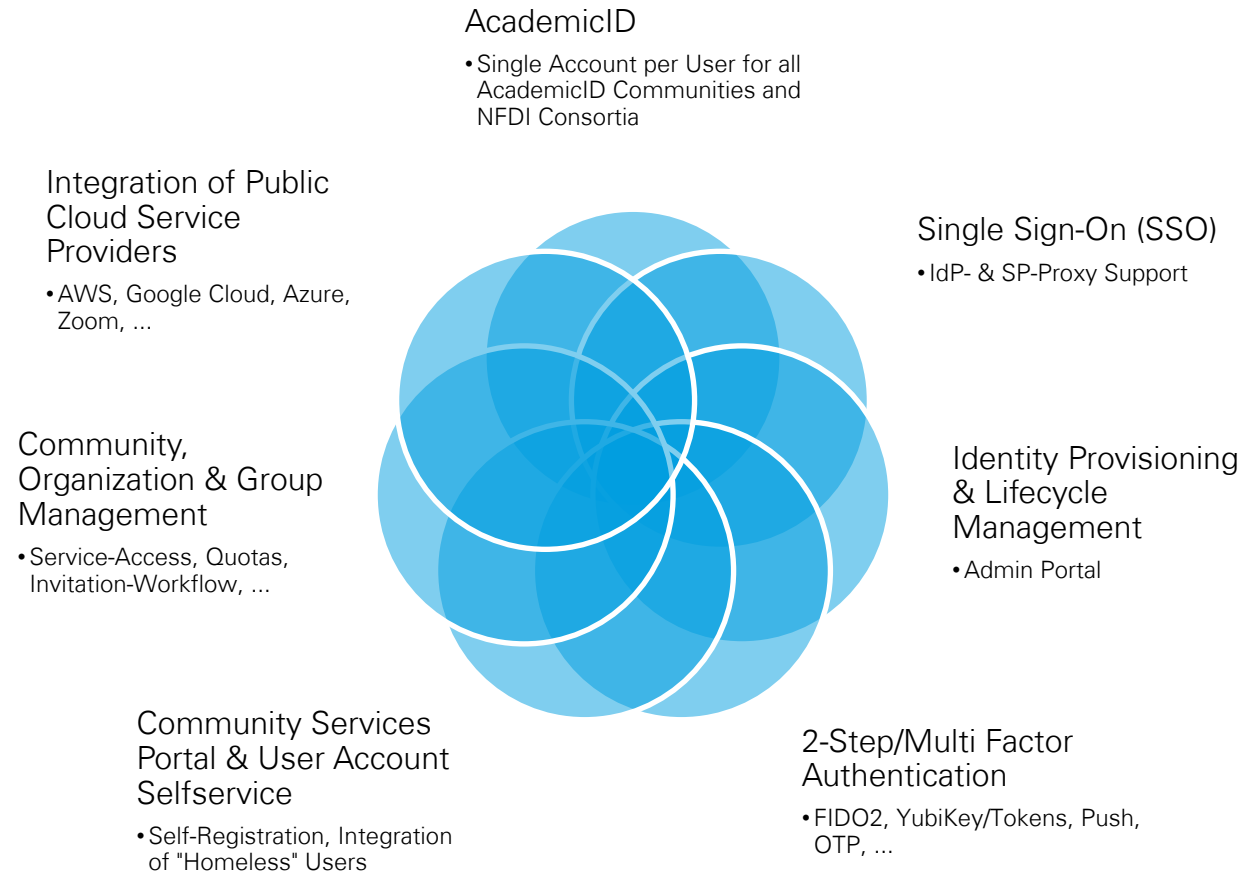
Sascha Krull – [sascha.krull@gwdg.de](mailto:sascha.krull@gwdg.de)

Christopher Menke – [christopher.menke@gwdg.de](mailto:christopher.menke@gwdg.de)

Christof Pohl – [christof.pohl@gwdg.de](mailto:christof.pohl@gwdg.de)



# AcademicID CAAI Solution

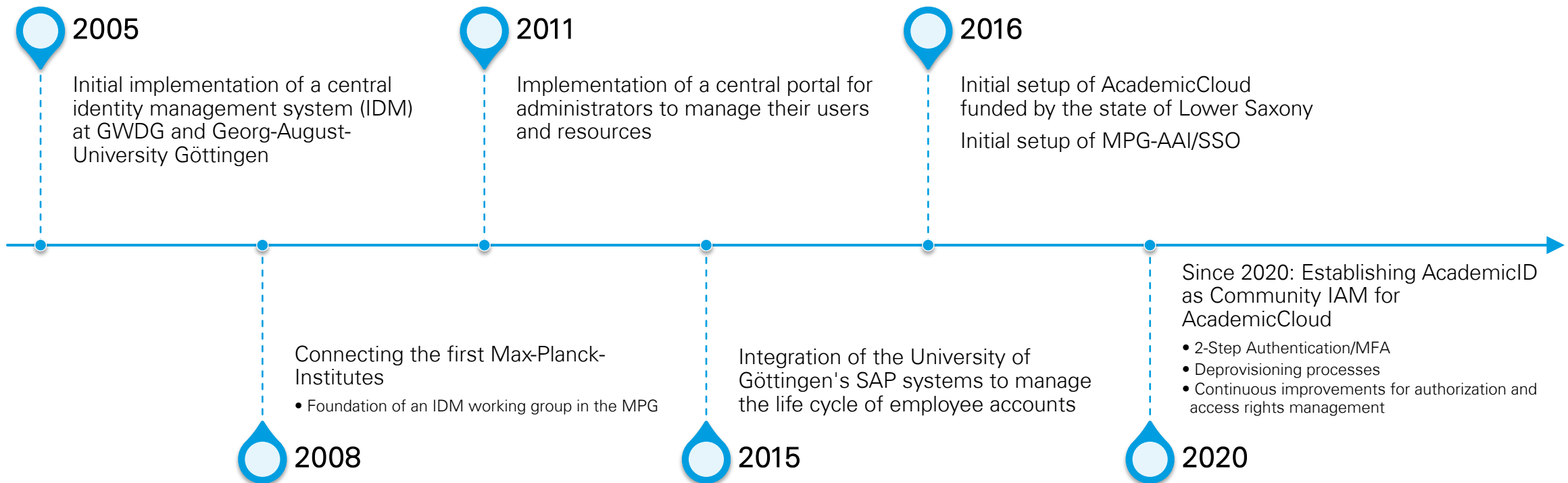


# Key Features

- 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).



# History



# 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)



**Max Weber  
Stiftung**

Deutsche  
Geisteswissenschaftliche  
Institute im Ausland



~180.000 User  
Accounts

~13.000 Groups

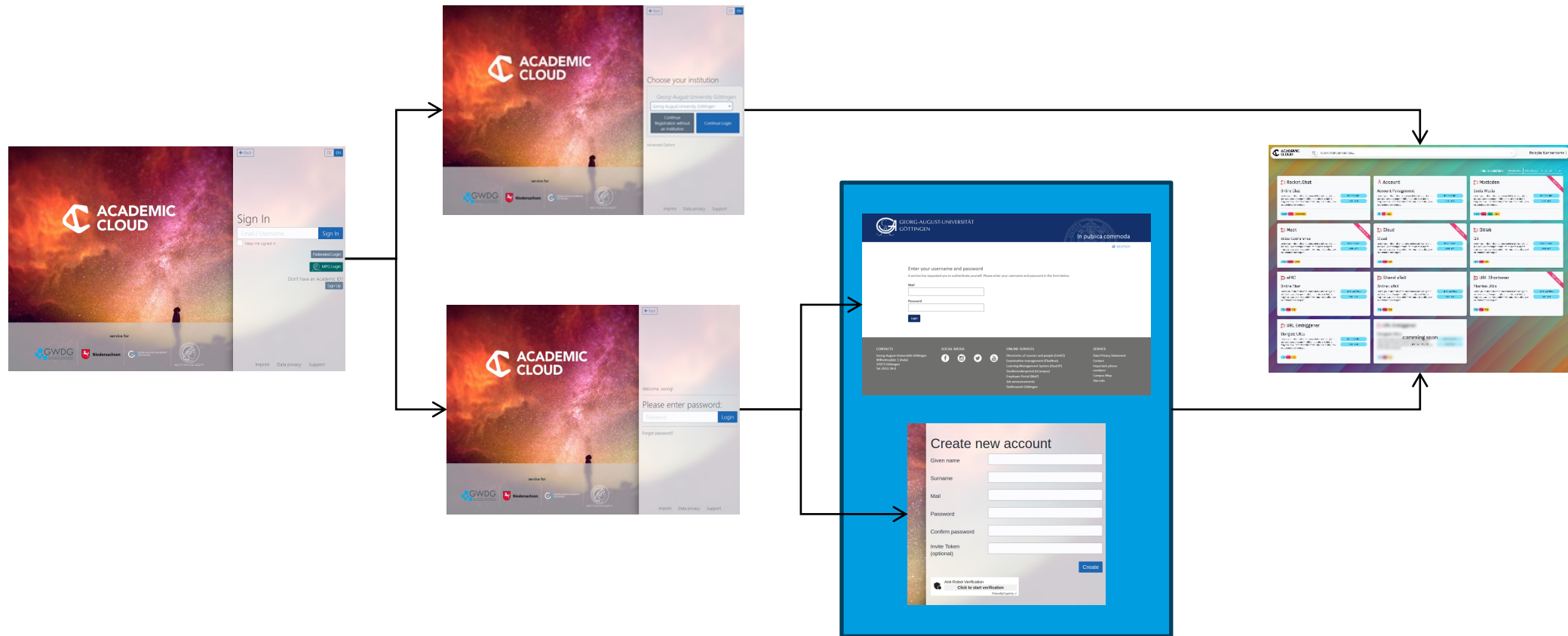
Over 160 connected  
systems (LDAP, AD,  
SQL, API,  
LoopBack)

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

# Login Flow



Welcome page



Self-registered or federated/AAI login



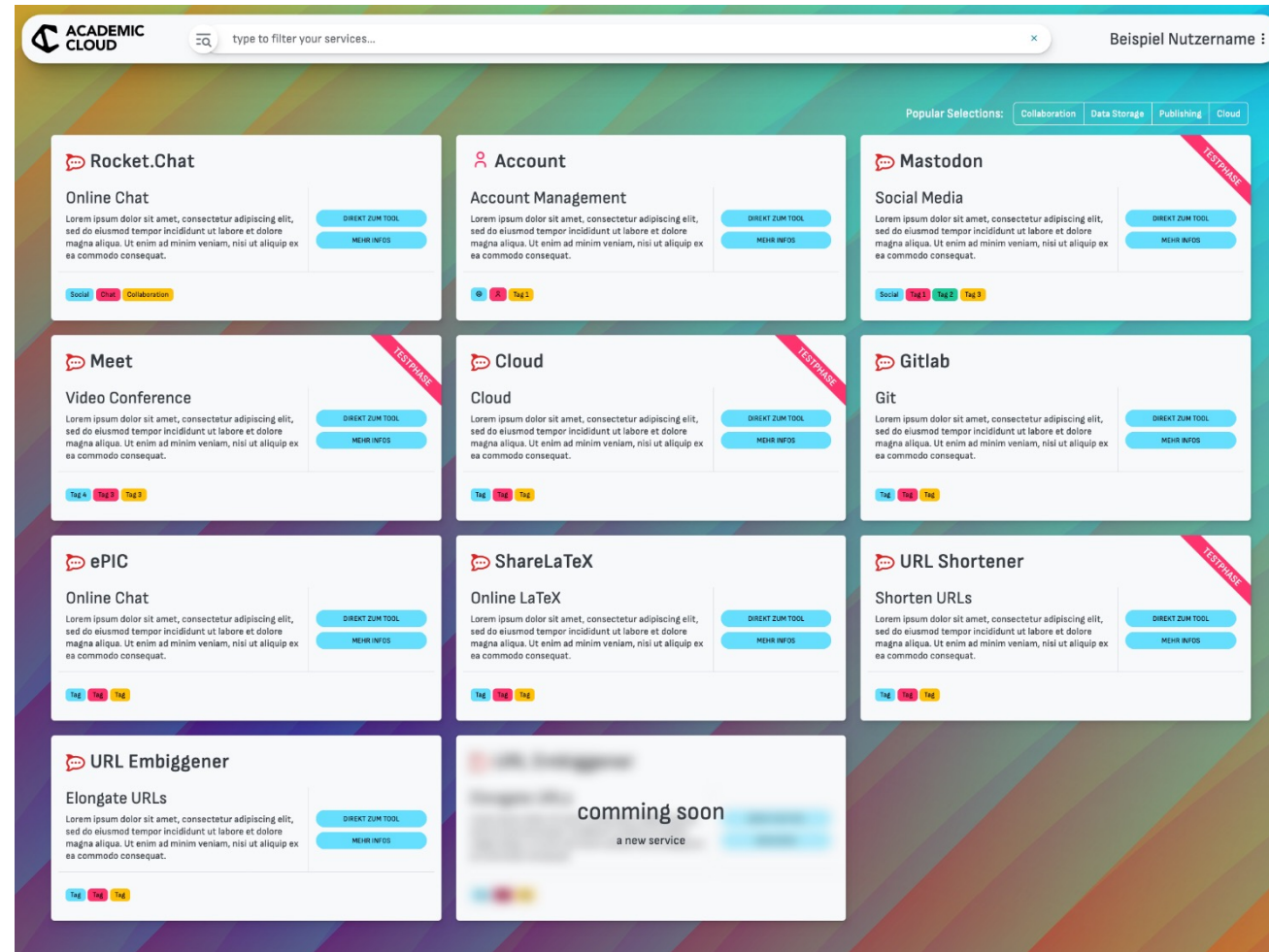
Login at home organisation or register new account



Access Community Services Portal



# Community Services Portal: Service Overview



The screenshot displays the Academic Cloud Community Services Portal. At the top left is the 'ACADEMIC CLOUD' logo. A search bar contains the text 'type to filter your services...'. On the top right, there is a user profile indicator 'Beispiel Nutzername :'. Below the header, a 'Popular Selections' bar includes categories: 'Collaboration', 'Data Storage', 'Publishing', and 'Cloud'. The main content area features a grid of service cards:

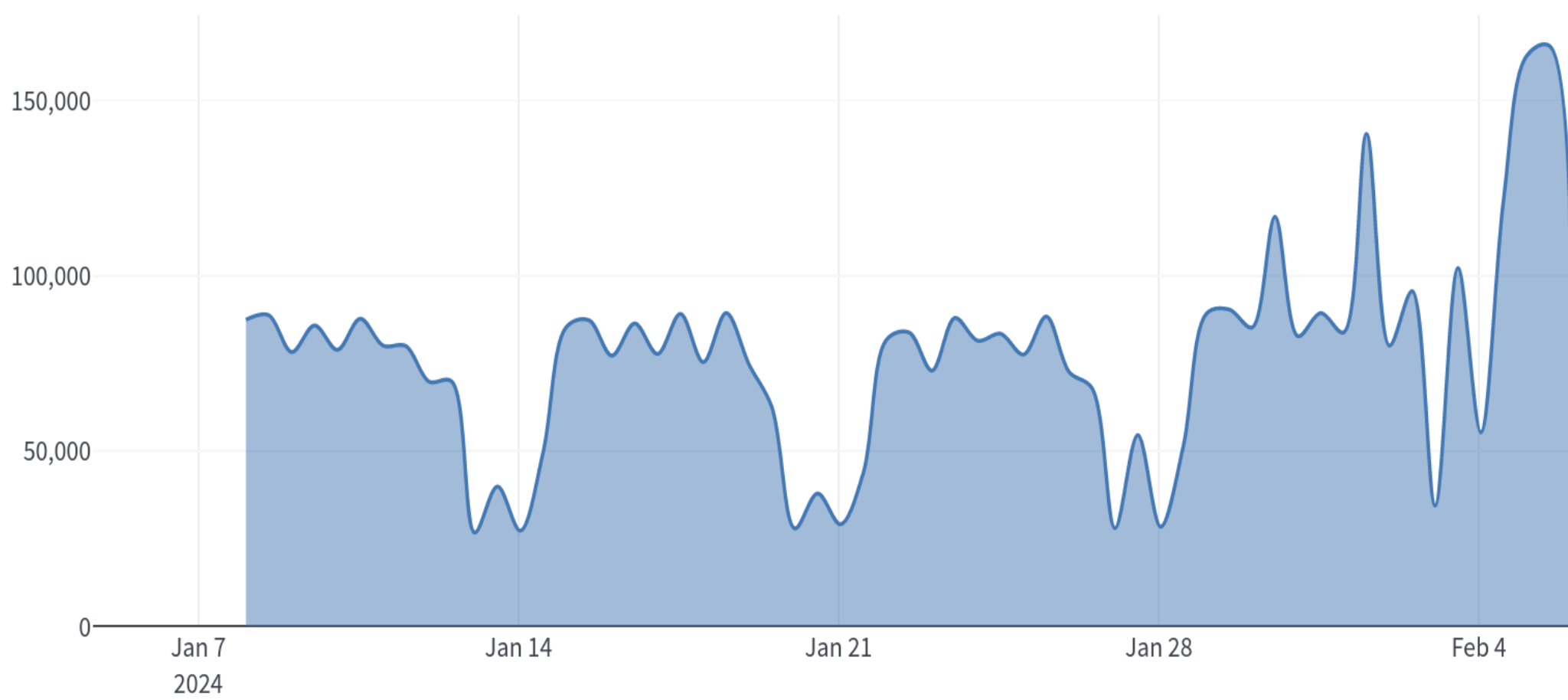
- Rocket.Chat**: Online Chat. Includes buttons for 'DIREKT ZUM TOOL' and 'MEHR INFOS'. Tags: Social, Chat, Collaboration.
- Account**: Account Management. Includes buttons for 'DIREKT ZUM TOOL' and 'MEHR INFOS'. Tag: Account.
- Mastodon**: Social Media. Includes buttons for 'DIREKT ZUM TOOL' and 'MEHR INFOS'. A red 'TESTPHASE' banner is present. Tag: Social.
- Meet**: Video Conference. Includes buttons for 'DIREKT ZUM TOOL' and 'MEHR INFOS'. A red 'TESTPHASE' banner is present. Tags: Tag 4, Tag 3, Tag 2.
- Cloud**: Cloud. Includes buttons for 'DIREKT ZUM TOOL' and 'MEHR INFOS'. A red 'TESTPHASE' banner is present. Tags: Tag 4, Tag 3, Tag 2.
- Gitlab**: Git. Includes buttons for 'DIREKT ZUM TOOL' and 'MEHR INFOS'. Tags: Tag 4, Tag 3, Tag 2.
- ePIC**: Online Chat. Includes buttons for 'DIREKT ZUM TOOL' and 'MEHR INFOS'. Tags: Tag 4, Tag 3, Tag 2.
- ShareLaTeX**: Online LaTeX. Includes buttons for 'DIREKT ZUM TOOL' and 'MEHR INFOS'. Tags: Tag 4, Tag 3, Tag 2.
- URL Shortener**: Shorten URLs. Includes buttons for 'DIREKT ZUM TOOL' and 'MEHR INFOS'. A red 'TESTPHASE' banner is present. Tags: Tag 4, Tag 3, Tag 2.
- URL Embiggener**: Elongate URLs. Includes buttons for 'DIREKT ZUM TOOL' and 'MEHR INFOS'. Tags: Tag 4, Tag 3, Tag 2.
- coming soon**: a new service. Placeholder card.

# 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

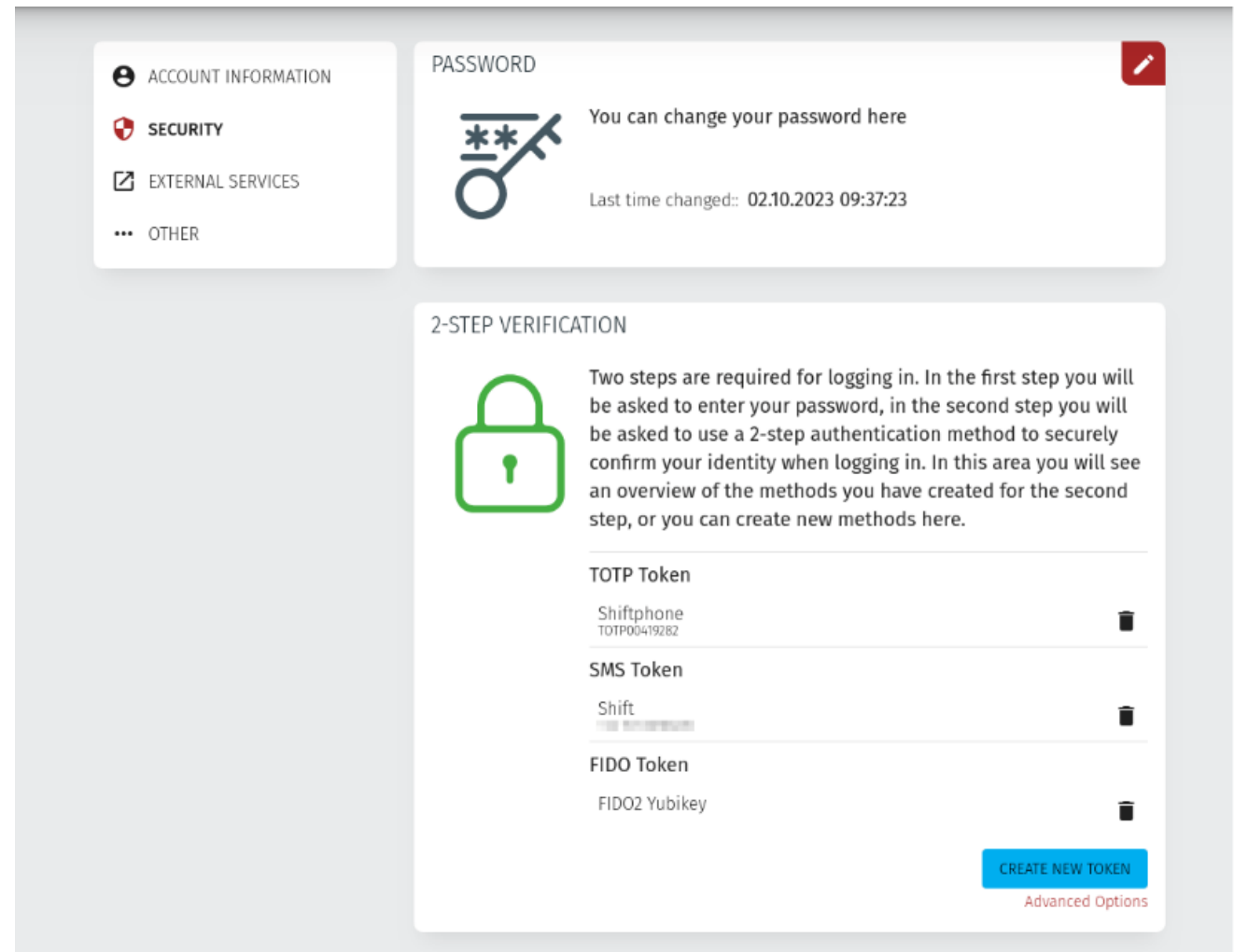


# Logins Counter (January 2024)



# Account Portal: My AcademicID & 2-Step Authentication

- User centric selfservice for basic account features
  - Email and contact information management
- Supported mechanisms for 2-Step authentication
  - FIDO2/Passkey
  - Hardware tokens (e.g. YubiKey)
  - Push (Android and iOS)
  - Time based tokens (TOTP)
  - SMS



The screenshot displays the 'My AcademicID & 2-Step Authentication' interface. On the left, a navigation menu includes 'ACCOUNT INFORMATION', 'SECURITY', 'EXTERNAL SERVICES', and 'OTHER'. The main content area is divided into three sections:

- PASSWORD:** A card with a key icon and the text 'You can change your password here'. It shows the last change date as '02.10.2023 09:37:23'.
- 2-STEP VERIFICATION:** A card with a lock icon and explanatory text: 'Two steps are required for logging in. In the first step you will be asked to enter your password, in the second step you will be asked to use a 2-step authentication method to securely confirm your identity when logging in. In this area you will see an overview of the methods you have created for the second step, or you can create new methods here.'
- Token List:** A table of existing authentication methods:

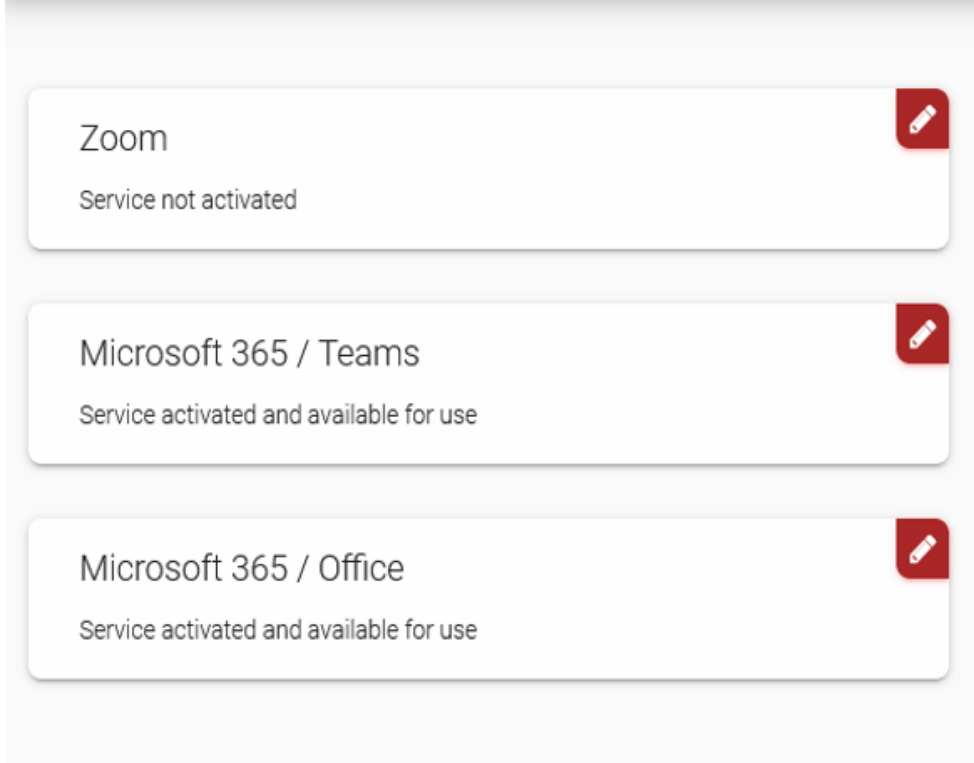
Method	Details	Action
TOTP Token	Shiftphone TOTP00419282	🗑️
SMS Token	Shift [REDACTED]	🗑️
FIDO Token	FIDO2 Yubikey	🗑️

At the bottom right, there is a blue button labeled 'CREATE NEW TOKEN' and a link for 'Advanced Options'.

# 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 Admin Portal (1/2)

- 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 feature



# AcademicID Admin Portal (2/2)

- 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

# High Quality & Secure Operations

- 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.

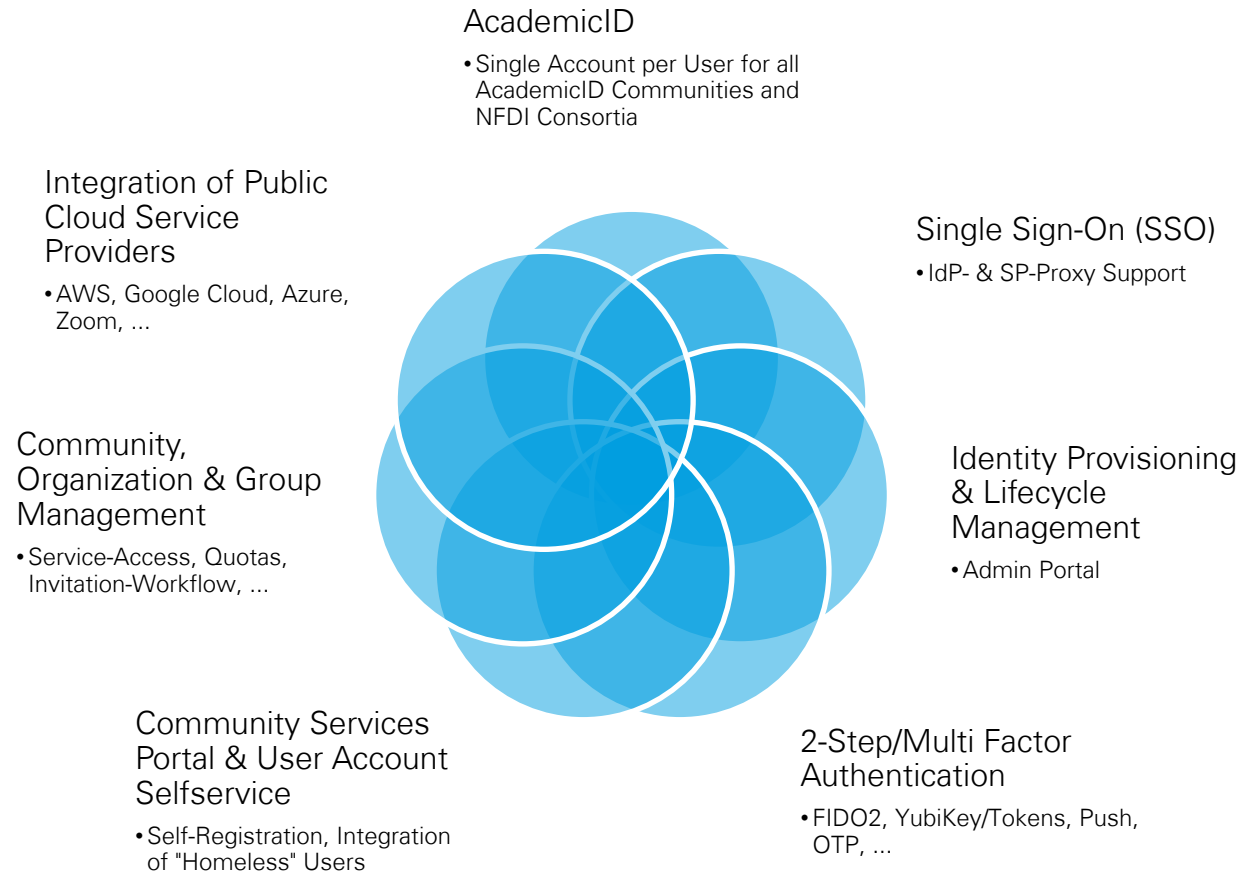




# How to get AcademicID?

- Contact us
  - [support@gwdg.de](mailto: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)!

# Your Questions, Comments and Suggestions



Contact:  
[support@gwdg.de](mailto:support@gwdg.de)

Powered by



GWDG  
Gesellschaft für wissenschaftliche  
Datenverarbeitung mbH Göttingen