Federated Identity- and Access Management for the Max-Planck Society

Organisational Aspects & Funding

Prof. Dr. Ramin Yahyapour
Christof Pohl, Andreas Ißleiber

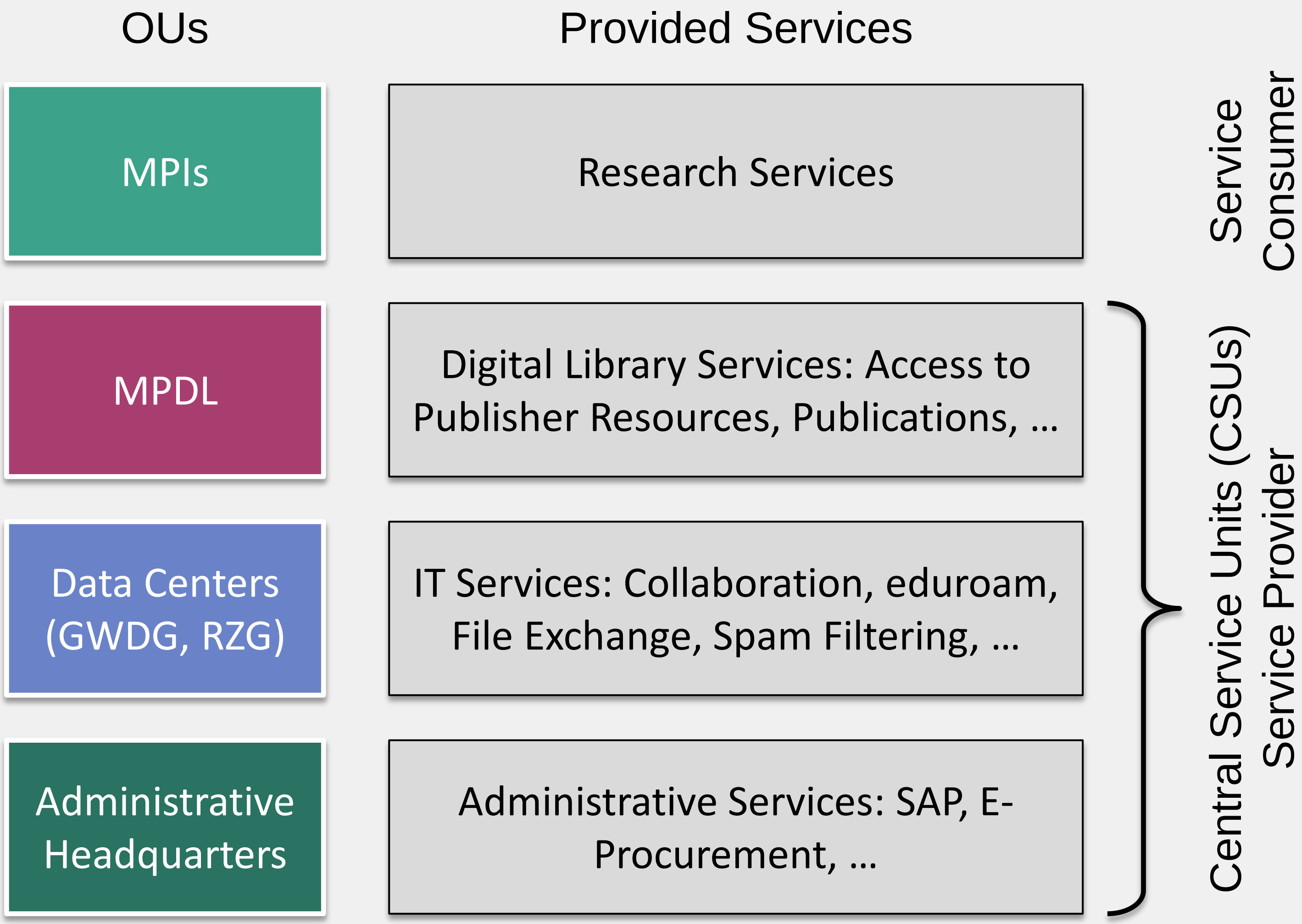
GWDG
Gesellschaft für wissenschaftliche Datenverarbeitung mbH Göttingen

Why FIM for the MPS?

- Growing importance of trans-institutional and external IT services and resources
- Examples:
  - Collaboration: Conferencing, File Exchange, Wiki, SharePoint, …
  - SAP & E-Procurement
  - Asset & License Management
  - MPDL Services & Publications
  - GWDG Customer Portal
  - WLAN, DFNRoaming/eduroam
  - Spam Filtering
- Paradigm:

  Support such applications without limiting the flexibility of local administration by centralization

Status Quo: MPS Organization and Service Roles



OUs

Provided Services

MPIs

Research Services

Service Consumer

MPDL

Digital Library Services: Access to Publisher Resources, Publications, …

Data Centers (GWDG, RZG)

IT Services: Collaboration, eduroam, File Exchange, Spam Filtering, …

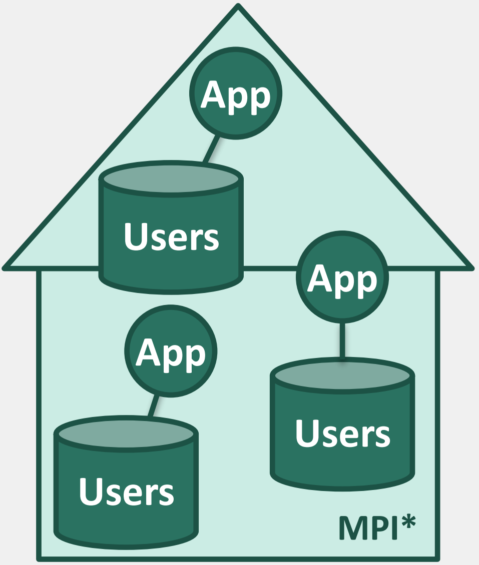
Administrative Headquarters

Administrative Services: SAP, E-Procurement, …

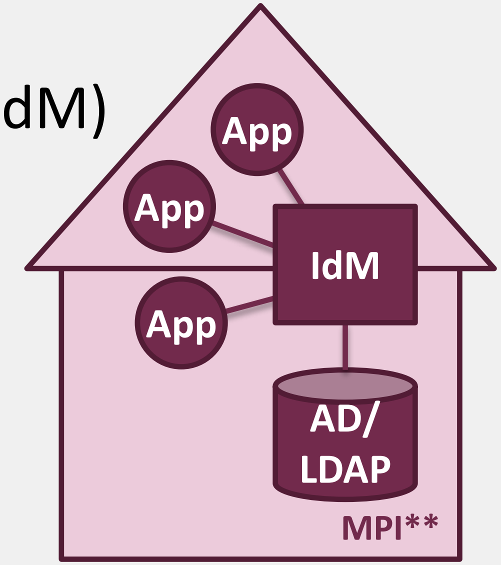
Central Service Units (CSUs)
Service Provider

Status Quo: Local Identity- & Access Management at the MPIs

- Varying from basic User Management…
  - Individual user accounts and -data in a multitude of application systems
  - Low level of User Management automation



- … to comprehensive Identity Management (IdM) solutions:
  - Central user account and data repositories
  - Only application specific data in application systems
  - High level of User Management automation



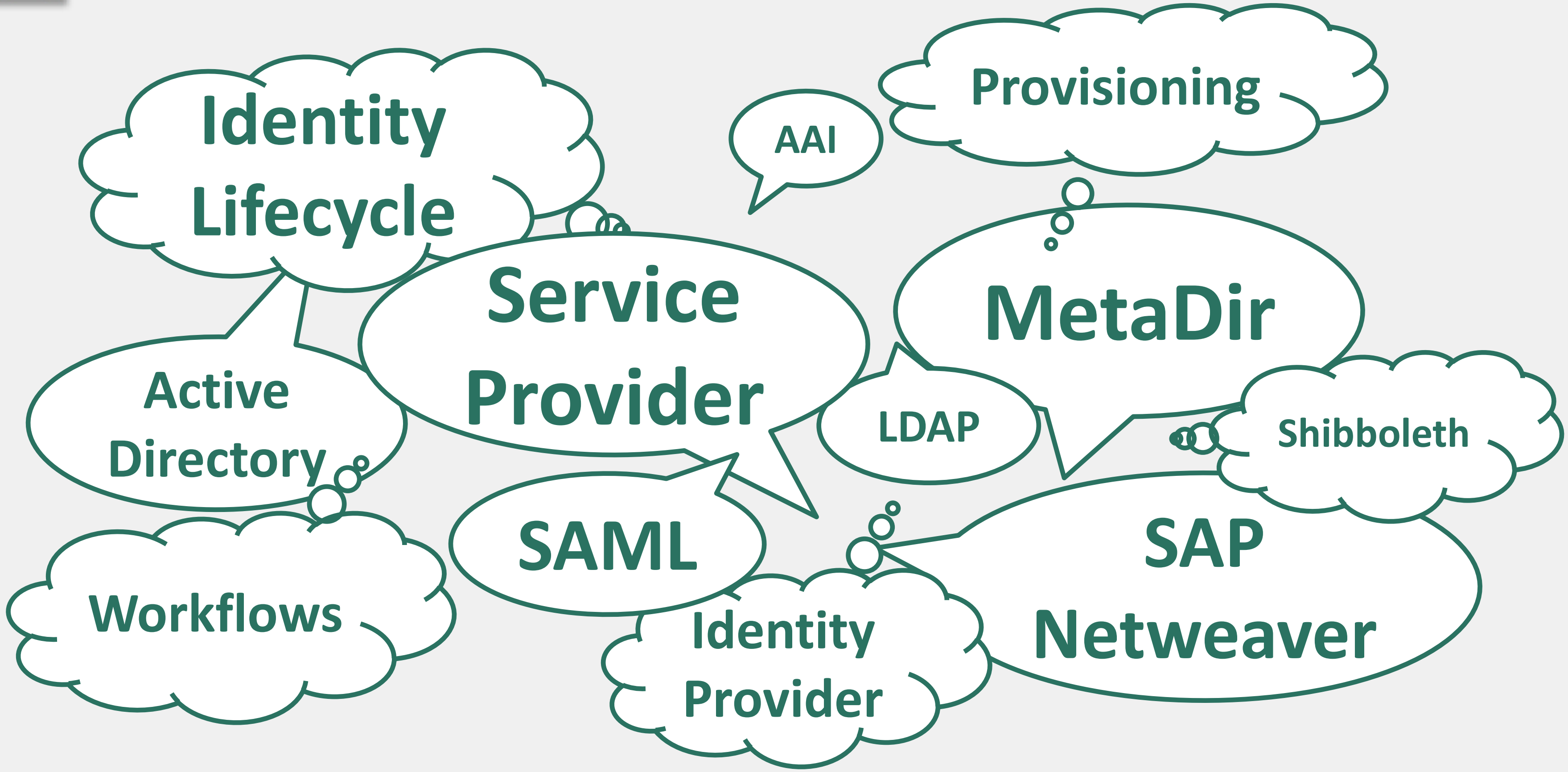
Status Quo: Local Identity- & Access Management at the CSUs

- MPDL
  - Basic IdM functionality for MPDL employees
  - Federated Access Management for Publisher Resources through MPS AAI (Shibboleth)
- GWDG
  - Advanced IdM solution (MetaDir) for identities of MPS and University of Göttingen
  - Local Access Management (GWDG Account), Participation in MPS AAI (Shibboleth)
- Administrative Headquarters
  - SAP Netweaver IdM for Management of MPS identities
  - Considering MPS AAI for Access Management

Status Quo: IdM Expansion Stages

Expansion Stages	*Basic*	*Advanced*	*Professional*
Repository Management	ID-Repository	MetaDirectory	n/a
Lifecycle Management	Manual Administration	Provisioning Role-Management Self Service	Priviledged User Management
Access Management	Login/PW	SSO RBAC Strong Authentication	AAI
Policies & Workflows	CRUD Basic Policies	Workflows Policy Repository	Federation
Compliance & Audit	Monitoring	Reports Audit	Compliance

Challenges: Understanding of IdM & AAI



- Challenge I:

  Unify understanding of Federated Identity & Access Management within the MPS

Challenges: Federated vs. Local IAM

- Federated Identity Management needs (at least) to handle all identities of the MPS
  - Advanced FIM Use Cases may also apply to external parties (partner institutions, companies, fellow researchers, …)
- Existing IdM activities of the CSUs should be considered as a starting point when inventing FIM at the MPS
- FIM needs to be connected to the local IdM solutions of MPIs and CSUs

- Challenge II:

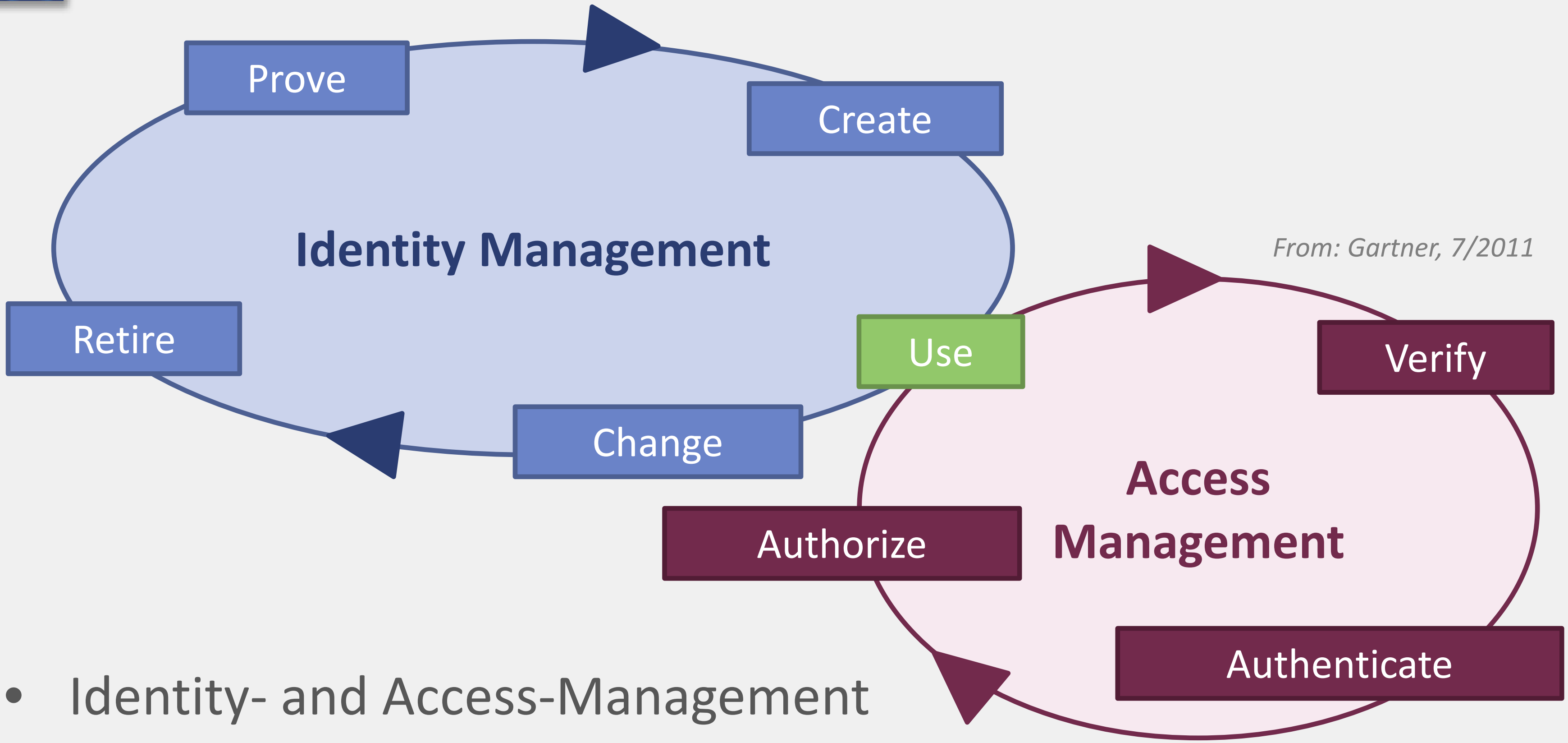
  Find technical solutions for an FIM infrastructure with appropriate interfaces to the (heterogeneous) IdM approaches at the MPIs and CSUs

Challenges: Efforts for inventing a FIM

- FIM work packages
  - Requirements analysis (Identity Lifecycle, interfaces to services and local IdMs, provisioning workflows, AAI Use Cases, …)
  - Conceptual design and IT architecture for FIM & FAM
  - Implementation (core FIM components, interface programming)
  - Testing, Documentation, initial Deployment
  - Rollout & Integration (connect 80+ MPIs and the CSUs)
  - Maintenance
- IAM projects tend to be time- and resource-intensive
- Challenge III:

  Ensure adequate funding of the FIM project

Challenge I: Understanding FIM



From: Gartner, 7/2011

- Identity- and Access-Management solutions focus on ***different aspects*** of IAM
- From an IT perspective, both are ***separate systems***
- But, they ***closely depend on each other*** in many use case scenarios

Challenge I: IdM vs. AAI solutions

- AAI solutions/Shibboleth…
  - … provide basic FIM features, e.g. transmission of user attributes
  - … are mainly designed for use with web applications (Web-SSO)
- IdM solutions…
  - … provide advanced FIM features, e.g. connectors to lots of IT systems (LDAP, AD, Exchange, SQL, …), workflow engines, etc.
  - … can be used for provisioning of AAI systems (Identity Provider)
- Complex IT infrastructures (Data Center Infrastructure, SAP Business Software) need advanced IdM functionality
  - FIM features of AAI solutions are not sufficient
  - Advanced features of IdM products are used
- FIM needs dedicated products for its IdM & AAI parts

Challenge II: Relation of Local and Federated IdM

Federated IdM

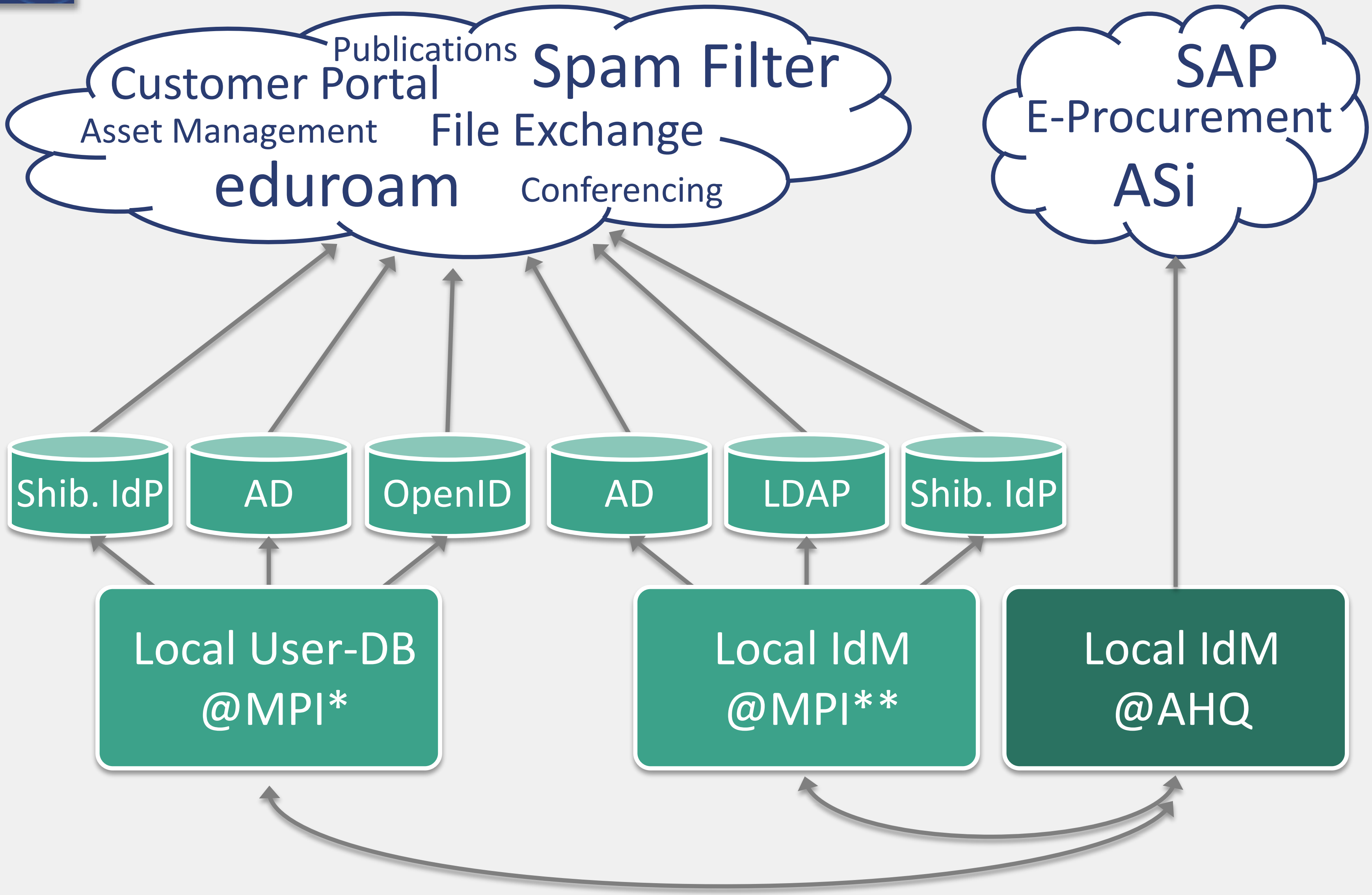
- First & Last Name
- User Id/Login
- E-Mail Address
- (eventually more)

Local IdM

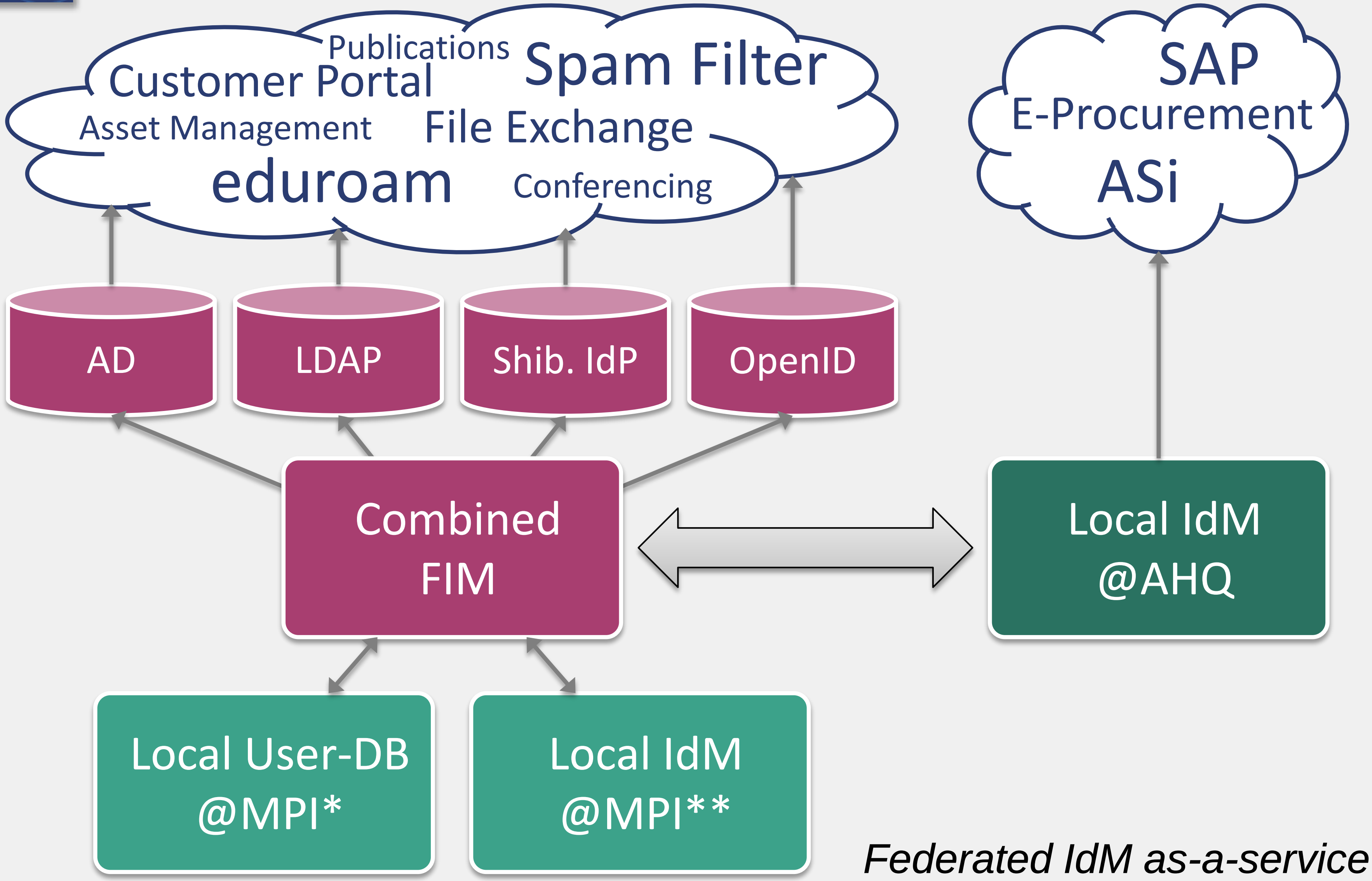
- First & Last Name
- User Id/Login
- E-Mail Address
- Birthdate
- Department
- Office
- Roles X, Y, ...
- ...

- Local and Federated IdM have a different level of detail
- Federated IdM does not replace local IdM!

Challenge II: IT-Infrastructures for FIM (Variant 1)

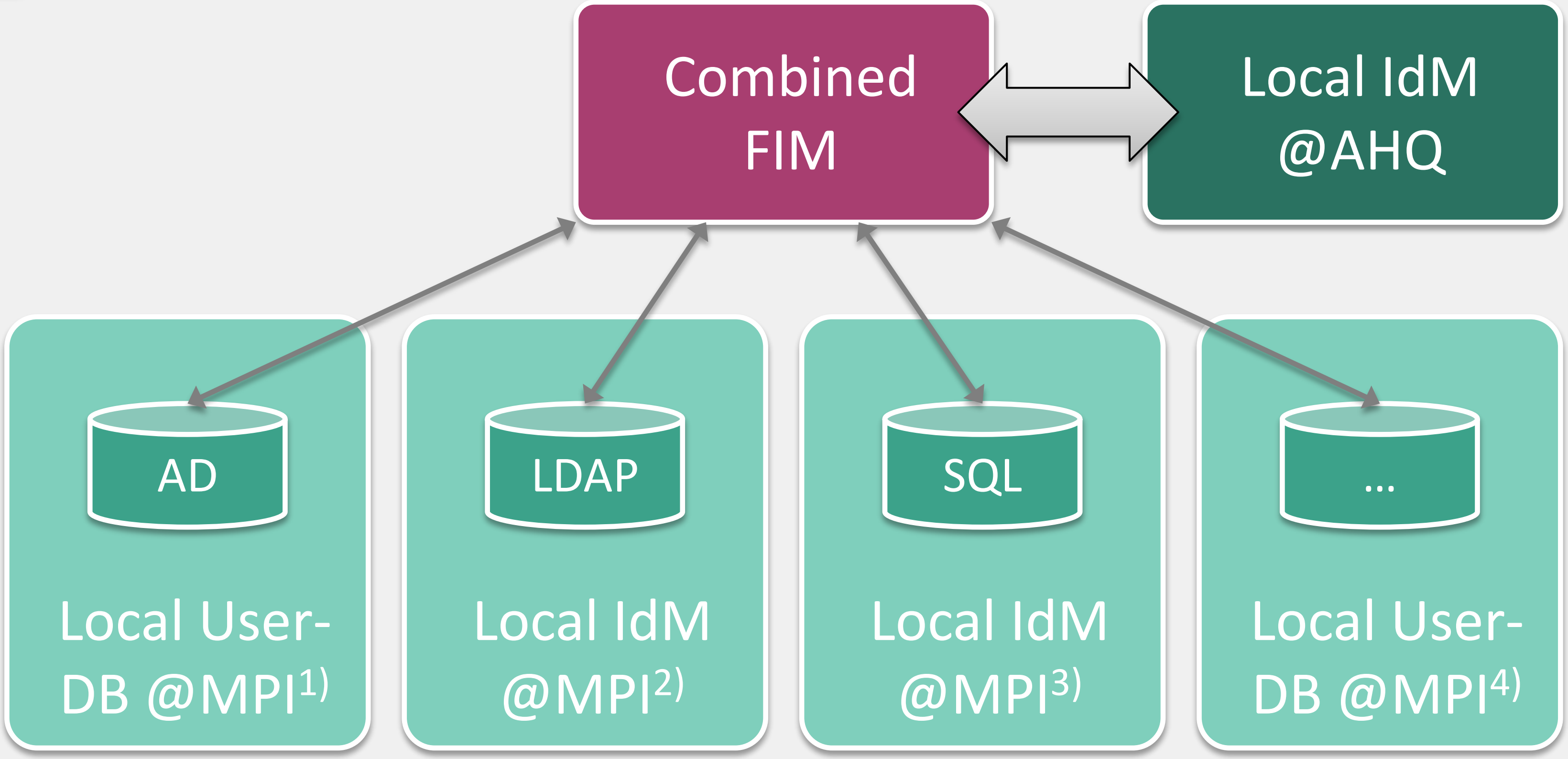


Challenge II: IT-Infrastructures for FIM (Variant 2)



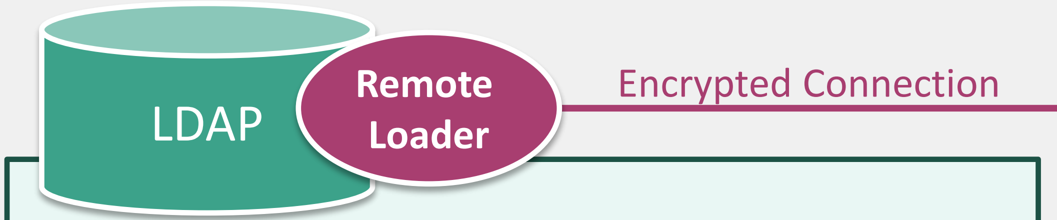
Federated IdM as-a-service

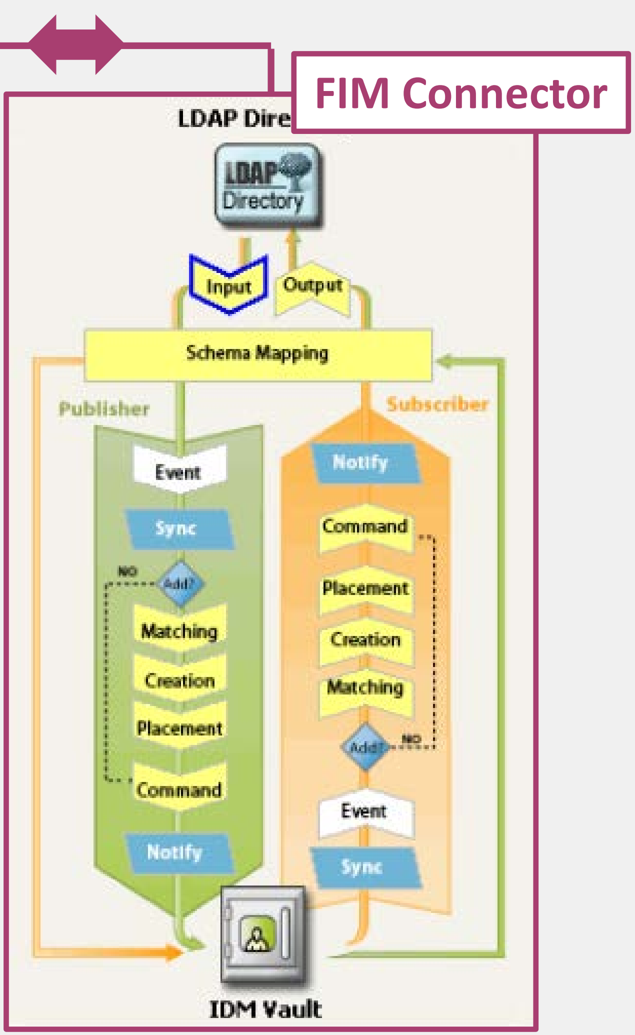
Challenge II: Connectors to a Combined FIM (1)



- MPI <-> Combined FIM through simple interfaces (LDAP, AD, SQL-DB, SAP, Flat File, Command Driver/Shell, etc.)
- Combined FIM <-> AHQ-IdM might use advanced features (e.g. workflows)

Challenge II: Connectors to a Combined FIM (2)





- Remote Loader
  - Java Application
  - Runs on the MPI’s Identity Repository
- Available Remote Loaders
  - Directory Services (AD, LDAP, ...)
  - Databases (Oracle, mySQL, …)
  - SAP
  - Command Driver (Shell-Scripts)
  - Flat File (e.g. CSV file)
  - ...

Challenge III: Awareness

- Identify relevant use cases which show the demand for a FIM
- Promote the benefits from an institutional approach and create critical mass for reference implementations
- Involve the MPS Stakeholders in fleshing out the use cases and convince them of the necessity to invent a FIM

- IAM and FIM are important infrastructure services that need a long-term strategy
- Establish a roadmap to consolidate the FIM with the selected added value service as part of a long-term strategy

Challenge III: Financing Models - Variant a)

- Central Funding
  - Invention of FIM through a central project with dedicated budget to establish the core functionalities
  - Maintenance of the resulting FIM solution

Activity focus:

- Development of core FIM components
- Realization of interfaces to important central IT systems
- Maintenance:
  - Updates
  - Bug fixes
  - Help desk

Challenge III: Financing Models - Variant b)

- Offer-driven Funding
  - An OU (e.g. Data Center) invents standardized FIM services, which are offered to all MPIs
  - Institutional funding, or
    fixed costs for offers, customers of these services are billed

Activity focus:

- Standardized interfaces between FIM and local IdM solutions (e.g. LDAP & AD)
- Connect own services to the FIM (added value)

Challenge III: Financing Models - Variant c)

- On-demand Funding
  - Realization of individual use-case scenarios on an on-demand basis; e.g. maintaining an interface for a specific local IdM or requested service
  - Invoicing based on time and cost in individual projects

Activity focus:

- Provisioning/Identity Lifecycle for individual services (e.g. research resources)
- Connection to non-standardized Local IdM solutions

Challenge III: Financing Models - Assessment

- Most likely a mix, especially of a) and c) would lead to sufficient but fairly distributed funding of a FIM invention project

- Core services need to be centrally funded or maintained, e.g. through the central service units.
- An FIM is never complete but needs to evolve through projects and maintenance services.

Status Max Planck Society:

- In an early phase for a MPS-wide FIM
- Mix of existing service provisioning and projects

Conclusion

- FIM is a future-oriented topic for the MPS
  - With the increasing importance of IT services and resources in science, the demand for an adequate FIM solution will grow
- For inventing FIM, a trans-institutional project must be established
  - A common understanding of FIM needs to be developed
  - The MPS AAI is not sufficient to cover the requirements of FIM
  - Current IdM activities of MPS OUs focus mainly on the local IT infrastructure
- Long-term Funding of a FIM project should be a mix of
  - central funding for the core FIM functionalities
  - offer-based funding for standardized FIM tasks
  - on-demand funding for individual, non-standardized FIM tasks

Questions?

Prof. Dr. Ramin Yahyapour

ramin.yahyapour@gwdg.de

www.gwdg.de

Tel.: +49 (0)551 201-1545/ -1510
Fax: +49 (0)551 201-2150

Gesellschaft für wissenschaftliche
Datenverarbeitung mbH Göttingen

Am Fassberg 11
37077 Göttingen