Überblick über zentrale und dezentrale IdM Lösungen in Göttingen

Sebastian Rieger
sebastian.rieger@gwdg.de

Gesellschaft für wissenschaftliche Datenverarbeitung mbH Göttingen

Am Fassberg, 37077 Göttingen

Fon: 0551 201-1510 Fax: 0551 201-2150
gwdg@gwdg.de www.gwdg.de

Agenda

- Ausgangsbasis und Motivation
- Differenzierung von zentralen und dezentralen IdM Lösungen
- Realisierung Meta-Directory und Benutzer-Portal
- Shibboleth im Umfeld der Max-Planck-Gesellschaft und Uni-Göttingen
- Ausblick

Ausgangsbasis und Motivation

- Beginn des Projekts Ende 2005
- Teilvorhaben im Rahmen des Kooperationsprojekts GÖ* (Wissenschaftliche IT-Dienstleister am Standort Göttingen)

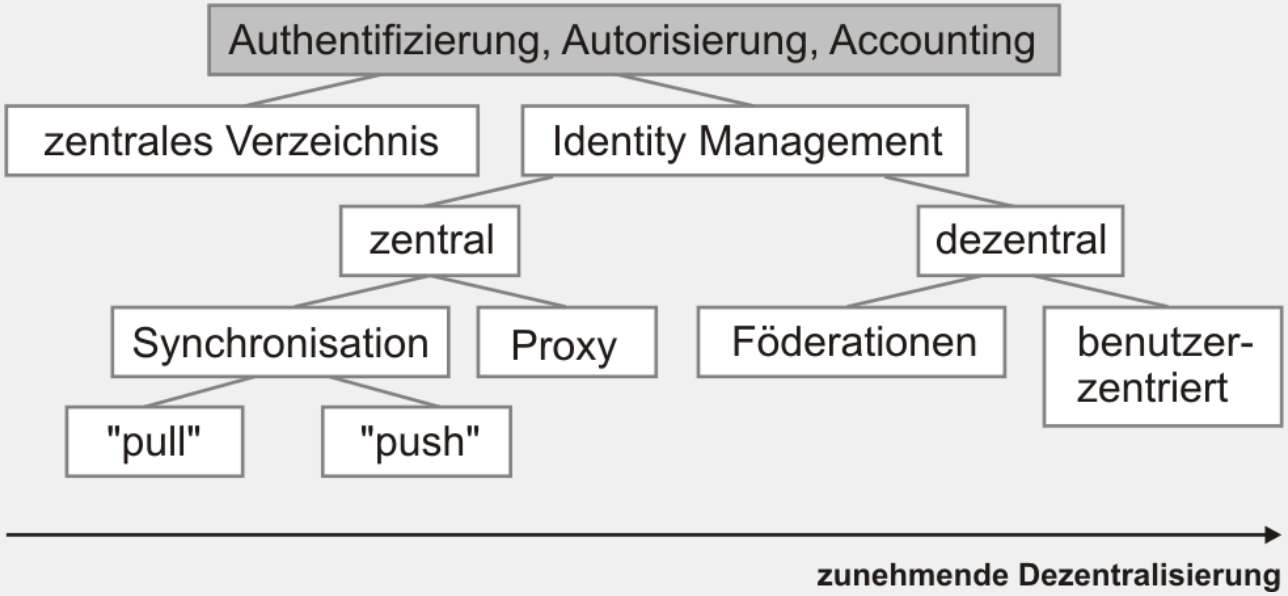
Ziel:

- Einheitliche Authentifizierung, einheitliche Benutzerverwaltung
- Pragmatischer Ansatz für Realisierung eines IdM
- Single Sign-On Lösungen

Ausgangsbasis:

- Universität-Göttingen (~25000 Studierende, ~6000 Mitarbeiter, Uniklinikum ~7000 Mitarbeiter, Staats- und Uni-Bibliothek), 6 Max-Planck Institute, …
- Heterogene, komplexe, teils manuelle Prozesse für die Benutzerverwaltung
- Zahlreiche separate Verzeichnisdienste, Datenbanken, flat files, …

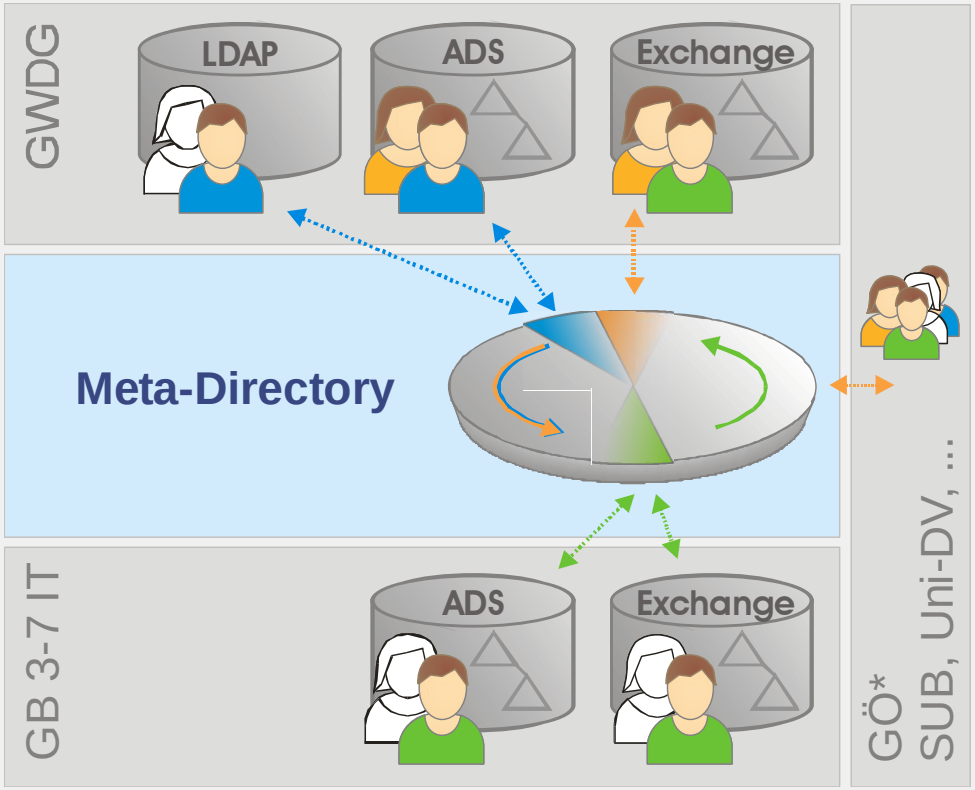
Dezentralisierung des IdM



- zentrale Verzeichnisse z.B.: NIS, LDAP, Passport, …
- Synchronisation: Skript-basiert, Meta-Directory
- Proxy: RADIUS, Virtual Directory, CAS…
- Föderationen: (Kerberos-Trusts, X.509), SAML, Shibboleth, simpleSAMLphp, ADFS, Liberty, OpenSSO, WS-Federation, …
- Benutzerzentriert (user-centric): OpenID, CardSpace, OAuth, sxip, higgins,...

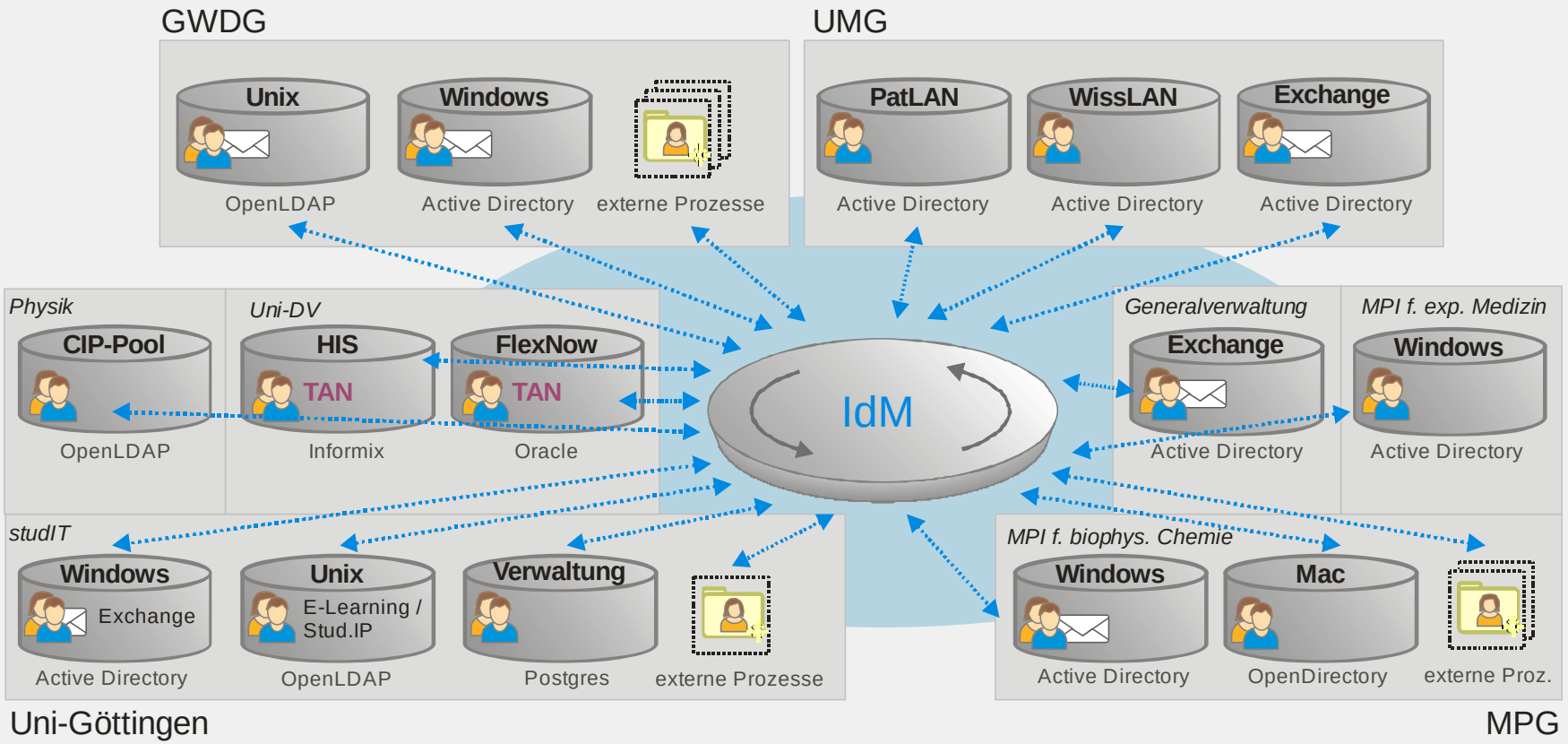
Realisierung eines Meta-Directory

- Einheitliche Benutzer-Accounts für Studierende und Mitarbeiter unterschiedlicher Systeme und Betreiber (GWDG, Uni, UMG …)
- Synchronisation von Org.struktur, Identität, Passwort, Gruppen, …
- Einheitliche Verwaltung, vereinfachte Verwendung (Single Password, Single Sign-On)
- Optimierung von Prozessen bei der Benutzerverwaltung (Anlage von Verzeichnissen, …)



- Produktentscheidung fiel auf Novell Identity Manager
- Integration externer Accounts (Gastwissenschaftler, Studierende anderer Hochschulen etc.) über dezentrales Identity Management (z.B. DFN-AAI)

Meta-Directory der GWDG (Uni und MPG)



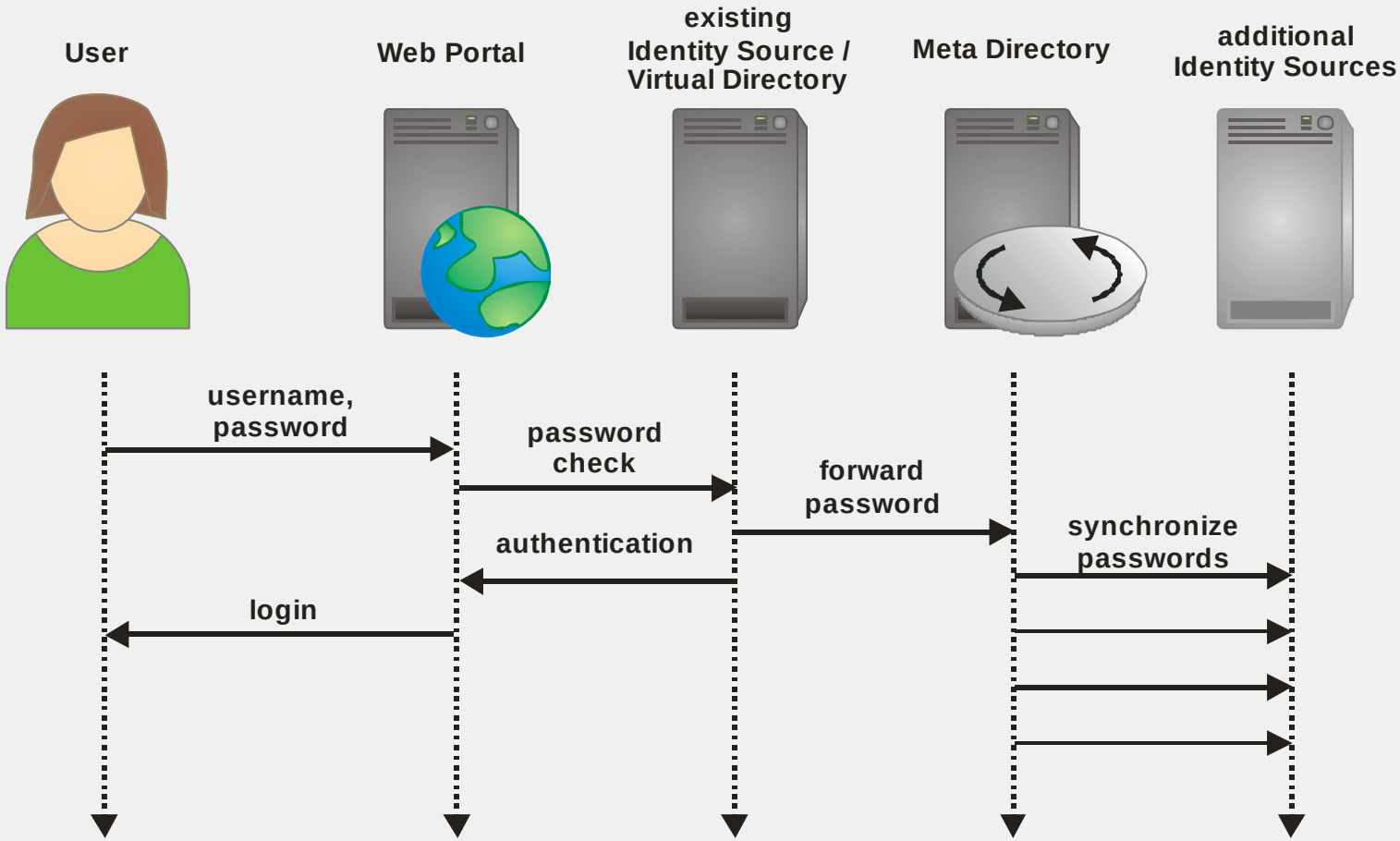
- 21 angebundene Systeme (Verzeichnisdienste, Datenbanken, Prozesse), ~70.000 Objekte
- Synchronisation: Benutzerkonten (z.B. einheitliche Studierenden-Accounts), Gruppen,...
- 3 redundante IdM Server (2 physikalische Maschinen, 1 VM), 2 VMs für Portal und Audit

Zentrale IdM Lösungen

- Einheitliche Accounts für Studierende
  - HIS SOS als initiale Quelle, Anbindung an Meta-Dir über Views, Trigger, ...
  - Erzeugung von Accounts für alle Studierenden der Uni-Göttingen im Meta-Directory der GWDG (z.B. max.musterfrau@stud..., Exchange-Postfach)
  - Abgleich der Studierendendaten (insb. zwischen HIS und FlexNow), Abgleich alle 10 Sek. (inkl. TANs) - Unix-, Windows-, CIP-Pools
  - Anbindung von E-Learning Systemen (Stud.IP) inkl. Bereitsstellung erforderlicher Attribute: Abschluss, Fachbereiche, Studiengänge usw.
- GÖ* Benutzer-Portal
  - Zentrale Passwort-Änderung, Passwort im IdM gespeichert, erzeugt Hashes
  - Dezentrale Benutzerverwaltung: z.B. eigenständige Verwaltung der Benutzerkonten (-passwörter) durch Institute, usw. (eigenes JSF Portlet)

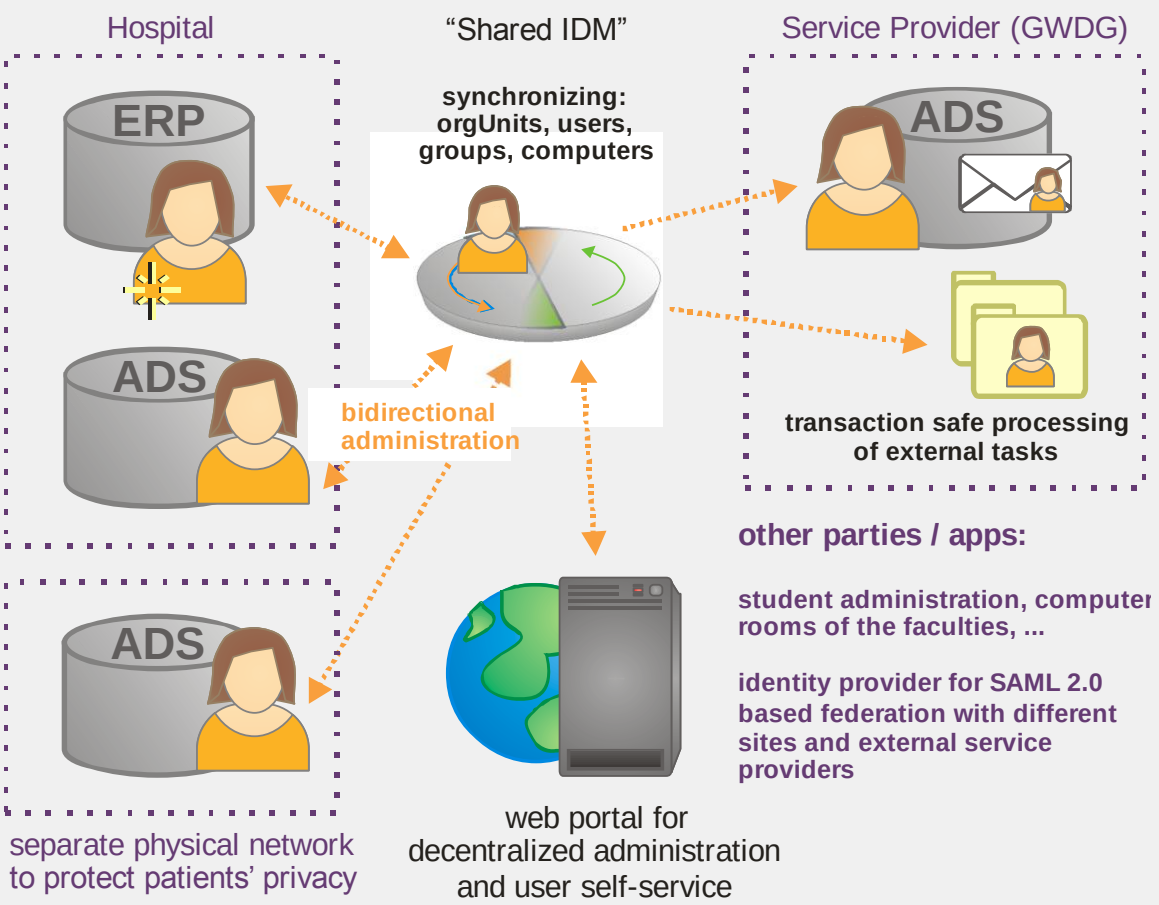
Passwort-Import-Portlet für Benutzer-Portal

- Import von existierenden Passwörtern aus bestehenden Applikationen
- Außerdem im Einsatz für Überprüfung des Passworts / Funktionstest



Zentrale IdM Lösungen (2)

- Zahlreiche Anwendungen unterstützen noch keine föderative Authentifizierung (z.B. basierend auf SAML), daher z.B. Synchronisation von Exchange Accounts
- Anlage der Benutzer im ERP System des Uni-Klinikums, Sychronisation in Exchange der GWDG
- Administration in ADs oder Benutzer-Portal
- Eigenentwicklung eines Treibers für fehlertolerante Ausführung externer Prozesse (Wiederholung bei Fehlern), sowie Changelog Unterstützung für OpenLDAP



Einheitliche Mitarbeiter-Accounts

- Einheitliche Accounts für Mitarbeiter (inkl. Dozenten etc.)
  - Quelle: mehrere SAP (HR) Systeme (Klinikum, Uni, ...)
  - Senken: bestehende Treiber für AD, OpenLDAP ...
    - Synchronisation für E-Learning Anwendungen, Telefon-DB, ...
    - Integration bestehender Benutzerverwaltungen
  - Redundante Identity Manager Instanz in Universitätsmedizin Göttingen
    - Failover-Lösung für IdM – Projekt: IdM Risikomanagement
  - Geplante Einführung Q3 2010
  - Schnittstellen für Autorisierung (Rollen, Funktionen aus SAP)

Federated Identity und Single Sign-On

- Schnittstellen zu anderen zentralen IdMs waren erforderlich:
  - Andere Hochschulen (z.B. in Niedersachsen, E-Learning Kooperation)
  - Eigenständigkeit der Max-Planck-Institute (eigene IdM Systeme)
- Bedarf für dezentrales IdM und die Einbindung in Föderationen
  - Tests verschiedener Lösungen für SAML Identity Provider am IdM (u.a. Novell Access Manager)
  - Entscheidung: Shibboleth Identity Provider (Akzeptanz und Kompatibilität)
- Gleichzeitig Single Sign-On für E-Learning Applikationen in Göttingen (Stud.IP, Medien-Portal, LSF, ...)
  - Integration von Shibboleth und CAS für Universitäts-Portal (erforderlich für Single Logout)
- Göttinger IdM ist derzeit angebunden an: DFN-AAI, NDS-AAI, MPG-AAI

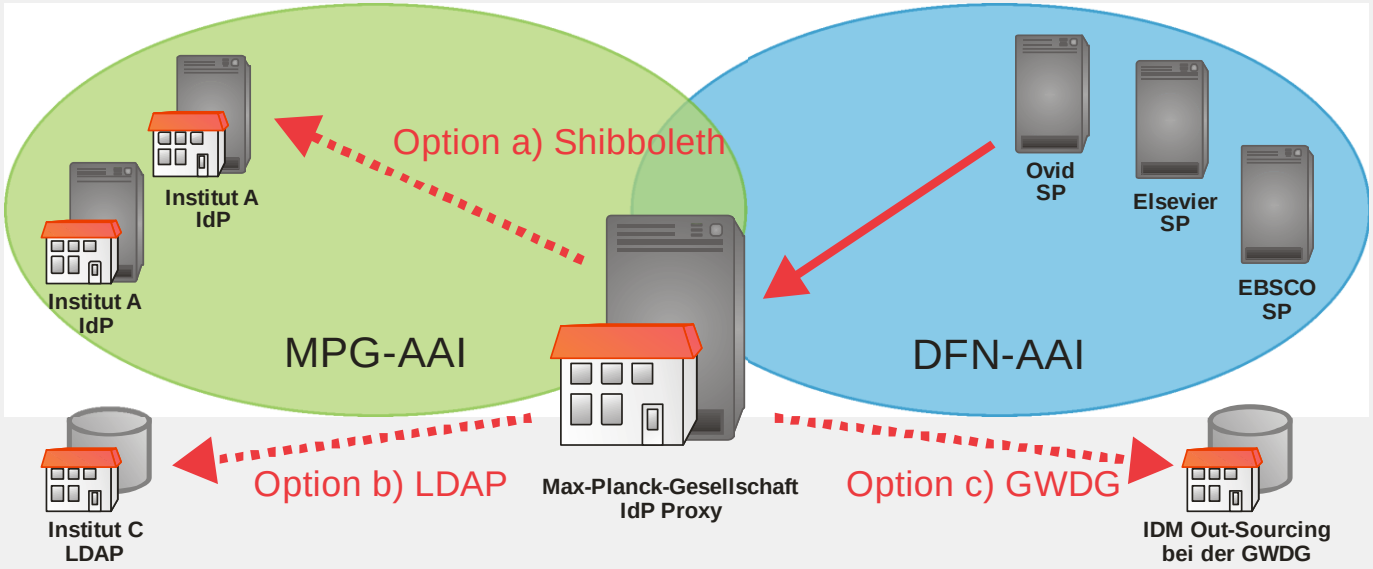
NDS-AAI

- Authentifizierungs- und Autorisierungsinfrastruktur für Niedersachsen - Initiative des “Landesarbeitskreises Niedersachsen für Informationstechnik / Hochschulrechenzentrum”
  - Finanziert vom Niedersächsischen Ministerium für Wissenschaft und Kultur
  - GWDG ist im Kernteam für Realisierung der Föderation (Braunschweig/Wolfenbüttel, Clausthal, Göttingen, Hannover, Osnabrück)
  - Implementierung / Betrieb erfolgt durch DAASI International GmbH
  - Alle Hochschulen erhielten im Projekt eine “Shibboleth Appliance”
  - Vorrangiges Ziel: Single Sign-On für E-Learning in Niedersachsen, Shibbolisierung von Stud.IP
  - Integration uApprove (Switch) - Anforderungen des Landesdatenschutzes
  - Integration in DFN-AAI geplant für 2010

MPG-AAI

- Authentifizierungs- und Autorisierungsinfrastruktur für die 80 Institute der Max-Planck-Gesellschaft (teilw. außerhalb von Deutschland)
  - Anbindung der Max-Planck-Institute an unterschiedliche Föderationen
  - Kooperationsprojekt zwischen GWDG, Rechenzentrum Garching und Max-Planck Digital Library
  - Entwicklung eines Betriebskonzepts für die MPG-AAI gemeinsam mit Rechenzentrum Garching, redundante Auslegung der Identity Provider und Discovery Services (DS)
  - Web-basiertes Verwaltungs-Interface für Metadaten (Teilnehmer, Zertifikate etc.) der MPG-AAI
  - Implementierung eines Identity Provider Proxy, ermöglicht Integration der MPG-AAI in unterschiedliche Föderationen (DFN-AAI) ohne zusätzlichen DS

Shibboleth IdP Proxy



- Java-basierte Erweiterung für Shibboleth Identity Provider (IdP)
- Redundante Instanzen mit Terracotta, zwei Instanzen bei GWDG eine in RZG
- Benutzerzentrierte Anmeldung an IdP Proxy: max.muster@mpi.mpg.de,kein weiterer Discovery Service
- Ermöglicht es die Max-Planck-Gesellschaft als Ganzes (einzelner IdP) in die DFN-AAI zu integrieren
- Institute können selbst Shibboleth IdP anbieten, bestehende Benutzerverwaltung (z.B. LDAP, DB, Kerberos) integrieren oder diese (z.B. kleine Institute) an die GWDG / das RZG auslagern
- Attribute werden am Übergang zwischen MPG-AAI und DFN-AAI gefiltert (Datenschutz), Benutzer muss der Übermittlung der Daten zusätzlich zustimmen

Ausblick und laufende Projekte

Zentrale IdM Lösungen:

- Realisierung einheitlicher Mitarbeiter-Accounts (Anbindung SAP - Meta-Dir)
- Risikomanagement für IdM
- Virtual Directory für Anbindung Instituts-IdM an IronPort (weniger Treiber)

Dezentrale IdM Lösungen:

- Realisierung IP Proxy für Institute (Shibboleth Login an Proxy), Abrechnung
- Integration weiterer Verfahren (OpenID Provider), aktuell laufend: simpleSAMLphp für foodle

Vielen Dank für die Aufmerksamkeit! Gibt es Fragen?