(Federated) Identity Management

Thorsten Michels

RHRZ at the RPTU

07. 03. 2023

RHRZ
Regionales
Hochschulrechenzentrum
Kaiserslautern-Landau

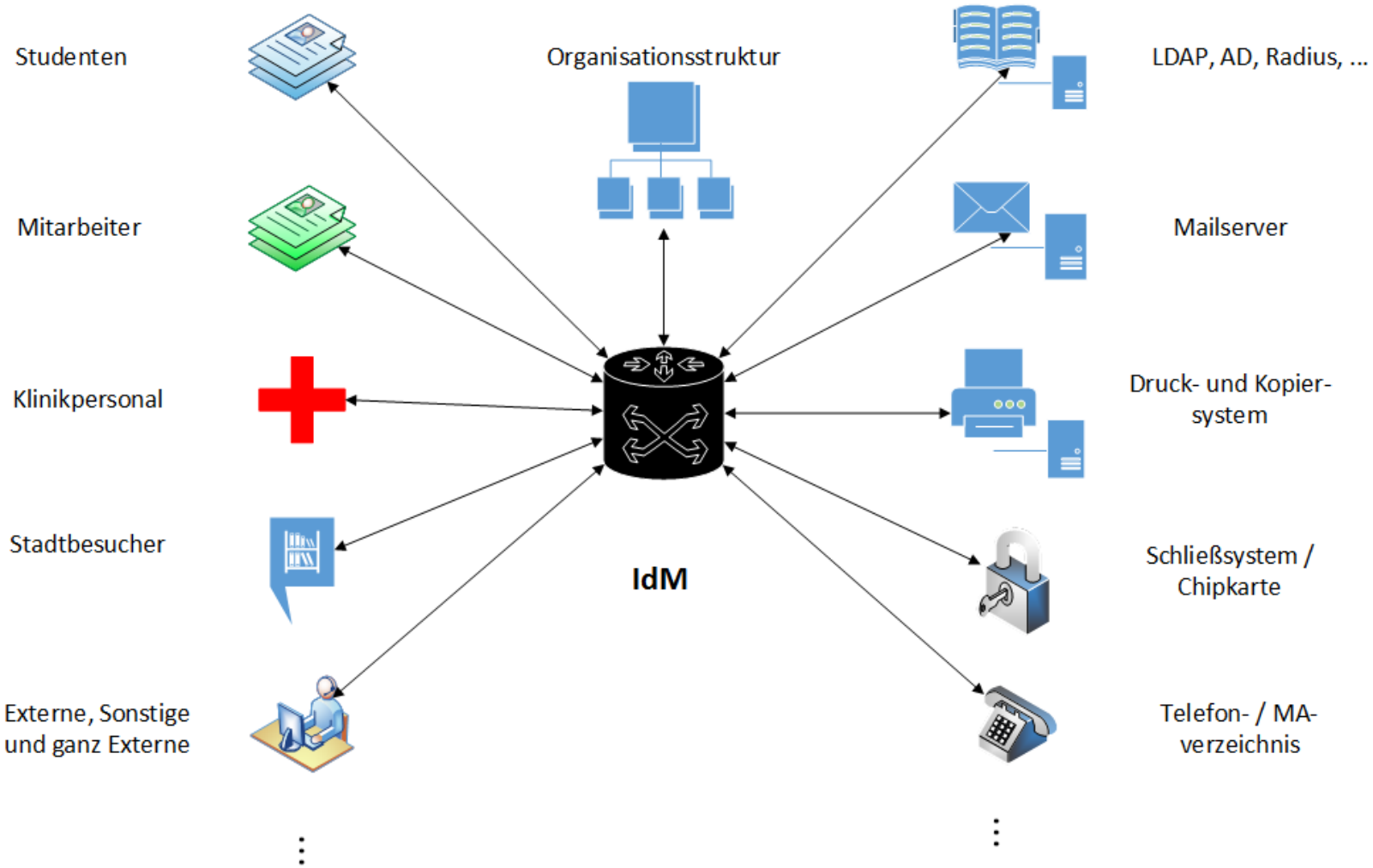
Identity- (and Access-) Management:

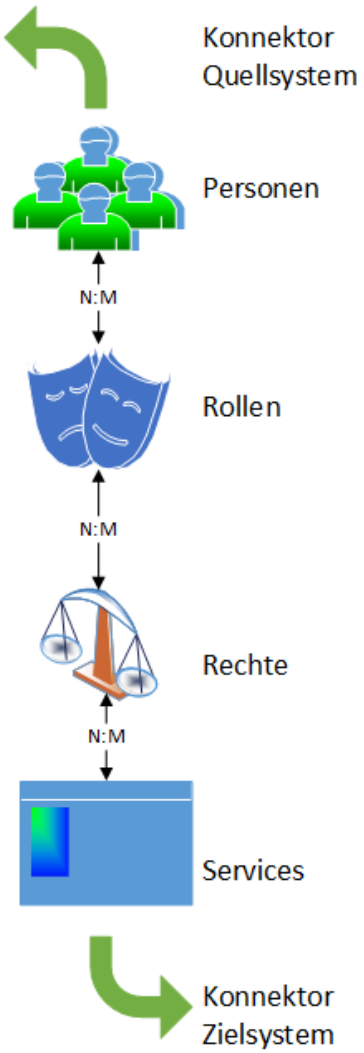
The correct group of persons has

at the correct time

the correct kind of access

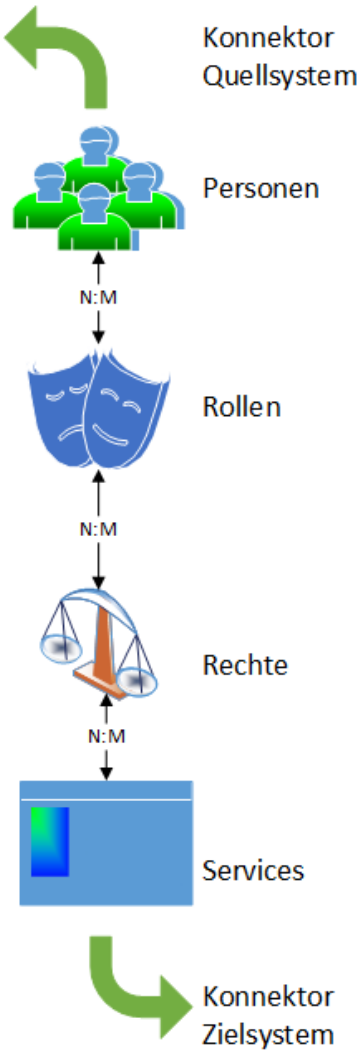
to the correct resources.


Studenten
Mitarbeiter
Klinikpersonal
Stadtbesucher
Externe, Sonstige und ganz Externe
Organisationsstruktur
IdM
LDAP, AD, Radius, ...
Mailserver
Druck- und Kopier-system
Schließsystem / Chipkarte
Telefon- / MA-verzeichnis



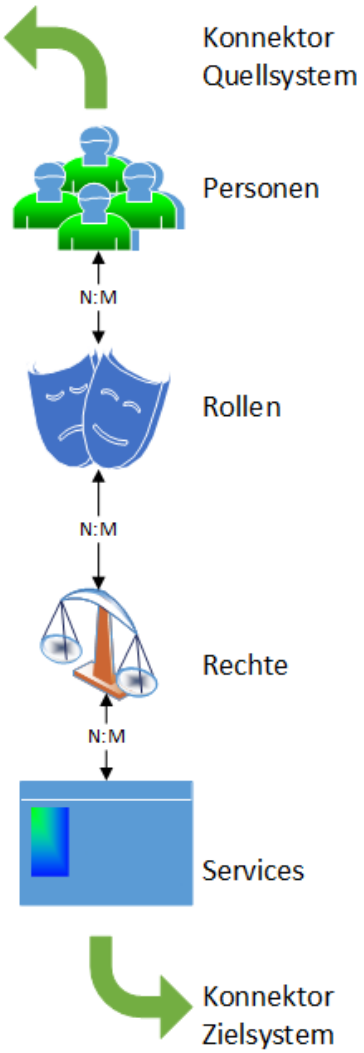
Persons: Identities:
How do you identify a person?

- Given name, surname, other parts of the name
- Date and place of birth



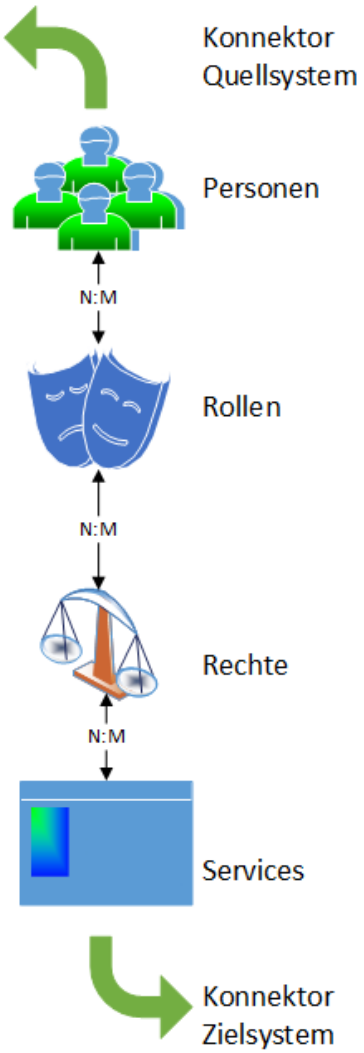
Persons: Identities:
How do you identify a person?

- Given name, surname, other parts of the name
- Date and place of birth
- Immatriculation number, employee number, ...



Persons: Identities:
How do you identify a person?

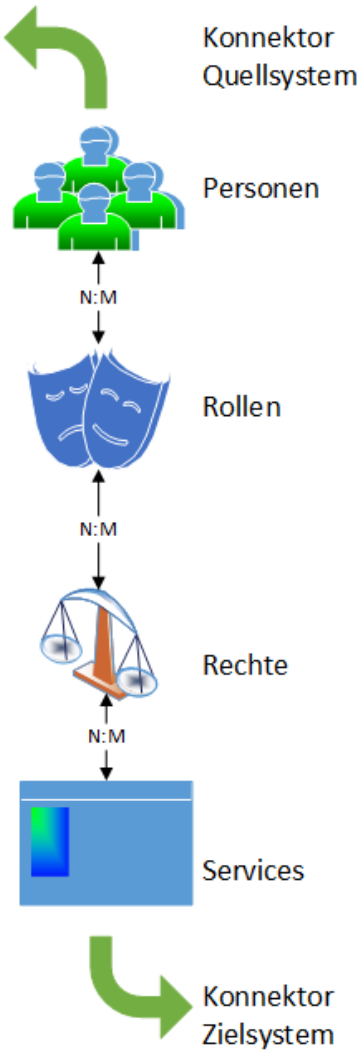
- Given name, surname, other parts of the name
- Date and place of birth
- Immatriculation number, employee number, . . .
- Don't use mail addresses as identifiers!
  They are prone to change!



Persons: Identities:
How do you identify a person?

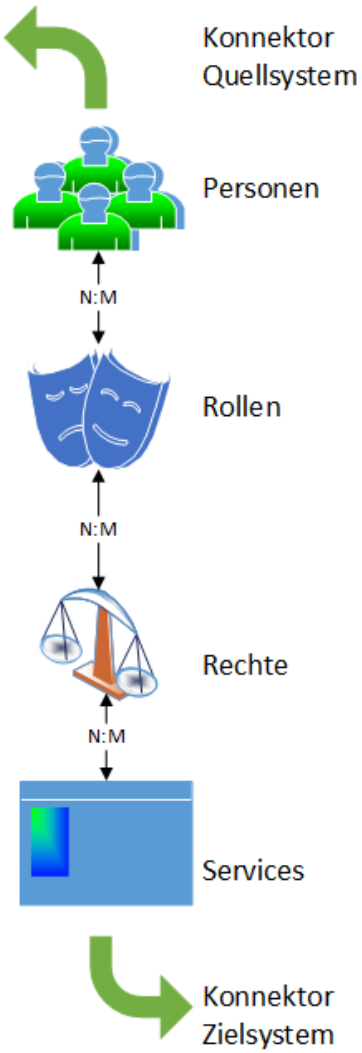
- Given name, surname, other parts of the name
- Date and place of birth
- Immatriculation number, employee number, . . .
- Don't use mail addresses as identifiers!
  They are prone to change!

Persons might just be one kind of object in IdM:
OUs, groups, roles, target system accounts, . . . ?



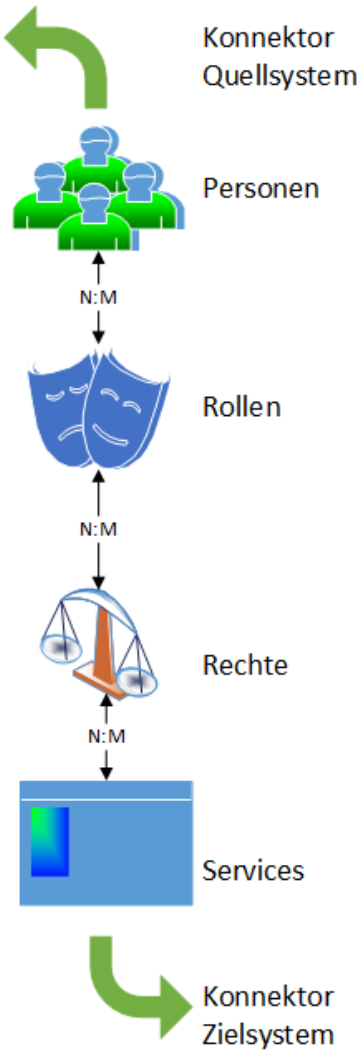
Persons and their attributes

Attribut	Wert
givenName	Frank
sn	Stein
uid	mus42ter
ou	Biologie
displayName	Dr. Frank N. Stein
mail	stein@hs-pw.de, frank.stein@bio.hs-pw.de



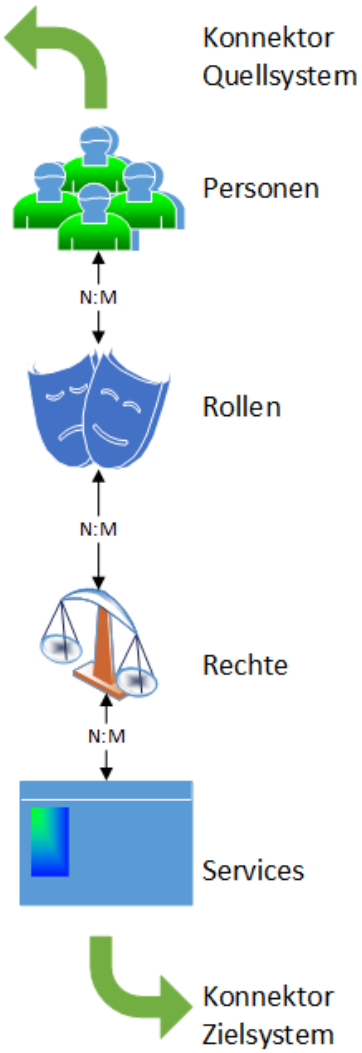
Persons and their attributes

Attribut	Wert
givenName	Frank
sn	Stein
uid	mus42ter
ou	Biologie
displayName	Dr. Frank N. Stein
mail	stein@hs-pw.de, frank.stein@bio.hs-pw.de
eduPersonPrincipalName	mus42ter@hs-pw.de



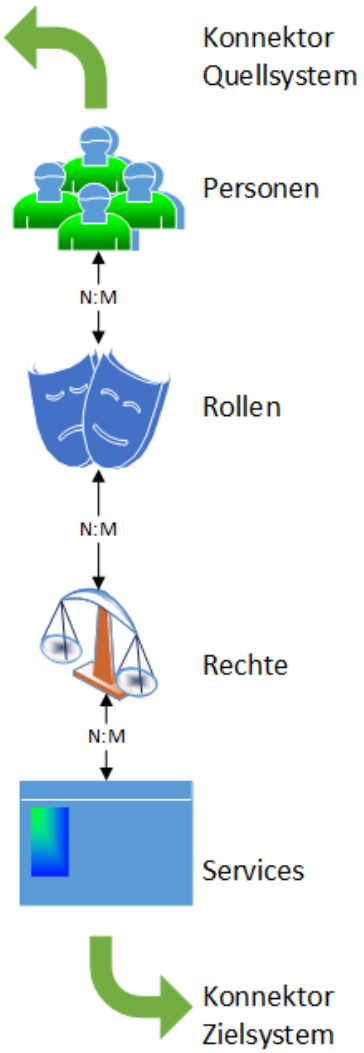
Persons and their attributes

Attribut	Wert
givenName	Frank
sn	Stein
uid	mus42ter
ou	Biologie
displayName	Dr. Frank N. Stein
mail	stein@hs-pw.de, frank.stein@bio.hs-pw.de
eduPersonPrincipalName	mus42ter@hs-pw.de
eduPerson[Scoped]Affiliation	member, employee, faculty, staff, student, affiliate [@hs-pw.de]



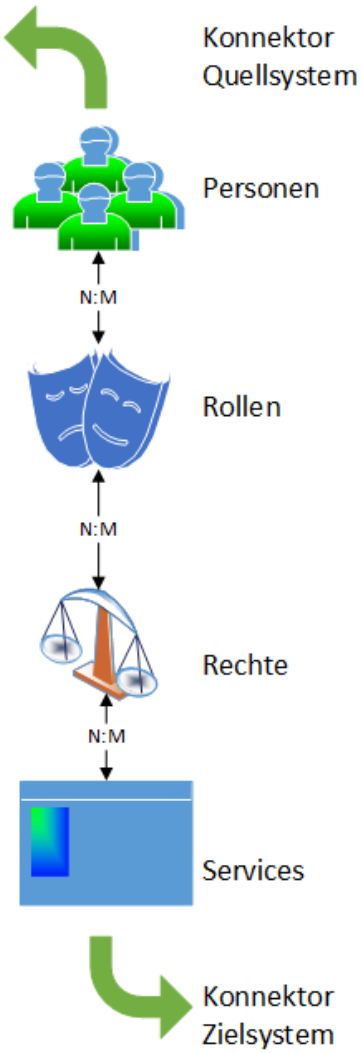
Persons and their attributes

Attribut	Wert
givenName	Frank
sn	Stein
uid	mus42ter
ou	Biologie
displayName	Dr. Frank N. Stein
mail	stein@hs-pw.de, frank.stein@bio.hs-pw.de
eduPersonPrincipalName	mus42ter@hs-pw.de
eduPerson[Scoped]Affiliation	member, employee, faculty, staff, student, affiliate [@hs-pw.de]
eduPersonEntitlement	urn:mace:dir:entitlement:↵ common-lib-terms http://rarp-kl.de/entitlement/hpc



Persons and their attributes

Attribut	Wert
givenName	Frank
sn	Stein
uid	mus42ter
ou	Biologie
displayName	Dr. Frank N. Stein
mail	stein@hs-pw.de, frank.stein@bio.hs-pw.de
eduPersonPrincipalName	mus42ter@hs-pw.de
eduPerson[Scoped]Affiliation	member, employee, faculty, staff, student, affiliate [@hs-pw.de]
eduPersonEntitlement	urn:mace:dir:entitlement:↵ common-lib-terms http://rarp-kl.de/entitlement/hpc
schacPersonalUniqueCode	urn:schac:personalUniqueCode:de:↵ hs-pw.de:MatrikelNummer:123456



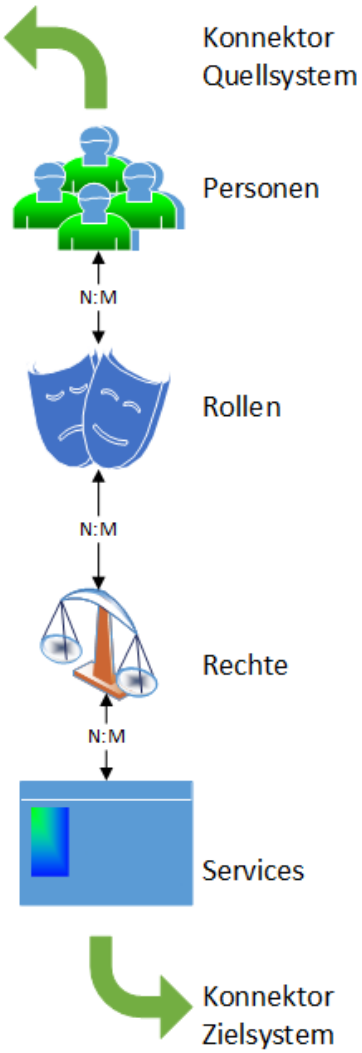
Persons and their attributes

Attributes to use as Primary Keys for persons:

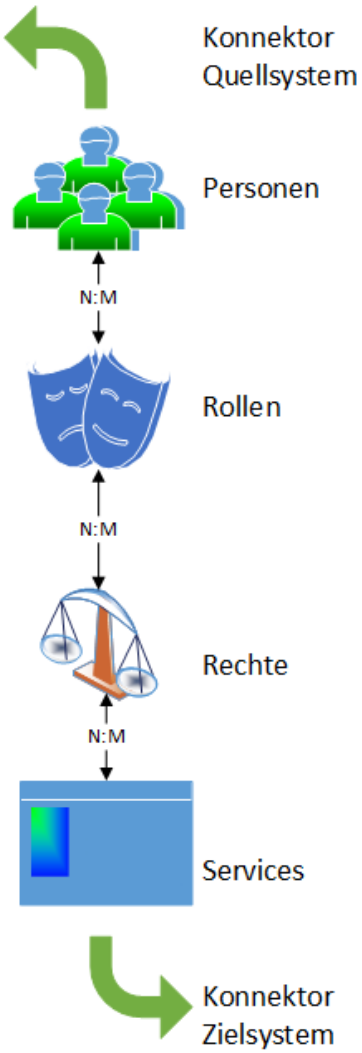
Subject ID — long-lived, non-reassignable, *omni-directional* identifier suitable for use as a *globally-unique* external key

Pairwise ID — long-lived, non-reassignable, *uni-directional* identifier, suitable for use as a unique external key *specific to a particular relying party*

Bsp.:
`MCE6NXEQ3FC3PUKY4M75EYCOWN4TGKBH@testscope.dfn.de`
https://doku.tid.dfn.de/de:aai:attributes_best_practice
https://cvs.data.kit.edu/nfdi-aai-doc/attributes/

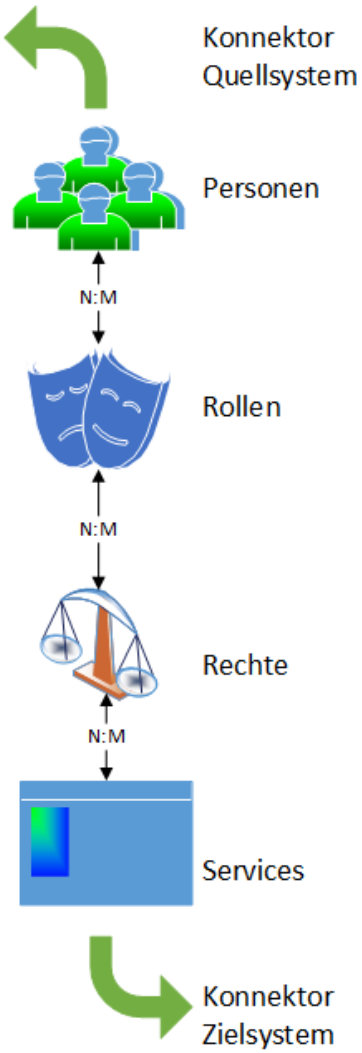


(„Primary“-)Roles:
Professors, research staff, administrative and service staff, students, „Hiwis“, interns, alumni, emeriti, guests, affiliates, whathaveyou. . .

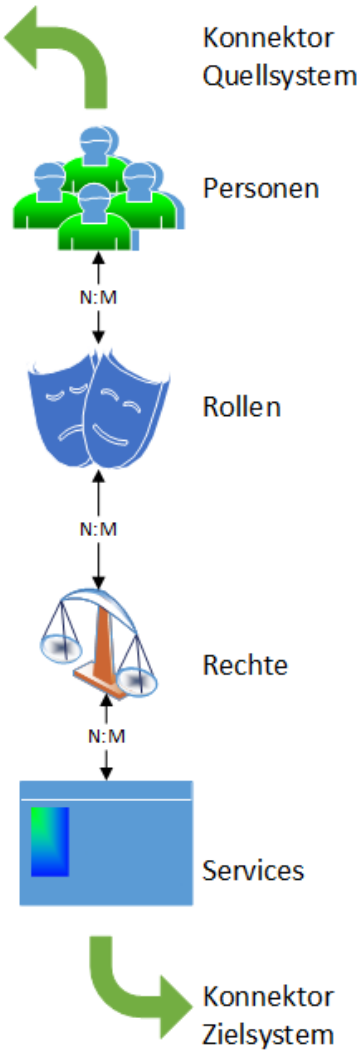


More roles:

Leader of an organizational unit (OU), president, members of committees or departments,
students of study path X, dean of department X,
members of a project,
substitutes,
...



Rights:
Read (in a certain area?), change, create, delete, discover, search, compare (→ authentication), execute



Services:
IdM-internal representation of target systems,
to which accounts are provisioned

- Transformation of accounts and attributes
- Reconciliation: Comparison of target state and actual state;
  treatment of local / orphaned accounts
- Admin / Manager account

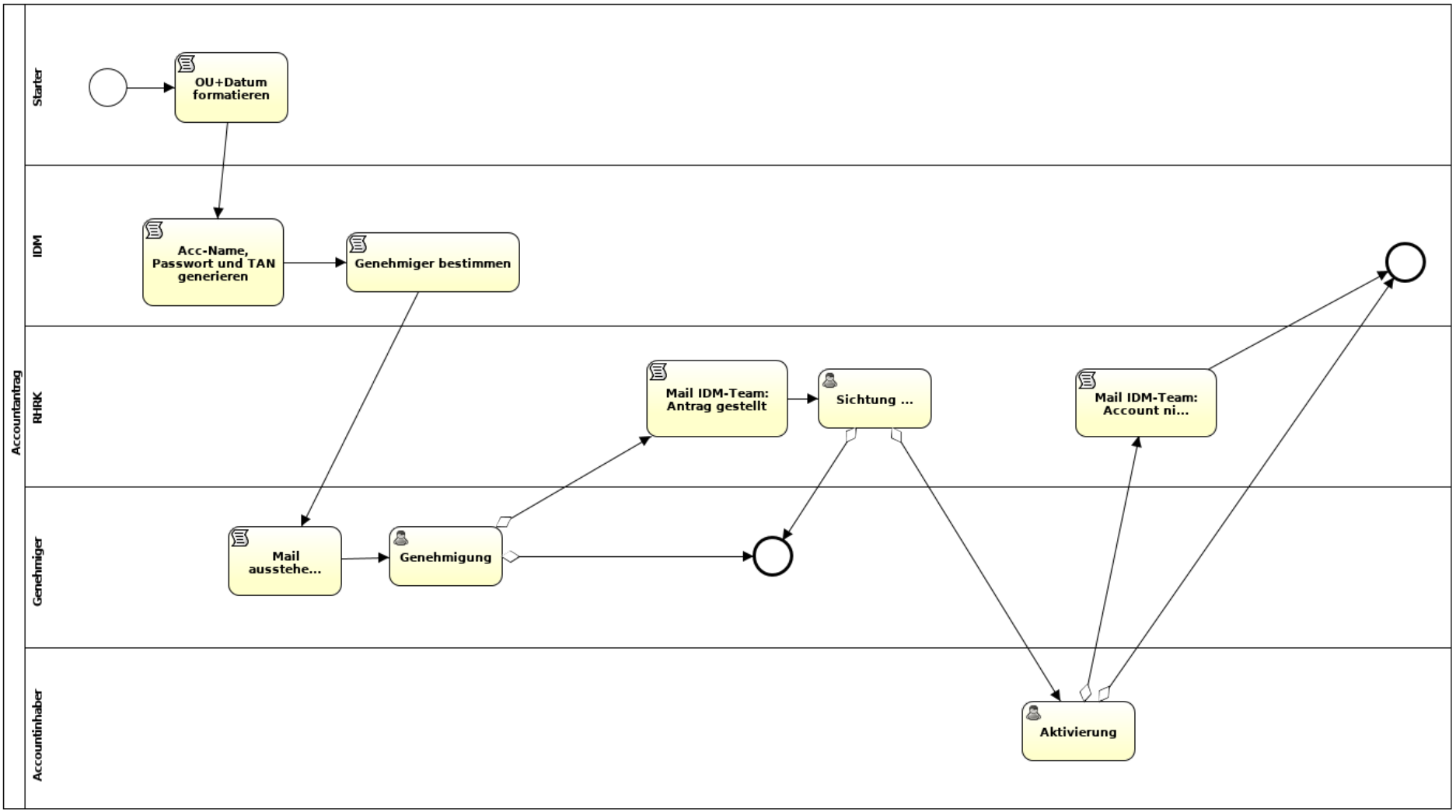
→ Cooperation with admins of target systems!

Processes: Example: Deletion of accounts

1. When the time limit of an account is reached:
   Send a warning mail to the user.
2. Two weeks later: Lock the account.
3. One month after that: Delete the account
   (and initiate account deletion on target systems).

→ Have arrangements ready to exit the process, when the account gets prolonged.

Processes:


Accountantrag
Starter
IDM
RHRK
Genehmiger
Accountinhaber
OU+Datum formatieren
Acc-Name, Passwort und TAN generieren
Genehmiger bestimmen
Mail IDM-Team: Antrag gestellt
Sichtung ...
Mail IDM-Team: Account ni...
Mail ausstehe...
Genehmigung
Aktivierung

Processes: Recurring questions:

- Where does the data come from?

Processes: Recurring questions:

- Where does the data come from?
- Which kind of data / attributes are being delivered?

Processes: Recurring questions:

- Where does the data come from?
- Which kind of data / attributes are being delivered?
- When and how often is the data delivered?

Processes: Recurring questions:

- Where does the data come from?
- Which kind of data / attributes are being delivered?
- When and how often is the data delivered?
- How reliable are quality and up-to-dateness?

Processes: Recurring questions:

- Where does the data come from?
- Which kind of data / attributes are being delivered?
- When and how often is the data delivered?
- How reliable are quality and up-to-dateness?
- Who sends notices about sporadic changes (e. g. transfer of personnel)?

Processes: Recurring questions:

- Where does the data come from?
- Which kind of data / attributes are being delivered?
- When and how often is the data delivered?
- How reliable are quality and up-to-dateness?
- Who sends notices about sporadic changes (e. g. transfer of personnel)?
- Who approves or confirms this?

Further topics:

- Reporting and audit

Further topics:

- Reporting and audit
- Identity matching

Further topics:

- Reporting and audit
- Identity matching
- IDs: ORCID, Edu-ID, identity card

Further topics:

- Reporting and audit
- Identity matching
- IDs: ORCID, Edu-ID, identity card
- Group management

Further topics:

- Reporting and audit
- Identity matching
- IDs: ORCID, Edu-ID, identity card
- Group management
- User selfservice

Further topics:

- Reporting and audit
- Identity matching
- IDs: ORCID, Edu-ID, identity card
- Group management
- User selfservice
- Password management

Further topics:

- Reporting and audit
- Identity matching
- IDs: ORCID, Edu-ID, identity card
- Group management
- User selfservice
- Password management
- Authentication techniques

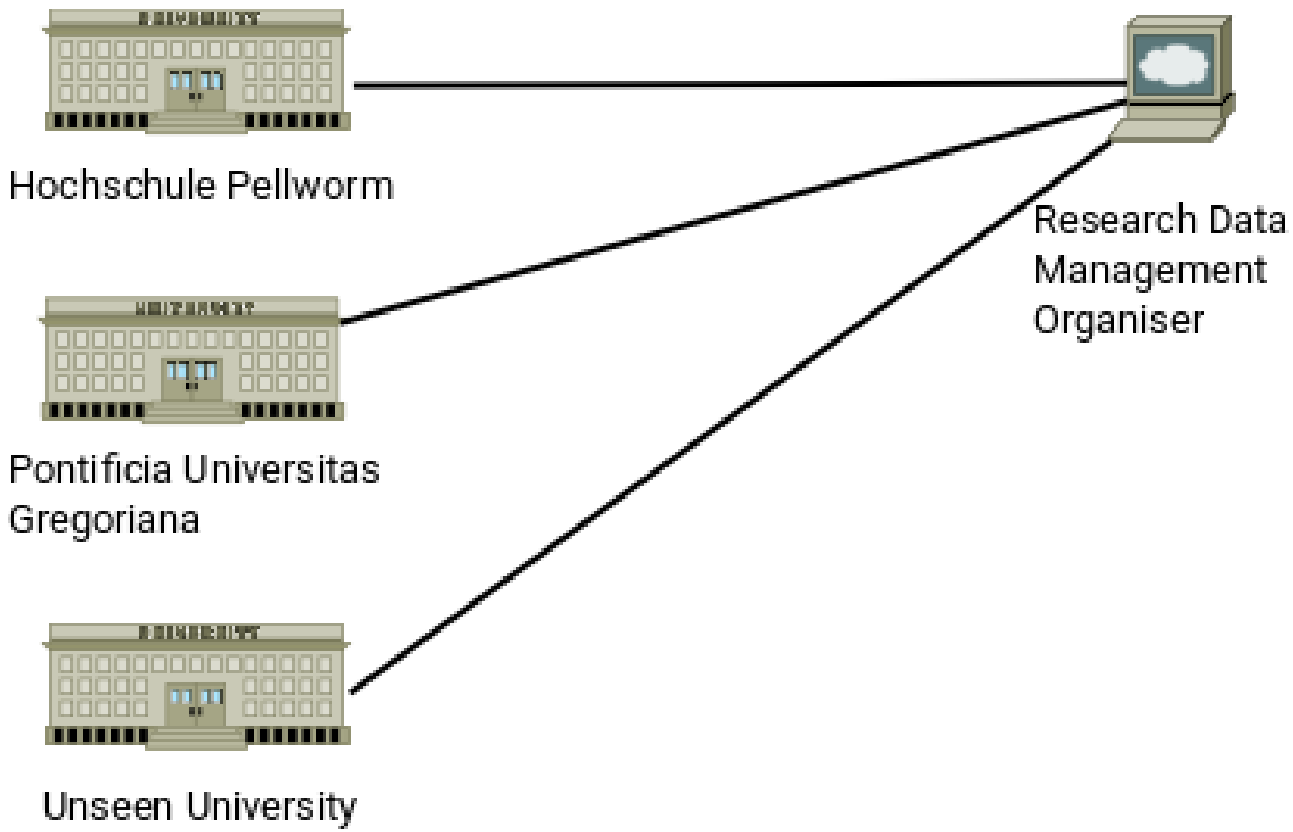
Further topics:

- Reporting and audit
- Identity matching
- IDs: ORCID, Edu-ID, identity card
- Group management
- User selfservice
- Password management
- Authentication techniques
- Single sign on

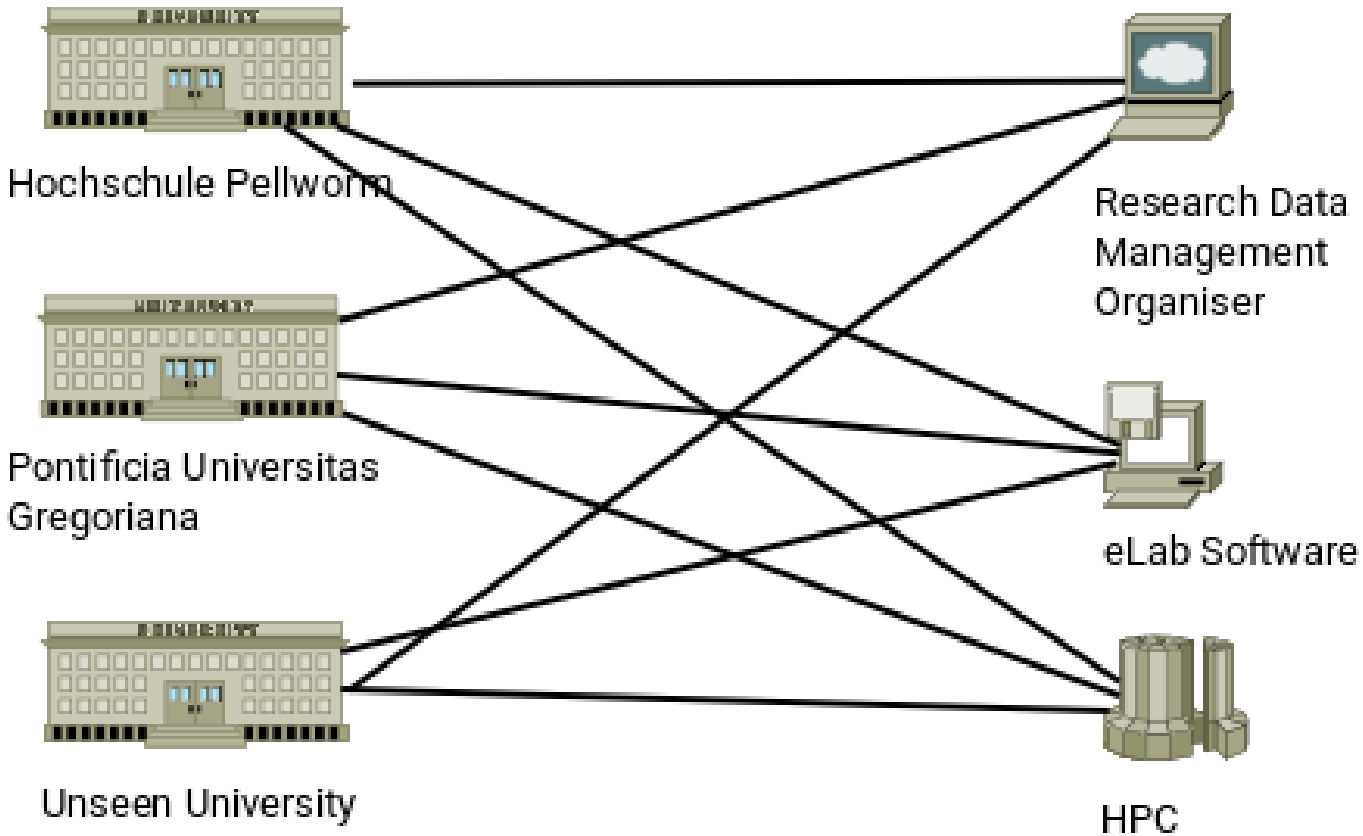
Further topics:

- Reporting and audit
- Identity matching
- IDs: ORCID, Edu-ID, identity card
- Group management
- User selfservice
- Password management
- Authentication techniques
- Single sign on
- Federated services

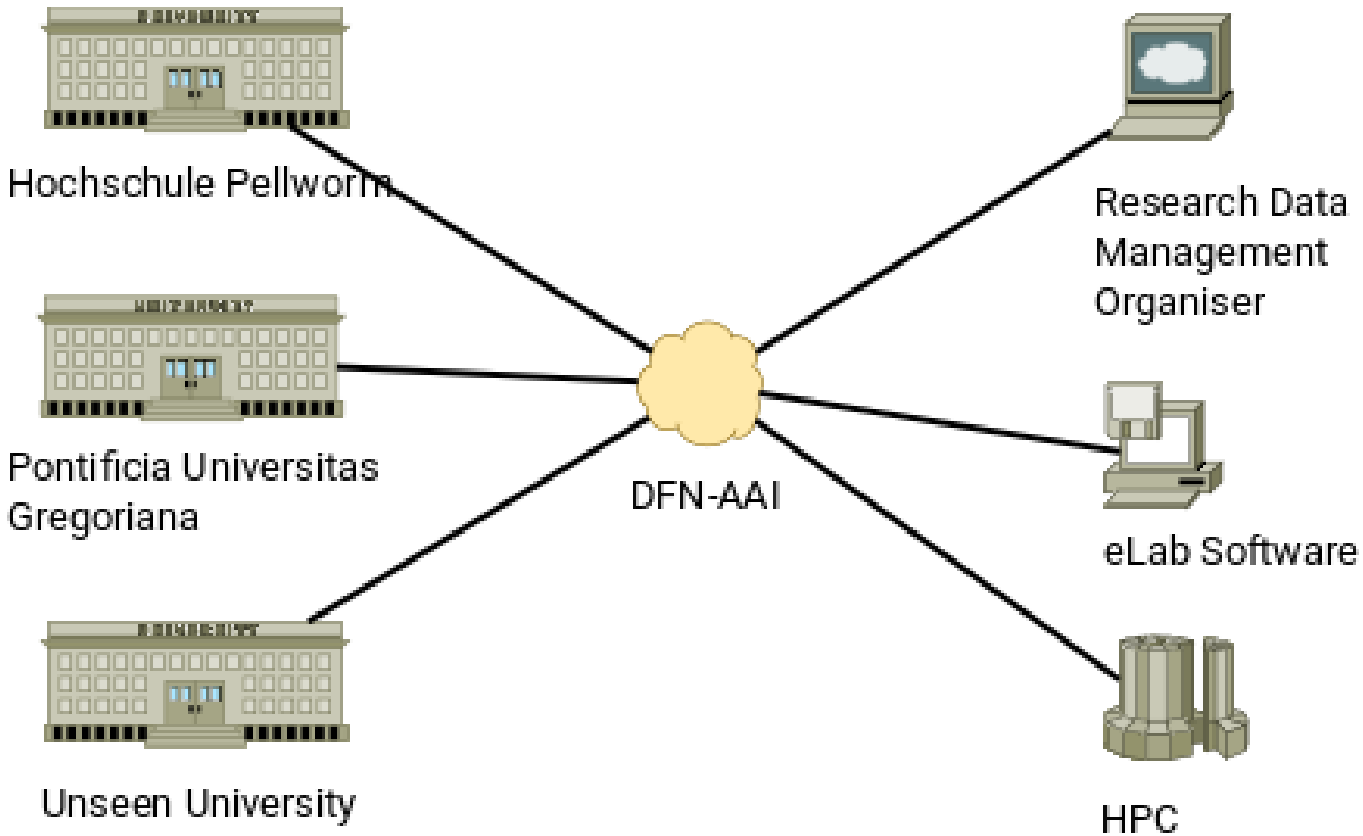
Federated Service



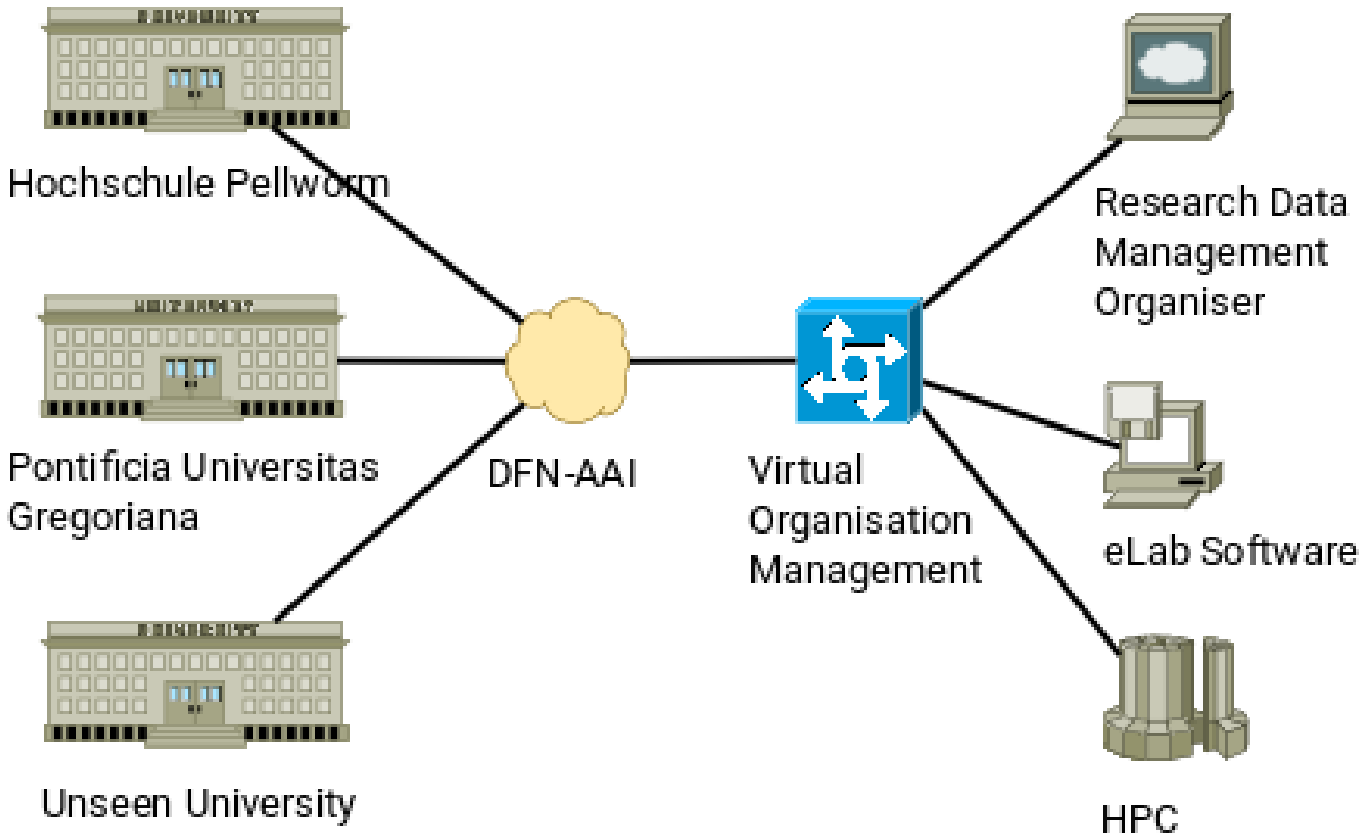
More Federated Services



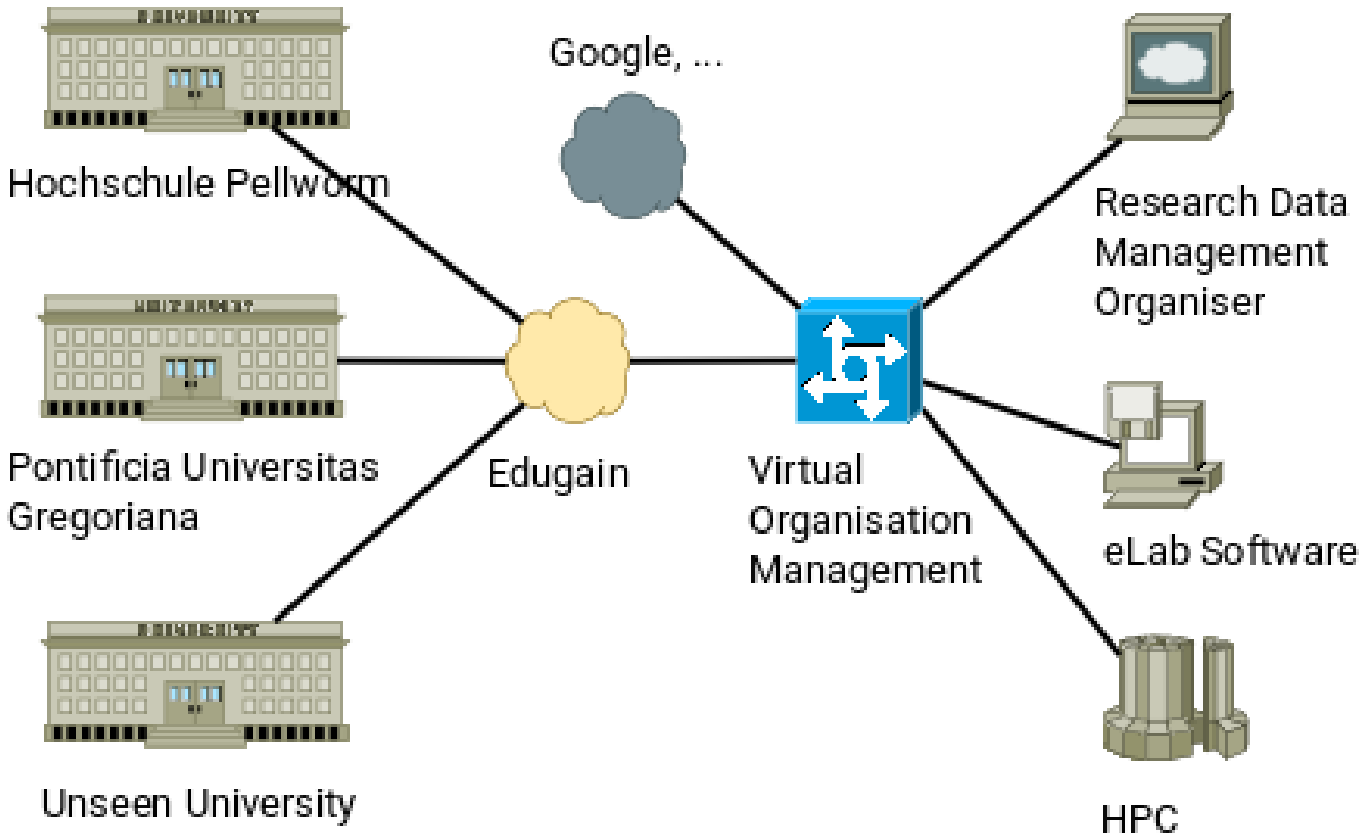
Use the DFN-AAI!



You might need a Community AAI



You might need a Community AAI



Why you might need a Community AAI

- To include users not belonging to German universities

Why you might need a Community AAI

- To include users not belonging to German universities
- To manage membership of the community

Why you might need a Community AAI

- To include users not belonging to German universities
- To manage membership of the community
- To centralize management of similar roles and rights for several services

Why you might need a Community AAI

- To include users not belonging to German universities
- To manage membership of the community
- To centralize management of similar roles and rights for several services
- To connect services that use different protocols
  (SAML ↔ OAuth/OIDC)

Things to consider in a Community IdM

- How to match identities coming simultaneously from several sources (Home-IdP, Google, ORCID, . . .):
  Do you need more attributes than the name?

Things to consider in a Community IdM

- How to match identities coming simultaneously from several sources (Home-IdP, Google, ORCID, . . .):
  Do you need more attributes than the name?
- What roles do you need for community management?

Things to consider in a Community IdM

- How to match identities coming simultaneously from several sources (Home-IdP, Google, ORCID, . . .):
  Do you need more attributes than the name?
- What roles do you need for community management?
- Who decides who gets which role?
  And is there a substitute for the decision maker, e. g. during holidays?

Things to consider in a Community IdM

- How to match identities coming simultaneously from several sources (Home-IdP, Google, ORCID, . . .):
  Do you need more attributes than the name?
- What roles do you need for community management?
- Who decides who gets which role?
  And is there a substitute for the decision maker, e. g. during holidays?
- What attributes about the user do you need to do authorization?
  Where do you get these attributes from?

Things to consider in a Community IdM

- How to match identities coming simultaneously from several sources (Home-IdP, Google, ORCID, . . .):
  Do you need more attributes than the name?
- What roles do you need for community management?
- Who decides who gets which role?
  And is there a substitute for the decision maker, e. g. during holidays?
- What attributes about the user do you need to do authorization?
  Where do you get these attributes from?
- Do you need reporting or audit features about events concerning a user?

Things to consider in a Community IdM

- How to match identities coming simultaneously from several sources (Home-IdP, Google, ORCID, . . .):
  Do you need more attributes than the name?
- What roles do you need for community management?
- Who decides who gets which role?
  And is there a substitute for the decision maker, e. g. during holidays?
- What attributes about the user do you need to do authorization?
  Where do you get these attributes from?
- Do you need reporting or audit features about events concerning a user?
- Deprovisioning: How do you know when to delete a user?
  And what happens to their data?