EduKEEP

Towards a User-Centric Identity Management Model

Maarten Kremers

Task Leader Trust and Identity Technology Development,
GN4-2 Project

Technical Product Manager, SURFnet, The Netherlands

NDN2016, Helsinki

22nd September 2016

Trend: The networked individual

- From local to global individual
- Increased mobility
- Anytime, anyplace
- Fragmentation, individual as part of multiple networks

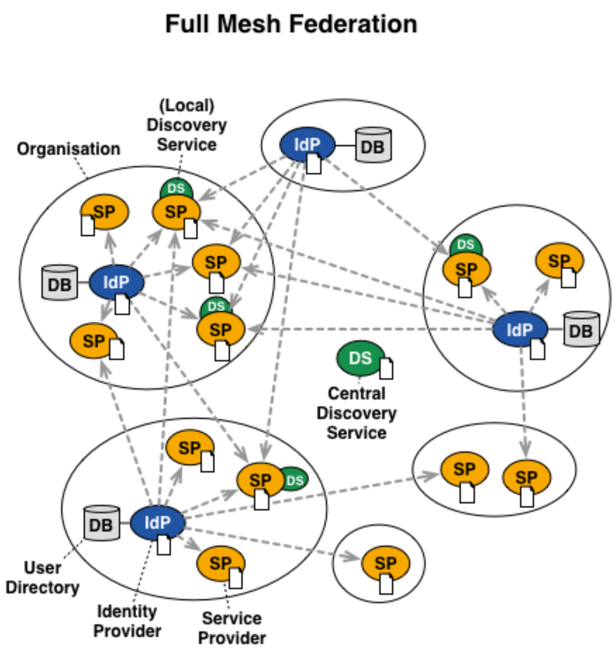
Also in Research and Education world

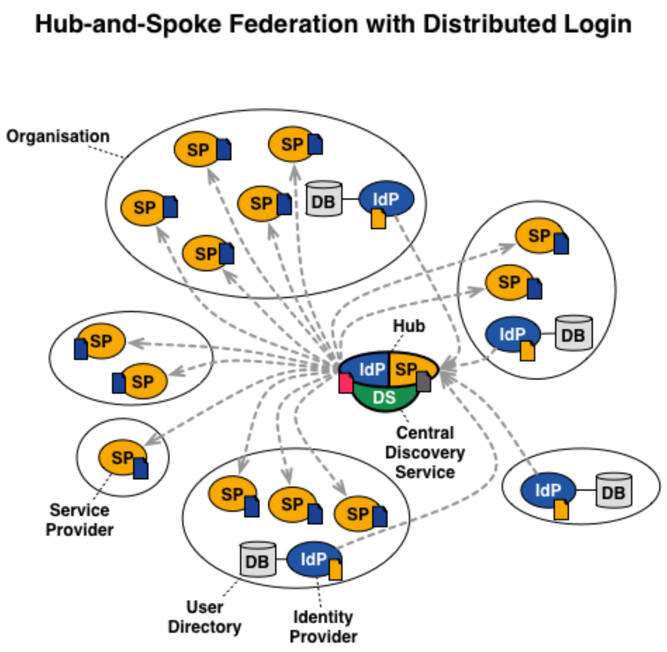
- Students: Building own curriculum, Life long learning
- Researcher: part of multiple research communities

Current Identity Management in the R&E Space: Organisation Centric

Most, if not all Identity Federations within eduGAIN manage users in an organisation centric way

Current Identity Management in the R&E Space: Organisation-Centric





Identity Management Lifecycle and Authentication is managed at each organisation

Issues with the Organisation-centric Identity Model

- The digital identity of an individual is linked to the membership with a specific organisation:
  → The former digital identity is destroyed when changing universities
  a new digital identify is created

- Digital identities are mostly restricted to individuals who are a member of an organization of the federation:
  → does not well support trusted interactions with external parties (projects)

- Life-long and flexible learning: A student can have concurrent, overlapping, intermittent relationships with educational organisations:
  → digital identities being created and destroyed many times, creates
  confusion, inefficiency

Issues with the Organisation-centric Identity Model

- Creating digital identities from scratch
  → Multiple identities are created for the same individual, which do not relate to each other & inefficient

- No support for services addressing individuals for periods extending beyond the relationship with a particular organisation
  → E-portfolio services, filestorage services

- Multiple concurrent affiliations (researchers and lecturers)
  → Multiple, concurrent, unlinked (even unliked or unwanted) identities

The EduKEEP architecture aims at transforming current Identity Federations to provide a user-centric approach for managing digital identities, that will bring user experience and simplicity of use at the heart of its processes

Starting Points User-Centric Identity Management Model

- Split Authentication and Authorisation (Attributes, Groups, Entitlements)
- Persistent Digital Identity:
  Same ‘identifier’ over time
- Longevity
  Make the identity reusable instead of the the lifetime of a specific role → Attributes will changes over time for one identity (e.g. affiliation)
- Inclusiveness
  To include individuals who are not (currently) affiliated with an organisation

Starting Points User-Centric Identity Management Model

- Low and high quality identities:

  To lower the entry burden for individuals accessing resources without high demands on quality → self-asserted basic attributes

  increase quality as needed → Enrich the identity with institutional attributes, increase LoA via vetting procedures

- Possibly build on eGov / eIDAS / BankID initiatives

- Service Provider can be a university, VO, Third Party, Cross-Sector

Implementations in progress

- SWITCH → EduID
  Central user-centric IdP, enriching identities with attributes from other sources

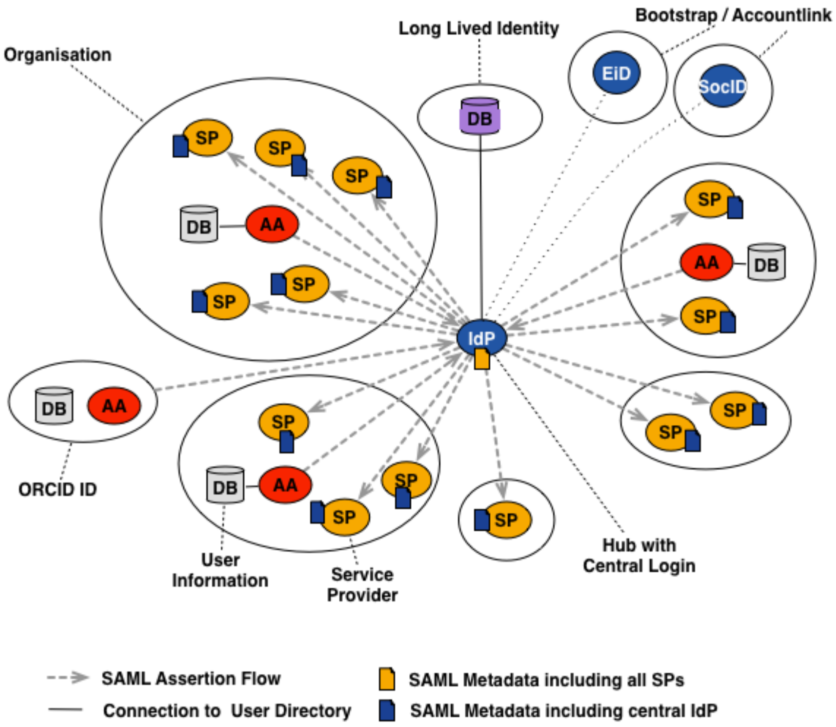
- SUNET → EduID
  Central user-centric IdP to bootstrap institutional processes

- GARR → eGOV ID
  Using a governmental ID to login

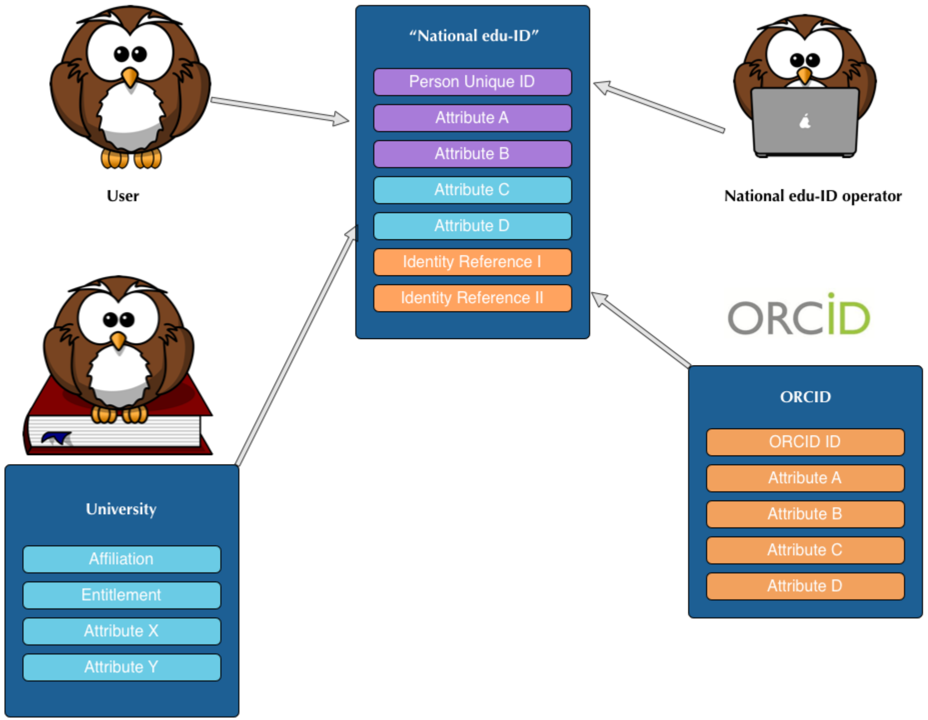
One architecture highlighted

- Central user-centric IdP, enriching identities with attributes from other sources
- Implemented by SWITCH in Switzerland

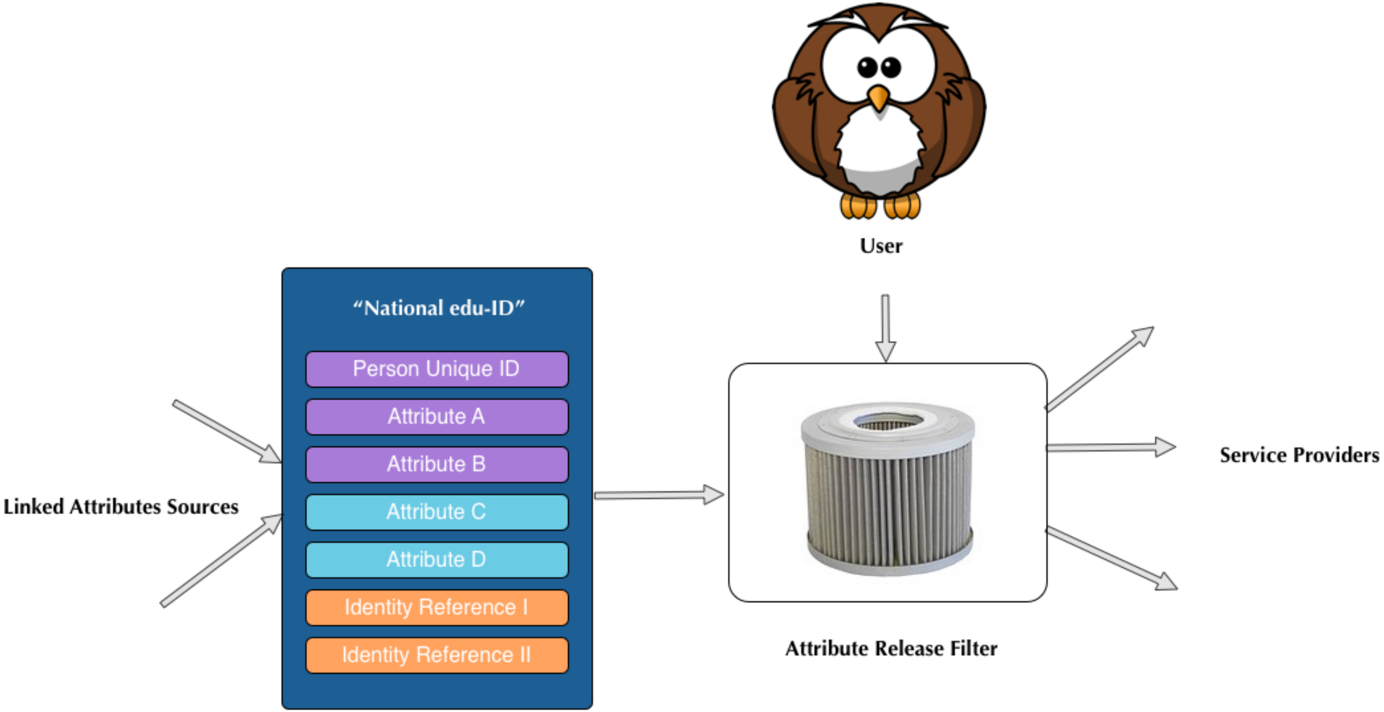
Architecture



Architecture



Architecture



Architecture

- Long-lived Identity
  - Self-serviced core attributes (name, addresses)
  - Attributes provided by organizations (Role, Entitlement), external providers (e.g. ORCID)

- Personal responsibilities of individuals
  - Create identity and / or link identities
  - Give consent about usage of personal attributes
  - Attribute maintenance (Core attributes)

Architecture

- Protocols behind the hub / gateway, invisible to the SPs, can be a hybrid mix (SAML AA, OpenID connect, …)

- Protocols towards the SP will SAML now, can be a hybrid mix in future (OpenID Connect)

- Possible / optional
  - LoA enrichment
  - eID
  - Social ID link / bootstrap

Use Cases / Benefits

- Pre-registration / Alumni / Lifelong learners

  → One identity for it all: LMS, e-portfolio, same identity when pre-register, you become an alumni and/or join another university

- Researchers

  → One identity in concurrent projects, multiple affiliations and for all publication work (with help of ORCID and friends)

- Teachers

  → One identity for interacting with their learners across multiple universities

- Third party Services

  → Supports longer-term client-relationship. Offerings and conditions can be based on attributes and affiliations available at given time (e.g. file storage)

Risk / Disadvantages

- Central Operations
- Security
- Critical process

Other aspects

- Legal implications & Policy
- Financial model / implications
- Government model

More information

High Level Architecture document

https://wiki.geant.org/display/gn41jra3/Task+1+-+Attributes+and+Authorisations

Best Practices for User Centric Federated Identity

What's out there, Architecture, Policy, Interfederation

Pilots

Next Steps

https://wiki.geant.org/display/gn42jra3/T3.1B+User-centric+identity+federation


EduKEEP
CALM
AND
ENJOY
#NDN2016

Maarten Kremers
maarten.kremers@surfnet.nl

GÉANT

Networks · Services · People
www.geant.org

This work is part of a project that has applied for funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No. 691567 (GN4-1).