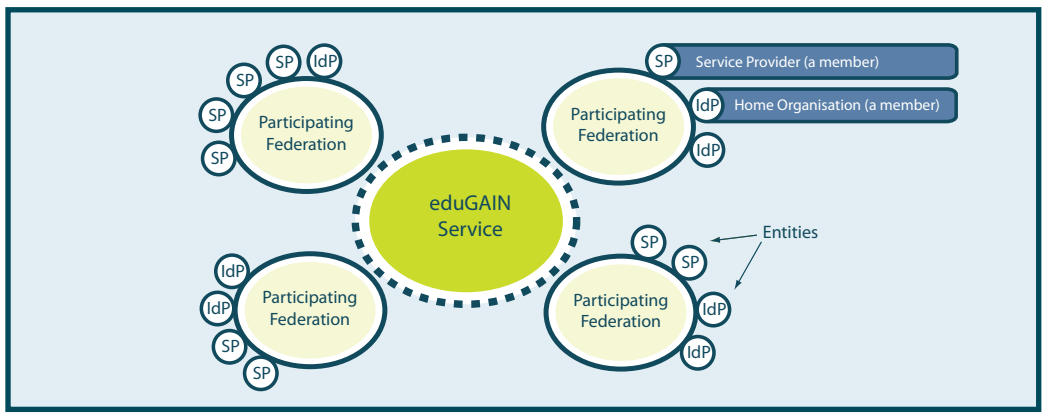
Federating GN3 Services

GÉANT

connect • communicate • collaborate

1 A Federated Environment

- Enables integration in the identity management realm, by allowing organisations to share identity information across their respective security domains.
- A trust relationship between a service provider (SP) and an identity provider (IdP), which allows an end user to use a single federated identity.



2 Motivation

- A fully functional federation required to federate GÉANT services.
- Federation incurs high overheads.
- Connecting GÉANT services to IDPs directly feasible but not scalable.
- Needed a quick and simple solution.

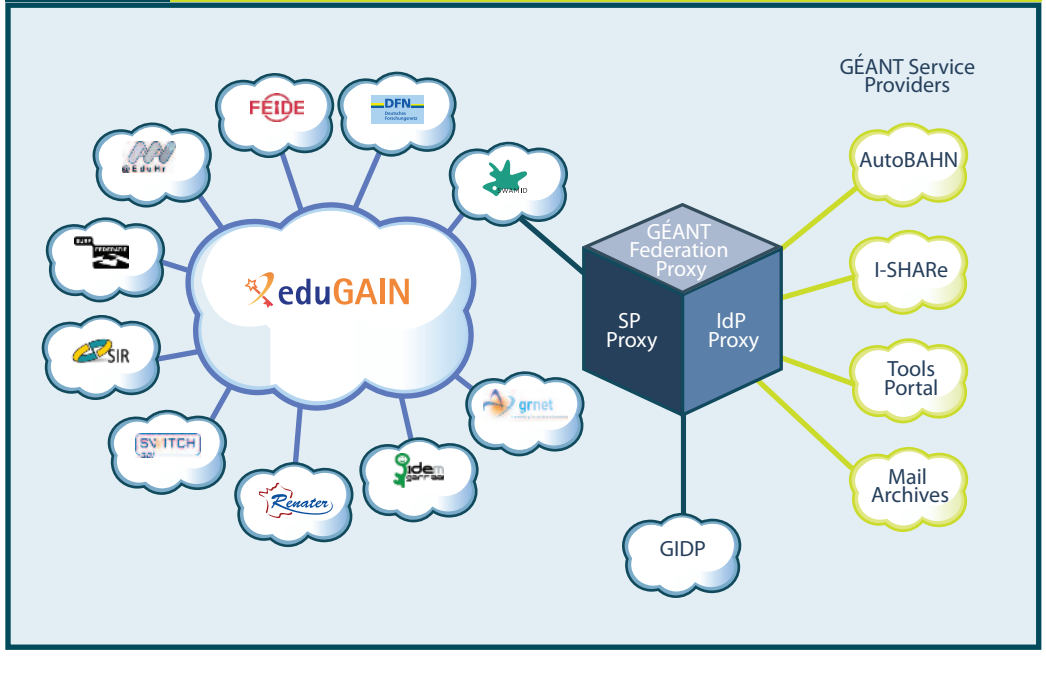
3 Proposed Solution

- Use of existing GÉANT (GN3) Partners' federation to join eduGAIN via Federation Proxy
  - Swedish Academic Identity (SWAMID)
  - Implemented GÉANT Federation Proxy using simpleSAMLphp
  - Provides a DiscoJuice based discovery service.

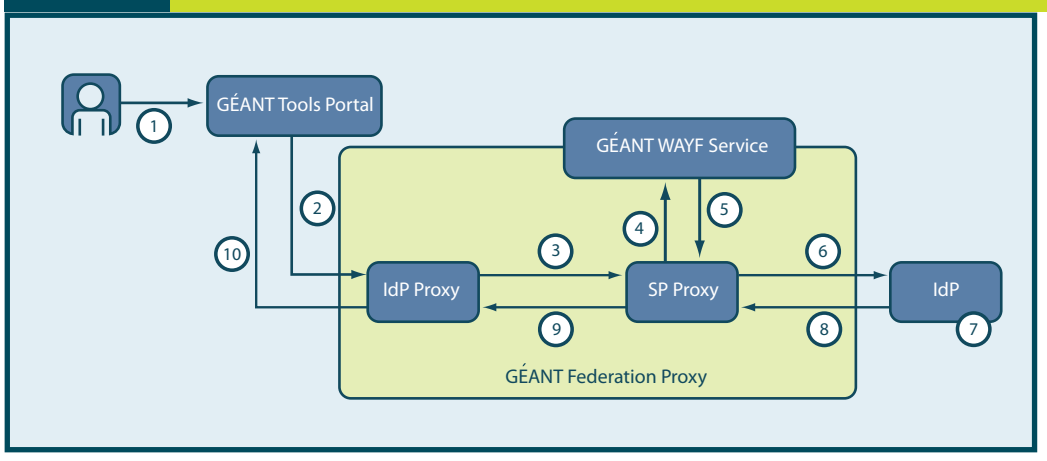
4 GÉANT Federation Proxy

- Acts as a bridge between SPs and IdPs
- Has two aspects:
  - IdP Proxy
    - Seen as an IdP for SPs
    - SPs consumes only the IdP Proxy's metadata of Federation Proxy
    - All authentication queries from SPs relayed to Federation Proxy
    - SPs does not use its own discovery service
  - SP Proxy
    - Seen as a SP for federation
    - Federation publishes SP Proxy's metadata
- Publishes the list of common required and optional attributes for all its SPs.
- Allow access to all SPs behind it by IdPs that consume federation's metadata.

5 Architecture



6 Sequence Diagram



1. User sends request to access the service
2. Service forwards request to IdP Proxy of the GÉANT Federation Proxy, assuming it's the IdP
3. IdP Proxy forwards request to SP Proxy of the GÉANT Federation Proxy .
4. SP Proxy forwards request to GÉANT WAYF service that presents list of available IdPs to the user.
5. Selected IdP is forwarded back to the SP Proxy
6. SP Proxy, who will act as a SP to the chosen IdP in further interactions, forwards authentication request to the IdP
7. IdP performs authentication
8. IdP sends the signed assertion back to the SP Proxy.
9. SP Proxy forwards contents of assertion back to the IdP Proxy.
10. IdP Proxy creates signed assertion and sends back to the SP.

7 Advantages

- Easy to implement
- Scalable Approach
- Avoids writing federation policy and approvals.
- Centralised WAYF service
- Quickly Federates Service into eduGAIN
- Access to GÉANT Services via GIdP for those not yet connected to eduGAIN

DANTE
www.dante.net

For Further information please contact:
- **Mandeep Saini,** *DANTE*, mandeep.saini@dante.net
- **Brook Schofield,** *TERENA*, schofield@terena.org
- **Maja Wolniewicz,** *UMK*, mgw@umk.pl

www.geant.net

This poster has been produced with the financial assistance of the European Union. The contents of this document are the sole responsibility of DANTE and can under no circumstances be regarded as reflecting the position of the European Union