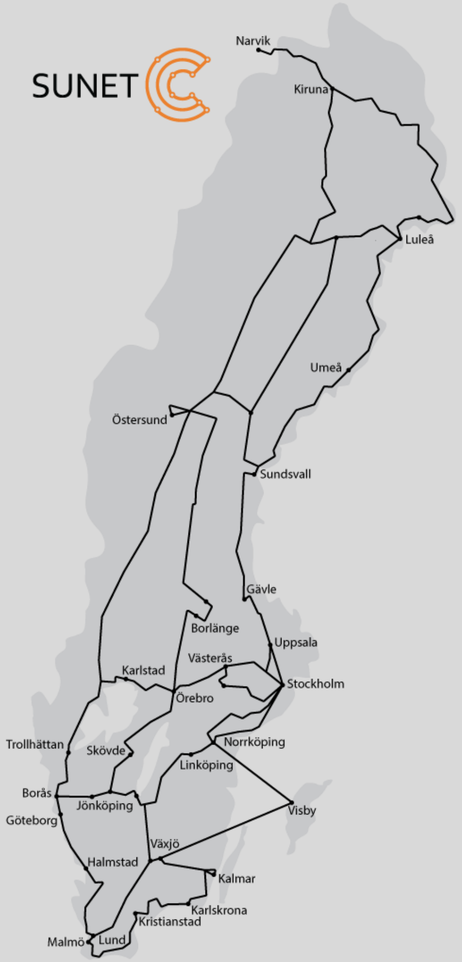
SWAMID

The Swedish Academic Identity Federation

Pål Axelsson, Sunet
pax@sunet.se

SUNET – The Swedish NREN

- SUNET is bringing services to higher educational institutions, other research organisations, national museums, the national library and higher research and educational support governmental agencies
  - Network connectivity together with the identity federation is the infrastructure
  - On top of the infrastructure Sunet delivers a wide range of vital research and educational services (at self-cost pricing) such as video conferencing, media services, learning management systems and cloud services

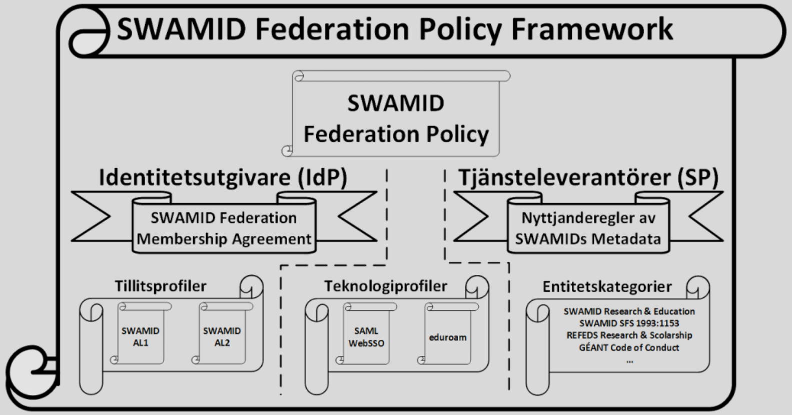


SWAMID – Use institutional accounts outside the institution

SWAMID

- SWAMID is a community, a policy framework and a technical implementation that helps students, researchers and educators to use their home organisation accounts locally, nationally and internationally
  - Webbased services via multilateral SAML identity federation
  - Home for the Swedish branch of eduroam
- 57 member organisations (49 SAML2 and 55 eduroam)
- SWAMID is goverend by SWAMID Board of Trustees
  - 4 university CIOs, 2 representatives for student services, 2 representatives for research infrastructures and one Sunet
- SWAMID is included in the organisational SUNET fee

SWAMID Federation Policy Framework



- The policy framework is defined in the SWAMID Federation Policy
  - In the SWAMID Federation Policy all responsibilities of the different parties are defined
  - In the Identity Assurance Profiles organisational behaviour of the Identity Provider is defined including autentication techniques and user identity proofing
  - In the Technology Profiles the technical behaviour of the multilateral SAML and eduroam is currently defined

SWAMID Identity Assurance Profiles

SWAMID

- SWAMID Identity Assurance Level 1 Profile
  - It’s a natural person
  - Password or multi-factor authentication
- SWAMID Identity Assurance Level 2 Profile
  - It’s a defined natural person
  - Password or multi-factor authentication
- A new identity assurance profile is under development for secure multi-factor authentication including high level of identity proofing (verified natural person)
- The SWAMID Identity Assurance Profiles are mappable to the different parts of the REFEDS Assurance Framework

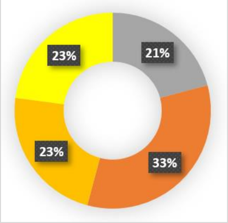
SWAMID Operations

SWAMID

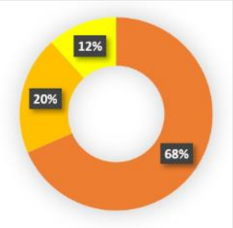
- SWAMID Operations is the daily operations
- SWAMID Operations is a distributed team of 10
  - 1 FTE SWAMID Operations Manager (Sunet)
  - 1 ½ FTE DevOp running the technical infrastructure (Sunet)
  - ~2 FTE distributed on 8 identity specialists from Swedish universities doing membership administration, metadata administration, policy development and technical support to entities
- SWAMID Operations is building and maintaining the SWAMID Community via workshops, webinars and mailing lists

SWAMID membership statistics

- Higher educational institutions (HEI) memberships
  - 16 HEI are certified for SWAMID Identity Assurance Profile 2
  - 11 HEI are certified for SWAMID Identity Assurance Profile 1
  - 11 HEI are not certified for any SWAMID Identity Assurance Profiles
  - 10 very small HEI are not members of SWAMID today due to that they don’t have the manpower nor the capabilities to run an Identity Provider



- There are more than 365000 students in Sweden (~3,6% of the Swedish population)
  - 250000 students has the possibility to be verified as SWAMID AL2
  - 323000 students has the possibility to be verified as SWAMID AL1



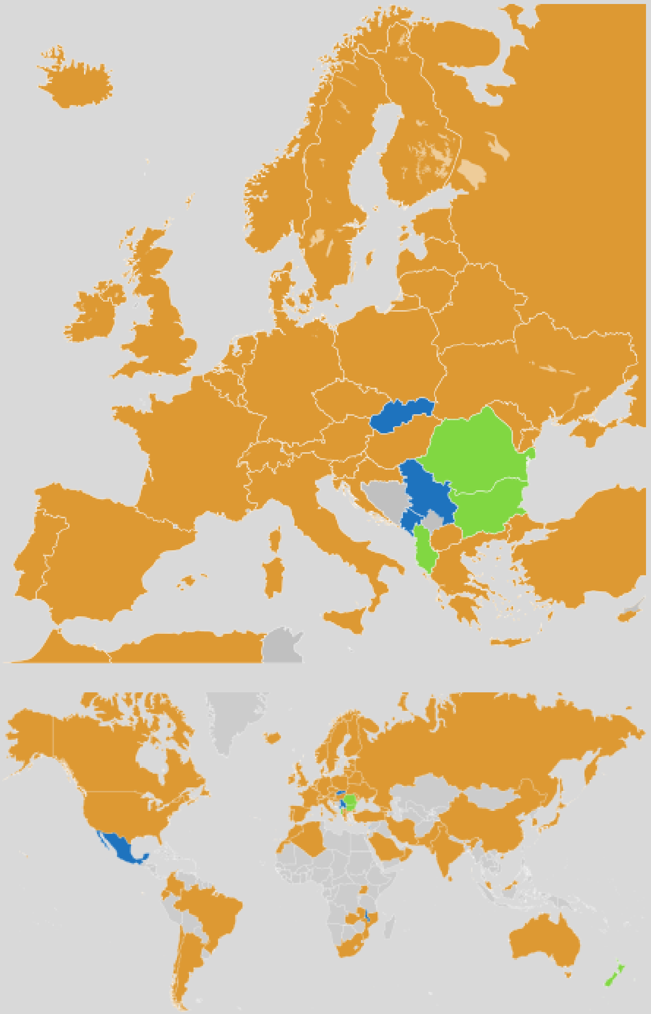
SWAMID for webbased services

SWAMID

- Standard based federation technology for multilateral federations
  - A full mesh SAML2 multilateral identity federation with a few hybrid solutions
  - OpenId Connect Federations is still under development
- Standard based attribute release based on entity categories and data minimalization
  - Login and standard attributes from home organisation identity provider via the entity categories REFEDS Research & Scholarship (R&S) and Géant Data protection Code of Conduct (CoCo)
  - Authorization attributes within the service or from an research infrastructure
- REFEDS community standards on multifactor login

SWAMID in an internationell context

- SWAMID is a member of the interfederation eduGAIN
  - 68 active academic federations
  - More than 3100 Identity Providers
  - More than 2600 Service Providers
  - Reaches over 27,000,000 students, researchers and educators
- Sister identity federations
  - FEIDE in Norway
  - Haka in Finland
  - WAYF in Denmark
  - …
  - https://technical.edugain.org/status



eduroam for wireless access

- SWAMID is the policy home for eduroam in Sweden
- SWAMID Operations is managing membership
- SUNET network operations team is running the technical infrastructure
- Member organisations normally uses the authentication mecanism PEAP-MSCHAPV2 due to EAP-TLS is to hard for end users to configure
- SUNET together with our Nordic neighbours in NORDUnet are working on a solution under the working name geteduroam where the users get TLS certificates onto their devices with help of operating system native tools
  - Certificates will be created on a web page were the user authenticate with the help of the SAML identity federation

eduID – A national identity provider

- A user centric identity management solution
- A fully functional baseline identity provider within SWAMID
  - Used by universities to technically onboard students
  - Used by users outside the SWAMID community to get access to services within the community
  - Used by users within the SWAMID community for access to services that demands functionality not supported by their home organisation
- Supports identity proofing based on SWAMIDs assurance profiles
- Supports high assurance multifactor

Identity Provider as a Service (IdPaaS)

- An Identity Provider solution for smaller organisations that don’t have the possibility to manage their own Identity Provider
- Adds an organisational layer on top of eduID
- Conceptually IdPaaS is a hybrid solution with an Identity Provider Proxy based on Satosa
  - User accounts managed in eduID
  - Organisational attributes for the user is managed in an organisational registry based on Comanage
  - Users are onboarded to the organisational registry with an invitation flow based on their eduID account

What makes an identity federation fly?

- Find services that all home organisations or users within them want to use
- Offer those services via the identity federation
- For all policy iteration find a new service

- Initial killer services in SWAMID
  - Video conferencing via Adobe Connect boosted the federation (superseded by Zoom)
  - International research access is the driving force behind eduGAIN
  - Ladok, a national system for study administrative processes, drives the adoption of SWAMID AL2
  - Student health systems drives the adoption of secure authentication

Questions, answers and more info!

Thank you for listening!

Pål Axelsson, SUNET/SWAMID

pax@sunet.se