Need of assurance within Sweden and international

Marina Adomeit, SUNET Fredrik Domeij, SWAMID/UmU

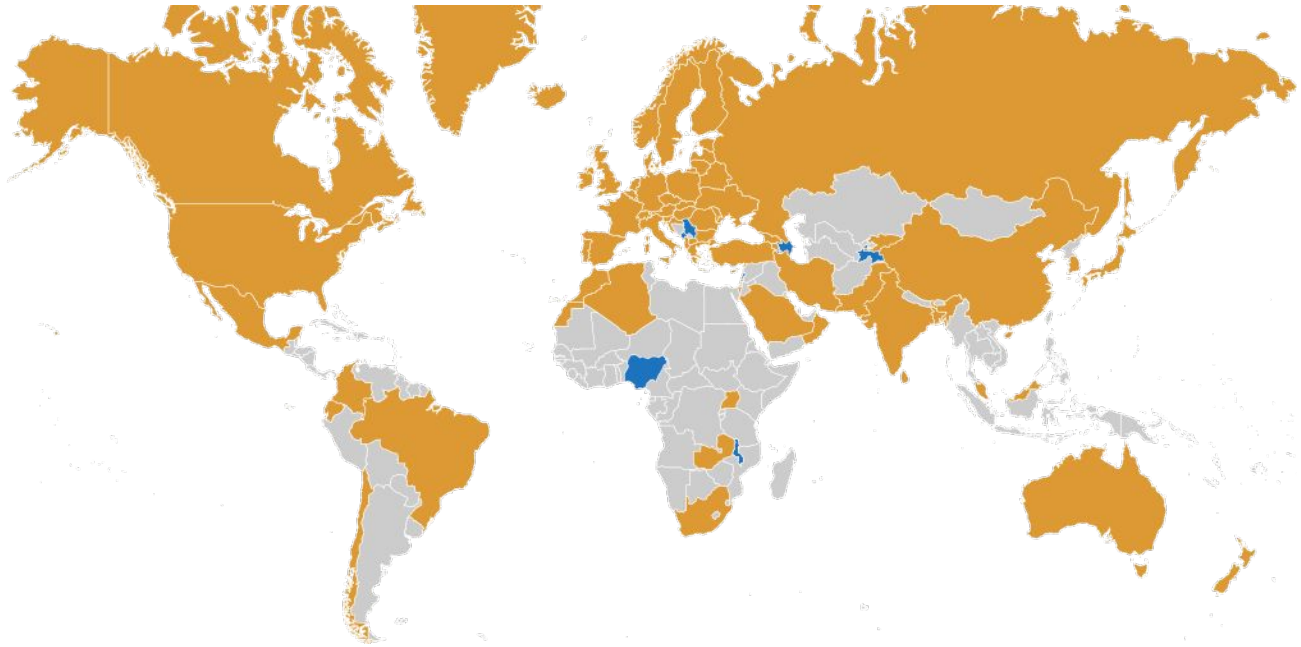
Sunetdagarna 13. October 2021

SWAMID

International use cases for assurance

SWAMID

International identity landscape



73 Identity Federations in global R&E space, but
- No common policy for identity management

International SPs require trustworthy identity and authentication
- Use cases in research: access to sensitive data, compute resources, collaboration services etc.

How do we express this thrust?
- By using REFEDS Assurance Framework

But why is this so hard?
- Research collaborations are usually spread across many institutions - hard to generate strong incentives for IdPs

International use cases for LoA

European Research Infrastructures

EOSC-Life

panosc
photon and neutron open science cloud

SSHOC
social sciences & humanities open cloud

ENVRI community

EUROfusion

ESCAPE
European Science Cluster of Astronomy & Particle physics ESFRI research infrastructures

High Performance Computing

FENIX
RESEARCH INFRASTRUCTURE

LUMI

PRACE

EuroHPC
Joint Undertaking

NIH
National Institutes of Health

★ Uses REFEDS Assurance Framework (RAF)

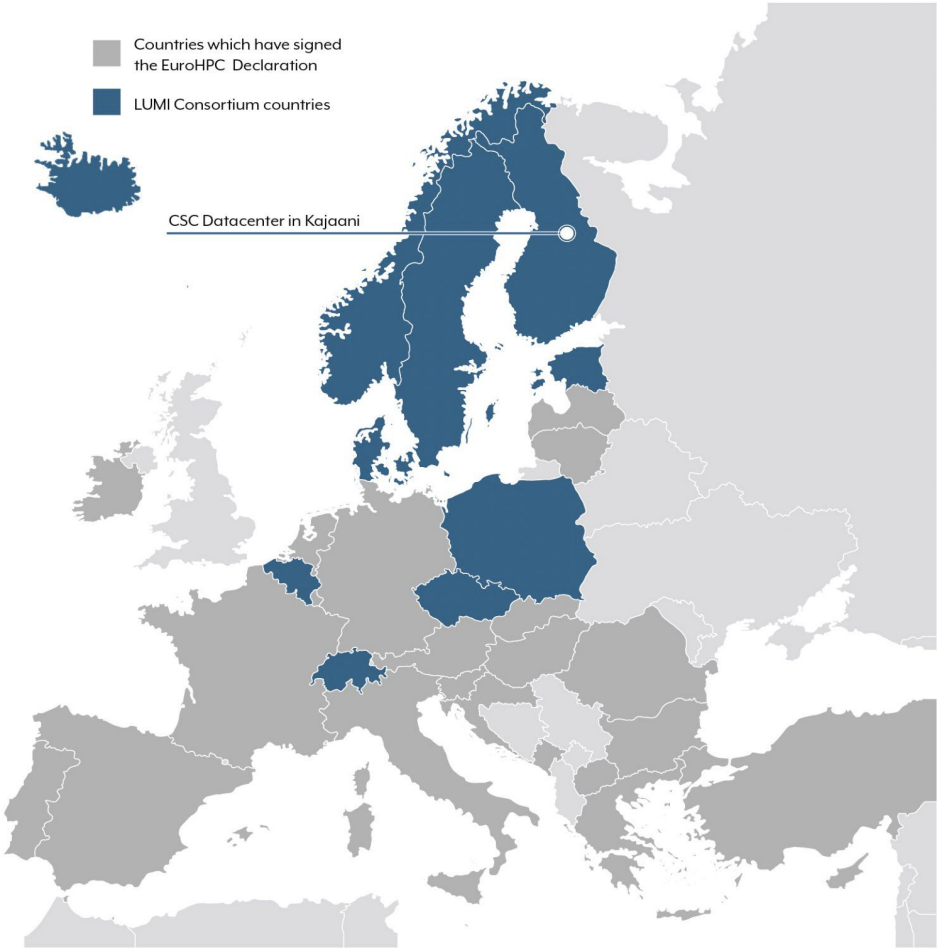
SWAMID

International use case for LoA

LUMI

- LUMI, one of the EuroHPC pre-exascale supercomputers, located at CSC's data centre in Kajaani, Finland
- The supercomputer will be hosted by the **ten European countries** of the LUMI consortium:

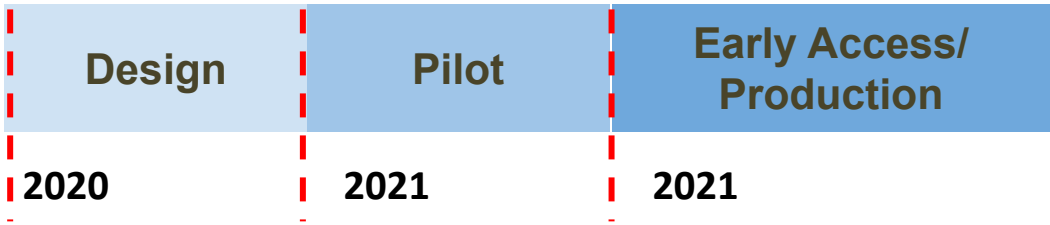
  Finland, Belgium, the Czech Republic, Denmark, Estonia, Iceland, Norway, Poland, Sweden, and Switzerland
- Bringing together their unique expertise and experience, these countries will together provide added value for the whole of Europe



SWAMID

Puhuri AAI

- Enable resource allocation and access to LUMI resources (and other services in future)
- Puhuri is funded by Neic and shall in future support other project from Nordic region
- Puhuri consists of:
  - Puhuri AAI services - controls access to resources
  - Puhuri Resource Allocation services - National and Puhuri provided portals



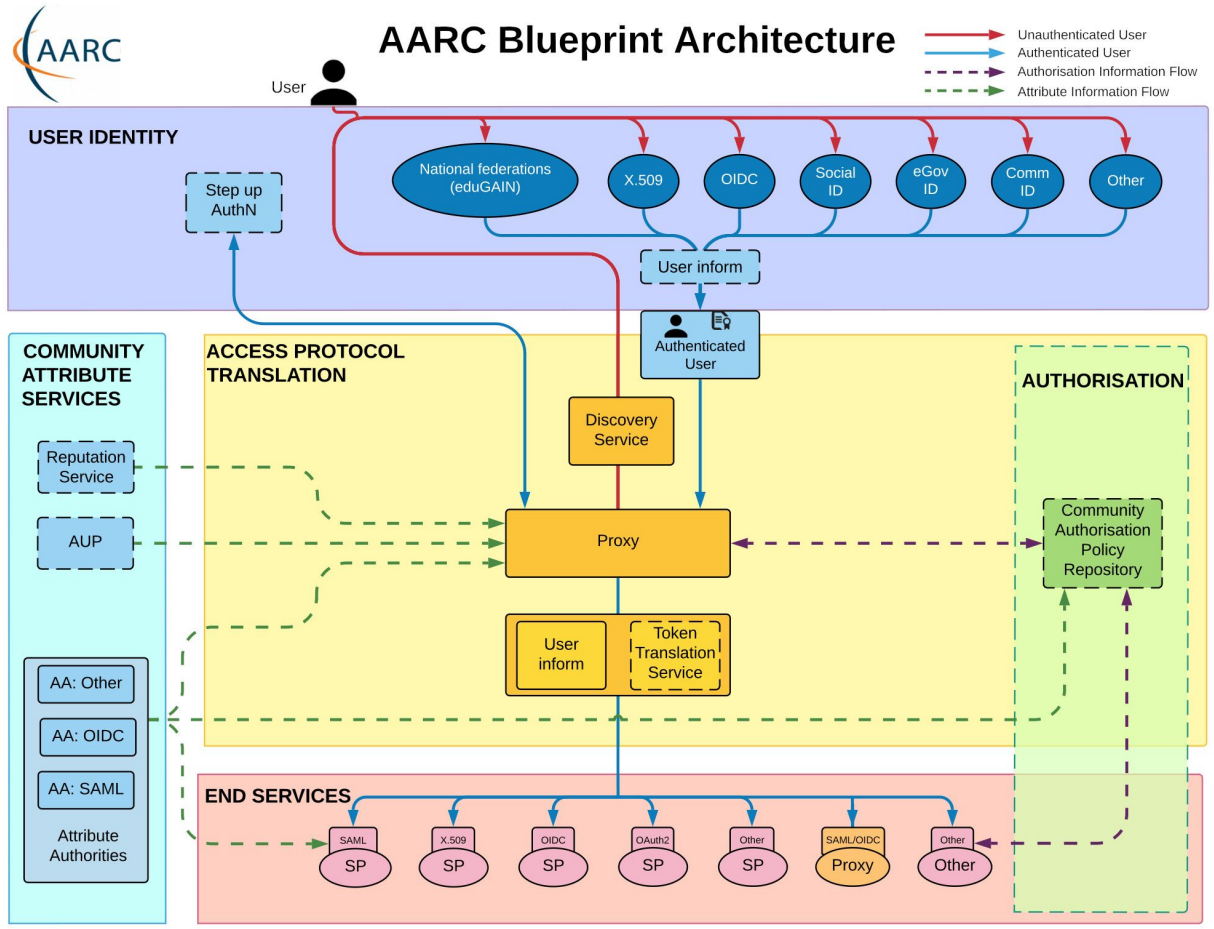
SWAMID

AARC Blueprint Architecture - BPA

Blueprint for Research Infrastructure (RI) AAIs

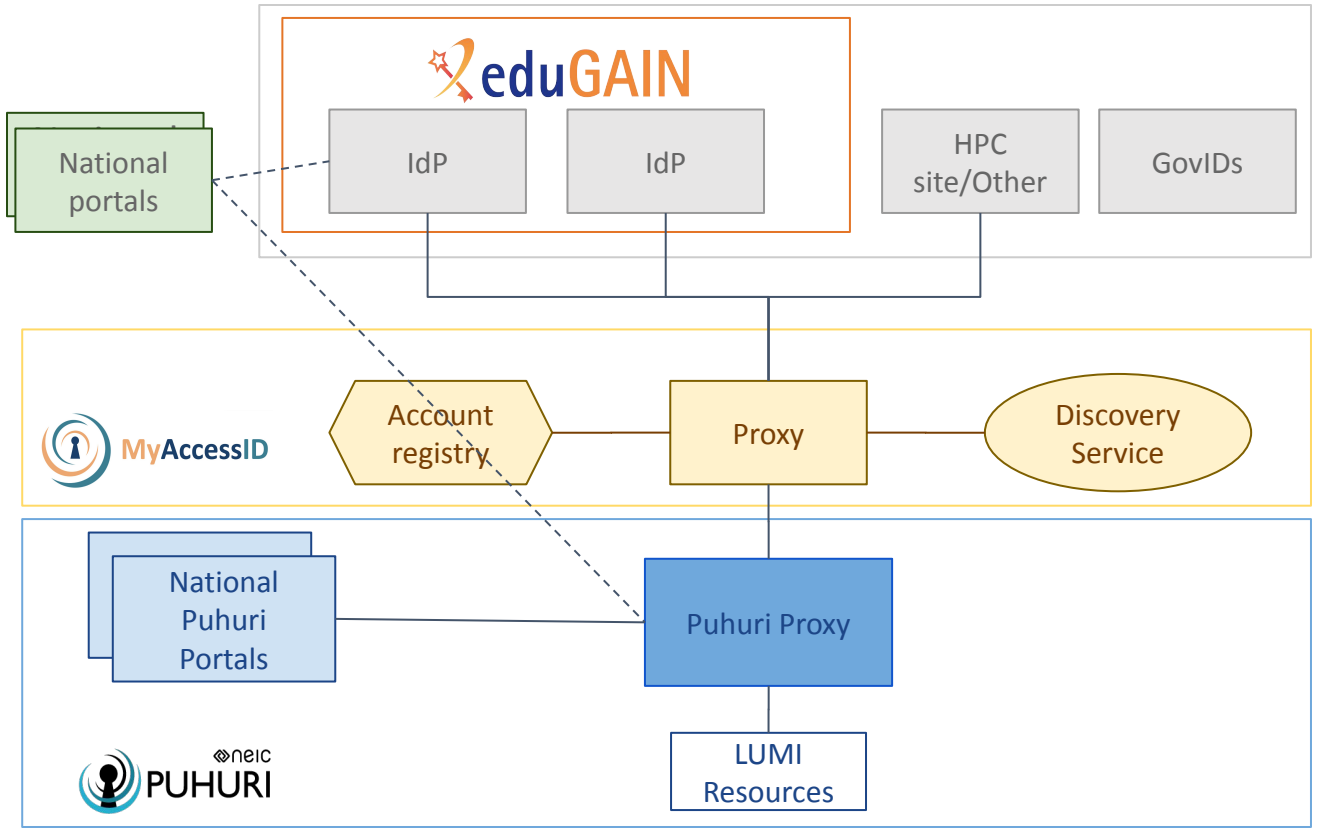
RI AAI Specifics:

- Manage roles and membership attributes that are in context of research collaboration
- Connect specific SPs in context of research collaboration via AAI Proxy
- Integrate eduGAIN and other IdPs
- Have trust requirements for IdPs



SWAMID

Puhuri AAI Architecture



SWAMID

This infrastructure will connect other services and infrastructures:

- Other services from Nordics will connect to PUHURI
- Other infrastructures will connect their domains to MyAccessID
- Will rely on LoA to trust different IdP sources

Simplifies researcher access to services and resources from different providers

Level of Assurance - Vectors of Trust

- How much SPs ought to trust the assertions made by the Identity Providers
- There are several vectors of trust
- **According to REFEDS Assurance** suite https://wiki.refeds.org/display/ASS :
  - **Identity Assurance**, that talks about quality and trustworthiness of the identity, and
  - **Authentication Assurance**, that talks about quality and trustworthiness of the authentication method.

SWAMID

Puhuri LoA requirements

https://refeds.org/assurance/ID/UNIQUE; or

https://refeds.org/assurance/ID/eppn-unique-no-reassign

https://refeds.org/assurance/IAP/medium; or

https://refeds.org/assurance/IAP/high

https://refeds.org/profile/mfa for access to certain resources, or to be able to perform certain functions or actions

SWAMID

Puhuri Status

- All infrastructure is production ready - currently in Pilot/EarlyAccess
- Integration of IdPs:
    - Integration of federated IdPs done via eduGAIN
    - Direct integration of IdPs per request
    - All IdPs need to fulfill minimum requirements
        - Attributes
        - LoA will become mandatory in 2022
        - SP to test attribute release https://myaccessid.devtest.eduteams.org/
- Collaboration with other research infrastructures using MyAccessID to harmonise LoA requirements as possible

SWAMID

National use cases for assurance

SWAMID

SWAMID Identity Assurance Profiles

https://wiki.sunet.se/display/SWAMID/SWAMID+Policy

Tillitsnivå	Vad vet vi	Lägsta identifieringsnivå	Attribut	MFA
SWAMID AL1	En person	Har klarat en CAPTCHA	Självuppgivna	Tillåts
SWAMID AL2	Bekräftad person	Har fått PIN-kod till sin folkbokföringsadress	Kontrollerade mot andra system, ex. personnummer	Tillåts
SWAMID AL3	Verifierad person	Har uppvisat legitimation för betrodd part	Kontrollerade mot andra system, ex. personnummer	Alltid

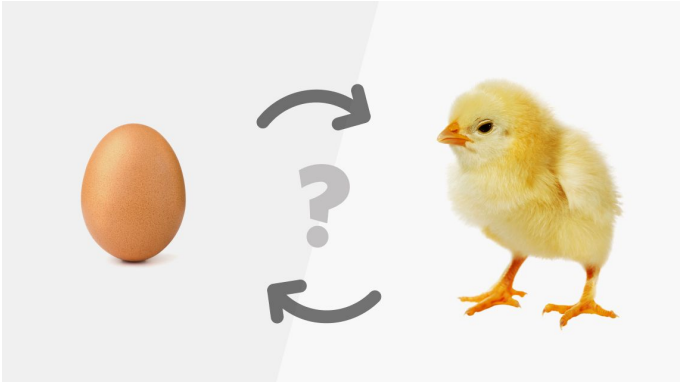
SWAMID

Tillitsnivåer för medlemmar i SWAMID

SWAMID har idag 56 identitetsutfärdare (IdP:er) för WebSSO

Tillitsnivå	Godkända idag	Förväntat i slutet av Q1 2022
ingen	6	0
SWAMID AL1	13	19 (minimikrav 2022-01-01)
SWAMID AL2	30	32
SWAMID AL3	3 (AL2-MFA-HI idag)	5

- Tjänster vill ha tillförlitliga identiteter, men kan inte kräva det innan identitetsutfärdare kan leverera dem
- Identitetsutfärdare har lågt incitament för att implementera tillförlitligare identiteter innan tjänster kräver det
- Kostnad för identitetsutfärdare - Nytta för tjänster



SWAMID

Användning av SWAMIDs tillitsnivåer

Kontoaktiveringsportaler

- Alla kontoaktiveringsportaler (för SWAMID AL2) kräver SWAMID AL2

Nationellt administration- och informationssystem för samordnare

- Nais kräver SWAMID AL2-MFA-HI (snart SWAMID AL3)

Ladok

- Lärosäten får själva välja krav på tillitsnivå
- Ladokkonsortiets rekommendation är att lärosätet:
  - Ser till att lyfta upp alla sina användare som använder Ladok till SWAMID AL2-nivå
  - Konfigurerar Ladok så att SWAMID AL2 krävs för inloggning för personal mot det egna lärosätet
  - Ser till att lärosätet implementerar och blir godkänt för SWAMID AL3
  - Konfigurerar Ladok så att SWAMID AL3 krävs för alla extra känsliga aktiviteter i Ladok (ex. attestering av resultat, utfärdande av examen)
  - Konfigurerar Ladok så att SWAMID AL2 krävs för inloggning för studenter med svenskt personnummer

SWAMID

REFEDS Assurance Framework (RAF)

https://refeds.org/assurance

- Gemensamt ramverk för tillitssignalering inom eduGAIN
- Tre nivåer - uppfylls av SWAMIDs AL-nivåer
  - **low** - SWAMID AL1 (obekräftad)
  - **medium** - SWAMID AL2 (bekräftad)
  - **high** - SWAMID AL3 (verifierad)
  - **local-enterprise** - “Vi litar tillräckligt på identitetshanteringen för tillgång till lokala system”
- Ytterligare identifierare för att signalera andra egenskaper
  - **unique** - Kommer aldrig att återanvändas för annan person
  - **eppn-unique-no-reassign** - eduPersonPrincipalName återanvänds ej
  - **ePA-1m** - eduPersonAffiliation uppdateras inom en månad

Dessa följer av SWAMIDs tillitsprofiler och kommande WebSSO-profil.

SWAMID

REFEDS Assurance Framework (RAF)

RAF har även två tillitsprofiler där nivåer och övriga identifierare kombineras:

Cappuccino

- unique
- medium
- ePA-1m

Espresso

- unique
- high
- ePA-1m

SWAMID

Signalering av tillitsnivå i SWAMID

- RAF har lägre krav än SWAMIDs tillitsnivåer
- Det gör att direktöversättning är möjlig (men inte åt andra hållet)
- Vid signalering av tillitsnivå i SWAMID ska även RAF signaleras

https://wiki.sunet.se/x/94A_Bg

SWAMID AL1

eduPersonAssurance
- http://www.swamid.se/policy/assurance/al1
- https://refeds.org/assurance
- https://refeds.org/assurance/ID/unique
- https://refeds.org/assurance/ID/eppn-unique-no-reassign
- https://refeds.org/assurance/IAP/low
- https://refeds.org/assurance/ATP/ePA-1m

SWAMID AL2

eduPersonAssurance
- http://www.swamid.se/policy/assurance/al1
- http://www.swamid.se/policy/assurance/al2
- https://refeds.org/assurance
- https://refeds.org/assurance/profile/cappuccino
- https://refeds.org/assurance/ID/unique
- https://refeds.org/assurance/ID/eppn-unique-no-reassign
- https://refeds.org/assurance/IAP/low
- https://refeds.org/assurance/IAP/medium
- https://refeds.org/assurance/IAP/local-enterprise
- https://refeds.org/assurance/ATP/ePA-1m

SWAMID AL3

eduPersonAssurance
- http://www.swamid.se/policy/assurance/al1
- http://www.swamid.se/policy/assurance/al2
- http://www.swamid.se/policy/assurance/al3
- https://refeds.org/assurance
- https://refeds.org/assurance/profile/cappuccino
- https://refeds.org/assurance/profile/espresso
- https://refeds.org/assurance/ID/unique
- https://refeds.org/assurance/ID/eppn-unique-no-reassign
- https://refeds.org/assurance/IAP/low
- https://refeds.org/assurance/IAP/medium
- https://refeds.org/assurance/IAP/high
- https://refeds.org/assurance/IAP/local-enterprise
- https://refeds.org/assurance/ATP/ePA-1m

SWAMID

Stöd för signalering enligt RAF i SWAMID

Shibboleth Identity Provider

Exempel på attribute-resolver.xml finns på SWAMIDs Wiki

https://wiki.sunet.se/x/0IAdB

Microsoft ADFS

Instruktioner för ADFSToolkit kommer snart på SWAMIDs Wiki

SWAMID

Ge oss feedback!

- Vad tyckte du om detta pass?
- Vad är ditt intryck av höstens Sunetdagar i sin helhet?
- Har du någon annan åsikt du vill dela med dig av?

Vi skickar länken i chatten!

https://sunet.artologik.net/sunet/sunetdagarnaHT21

SWAMID

SWAMID

Swedish Academic Identity Federation