TERENA Grid Certificate Service pilot project

Jan Meijer at UNINETT dot NO

16th EUGridPMA meeting, Zürich,
11 May 2009

TERENA GCS project

- Establish a shared SLCS/MICS service for those European countries that don’t want to run their own
- Uses NREN AAI federations for identity assertions
- to scale cost effectively to 10.000s+ users
- work started in 2007
- personal certificates, SCS to do hosts

why?

improve user access to Grids

PKI equipment scales better then PKI people

project partners

National Grid projects of Denmark, Finland, Netherlands, Norway, Sweden

National .edu AAI federations of Denmark, Finland, Netherlands, Norway, Sweden

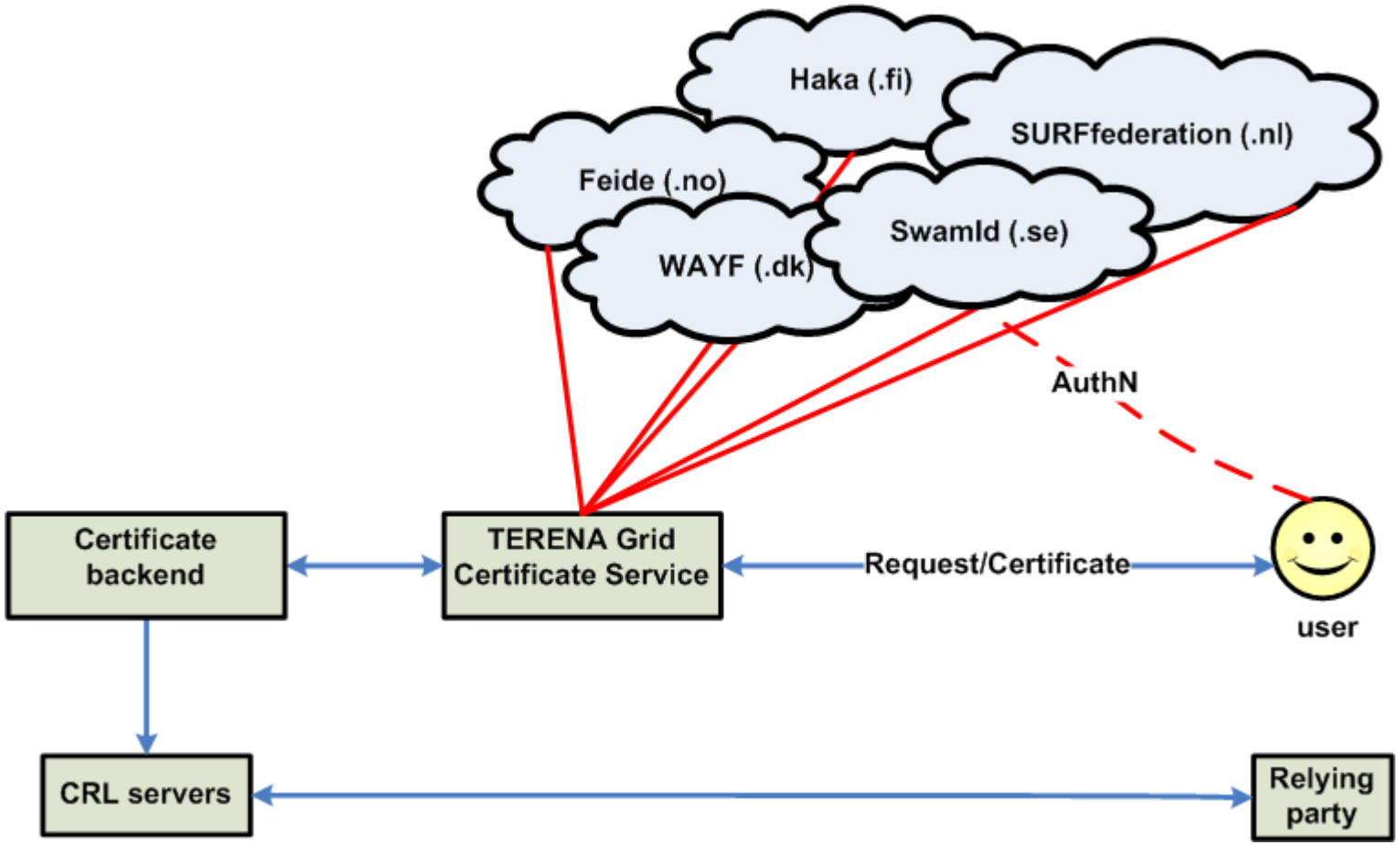
TERENA

NDGF

CESNET on SCS condition

- Belgium, Spain interested

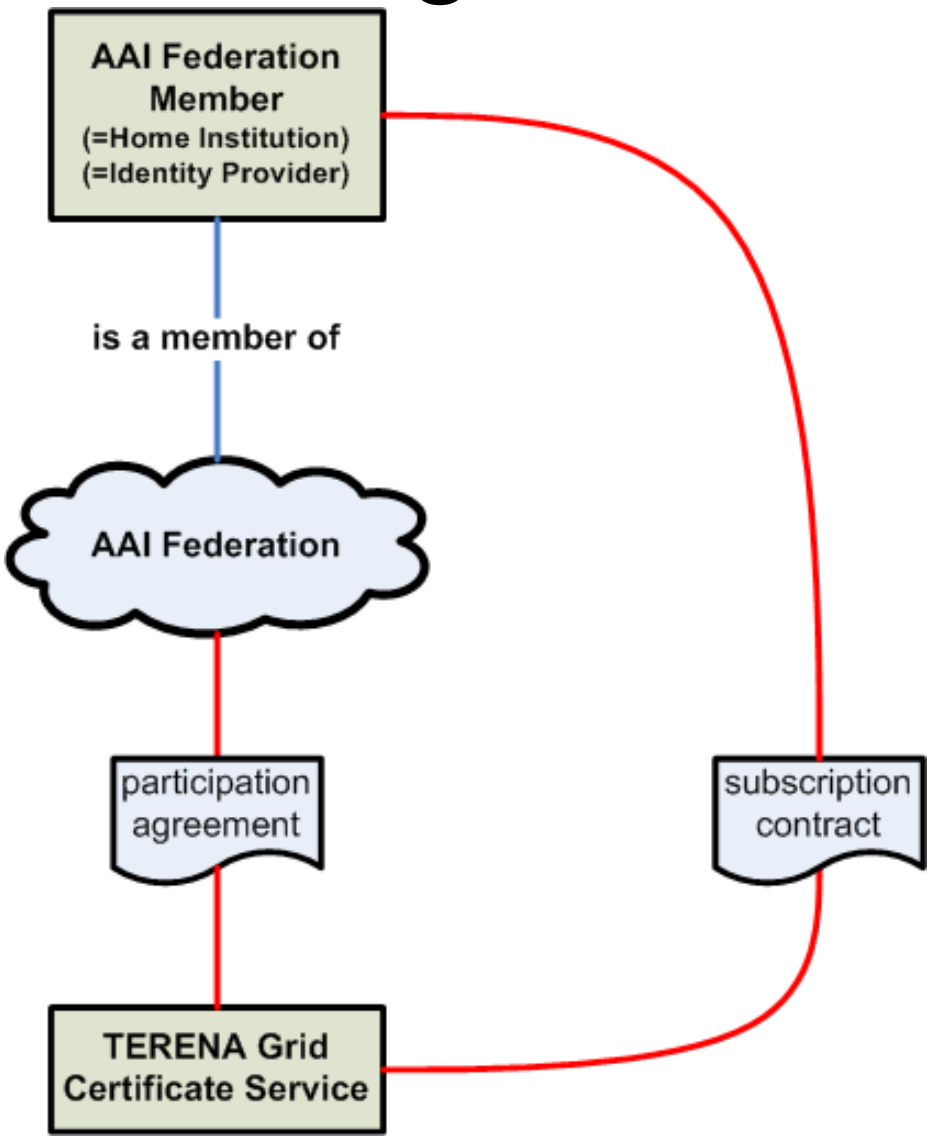
Service overview



where are we now

- Policy first: CPS draft
  - https://ow.feide.no/terenagcs:start
  - **thank you DFN!**
  - **thank you SWITCH!**
- Much ”does this work” discussion with federations
- Choosing certificate backends
- End-user portal

general framework



subscription contract covers:

- identity vetting
- persistent unique identity naming
- user entitlement
- certificate revocation on incidents
- traceback to physical person

we do not specify

HOW

the Identity Providers do their work

IdPs have the legal obligation

- to only give users that had a face-to-face meeting with passport-check the magic value in their **EduPersonEntitlement** attribute
- to pass a unique and persistent **eduPersonPrincipleName** attribute to the service for inclusion in the DN
- to revoke certificates if an AAI account is compromised

piggy-back on federation/IdP

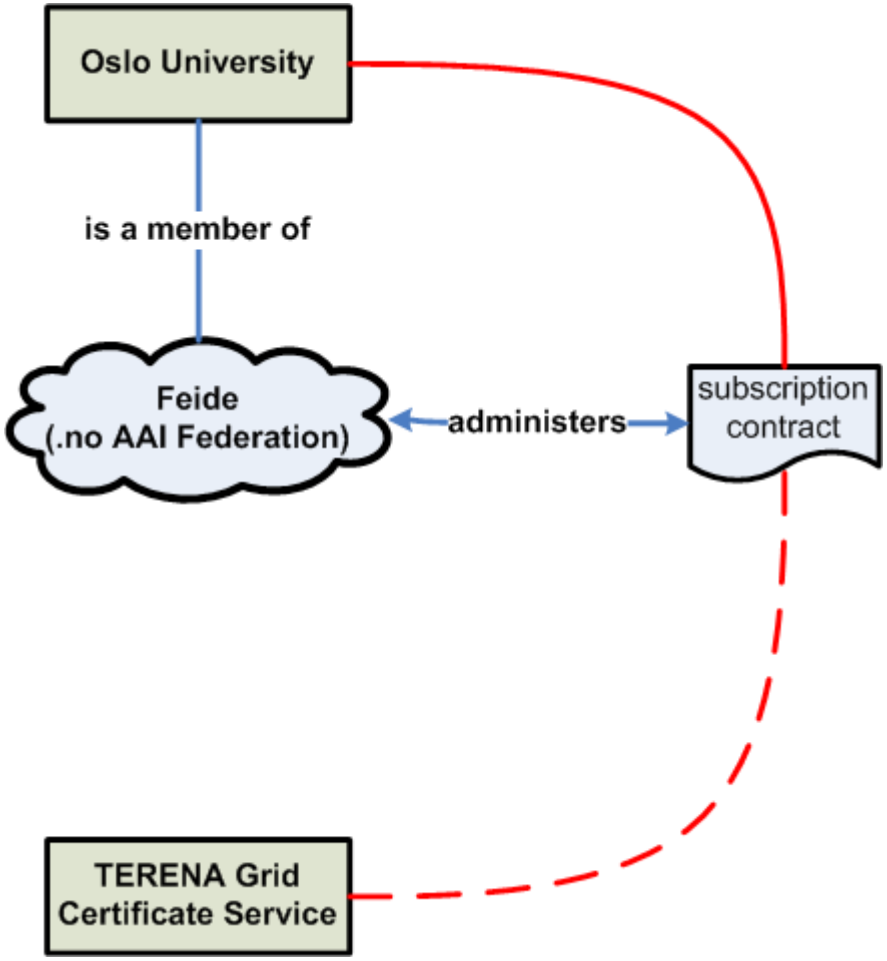
no interaction between CA staff and IdPs

no interaction between CA staff and end users

automated, scalable

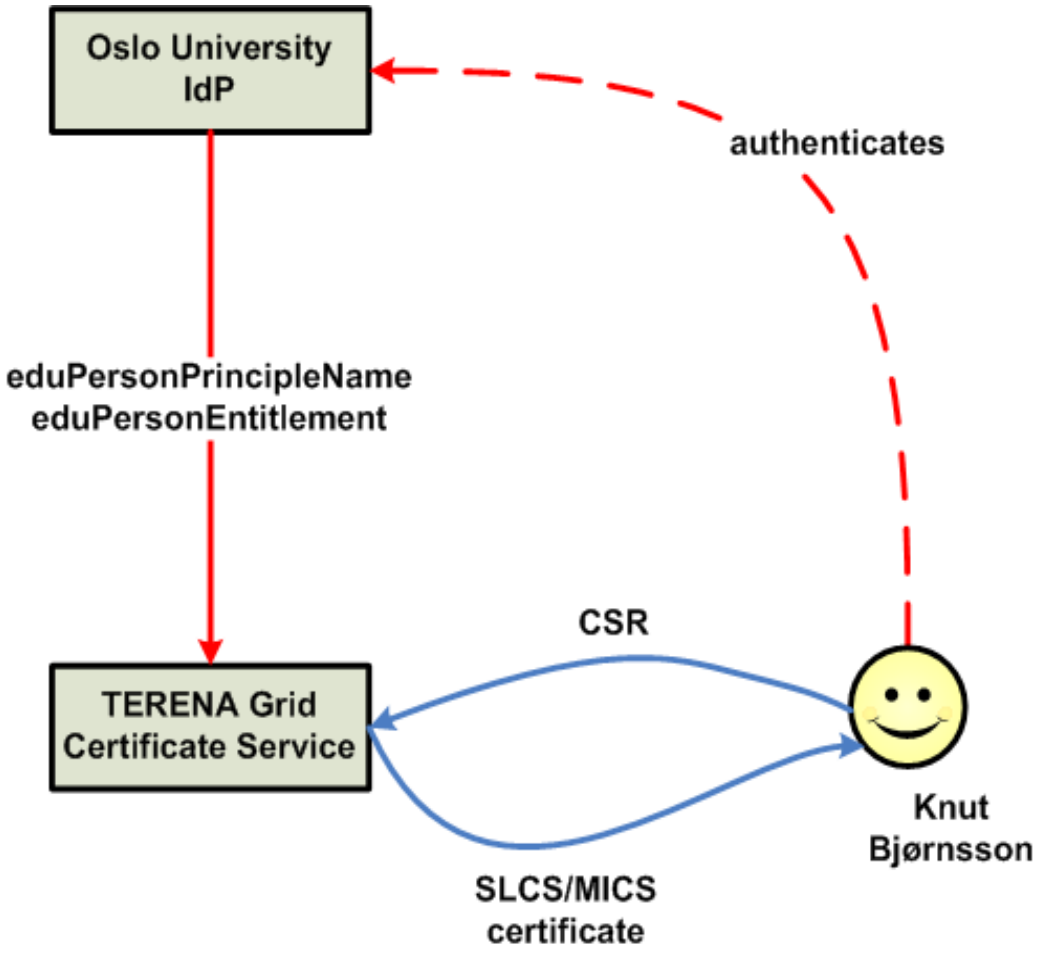
- Full use of properly maintained federations and IdPs
- Fraud for IdPs and Federations to willfully do it wrong
- Provide scalable revocation mechanisms to handle abuse

example: Oslo University joins



- signs agreement with TERENA GCS
- Feide administers agreement
- Feide registers Oslo University super user (for revocation)

Example: certificate issuing



- Entitlement set = face-to-face took place
- ePPN is persistent, unique over time

summarised

- face-to-face + passport for both SLCS/MICS
- entitlement of users (ePEntitlement)
- persistent identity naming uniqueness (ePPN)
- one federated AuthN element
- revocation on abuse

What do you think?

The identity validation consists of two process.

The first process is a one time process in which the identity of a requester is validated by the AAI Federation Member. The validation process used by the AAI Federation Member includes a face-to-face meeting using a passport or a similar valid official document.

The IdP of the AAI Federation Member expresses that an identity has been properly validated by setting the value “urn:geant:terena:…:gcs.user” in the eduPersonEntitlement attribute of the federated account of a requester.

The AAI Federation Member is contractually bound (see 1.3.2) to only set this specific eduPersonEntitlement value for users whose identity has been properly validated. Note that many IdP already did this face-to-face check on all regular staff and students either explicitly or implicitly; for these groups of users the TERENA GCS does not require a new explicit face-to-face authentication.

The Identity provider must set an eduPersonPrincipalName (ePPN) that is unique for every user that is assigned the TERENA Grid Certificate Service entitlement. The ePPN must allow a traceback to a natural person for at least 14 months. An Identity Provider must not re-issue an ePPN to another user.

For each each certificate request to the TERENA Grid Certificate Service, either the SLCS or the MICS variant, the TERENA GCS verifies that:

- the requester has successfully authenticated at his Identity Provider.
- the requester is entitled to a TERENA GCS certificate by checking the presence of the value “urn:” in the eduPersonEntitlement attribute of the requester