

TERENA Certificate Service - Status

Henrik Austad & Thomas Zangerl

April 12, 2010

Confusa and TNC eScience Portal



- Map a federated ID to X.509
- Use federations on non-federated services
- Move the federations into the CLI-dominated world.
- Multi-national TERENA Service.

Motivation for NDGF



- Replace NorduGridCA
- Easy access to X.509 certificates
- Outsource operations
- Foster collaboration

Technical status

- Or: What have we guys been doing since September?

- EUGridPMA accr.
- Personal certificates
- NREN customization and branding
e.g. <https://mijncertificaat.surfnet.nl>
- Non globally unique UIDs
- E-Mail address(es) in the subjAltName
- REST-API + OAuth







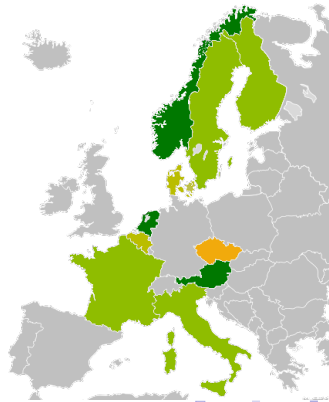
Personal vs. eScience certificates

	Personal certificates	e-Science certificates
Validity period	365 days, 730 days or 1095 days	395 days
Subject-DN: CN	Full name	Full name and UID
Subject-DN: unstructuredName	UID	-
Subject-DN: encoding	UTF-8	ASCII
E-mail addresses as rfc822name	one or more mandatory	optional
Signing-CA	TCS Personal CA	TCS eScience Personal CA

Operational status

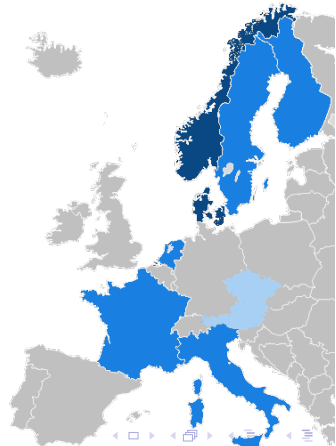
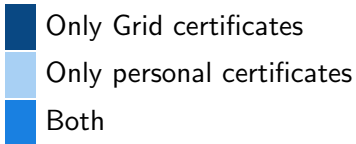
- Operated by the University of Tilburg
- Status of countries:

	At least 1 certificate issued
	Configuring/clearing details
	Participation announced
	Needing addtl. features



Operational status

- Operated by the University of Tilburg
- Status of countries:



Attribute Harmonization



- Federations are *national* entities.
- Different ideas about
 - Which attributes to release
 - How to construct these attributes
 - Encoding of attributes everything
 - Uniqueness of attributes
 - Organisation of IdPs
- **Heterogeneity**
honi soit qui mal y pense

Last minute requirements

- *extremely* important.
- Not always easy to understand what they *really* want.
- NRENs pay for shared operations, not for tailoring the software
- CPS was finalized February 1st and contained surprises



A challenge to *recognize* the problem.

Services

- Pure HTTP REST API
- authN via OAuth access token
 - List the certificates of the authN user
HTTPS GET /api/certificates.php
 - Request a new certificate
HTTPS POST /api/certificates.php
- Use by server 2 server API *and* desktop clients
 - BioPortal
 - jGridstart

Summary



- Service is operational, end of April marked as operational to all NRENs.
- 9 countries are using the shared portal.
- IGTF Accredited eScience CA