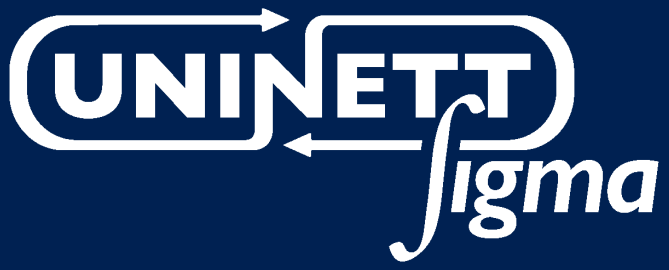


Confusa: technical intro

15th EUGridPMA Meeting, Nicosia CY

Henrik Austad

First things first - about:henrik

Name: Henrik Austad

Final year msc-student, engineering cybernetics, NTNU (eng: NUST)

Contact: henrik.austad@uninett.no

Role: software developer at UNINETT Sigma A/S, working with Confusa

Presentations is not my cup of tea – ask questions!

about:Confusa

- Map Federated identities to Grid-compatible X.509 certificates
- Fast (< 1 min)
- Secure
- Attributes will always be updated
- Started as a port of Swiss SLCS, will end up as an SLCS/MICS setup
- Moved to php and pure web-interface (simpleSAMLphp and Feide policy)

- https://slcstest.uninett.no/slcsweb/

Attributes

- ePPN (eduPersonPrincipalName)
  Unique attribute within a federation
- Full Name
- E-mail

- We deduce country based on federation

- Resulting subject:

/C=NO/O=Nordugrid/OU=Nordugrid/CN=henrikau@uninett.no

SLCS & MICS compliance

- Never re-issue certificates (for both SLCS and MICS)
- Unique CN in DN (ePPN)
- 2 separate 'CA-profiles' for SLCS and MICS based on attribute
- Dedicated CA with HSM (FIPS-140 lvl 3)

Secure

- Attributes are always updated
- Guaranteed unique CN (ePPN)
- SSO is stopped – user must always authenticate before using Confusa
- All coms via SSL
- CSR and Cert. Stored for limited time
- Monitor number of CSRs uploaded from single address (block abusive clients for approx 15mins)

Agile

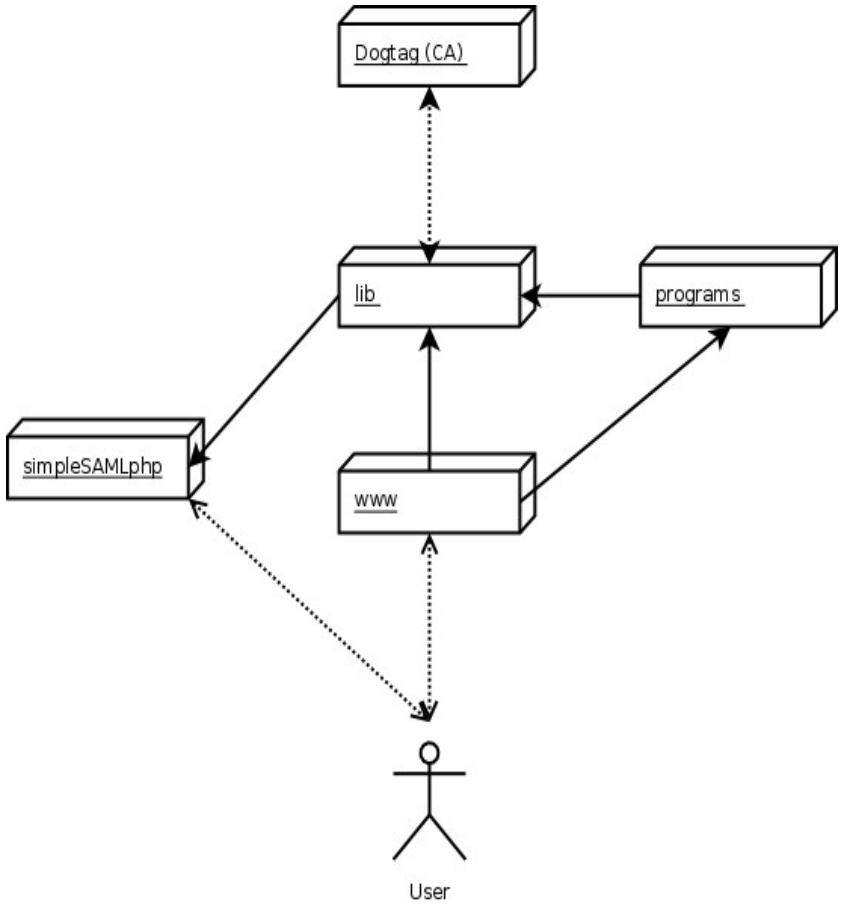
- We test fields of uploaded CSRs
- Tailor scripts for users
- Changes can be implemented fast (worst-case: user must download new script)

Current 'Members'

- Feide: Feb. '08
- Surfnet: Aug. '08
- DK-AAI: Sept. '08
- HAKA: Nov. '08
- Sweden: delayed (due to non-saml2)

Confusa setup

- SimpleSAMLphp handles all authN, integration with other Federations
- Browser handles redirect, SAML-header magic
- Client creates key and CSR
- ***We*** verify AuthN, compare attribs and create CMC for CA to sign



Steps

0. User downloads tailored script (need AuthN) [www]

1. Create key+CSR [script]

2. Upload CSR (part of step 1) [script]

3. Approve CSR for signing (req. AuthN) [www]

4. Download certificate [script, www, email]

Demo

Tell Henrik to stop – this is where he's supposed to demo Confusa for you ;-)

Further work

- One, single, integrated (user)step
- CRLs (required, plans ready)
- Differentiate between SLCS and MICS
- Test system (NorStore-test, grid1.uninett.no)
- Expand setup, collect user experience
- Add CA info to ARC-base (part of accred.)

Obtain source

- Via git:

```
git clone git://github.com/henrikau/conufsa.git
git clone git://git.assembla.com/confusa.git
```

- Via package:

http://www.assembla.com/spaces/confusa/documents

Thank you – I'm done!

- Project site: http://www.confusa.org
- Help: confusa-help@confusa.org
- Dev: confusa-dev@confusa.org
- PoC: https://slcstest.uninett.no/slcsweb/