

saml2int

Andreas Åkre Solberg

andreas.solberg@uninett.no

Vienna, February 2010

saml2int focus

- Minimize technical interoperability problems between entities that are connected through federations and confederations.

saml2int history

- Initiated in Seattle 2008
- Launched: saml2int.org
- Version 0.1 for a while.
- Used in Kalmar + Feide +++
- InCommon profile, December 2009
- Work re-vitalized Jan 10, new version


saml2int status

- new version being prepared these days.
 - InCommon's plan is to use saml2int deployment profile + an implementation profile.
 - Will be shared on various lists in few weeks.
- Input is important!

content of the profile

Metadata	Interoperable metadata profile. No PKI, embedded keys, technical contact, etc.
NameID	Transient + persistent
Attributes	URI format, recommend OIDs, EPTID as persistent nameid,
AuthnRequest	HTTP-REDIRECT, AssertionConsumerServiceURL
Response	HTTP-POST, Encrypted assertion or SSL on ACS, unsolicited response

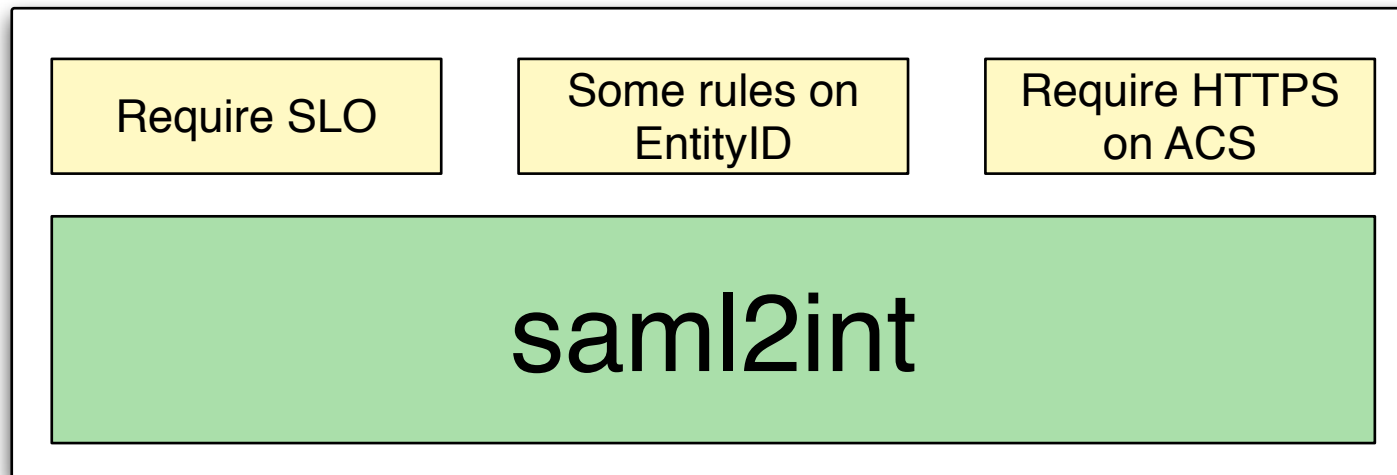
Informal Survey

- 1 Hands-up if you have a SAML deployment profile in your federation.
- 2 Hands-up if that profile is **identical to saml2int**.
- 3 Hands-up if that profile is **based on saml2int with extension** reqs.
- 4 Hands-up if you are in **dialogue with eGov** in your country discussing **SAML profiling**. 
- 5 Hands-up if your federation is **heavily relying on PKI** (for message signing and or metadata).
- 6 Hands-up if you think you will **not** manage to **get rid of the PKI** in foreseeable future.
- 7 Hands-up if your federation requires that SPs are using **HTTPS on ACS**.

Current draft of next v.

<http://saml2int.org/profile/draft>

Feide Profile



Challenge: additional requirements local, is not logic in a cross-federated world.
Real life example: feide + kalmar + slo