AUTH(Z/R)

@I2SMM 2011
roland.hedberg@adm.umu.se

Date

Tuesday, April 19, 2011
Problem spaces

- Federated services
  - Mostly web based
  - Small set of classes of users
  - Quite Static

- Internal services
  - More often than not, independent silos
  - Arbitrarily complex
  - Dynamic
  - Rights should follow/accompany work/tasks
Access management

- Keeping tabs on who can do what, when and where
- Business model
In a tangle?
federated context
Use of identity information

- Service providers use the end-user's metadata primarily to check whether access can be granted to the service provider's platform and commercial content. Secondarily, some personal data is also used to deliver the service to the end-user (e.g., to store a user's preferences or send him/her an email).
Necessary identity information?

- EduGAIN proposal
  - display name
  - common name (typically first name and last name)
  - email address
  - affiliation (such as faculty, student, alumnus, affiliate or library walk-in)
  - home organisation and
  - home organisation type.

![Bar chart showing the percentage of personalization, needed for Authz, and nice to have over the years 2002 to 2010.]

Tuesday, April 19, 2011
The reason for the drop.
Data protection Laws!

* It (the EU law) appears to say that anything that anyone can link to the individual must be treated as Personally Identifiable Information (PII) by everyone.

* It can therefore be assumed that all end-user metadata shared through eduGAIN qualifies as personal data – even when it would be pseudonomised – because the end-user's home organisation can always link the metadata back to the actual end-user.
Grounds for processing Identity information?

- consent of the end-user (the "data subject");
- necessity in order to execute a contract to which the end-user is a party;
- legal obligation for the data controller to process the personal data;
New kid on the block!

* "legitimate interests" legal ground can be invoked when the processing is necessary for the purposes of the legitimate interests pursued by the data controller (or by the third party or parties to whom the data are disclosed).
So where does this lead us?
Moving responsibility

- The service is always acting as a PEP

- Before:
  - Send the user identity and let the service do the access control (act as PDP)

- Soon:
  - Let the service know what gives and have it just enforce it.
Hence,

- Identity information as bases for authorization decision by the service will be exchanged for credentials constructed by the IdP.
An example

* A new web interface to the student registration system
* Presently two user categories

* urn:mace:swami.se:gmai:nya-dw:base:o=YY

* urn:mace:swami.se:gmai:nya-dw:department:o=YY:norEduOrgUnitUniqueNumber=ZZZZ

Tuesday, April 19, 2011
What about VO’s?

- Have not seen much use of this so far
- The use cases I have seen are of the type; the IdP handles the authentication and the AA provides the credential
So, how to handle this? 
The tools!

groups
roles
rulebased
same function different look
Conclusions

- Expect PDP functionality to mainly reside outside the service
- Authorization are going to be expressed as simple credentials
- You have to be able to handle lots of services each with their own set of credential types.
- So, be intelligent about how you do this!!
READY to go !?
Götheborg is a sailing replica of an 18th century Swedish East Indiaman, a wooden sailing vessel.

http://en.wikipedia.org/wiki/Götheborg (ship)