Metadata Aggregation

Ian A. Young
SDSS, EDINA, University of Edinburgh
ian@iay.org.uk

FAM09, Cardiff, 23-Nov-2009
What to expect

- Federated identity in a multi-federation world.
- Metadata aggregation: a technical approach.
- Aggregation engines: specific technology.
- Conceptual shifts are needed.
Dramatis Personae

• Alice, an entity and trusting friend of
• Bob, a second entity, desirous of conversation with Alice;
• Sally, the subject of their conversation;
• Sundry languages, cryptosystems and other technologies in attendance.
• (Hopefully) a chorus of interesting questions.
Rethinking Federation
“That” SAML Diagram
“That” SAML Diagram
It’s all about Alice and Bob
What is Trust?
Alice \rightarrow \text{“Trust”} \rightarrow Bob
Alice \[\rightarrow \] "Trust" \[\rightarrow \] Bob

Bob \[\rightarrow \] Alice \[\rightarrow \] "Trust" \[\rightarrow \] Bob
"This is Bob"

"I like Bob"

"Trust"
Consume

Bob's Request

Alice's Response

Bob's Metadata

Alice's Metadata
The software doesn’t know about federations

– Scott Cantor
  (every few days)
Rethinking Federations
“That” Federation Diagram

IdP → WAYF → SP

IdP → WAYF → SP

IdP → WAYF → SP

Federation
“That” Federation Diagram

IdP → WAYF → SP

IdP → WAYF → SP

IdP → WAYF → SP

Federation
Federations

- Primarily social, not technical, structures;
- Do not contain entities, but members;
- *Enable* communications by providing services;
- Many services involve being *trust brokers*. 
Federation Services

Alice's Metadata

Bob's Metadata

Alice  Register  Bob
Federation Services

Alice’s Metadata

Bob’s Metadata

Alice

Consume

Bob
Bilateral Exchange
Registrars, Aggregators and Publishers
.cf.ac.uk .ed.ac.uk ...
Aggregation Engines

- A configurable building block for “metadata networks” or “metadata layer”:
  - Subscribe,
  - Aggregate,
  - Transform,
  - Publish.
Transformation Steps

• Whitelist and blacklist by entity ID
• Whitelist and blacklist by XPath matching
• Digital signatures and signature verification
• Arbitrary XSLT
• Scripting languages
• ... or anything else you want to create
Result...

• All entities have access to (trustworthy) metadata for all potential partner entities.

• This can be seen as a “metadata layer” analogous to the DNS “naming layer”.
Scaling
UK federation entities

Entities

Dec 06  Apr 07  Aug 07  Dec 07  Apr 08  Aug 08  Dec 08  Apr 09  Aug 09
Scaling

• Observation: the UK federation is still getting bigger.

• Observation: the whole world is bigger still.

• If everyone has access to everything, won’t that become “too big”?

• Response: don’t download everything!

• Move to entity-at-a-time distribution.
I didn’t mention...

- Behavioural trust in large systems;
- Trust relationships between aggregators;
- The discovery problem.
Further reading

• Some Notes on Metadata Interchange:
  • http://www.iay.org.uk/blog/2008/10/metadata_interc.html

• Concepts and Methods:
  • http://www.iay.org.uk/blog/2009/05/concepts_and_me.html
Questions?