InCommon is More than Metadata: Long Live Metadata!

John Krienke
Tom Scavo
InCommon/Internet2
Agenda

- InCommon: The Who
- InCommon: The What
- InCommon: Technical Grounding
InCommon's primary purpose is:

"... to facilitate collaboration through the sharing of protected network-accessible resources by means of an agreed upon trust fabric."

§3.01(a), InCommon LLC articles
Who is the Federation?

http://www.deviantart.com/art/Trek-Pepper-251576690
InCommon Governance & Community

<table>
<thead>
<tr>
<th>Internet2</th>
</tr>
</thead>
<tbody>
<tr>
<td>InCommon Steering Committee</td>
</tr>
<tr>
<td>Technical Advisory Committee</td>
</tr>
<tr>
<td>Working Groups</td>
</tr>
<tr>
<td>● External Identities WG</td>
</tr>
<tr>
<td>● Alternative IdPs WG</td>
</tr>
<tr>
<td>● New Entities WG</td>
</tr>
<tr>
<td>● eduGAIN Policy and Community WG</td>
</tr>
<tr>
<td>● IdP of Last Resort WG</td>
</tr>
<tr>
<td>● Metadata Distribution WG</td>
</tr>
<tr>
<td>○ Per-Entity Metadata Pilot</td>
</tr>
</tbody>
</table>

InCommon Mailing Lists

We're still baking!

*Image source: wikipedia.org*
## InCommon Participants (691)

* [incommon.org/participants](http://incommon.org/participants)

<table>
<thead>
<tr>
<th>Higher Education Participants (460)</th>
<th>Government and Nonprofit Laboratories, Research Centers, and Agencies (33)</th>
<th>Sponsored Partners (198)</th>
</tr>
</thead>
<tbody>
<tr>
<td>A. T. Still University</td>
<td>Ames Laboratory</td>
<td>12Twenty Inc.</td>
</tr>
<tr>
<td>Aims Community College</td>
<td>Argonne National Laboratory</td>
<td>9STAR</td>
</tr>
<tr>
<td>Allegheny College</td>
<td>Brookhaven National Laboratory</td>
<td>Aastra USA</td>
</tr>
<tr>
<td>American University</td>
<td>ESnet</td>
<td>Academic Works, Inc.</td>
</tr>
<tr>
<td>American University of Beirut</td>
<td>Fermilab</td>
<td>Acatar</td>
</tr>
<tr>
<td>American University of Sharjah</td>
<td>GENI Project Office</td>
<td>Accessible Information Management, LLC</td>
</tr>
<tr>
<td>Amherst College</td>
<td>Idaho National Laboratory</td>
<td>Acate</td>
</tr>
<tr>
<td>Arizona State University</td>
<td>Internet2</td>
<td>Accessible Information Management, LLC</td>
</tr>
<tr>
<td>Arkansas State University</td>
<td>Jefferson Lab</td>
<td>Advantage Connect Pro Inc.</td>
</tr>
<tr>
<td>Auburn University</td>
<td>Lawrence Berkeley National Laboratory</td>
<td>ALEKS Corporation</td>
</tr>
<tr>
<td>Augsburg College</td>
<td>LIGO Scientific Collaboration</td>
<td>Alexander Street Press</td>
</tr>
<tr>
<td>Azusa Pacific University</td>
<td>LTERN (Long Term Ecological Research Network)</td>
<td>AliveTek</td>
</tr>
<tr>
<td>Ball State University</td>
<td>Marine Biological Laboratory</td>
<td>AliveTek</td>
</tr>
<tr>
<td>Barry University</td>
<td></td>
<td>AliveTek</td>
</tr>
<tr>
<td>Bates College</td>
<td></td>
<td>AliveTek</td>
</tr>
</tbody>
</table>
InCommon: The What

Creating the Trust Fabric
InCommon Trust & Interop

● Federation
  ○ metadata aggregation service
  ○ Tags for metadata
  ○ other services: discovery, error handling
  ○ Interoperability requirements: eduPerson schema, SAML
  ○ Baseline criteria for transparency and trust
  ○ Software Guidelines & Recommended Practices

● Assurance (aka Bronze & Silver)

● Other Trust & Identity Partnerships
  ○ Certificates
  ○ Multifactor
Entities in Metadata

- Num IdPs
- Num SPs

Number of IdPs: 374
Number of SPs: 1959
IdP: Attribute Release

● **FERPA**: "...provided that the student record information being disclosed as "directory information" has been so designated by the institution and information on any student who has opted out of the institution's directory information is not included in the disclosure, then there would be not be a FERPA problem with [this] kind of release."
  [LeRoy Rooker](#), (The nation's leading authority on FERPA)

● Release directory information: you're already releasing this information in other places.
● But no one is asking: Make science easy
● How much does "No" cost?
IdP: Attribute Release

The Research & Scholarship (R&S) 'Tag'

- 100 IdPs supporting 28 SPs
- The criteria
- SP info for registering
- IdP info for registering
Terminology

Some basic terminology:

- **Security Assertion Markup Language (SAML)**
- **Entity**: A single logical construct for which metadata is provided, usually a service provider (SP) or an identity provider (IdP).
- **Federation**: A trusted 3rd party that facilitates secure and interoperable interactions between entities.
What is SAML Metadata?

*Metadata*: a machine-readable description of certain entity characteristics such as name, identifier, endpoints, keys, etc.

SAML metadata drives the SAML exchange
What SAML Metadata is NOT

Metadata does not address these important questions:

- Does the IdP trust the SP to keep the user data private?
- Does the SP trust the IdP to assert correct user data?
- Does the user trust both the IdP and the SP?
Federation at Scale

Federation @ Scale: Metadata Registry (from Ping Labs)

"One of the primary bottlenecks to building Federations with thousands or tens of thousands of members is the manual nature of connection management"
Aetors

Check all that apply:
1. I am an IdP operator
2. I am an SP owner
3. I am an end user
IdP Operator

The best advice I can give is:

Keep it Simple!
SAML Software

Most SAML implementations do a decent job conforming to the SAML protocol. Beyond that, the most important consideration is your ability to consume metadata.

See: SAML Software Guidelines
Protocol Support

At the IdP,

- Support SAML2 Web Browser SSO
- Support SAML2 HTTP-Redirect binding
- Support front-channel protocols
- Avoid back-channel protocols
- Avoid SAML1 altogether!

See: New IdPs in Metadata
IdP Deployment Goals

As an IdP operator, your goal is to deploy a trustworthy and interoperable IdP

This is not a trivial task!

See: IdP Deployment Checklist
Attribute Release

Release eduPersonPrincipalName to all SPs

Support Research & Scholarship Category
(ePPN, mail, person name)
Finally, after all that, log into the Federation Manager and submit your IdP metadata

See: Federation Info
SP Owner

What category of SP do you represent?

- Vendor SP? (Sponsored Partner)
- Enterprise SP?
- Promiscuous SP?
Vendor SP

As a Sponsored Partner, your first decision point is how best to expose metadata to your customers: **SP Metadata Management**

Basic question: One comprehensive entity descriptor or one entity descriptor per client?
Enterprise SP

An Enterprise SP interoperates with at most a few IdPs (often just a single IdP)

If the metadata of an Enterprise SP is in the InCommon aggregate, it is primarily for convenience.
Promiscuous SP

A “promiscuous” SP is a Federation-wide SP, that is, every IdP in the Federation (or the world!) is exposed on the SP’s discovery interface.

See: Recommend Practices
Delegated Administration

A Federation Site Administrator can delegate the administration of SP metadata to anyone.

See: Delegated Administration
User Experience

All of us are federated users

- Seamless SSO is a primary goal
- Federated user interfaces
  - IdP discovery interface
  - Login interface
  - User consent interface
- User controlled attribute release is a goal
Questions?

What you ask in Indy, stays in Indy.

Stay tuned in: IAM Online, participants@incommon.org, and more at incommon.org/educate.