Shibboleth Update
Fall 2014
Background

• Shibboleth evolved out of Internet2 Middleware Activity in 2000, with first release in 2003.
• Significant funding from Internet2 (USA) and latterly JISC (UK) resulted in wide adoption by research and education communities enterprises around the world.
• Used by 26 national federations:

  UKAMF (UK), InCommon (US), SWITCHaai (Switzerland), AAF (Australia), AAI@EduHR (Croatia), AConet (Austria), Belnet (Belgium), CAF (Canada), CAFE (Brazil), CARSI (China), CESNET (Czech Republic), COFRe (Chile), DFN-AAI (Germany), Edugate (Ireland), eduID.hu (Hungary), GakuNin (Japan), GRNET (Greece), Haka (Finland), IDEM (Italy), LAIFE (Latvia), Tuakiri (New Zealand), RCTSaai (Portugal), RENATER (France), SIArnesAAI (Slovenia), SWAMID (Sweden), TAAT (Estonia) and ULAKAAI (Turkey).
Consortium Structure

**Board:**
Governing body of the Consortium
Currently 4 (max 12) members, consisting of:
- all principals
- representative of committers
- 1-2 elected members

**Consortium Operator:**
Executive body of the Consortium
- day-to-day operation
- appoints Consortium Manager

- S. Cantor (Ohio State)
- J. Sharp (Janet)
- S. Waggener (I2)
- C. Witzig (SWITCH)

**Members**
Principals
Commissers

- J. Knight (Janet)

**Reports**
operational plan
roadmap
contracts

**Elects / Nominates**
- operational plan
- roadmap
- contracts
Consortium Membership

Principal Members (those contributing €120K per year)
  Internet2 (US), Janet (UK) & SWITCH (Switzerland)

Federation Members
  ACOnet (Austria), NII/GakuNin (Japan), CSC/Haka (Finland),
  RENATER (France), NORDUnet (Nordic region), Belnet (Belgium),
  CANARIE (Canada), DFN (Germany), & The European Space Agency

Academic / Non-Profit Members
  Carnegie Mellon University (US) & LIGO Scientific Collaboration (US)

Commercial Members
  Overt Software Solutions, Clareity Security, Gluu & 9STAR
## Membership Fees

<table>
<thead>
<tr>
<th>Category</th>
<th>Small</th>
<th>Medium</th>
<th>Large</th>
</tr>
</thead>
<tbody>
<tr>
<td>Principal Member</td>
<td>€120,000</td>
<td>€120,000</td>
<td>€120,000</td>
</tr>
<tr>
<td>NREN/Federation Member</td>
<td>€10,000 &lt;250 IdP+SPs €20,000 251-750 IdP+SPs €40,000 &gt;750 IdP+SPs</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Academic/Non-Profit Member</td>
<td>€2,000 &lt;10K users €4,000 10-50K users €6,000 &gt;50K users</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Commercial Member</td>
<td>€4,000 &lt;€10M €8,000 €10-100M €16,000 &gt;€100M</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
# Projected Income & Expenditure

<table>
<thead>
<tr>
<th>Income</th>
<th>£285,964</th>
</tr>
</thead>
<tbody>
<tr>
<td>Principal Members</td>
<td>£131,600</td>
</tr>
<tr>
<td>Other Members</td>
<td>£93,220</td>
</tr>
<tr>
<td>Carried over from previous Financial year</td>
<td>£61,144</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Expenditure</th>
<th>£247,978</th>
</tr>
</thead>
<tbody>
<tr>
<td>Developers</td>
<td>£194,292</td>
</tr>
<tr>
<td>Consortium Management</td>
<td>£43,686</td>
</tr>
<tr>
<td>Travel</td>
<td>£5,000</td>
</tr>
<tr>
<td>Website</td>
<td>£5,000</td>
</tr>
</tbody>
</table>

Internet2 Expenditure: $157,912 (¬£97,858)
Federations using Shibboleth

![Bar chart showing the number of IdPs & SPs for various federations using Shibboleth.](chart.png)
PRODUCT UPDATE
IDENTITY PROVIDER VERSION 3
IdPv3 Status

• Two alphas issued, a third and last alpha out imminently (this week?)

• One beta will follow as soon as attribute consent code is stable

• Release will follow based on testing and feedback, very unlikely to slip into 2015

• Soft launch, documentation will not be adequate for new deployers until 2015, meantime focus on testing and eval of upgraded installations
IdPv3 Highlights

• A rough enhancement list posted to mailing list, see http://tinyurl.com/idpv3

• Highlights:
  • Authentication flexibility
  • Error handling much improved, including some i18n
  • Clustering improvements (client-side, Hibernate, memcache, TBD)
  • Hopefully fixes the multi-tab login bug
  • CAS server implementation
  • Simpler to grok NameID generation / selection
  • More powerful per-RP grouping and options
  • Extensive customizing via scripting
Upgrades from V2

• Install script can upgrade a V2 install by:
  • backing up conf and war
  • installing new files, but copying in old relying-party.xml, attribute-resolver.xml, attribute-filter.xml
  • setting a property in new idp.properties file to enable legacy relying-party.xml support
  • generating password-protected secret keystore
  • leaves your public/private credentials alone
• Cannot upgrade any other settings, including authentication
Future Upgrades

• We're hoping to detect or prompt for "legacy" V3 configs vs. fresh or migrated configs

• If you don't touch system/ we won't break your deployment on any 3.x upgrade
SIX MONTH OUTLOOK
Creep, creep

- Contracted effort ~ 2.7 FTE
- After ship, contracted effort - overhead ~ 1.5 FTE
- No official statement on V2 support, but end of 2015 seems pretty likely to me, absent a paid support partner
Looking Forward

- [https://wiki.shibboleth.net/confluence/x/M4AOAQ](https://wiki.shibboleth.net/confluence/x/M4AOAQ)

- Proposing a 6 month workplan for the team to:
  - Finish first batch of real V3 documentation
  - Patch and refresh SP (2.5.4) and Embedded DS (1.1)
  - Complete a server migration of shibboleth.net
  - Add consent polish, ECP delegation support (IdP 3.1)
  - Finish a full SAML Logout implementation (IdP 3.2)
  - Move Centralized DS code base to V3 libraries and metadata features (CDS 2.0)
2015-2016

• Member / Board input into workplan for the next contract cycle based on a menu of larger work:
  • First SP enhancements in a couple of years
  • Java SP
  • OpenID Connect prototypes and/or full impls
  • SAML-ECP GSS-API work
  • Developer documentation (including extension authors)
  • Introductory and/or enhanced product documentation
  • GUI work (very unscoped, so hard to estimate)