

The Shibboleth Consortium: Sustainability and Future Directions

IAM Online May 10, 2017

Justin Knight, Jisc (Justin.Knight@jisc.ac.uk)

Scott Cantor, Ohio State, Shib Developer and Board Member (cantor.2@osu.edu)

Kevin Morooney, Internet2 (kmorooney@internet2.edu)

Steve Zoppi, Internet2 (szoppi@internet2.edu)

Introductions

Justin Knight, Jisc

Jisc operates the Shibboleth Consortium

Scott Cantor, OSU, Shib Developer and Board Member

Scott is at Ohio State and represents the developers on the Consortium board

Kevin Morooney, Internet2

Kevin is Vice President for Trust and Identity at Internet2

Steve Zoppi, Internet2

Steve is Associate Vice President for Service Integration at Internet2

Steve and Kevin represent Internet2 on the Consortium board

Shibboleth Consortium

Justin Knight, Jisc



Background

- Shibboleth evolved out of Internet2 Middleware Initiative 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 (maybe more?):
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).



The Consortium

- Comprised of a Board, Members, Manager and Developers
- The body which handles financial and contractual management
- Provides strategic direction to the Shibboleth Project
- Not a legal entity in itself
- Requires an Operator (Jisc) and has a Manager (Justin)

Key risk factors

- Current form is non-obligatory Membership payments and contracts with Developers
- The Operator isn't liable if the Consortium's finances go into deficit
- If the finances go under, the contracts do, too



Consortium Board

- Principal Members' Representatives:
 - Internet2 (US): Kevin Morooney and Steve Zoppi
 - Jisc (UK): Josh Howlett
 - SWITCH (Switzerland): Ann Harding and Christoph Witzig
- Members' Representatives:
 - Lalla Mantovani, GARR (Italy)
 - Wolfgang Pempe, DFN (Germany)
- Developers' Representative:
 - Scott Cantor (Ohio State, US)



Consortium Membership

- **Principal Members**

Internet2 (US), SWITCH (Switzerland) & Jisc (UK)

- **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, GARR (Italy), CESNET (Czech Republic), HEANet (Ireland), REANNZ (New Zealand) & RNP (Brazil)

- **Academic / Non-Profit Members**

Carnegie Mellon University (US), LIGO Scientific Collaboration (US), The Space Telescope Science Institute (US), CINECA (Italy) & Lawrence Berkeley National Laboratory (US)

- **Commercial Members and Donors**

Digital Identity Labs, Overt Software Solutions, Clareity Security & InfoStreet



Financials

Income: Membership payments and donations. Equate roughly to £370K / €430K / \$460K per annum.

Expenditure: Development contracts; Consortium Manager. Equate to £400K / €465K / \$495K per annum.

Currently surviving on reserves built up in first two years of operation when Principal fee was significantly higher.

Developer hours were cut by 20% in August 2016 so as to avoid a deficit in 2016.

January 2017 has seen an increase in fees of 25% to avoid a 2017 deficit.

The current level of income and expenditure will keep the Consortium afloat until ~Q1 2018 before the reserves are exhausted.



Membership Fees

Category	Small	Medium	Large
NREN/Federation Member	€ 12,500 (~\$13,500)	€ 25,000 (~\$27,000)	€ 50,000 (~\$54,000)
Academic/Non-Profit Member	€ 2,500 (~\$2,700)	€ 5,000 (\$5,400)	€ 7,500 (~\$8,100)
Commercial Member	€ 5,000 (~\$5,400)	€ 10,000 (~\$10,800)	€ 20,000 (~\$21,500)

To become a Principal Member and get a seat on the Board, an additional EUR 20K will qualify any level.

Please note: the conversions to US dollars are approximate.



Shibboleth Consortium

Kevin Morooney, Internet2



Project Areas

- Consortium
- Project and Program
- Core Technology



Project Area - Consortium

- Consortium Management (20%)
- Consortium Marketing/Business Development (0%)



Project Areas - Project and Program

- Project Management (5%)
- Infrastructure Management (10%)
- Community Technical Support (10%)
- Standards Development (0%)



Project Areas - Core Technology FTE

Identity Provider

- Core (50%)
- Authentication (15%)
- Integration (25%)
- Consent / Privacy Mgmt (5%)
- SAML (60%)

Service Provider (Native) (15%)

Metadata Aggregator / Fed. Mgmt (10%)

QA / Testing (20%)

Packaging / Installation (20%)

Unallocated Work

Command Line / Non-Traditional Integration

Service Provider (Java)

Discovery / User Interface / GUI Design

Documentation / Training

Identity Provider (OIDC / OAuth)

Pair Programmer / Backup Engineering Support



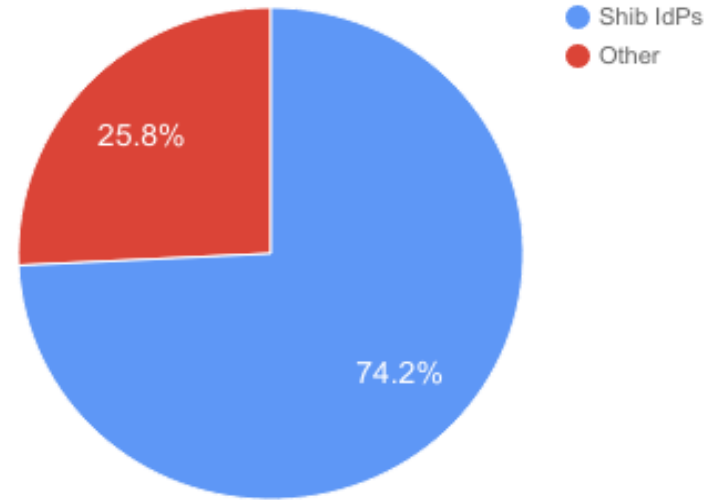
Scenarios being considered

- Minimum sustainable
- Optimal sustenance and moderate growth



Shibboleth Usage in edugain

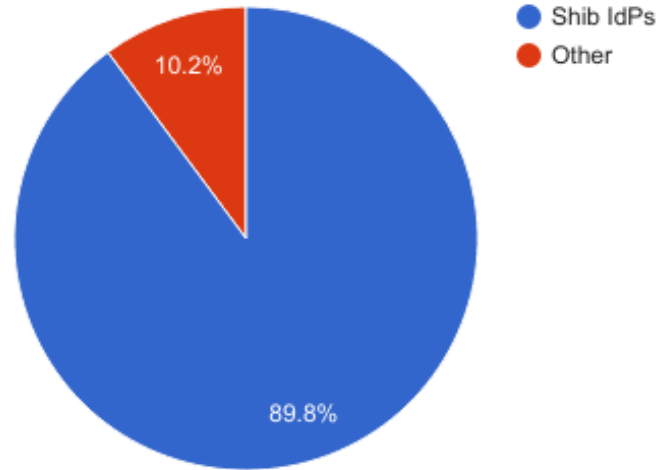
IdP deployments in edugain



2,367 IdPs (as of 27 March 2017)



Shibboleth Usage in InCommon



433 IdPs (as of 27 March 2017)



Next steps

- Develop alternatives to closing the gaps, continue community consultation
- Continue to refine this presentation/material
- CEO engagement strategy
- Develop a communications plan



Shibboleth Project

Scott Cantor, Ohio State and Shibboleth Developer



The Developers

Scott Cantor

Project infrastructure, board liaison, Service Provider, lead on IdP and IdP's clustering, authentication, SAML support

Daniel Fisher

LDAP library author, and LDAP support consultant

Brent Putman

OpenSAML in Java, security design and code

Rod Widdowson

SP, software installation on IdP and SP, IdP's attribute capabilities, embedded discovery service

Ian Young

Metadata Aggregator

Tom Zeller

Project infrastructure, testing, IdP consent support

Marvin Addison (committer, not contracted)

CAS implementation and maintenance



Project Plan for 2017-2018

- Assumes relatively flat funding
- Avoids larger, multi-year project commitments
- Avoids additional maintenance debt



Identity Provider

- V3.4 in 2017
- Final V3 release to prepare for V4 changes:
- Identify, warn on deprecated features scheduled for removal
- Redesigned Dependency syntax for attribute resolution
 - <InputAttributeDefinition>, <InputDataConnector>
 - Formalizes distinction between single- and multiple-input plugins
- TIER-sponsored work on metadata-driven configuration
 - https://wiki.shibboleth.net/confluence/x/VQC_AQ
- Evaluating community-built plugins to aid proxying



Identity Provider cont.

- V4.0 in 2018, perhaps 2019
- Spring 5, Java 8+ (no Java 7)
- Elimination of various V2 holdovers and some bad design decisions
- Likely installation/deployment improvements
- Short window for V3 support, perhaps a year



Service Provider

- V3.0 in 2017, perhaps 2018
- Technical debt
 - OpenSSL 1.1 compatibility (major transition on many Linux distros)
 - Updated Windows compiler
 - XML parser vulnerabilities on RH7 platform
 - Separate and clean up documentation



Service Provider cont.

- Unlikely to involve redesign, big configuration changes, or other improvements one might associate with a major release
- Substantive ideas:
 - Rebase IIS support on IIS7 with more native functionality and better security guarantees
 - New session cache options borrowed from IdP to improve clustering
- Very short window for V2 support, likely minimal depending on upgrade implications



Other Activities

- Finalizing V1.0 Metadata Aggregator (used by multiple large federations for their metadata processing today)
- Better alignment and support for third-party installation and packaging projects
- As much consultation, design assistance, and possibly library development as we can spare on third-party OIDC/OAuth projects (see slide 1)



Questions?

Contact Information

Justin Knight, Jisc (Justin.Knight@jisc.ac.uk)

Scott Cantor, Ohio State, Shib Developer and Board Member (cantor.2@osu.edu)

Kevin Morooney, Internet2 (kmorooney@internet2.edu)

Steve Zoppi, Internet2 (szoppi@internet2.edu)



Evaluate Today's IAM Online

<https://www.surveymonkey.com/r/IAM-Online-May-2017>

InCommon Shibboleth Installation Workshops

www.incommon.org/shibtraininging

- June 14-15, Denver, Colorado
- July 19-20, Easton, Pennsylvania
- November 7-8, Bethesda, Maryland [Starting with this session, the curriculum will shift to Shibboleth incorporated with TIER]

June IAM Online

Consent and Attribute Management

June 21, 2017

2 pm ET

Rob Carter, Duke University

Ken Klingenstein, Internet2