Minutes of Shibboleth Consortium Board Meeting #99

11th May 2022 – Videoconference

Attendees

Name	Organisation	Country
Scott Cantor (SC)	Developer Representative	United States
Kevin Morooney (KM)	Internet2	United States
Emily Brown (EB) *Secretary*	Jisc	United Kingdom
Alex Stuart (AS)	Jisc	United Kingdom
Steve Zoppi (SZ)	Internet2	United States
Joe Steele (JS)	Jisc	United Kingdom
Davide Vaghetti (DV)	GARR – Member Representative	Italy
Wolfgang Pempe (WP)	DFN – Member Representative	Germany
Bryony Hitchcock (BH)	Jisc – Online Surveys Team	United Kingdom

Apologies

Manne Miettinen (MM)	NORDUnet	Finland

Minutes of the previous meeting on 13th April were approved.

1. **Actions**

Ref	Description	Owner	Complete by	Status
93.1	Creation of a Shibboleth survey to acquire future development options from the community.	All	2022	**Ongoing May 2022**

96.1	FAQ page	All	March 2022	**All Board members are advised to read over the FAQ page and provide suggestions in an attempt to reduce the confused applications from customers surrounding the Consortium & software.**
99.1	Developer Contracts	EB	May 2022	**Emily is in the process of reviewing the contracts for 22/23.**
99.2	Survey Actions	SC	May 2022	**In response to the discussion surrounding the survey, Scott will provide clarity on the questions stated in the email.**

2. Financial and membership updates

Emily noted that an incomplete report had been provided by Credit Control and therefore she cannot comment on any outstanding payments.

Renewal requests are out, up until June: University of Michigan & Marymount University

Renewal requests have been confirmed by: Switch, Northwestern University, Temple University, MIT & Cincinnati Children's Hospital medical Centre. Texas State University, Stockholm School of Economics, University of North Carolina at Charlotte, The University of Texas at Austin, RNP, CESENT, Gakuin, CINECA, Los Rios Community College District, Brown University, Pacific Lutherean University, James Madison University, Oakland University &University of Illinois at Urbana-Champaign.

Emily reported that we have not received any new interest this month

3. Development update

https://shibboleth.atlassian.net/wiki/spaces/DEV/pages/2973597707/May+2022+Update

With IdP V4.2 released, I'll focus on two topics this month: what's actually new in this release, and what the active projects are for the remainder of this year (the roadmap is also updated in this regard).
A third topic is just to point out that Jetty 9.4 is now in commercial support mode, which means it will get critical fixes only for a few years. Anyone using it should be moving to Jetty 10.

4.2 Highlights
The main purpose of the 4.2 changes was to add some APIs needed to support new features in the OIDC plugins, and the OP enhancements are much more significant than anything in the IdP itself, which will continue to be true going forward. But with the opportunity for an update, a few changes were added, several involved with logout to improve some things I noticed while enabling it more widely.

The most visible change is probably the new default view templates and styles, which were produced by a design agency to make the defaults more modern, mobile-friendly, and simpler to adjust. This is obviously largely irrelevant to anybody with an existing deployment.

The logout changes are a combination of internal/mechanical updates and one change to the supported UI. A property was added that toggles the new default templates such that the status reporting of individual logout results can be hidden from the user. This was added for a couple of reasons and is the recommended approach. The information is essentially not actionable for the user (there's nothing you can do if logout fails) and is almost always the same result: lots of services that failed or don't support logout at all, and a few that worked. A message to that effect is as useful as displaying it all. Secondly, it's not known to any of us how to make the reporting of the results accessible, and so hiding it is intended to achieve better ADA compliance for deployers in the US.

The other changes are more internal and are designed to improve efficiency and to reduce failures and noise in the log. The system now looks for logout support by SPs up front, and tracks things so that attempts to locate endpoints and issue requests during a logout are eliminated, preventing a lot of spurious EndpointResolutionFailed errors. The implementation also does some better guessing about which logout endpoint to use when an SP advertises endpoints on many different vhosts, by selecting the endpoint that overlaps the best with the original response location during login. This is not defined by the standard, but works a bit better with the Shibboleth SP when virtually hosting applications under a single entityID.

A property was added to deal with a common anti-pattern, SPs that can issue logout requests but cannot handle (or do not honor) logout responses. Typically SPs that issue logout requests must either advertise logout endpoint, or include an extension in the request to signal that no response is expected. The property allows requests from any SP without logout endpoints to issue requests that will be treated as if the extension were present and forego the response, allowing the endpoints to remove from the metadata.

Finally, a bean can be defined with a list of <NameID> formats to leave unencrypted in logout requests, which improves efficiency for (e.g.) common cases like transient identifiers that don't benefit from encryption. This will likely be the default in the future.

Some small changes possibly of great interest to subsets of deployers:

- It's now possible to override the value used to tie requests together for session validation purposes and it need not be an IP address, allowing disjoint network-based affinity basing it on other criteria, or even combining addresses with other information for enhanced security.

- An easy way to add CORS headers to the IdP using Spring is available.

- Support for Google's invented trick for decorating cookie names with a "__Host-" prefix to prevent cookie hijacking within a domain was added, allowing prefixing of all the different cookies supported by the software.

Roadmap:

We're actively working on the following, which will likely take us through the rest of this year:

- Work on an OIDC proxying support plugin continues and hopefully will wrap up this summer.

- A replacement plugin that implements support for database storage without Hibernate is under development so that we can remove Hibernate from V5 entirely. Its lack of reliability and the lack of provenance of its software artifacts make this a high priority. The new plugin should be a drop-in replacement.

- Another significant feature update for the OP plugin is under development on an aggressive timeline to meet some member requirements. The scope is not fully defined, but is under discussion and definitely includes expansion of JWT support and some revocation enhancements. Logout is under discussion but is not a committed work item, mainly because much of that work (and what we've already done) will probably be moot with the changes coming to browsers soon.

- A parallel work stream is underway to port and test the code base on Java 17 and Spring 6 with the Jakarta EE changes, and address the likely end of the road for Spring Web Flow as a third-party project. We have POC code running successfully on Spring milestones now. We are actively looking at code reorganization for this release but we will be focused on reducing impact to deployers as much as possible.

- Finally, work has started on the SP redesign, though if the new release is the top of Mount Everest, we've basically started researching tickets to Nepal. The work should take further shape over the next few months and allow more of the work to be devolved to the team in certain areas.

4. Discussion of Development Roadmap and sustainability of Development team

Roadmap:

We're actively working on the following, which will likely take us through the rest of this year:

- Work on an OIDC proxying support plugin continues and hopefully will wrap up this summer.

- A replacement plugin that implements support for database storage without Hibernate is under development so that we can remove Hibernate from V5 entirely. Its lack of reliability and the lack of provenance of its software artifacts make this a high priority. The new plugin should be a drop-in replacement.

- Another significant feature update for the OP plugin is under development on an aggressive timeline to meet some member requirements. The scope is not fully defined, but is under discussion and definitely includes expansion of JWT support and some revocation enhancements. Logout is under discussion but is not a committed work item, mainly because much of that work (and what we've already done) will probably be moot with the changes coming to browsers soon.

- A parallel work stream is underway to port and test the code base on Java 17 and Spring 6 with the Jakarta EE changes, and address the likely end of the road for Spring Web Flow as a third-party project. We have POC code running successfully on Spring milestones now. We are actively looking at code reorganization for this release but we will be focused on reducing impact to deployers as much as possible.

- Finally, work has started on the SP redesign, though if the new release is the top of Mount Everest, we've basically started researching tickets to Nepal. The work should take further shape over the next few months and allow more of the work to be devolved to the team in certain areas.

5. AOB

Emily is in the process of reviewing the developer contracts for 22/23.

6. Next Meetings:

Wednesday 8th June
Wednesday 13th July