



Minutes of Shibboleth Consortium Board Meeting #122 10th July 2024 – Videoconference

Attendees

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

Apologies

Pal Axelson (PA)	NORDUnet	Sweden
Grace Moore	Jisc	United Kingdom

Meeting Minutes pending approval from 08/05/2024.

1. Actions

Ref	Description	Owner	Complete by	Status
106.6	Board to agree plan to discuss income generation, review of regulations and succession planning	Board	End of May 2024	Ongoing – Review in workshop 3. (April-May 24)
109.1	Revise membership documents. Move away from ‘charter’ language. Look at what it means for a member to join.	Board	TBC once 106.6 complete.	On hold until 106.6 progresses.
109.2	Investigate legal status.	SZ	TBC once 106.6 complete.	On hold until 106.6 progresses.

120.2	Davide to seek feedback on the grant application, from GEANT, and explore potential to benefit from incubator	DV	End of May 24	Closed.
121.2	Rate increase comms to be drafted.	EB & Board.	June 2024	Closed.
122	Finalise and send rate increase comms	SC & EB	July 2024	Open.

2. Financial and membership updates

Shibboleth Consortium Like4Like – attached to Agenda.

3. Development update

<https://shibboleth.atlassian.net/wiki/spaces/DEV/blog/2024/07/05/3713695745/July+2024+Update>

In between various summer vacations, work has continued on a number of fronts this summer.

The Duo plugin upgrade adding dedicated single-factor passwordless support is now available. The WebAuthn plugin has reached beta status while work continues on a few final additions such as better auditing support. With the plugin largely stable now, testing can be conducted using nightly snapshots, allowing any bug fixes to be immediately available. As I mentioned in May, we have built a new page to improve project transparency regarding the state of our Java projects and links to the stable and in-development distributions at <https://shibboleth.net/cgi-bin/projstatus.cgi>. See my note for more on this. We will work on finding ways to expose a pointer to this page wherever it makes sense to do so.

Work has progressed on OAuth PAR and DPOP features in the OP plugin along with other minor improvements. Documentation of the new features is in progress and a release is expected later this summer. That should clear the decks for work to start on the OpenID Federation implementation this fall.

We are close to shipping an upgrading Windows installer for Jetty 12 to replace the Jetty 11 version; testing is underway. We are also starting to explore the possibility of migrating to a plugin-based approach that adds Jetty to an existing IdP.

I am considering a minor SP update this fall to pick up a small number of fixes and substantially freshen the WIndows library set, which is getting increasingly out of date, OpenSSL in particular. Part of this release may include a new release of the xml-security library that has now formally been forked by the Shibboleth Project with the original library retired at Apache due to lack of committers. Taking over the code in fact as well as practice provides more freedom to make changes and possibly remove many unused features (and attack surface). The official transition of that library has not exactly been finalized, but we have published the converted Git repository and any future SP 3.x packages will rely on that fork. It is not inconceivable that we may do something similar to Xerces, but doing so would be more contentious and probably require a formal fork because Apache is unlikely to retire that code (even though it probably should IMHO).

I have also made relatively substantial progress on the new SP plugin in Java. I have started to build foundational code for building SP web flows, including a configuration design for the agents, applications, and (in unusual cases) relying party configurations. SP flows are proving very simple to build now that the foundation is in place and we have a testing framework allowing independent unit testing of flows without requiring agents to be built ahead of time.

For now, the SP flow framework is reliant on agents providing HTTP Basic Authentication credentials to secure agent requests and allow the plugin to identify and compartmentalize work on behalf of multiple agents connecting over an insecure network. This compartmentalization extends to the use of the StorageService and DataSealer IdP components, allowing multiple agents to safely store, retrieve, and secure data without any risk of cross-contamination by other agents.

I have working (and “sort of documented”) flows for a few early utility tasks, most notably one that will parse the XML-based RequestMap syntax on behalf of agents (which will no longer require native XML parsing support). For now, the RequestMap syntax is largely, though not entirely, identical to the current V3 schema, so exists in a new V4 namespace. The hope is that this will be the extent of agents' reliance on XML as a configuration format, with any other configuration handled in simpler ways.

While a lot of uncertainty remains, my plan at this stage is to focus on building out the required functionality without worrying too much about the migration path. It should be possible to look at providing XSLT that can transform the current RequestMap into the new syntax, but I think it very unlikely that a seamless upgrade will be possible given the huge differences. The hope would be that, once a hub is configured to support an existing SP's SAML needs, that translating an existing RequestMap (or minor adjustments to some Apache commands) should allow for a fairly painless transition. But I don't see the kind of direct package upgrade that made the transition from 2.x to 3.x transparent. An uninstall, new install, and migration of files and settings is probably going to be required.

The next step will be to begin actual implementation of SAML request and response handling, at least enough to get an actual exchange done. Once this is tested and working, it will be time to branch the current SP to begin implementation of the more stripped down agents and get to a working proof of concept. It is possible, though not perhaps incredibly likely, that we may have demoable code by TechExchange in December, but either way I'm pleased with the progress and how things are turning out so far.

4. Discussion of Development Roadmap and sustainability of Development team

- **Scott will publish a new version of the roadmap by EOY to support the rate increase comms.**

Roadmap:

Updated Aug '23 -

<https://shibboleth.atlassian.net/wiki/spaces/DEV/pages/1120895029/Project+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.

Note: Scott intends to swap out the old roadmap page to the new forward-looking roadmap. Once this has been published it will be linked off from the rate increase comms. The historical roadmaps will be moved to an archive.

5. AOB

- Developer contracts are approved and complete from all sides.
- Final feedback is required for the rate increase comms.
- Scott will finalise this over the next week or so and then this will be ready to be circulated.
- The Board decided that a new list would be created to review and collate feedback. Emily and Alex will review all feedback from the list and liaise with the board when needed.

6. Next Meetings:

Wednesday 14th August

Wednesday 11TH September