



Minutes of Shibboleth Consortium Board Meeting #114 18th October 2023 – Videoconference

Attendees

Name	Organisation	Country
Scott Cantor (SC)	Developer Representative	United States
Steve Zoppi (SZ)	Internet2	United States
Grace Moore (GM)	Jisc	United Kingdom
Emily Brown (EB) Secretary	Jisc	United Kingdom
Kevin Morooney (KM)	Internet2	United States
Wolfgang Pempe (WP)	DFN – Member Representative	Germany
Davide Vaghetti (DV)	GARR – Member Representative	Italy
Manne Miettinen (MM)	NORDUnet	Finland

Apologies

Alex Stuart (AS)	Jisc	United Kingdom
------------------	------	----------------

Minutes of the previous meeting on 13th September are approved.

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	February 2023	Ongoing - Will be addressed in the Jan 2024 workshop.
109.1	Revise membership documents. Move away from 'charter' language. Look at what it means for a member to join.	Board	September 2023	Open – Will be addressed in the Jan 2024 workshop.
109.2	Steve – Investigate regarding donations / tax identifier number? How to make donations possible via PayPal	SZ	September 2023	Open – Steve has sent over a paper with options outlined. Discussion ongoing.

				Likely to be addressed in the Jan 2024 meeting
112.2	Daasi	EB	September 2023	Ongoing – awaiting response from Jisc legal. Likely to be finalised in time for the start of the first sprint on 15/11/2023.
114.1	Financial Data Presentation	EB&GM	November 2023	Ongoing – EB&GM to present financial data.
114.2	Draft Agenda for January workshop.	EB,GM &KM	November 2023	Ongoing.
114.3	Agree dates for January workshop.	EB & GM	November 2023	Ongoing.
114.4	Send out communication around 2025-member rate increase.	All.	October 2023.	Ongoing.

2. Financial and membership updates

All renewals are out until December.

Yet to renew: GakuNin, Aktia Bank PLC, Lafayette College.

Offboards: ‘Augstākās izglītības un zinātnes informācijas tehnoloģijas koplietošanas pakalpojumu centrs, Lafayette College & Akita Bank

Onboards: in 2023: Omnibond, IDF Connect, Harvard University, University of Arizona, Open University, Illinois state, AAF

The only outstanding payment from 2022 is now university of Montana.

3. Development update

<https://shibboleth.atlassian.net/wiki/spaces/DEV/blog/2023/10/17/3288072197/October+2023+Update%EF%BB%BF>

The IdP (and OpenSAML) V5 release was completed on schedule last month ahead of TechExchange, though with a fair number of bumps due to the refactoring work and the increased number of projects to release, including all of the plugins. Some glitches aside, the software release went fine (with a notable exception) and we have not gotten much in the way of bug reports so far. One did come in today, indicating a regression handling some kinds of SAML metadata extensions in conjunction with the new “strict parsing” implemented in OpenSAML. It has been reported, triaged, and documented on the ReleaseNotes page as a known bug with the workaround for now. It’s serious enough to probably warrant a patch relatively soon.

As previously announced, the EOL for V4 will be September 2024.

The notable exception to “fine” was that our Javadoc generation process turned out to have atrophied and wasn’t correct at the time of the release. A lot of time has been spent (during TechEx and since then) to get that cleaned up, design new approaches to managing the links between projects, and ultimately re-publish new copies of the Javadocs under a new home at <https://shibboleth.net/api>. We had a long-standing desire to dump the Maven site feature and stop using that to generate the Javadocs, but it has turned into a substantial project to get Maven to do it some other way, and we’re still working that out. These are the times “dump Maven” starts to sound very attractive, but we’re not quite there yet given the time that would take.

The other notable event was an avalanche of security advisories all dropping last Wednesday. They all turned out to be relatively unimportant to us, but we released Jetty and libcurl updates anyway. The Jetty update allowed us to reorganize the way we will be publishing those since they are decoupled from the V5 IdP releases now, and needed to be housed separately.

I feel the need, out of personal frustration, to note that the total amount of time spent on the fact that Red Hat foolishly and needlessly chose to rebase curl on NSS in Red Hat 7 has cost the project well over a hundred hours of time to deal with. All for no reason, for a change that had no chance of succeeding, and that they inevitably reverted in the next version. Incredibly frustrating and we’re still paying the cost of that, because Amazon Linux 2 inherited the same bug and isn’t going away any time soon. If I seem grouchy a lot, this is the kind of thing that causes it.

TechExchange itself was a good event, well attended, and I know I attended a lot of good sessions throughout the week (and missed many more I’m sure). A lot of good discussion was had about the project’s next steps, particularly in areas like WebAuthn support and personal data and profile management for end users (a GEANT project that we are eager to see mature and eventually turn into a supported plugin). As I noted last month, we’re going to be doing a lot of project planning before diving into some of the major work items on our list, but one clear task we know has demand will be prototyping a WebAuthn plugin, so that work will certainly start this fall.

Another non-trivial but hopefully not huge work item will be to finally incorporate CSP support into the views we ship, to provide some hardening against XSS threats by locking down the Javascript the pages can run. These will not be changes forced on anybody since upgrades don’t replace the views in general, but for new installs and as a sample to work from, it’s a necessary bit of work that’s been neglected for a while. While I don’t think a lot of the major threat models can be addressed with this change, it’s still good practice to do it.

One of those threat models is that mobile apps that use captive login windows have carte blanche to attack the user’s session because naturally they have access to the cookies. That’s one reason the IdP continues to default to binding sessions to IP addresses. Ultimately, nothing we do on the server or with CSP can prevent a malicious client from sniffing passwords or stealing cookies. And SSO will always inherently depend on bearer cookies because Google killed the Token Binding initiative that could have shored that up.

Members should expect to start seeing some communication from the Board fairly soon as we work through the budget issues we’re facing. A formal announcement of the planned rate increases for individual academic and commercial members in 2025 will be coming as soon as it can be drafted. After the low hanging fruit, the harder work of crafting different costing proposals for different sets of work items will be underway this fall.

4. Discussion of Development Roadmap and sustainability of Development team

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.

5. AOB

- GM & EB to work with KM to create an agenda for the January 3 half-day workshop.
- GM&EM to present financial date. This will include an internal and external version.
- Board agreed to a 2-3 half-day workshop in January to address:
 - 3-5 year plan
 - Financial plan
 - Review of the Charter
 - Succession planning
- Board agreed brining other subject matter experts, a trusted party who could contribute to the workshop.

- Scott proposed that Phil Smart and Ian Young attend to address succession planning and a view from the developers.
- The Board are not averse to an external facilitator.
- The workshop will run over a max of 3 half days in 3-4 hour blocks.

6. Next Meetings:

Wednesday 8th November

Wednesday 13th December