



Minutes of Shibboleth Consortium Board Meeting #120 10th April 2024 – Videoconference

Attendees

Name	Organisation	Country
Scott Cantor (SC)	Developer Representative	United States
Grace Moore (GM)	Jisc	United Kingdom
Davide Vaghetti (DV)	GARR – Member Representative	Italy
Wolfgang Pempe (WP)	DFN – Member Representative	Germany
Pal Axelson (PA)	NORDUnet	Finland
Steve Zoppi (SZ)	Internet2	United States
Alex Stuart (AS)	Jisc	United Kingdom

Apologies

Kevin Morooney (KM)	Internet2	United States
Emily Brown (EB) Secretary	Jisc	United Kingdom

Meeting Minutes approved from 13/03/2024.

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.

120.1	Jisc to revise financial presentation and resubmit by end of April	EB & GM	End of April 24	Open.
120.2	Davide to seek feedback on the grant application, from GEANT, and explore potential to benefit from incubator	DV	End of May 24	Open.

2. Financial and membership updates

- EB had provided financial presentation alongside agenda, on 28/3/24
 - Board confirmed they are happy with template – simpler the better, contract key from accessibility perspective, don't need to mirror brand colours too closely
 - Board did have feedback on how to improve the presentation, which is now a new action for us to complete for the end of April update
 - Board acknowledged that the payment delays between institutions will likely always cause issues in getting accurate reports, but agree it will catch up eventually
- Improvements to cost reporting:
 - Expand table out to look at costs over full year, by month
 - Introduce 3rd column so we have target / actual / forecast costs. Will need to consider how we get visibility of the forecast costs each month. Example table below. Recommend we pick this up with Alex to get more feedback before submitting next version as he was quite critical in the meeting.
 - Separate out or remove YTD reporting as board didn't feel it was helpful without context of full year.
 - Chart is incorrect – needs to be correct. Board more concerned about access to raw data than charts. This can be put onto a separate slide if more detail needed.
 - Provide more commentary on the costs so board have more context when reviewing – what's been invoiced, what's upcoming etc.
- Improvements to income reporting:
 - Board asked for confirmation that income targets are modelled based on renewal dates
 - Asked to expand table out to look at income over full year, by month (same as with costs)
 - Introduce 3rd column so have target / actual / forecast income. Forecast likely to be based on renewal dates although we acknowledge that the lag in receiving payments will cause issues with accuracy. Can improve this over time. Example table below. Recommend we pick this up with Alex to get more feedback before submitting next version as he was quite critical in the meeting.
 - Separate out or remove YTD reporting as board didn't feel it was helpful without context of full year.
 - Chart is incorrect – needs to be correct. Board more concerned about access to raw data than charts. This can be put onto a separate slide if more detail needed.
- Other requested improvements:

- Once these tables have been fleshed out, should then incorporate slide to show overall Profit & Loss over course of the year.
- Feedback on outstanding payments / renewals:
 - GakuNin are key to confirm as renewing as they represent a larger % of income, as an NREN member
 - CESNET also important to chase for payment but may be resolved by time you're back
 - InCommon have said to reach out if support needed chasing the state universities as they have contacts on that side.

3. Development update

<https://shibboleth.atlassian.net/wiki/spaces/DEV/blog/2024/04/09/3536617478/April+2024+Update>

Since the previous update, we have shipped the IdP V5.1 update, and a V5.1.1 patch to address a Spring issue announced the day after and a couple of regressions.

Regressions are never fun, but they were pretty minor and the update has been otherwise a non-event, which is always the goal.

Because of the Spring issue, we were forced to go ahead and issue a V4 patch update as well, which is likely to be the “if we have to, we will” final rollup release of that branch. Barring another security issue in the next 4 months, that will be it for V4.

Updating our plugin development status, we are on track to release updates to the OIDC plugins this week. Those plugins will be compatible with V5.0, notwithstanding that support for that ended with the V5.1 release. We will likely be dropping an updated alpha release of the WebAuthn plugin relatively soon.

The Duo Passwordless update is coming, but (somewhat unusually for us) we have been able to get a significant amount of feedback from testers and I have been substantially rethinking things to take a fresh approach that should be easier to configure, and allows for more gradual adoption, which I think is a critical requirement for something like this to be successful. We have a new snapshot being tested, but there's a bit more to do and unit tests to finish, so May is probably a more realistic guess for a release. It will also require V5.1 in order to leverage some newer cookie-related APIs. There aren't any important “fixes” in this update to those using the current plugin, so we do not anticipate a major amount of pressure to update to it independently of the passwordless feature.

A note (and something of a warning?) about Jetty 12: in response to some early testing issues reported on the mailing list, we did the initial work to prepare a Jetty configuration suitable to it and created a page for that. One issue encountered by testers was isolated and reported as a bug in Jetty and that's already been fixed upstream, so we believe the current 12.x release is now usable in production. There are a couple of notes about it that I would highlight, one particularly significant.

Likely a minor issue is that Jetty 12 does not include CGI support for reasons that are not clear to me. Those using Jetty by itself rather than behind Apache, for example, could be impacted by this

limitation (I personally use CGI scripts extensively for various things, I don't know how common that is).

The more significant warning I hope affects very few people at this point, and if not, well, it's time: we do not know of a way to allow for the "accept any TLS client certificate for authentication" support on a second port that was part of the oldest Shibboleth deployments prior to SAML 2.0 adoption, i.e. the so-called "back-channel port" for SOAP traffic that often runs on port 8443 or a similar alternative port. So given that Jetty 11's official EOL may not be that far off, anybody still relying on and supporting a second port in that fashion needs to pay off that technical debt and move on. It has been easily over a decade since that approach was even suggested, let alone advised.

We will put together a new page outlining more of the concrete considerations around migrating away from that approach, mostly for use by federations needing help crafting advice for their members. In a nutshell, you need to know what profiles your IdP supports, which ones are in use, and what services relying on that port might support or not support in terms of SAML metadata to allow a smooth migration away from it. In the meantime, the SecurityAndNetworking topic contains good information about why the additional port is largely a historical footnote at this point.

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.

Notes captured from GM:

- OIDC release likely to happen next week =.
- WebAuthn close but not quite ready
- Scott is focused on the duo work – some progress these that should make it easier to allow for gradual adoption. Aiming for a May launch.
- IdP release is now done, including V4 patch.
- Jetty bug is now fixed, which means Jetty 12 is viable but more testing to do. Need to be careful that we're just packaging their software but not responsible for it. Scott to write up some more support documentation.
- Scott has made some mail changes to address DMARC/DKIM issues.
 - Support from John O'Brien
 - In response to feedback from community
 - Will reduce spam into us too.
- Scott also working on more detailed roadmap write-up that can be published / made accessible to the community.
- Discussion about Ian's hours on MDA and who else might be able to support.
 - Scott speaking with Nicole Roy from Internet2 as they may have a new contractor who can support.
 - Not recommended that Phil Smart is deployed onto this as has bigger priorities and there are better ways to resource it.
- Discussion about the GEANT grant
 - Agreed that it has been a good learning experience and won't prevent us from still working on the OIDC federation.
 - Agreed that Davide will seek more feedback on the grant / what we could do to secure this in future.
 - Agreed that Davide will also explore whether there are opportunities for us to work alongside the GEANT incubator to support this development.
 - These are now captured as a new, single action.

5. AOB

- Developer % Increase
 - SZ requested we agree this in workshop on 15/4/24 as himself and Kevin want to feedback/get clarifications on member price increase strategy ahead of confirming this
 - Key for SZ is that even if we offer a freeze for 2 years, to make the initial increase more palatable, we should then commit to a floor (i.e. 3% minimum annual increase)

after a certain point. This allows us to more easily increase developer costs in conjunction.

- Board agreed. Decision to be made on 15/4/24.

6. Next Meetings:

Wednesday 8th May

Wednesday 12th June