Minutes of Shibboleth Consortium Board Meeting #113
13th September 2023 – Videoconference

Attendees

Name	Organisation	Country
Scott Cantor (SC)	Developer Representative	United States
Steve Zoppi (SZ)	Internet2	United States
Alex Stuart (AS)	Jisc	United Kingdom
Grace Moore (GM)	Jisc	United Kingdom

Apologies

Kevin Morooney (KM)	Internet2	United States
Davide Vaghetti (DV)	GARR – Member Representative	Italy
Emily Brown (EB) Secretary	Jisc	United Kingdom
Wolfgang Pempe (WP)	DFN – Member Representative	Germany
Manne Miettinen (MM)	NORDUnet	Finland

Minutes of the previous meeting on 16th August are pending approval.

1. **Actions**

Ref	Description	Owner	Complete by	Status
102.1	Emily & Grace to look to better present financial data	GM / EB	Sept 2023	**Closed.**
106.6	Board to agree plan to discuss income generation, review of regulations and succession planning	Board	February 2023	**Ongoing – on the agenda for Oct meeting**
107.1	The Board to discuss the possibility of revising the lower membership rates in the near future.	Board	February 2023	**Closed.**
109.1	Revise membership documents. Move away from 'charter' language. Look at what it means for a member to join.	Board	September	**Open – on the agenda for Oct meeting.**

109.2	Steve – Investigate regarding donations / tax identifier number? How to make donations possible via PayPal	SZ		**Open – Steve to send over a paper with options outlined.** **Discussion ongoing.**
112.1	Re-send survey data for techex.	EB	Aug 2023	**Closed.**
112.2	Daasi	EB	September 2023	**Ongoing – awaiting a response from Daasi.**

2. **Financial and membership updates**

All renewals are out until November.

Response rates are looking healthy.

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

3. **Development update**

https://shibboleth.atlassian.net/wiki/spaces/DEV/blog/2023/09/11/3274014738/September+2023+Update

The past month has been spent getting betas of the IdP and all our plugins available for testing and getting ready for the V5 release, which is expected to occur over the course of this week. Nothing significant has come up while testing, though thanks to a member reporting a problem when Duo fell over a couple of weeks ago, we identified what is probably an HTTP connection leak that happens mainly when certain kinds of connection failures occur. That's been fixed for the release obviously.

The initial EOL date for V4 is probably going to be set at a year out, consistent with past major releases. Based on how some of our own upgrades have been going, it is likely if not certain that we may reduce this further simply to free up time that can be better spent on new work than issuing patches. So far the upgrade process has been very smooth, and this appears to be the least impactful major upgrade in the project's history. Ultimately we are driven by the feedback we get, so these plans are based on only our own internal sense of what the upgrade looks like and is always subject to revision. Even if it costs us some support time to help members upgrade, that's time better spent than patching old code.

Of course all of the plugins are ready to go and we have re-run the OpenID certfication tests on both the OP and RP successfully. Note that:

- All plugins will require updating after the upgrade. The installer notes this.

- Some plugins are more or less required now due to changes, such as the need for a scripting plugin for Javascript support due to Java changes, and the need to migrate to the JDBC storage plugin if currently using the older Hibernate/JPA-based option, which has been removed.

The OP includes some small and some not-so-small improvements and new features that will take some time to document, but we are moving toward what I consider the holy grail, the ability to operate the OP without any form of client registration or metadata at all for internal, commonly-configured services. That will never meet all needs, but if 95% of the clients one supports can be defaulted, that's a 95% work reduction compared to other OP implementations.

The next steps for the project, aside from obvious things like possible patches to the older software and a few backlogged work items, are going to be to get the roadmap in order and start producing some estimates for our potential future work which the Board will work into budget proposals for the membership to consider. We have plenty of work to keep us busy will that gets done, but we need to make some decisions by early to mid-2024 before we go too far on any major work items.

Among the more obvious candidate work items are:

- the SP redesign
- a plugin for FIDO 2 / WebAuthn support
- a user profile capability that likely will include self-management of features like consent and the aforementioned WebAuthn features
- various OAuth enhancements and additions (e.g., proof of posession tokens)
- OIDCfed support
- some kind of plugin to deliver a working Jetty container
- the usual documentation backlog
- code auditing

I will be at TechExchange in Minneapolis next week to present a project update along with sitting on a couple of panels, so I will see some of you in person for the first time in a few years.

A final note: Albert Wu of Internet2 has managed to recover a long-lost artifact, the original (and insanely overspecified) Shibboleth Message Flow diagram, and for a limited time it's once again available on clothing for people who truly don't care what others think of their wardrobe.

The OG Shibboleth Message Flow

(Notably, there's no money coming back to us from this, so don't buy one as a donation.)

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 – notes from Grace Moore**

Fed CM Messaging at TechEx:

- Group discussed the Fed CM threat and how Jisc / GEANT are starting to respond to this, with a particular focus on the need for awareness raising, thought leadership and lobbying
- Discussed that from a US perspective – National Institute of Health (NIH) and the National Science Foundation (NSF) could be key allies as both have a significantly vested interest in Shibboleth and SAML
    - For NIH – they have mandated a top down approach on both IdPs and SPs
    - For NSF – it is not mandated but has been heavily adopted by existing insitutitions within their network, so there is a significant groundswell among their community
- Discussed / agreed that a loose form of words should be provided for board members attending TechEx, in case they were asked about this by the community
- Discussed that any 'ruckus' would need full government and institutional backing, but was unlikely to be successful
- Discussed that privacy legislation, such as anti-trust matters going through in California, may be key to battling this change and is vital for us to monitor
- The Consortium may need to be prepared to make a statement, in the longer term, and should consider how it's influence and community can be used

- Discussed need for a defensible and agnostic approach – one that is non-combative but likely to get attention
- Agreed that this should be discussed in next board meeting, including whether any support is required to support this (and subsequently any investment)
- The form of words that were shared with the board, to support conversations at TechEx, were:
    - The consortium has people on the development team, and at board level, who are actively participating in discussions and working groups
    - The consortium is also working with external partners, who have a shared interest in exploring work arounds / solutions, such as DAASI
    - At this stage – we are unsure of the outcome and unable to offer clarity on next steps

Charging Increase:

- Scott was keen to announce this as a soft launch at TechEx – didn't anticipate blow back but key to start socialising early and particularly as this was the key audience affected, all in one place
- Board had not returned votes by requested date. Agreed that Consortium Manager needs to chase these responses in future to ensure a timely conclusion of votes.
- Agreed that Consortium Manager would chase board members for an indicative response before end of week, so that soft launch announcement could go ahead so long as no fundamental objections
- Agreed that the formal press release can be developed and distributed after the event

Survey Results:

- Discussed that we would need to get a data analyst to assess the data as it's hard to make much sense / value from it, in it's current format
- Agreed to try and present a few key highlights at TechEx so community could see how this would feed into future plans
- Points of note include:
    - 53 respondents were using the OIDC plugin – interesting as this is organic growth although shows it's not yet at mass adoption by the community
    - 48% still find Shibboleth very (5%) or fairly (43%) difficult to use. Scott discussed that the dev team are working to hide the guts but there is a limit as to what can be hidden.
    - Almost 57% of members have used Shibboleth for 10 years or more
    - Familiarity with SAML was highest among respondents with OIDC coming in 2nd (167 respondents were familiar) and OAuth in 3rd (respondents were familiar with the protocol / standards)
    - The majority of organisations rely on in-house experts to provide support and training, with seeking support/training from NRENs coming in 2nd place, and the Consortium largely being the source of last resort
    - Overall satisfaction with Shibboleth sits at around 83%

SSTM/Oasis:

a. Alex raised discussion about new metadata thought to be being developed.
b. Leif was trying to get through OASIS as an extension.
c. **Scott didn't think anything was happening with this and it's not on the Oasis website.**

6. **Next Meetings:**

Wednesday 18th October
Wednesday 8th November