# Minutes of Shibboleth Consortium Board Meeting #108
# 8th March 2023 – Videoconference

## Attendees

| Name | Organisation | Country |
|---|---|---|
| Scott Cantor (SC) | Developer Representative | United States |
| Davide Vaghetti (DV) | GARR – Member Representative | Italy |
| Emily Brown (EB) Secretary | Jisc | United Kingdom |
| Steve Zoppi (SZ) | Internet2 | United States |
| Alex Stuart (AS) | Jisc | United Kingdom |
| Manne Miettinen (MM) | NORDUnet | Finland |

## Apologies

| | | |
|---|---|---|
| Wolfgang Pempe (WP) | DFN – Member Representative | Germany |
| Kevin Morooney (KM) | Internet2 | United States |

Minutes of the previous meeting on 11th January are pending approval.

### 1. Actions

| Ref | Description | Owner | Complete by | Status |
|---|---|---|---|---|
| 102.1 | Emily & Grace to look to better present financial data | GM / EB | December 2022 | **Ongoing. Completed first draft.** Revisions to be made moving into Jan 23 (Developer Contract & Hours Info). **We aim to have this completed by the end of Jisc financial year (July).** |
| 106.3 | DAASI? discussion about Privacy idea | SC | January 2023 | **Emily working with legal to draft up a contract.** |
| 106.6 | Board to agree plan to discuss income generation, review of regulations and succession planning | Board | February 2023 | **Ongoing. Grace will be joining April's meeting to discuss further.** |
| 107.1 | The Board to discuss the possibility of revising the lower membership rates in the near future. | Board | February 2023 | **Ongoing.** |

| | | | | |
|---|---|---|---|---|
| 108.1 | Steve/Scott & Rodd looking into making formal documentation public. Onboarding calls / navigating the software. | SC & SZ | March 2023 | **Ongoing.** |
| 108.2 | Emily to send over the initial survey results to board. | EB | March/April 2023. | **Ongoing.** |
| 108.3 | Board agreed to plan an increase in rates from Jan 2024. | EB | July/Aug | **Currently Emily is focusing on moving our financial data into Quickbooks. Once this has been achieved, we will look at the projections for future rate increases.** |

## 2. Financial and membership updates

Renewal requests are out up until July, with response rates looking good.

All renewal requests are out for 2022. Awaiting 2 confirmations from Akita Bank and Lafayette College.

Indiana University of Pennsylvania have stated that they are no longer interested in membership.

## 3. Development update

Following on from February, I have been primarily working on refactoring code into a new java-shib-profile project, the third new library in between OpenSAML and the IdP. Of late, we've also been discussing the possibility of migrating some of the OpenSAML "implementation" classes that pertain to the IdP to reduce the size of the that library and migrate out code that is largely unique to our projects. In the meantime, my focus has been on reviewing and refactoring the RelyingParty and ProfileConfiguration classes in the IdP. The end goal is to ensure that for the most part only interfaces remain public, moving the concrete classes out of the API since they are implementation details for the most part.

In addition, I have been refactoring and altering the various profile configuration interfaces to both add new settings introduced by the needs of the SP (where they also make sense for the IdP) and also moving around settings that were "too high" in the interface tree. For example, settings pertaining to signing and encrypting assertions were visible on profiles (like logout) that obviously don't include assertions. Some of this work is already reflected in the V4 documentation to better reflect where the settings will be available in the future. These changes could technically impact deployers but it seems unlikely in practice since one would have to have applied a setting that was being ignored anyway.

One new feature introduced by this work is a functional hook to install code that can make changes to incoming or outgoing SAML messages more simply than having to create an entire interceptor flow. This isn't a common need but once in a while it comes up on the list.

The end result is a package of shared profile interfaces with common behavior, with IdP- (and SP-) specific extensions to those interfaces where necessary, and a focus on making sure settings are only available where they actually make sense.

In addition I have continued to work out in draft form how the SP configuration might work and relate to these existing designs before really working on any code for it. In the process, I abandoned my original plan to produce an "AssertingParty" parallel in favor of going back to the existing (though relocated) RelyingParty concept from the IdP. The SP already uses that nomenclature in its configuration so breaking with this seemed to offer little benefit, even if it's a little awkward conceptually. How much actual code will be reused is unclear, but one change is that most of the RelyingParty machinery is now outside the IdP, and the changes to package names will impact deployers a little bit, requiring some additional mechanical string replacement in scripts. We hope to extend the installer to scan the configuration to flag as much of this as we can.

My current (as of today, it changes a lot) thinking about the SP is that I would like to try and adapt at least some of the general structure of the existing configuration in this area. Much like with the transition from IdP V2's relying-party.xml from custom XML to Spring, a similar kind of change will play out here, retaining (in Spring syntax) the notion of an "Application" as a containing object that optionally includes "RelyingParty" overrides. Notably we cannot support the existing SP syntax the way we did for the IdP, but the hope is to make the transition less structurally jarring than a completely different approach would be. A lot of this will start to take shape now as I wire things up and see how it fits together, and incorporates all of the IdP's security configuration wiring.

On other fronts, we released another snapshot of the OIDC RP plugin, and we have snapshots released now of the first interations of all the OIDC plugins in a form allowing them to co-exist with each other. This marks a milestone signaling we're pretty close to being able to ship all that work.

Phil Smart ably represented the project at the recent FedCM session in San Francisco. New proposals to adapt the FedCM work to allow for SAML and OIDC to keep working were crafted with representatives from Google and Mozilla , and now have to be prototyped and "sold" to the wider community. Moving in a cross-protocol direction is hugely important to head off an OIDC-specific approach. An interesting aspect of this effort is the spreading realization that metadata-based federations are the only infrastructure (for either protocol) that actually provides any trust that a particular SP or IdP endpoint is legitimate. Typical commercial use of SAML has no such source of "truth", and OIDC was trustless by design. Perhaps for the first time, the limits of self-asserted metadata are dawning on more people.

4. **Discussion of Development Roadmap and sustainability of Development team**

Scott will update the roadmap in the new year to reflect the results of the survey.

## 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**

- Survey – closed

**6. Next Meetings:**

**Wednesday 12th April**
**Wednesday 10th May**