



## Minutes of Shibboleth Consortium Board Meeting #121 8<sup>th</sup> May 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 Axelsson (PA)          | NORDUnet                     | Sweden         |
| 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  |

### Apologies

|                     |                             |         |
|---------------------|-----------------------------|---------|
| Wolfgang Pempe (WP) | DFN – Member Representative | Germany |
|---------------------|-----------------------------|---------|

Meeting Minutes approved from 10/04/2024.

### 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 | <b>Closed.</b>                          |
| 120.2 | Davide to seek feedback on the grant application, from GEANT, and explore potential to benefit from incubator | DV          | End of May 24   | <b>Open. No feedback as of 08.05.24</b> |
| 121.1 | Create workshop date for September                                                                            | EB          | May 2024        | <b>Open.</b>                            |
| 121.2 | Rate increase comms to be drafted.                                                                            | EB & Board. | June 2024       | <b>Open.</b>                            |

## 2. Financial and membership updates

Shibboleth Consortium Like4Like – attached to Agenda.

## 3. Development update

<https://shibboleth.atlassian.net/wiki/spaces/DEV/blog/2024/05/06/3580526593/May+2024+Update>

April saw the planned release of the latest round of OpenID Connect plugin minor upgrade (per OPReleaseNotes and OIDCRelyingPartyAuthnConfigurationReleaseNotes). The most significant addition is probably the first release of logout support in the OP, which is designed to integrate into the IdP's existing logout framework for SAML SPs. The plugins are designed to be compatible with both V5.0 and V5.1 to make upgrades simpler for people on different patching cycles.

A second alpha release of native WebAuthn support for the IdP is also available for testing.

Work on the Duo plugin update is finally complete at this point, so a release should be expected this month. We have updated and cataloged a number of demonstration videos covering the new passwordless features, so check those out if the documentation isn't clear enough on how it works.

Active work at this point is focused on finishing up the first WebAuthn plugin release and on the next iteration of feature work on OpenID Connect. The next two OpenID priorities are adding support for  RFC 9126: OAuth 2.0 Pushed Authorization Requests and some initial Proof of Possession features to support stronger token verification. Work on OpenID Federation support is expected to start later this year. We are largely basing our decisions on future work on member input at this point, as there's more demand for features there than capacity at the moment.

Because we have been receiving more feedback and testing input than in the past on some of these newer releases, we will be making a concerted effort to be more transparent and public about our work schedule and the state of the various software projects as they trend toward beta or release candidate quality. This is not so much about planning our schedule out farther in advance or meeting

deadlines but about simply giving more people a clearer indication of when work on a release is wrapping up and testing would be more helpful.

As part of this effort, I'll be circulating updates to the dev list more frequently, and we will be working on scripts to provide a simple web-based view of all our software activity and the state of each project together with links to the latest snapshots in Nexus to make testing simpler for those so inclined. The intent is just to associate the snapshots with some simple labels indicating how close they are to being stable or ready for serious testing. We will hopefully be making the information available in both human and machine-readable form.

I have also returned to work on design and prototyping for the SP, mostly a lot of mental exercises thinking about different ways of organizing the configuration. In particular the challenges of actually supporting a hub capable of being shared across many different agents operating in different web sites is proving to be a major complication as compared to the current design that tightly couples shibd to the agents it serves. Coming up with a design that keeps common cases as simple as possible is the priority, as the less common cases will likely be somewhat harder to express (e.g., consider if you want to override a behavior for a specific IdP for only a subset of agents and how that might be expressed).

A major change in the planned design is a move to replace the socket-based remoting protocol in the current SP with HTTP. This was something I tried to avoid specifically because Apache's server API lacks an HTTP client, so making this change definitely complicates matters and will likely introduce dependencies on Microsoft's HTTP client (on Windows) and libcurl (everywhere else). That isn't ideal, but this use of libcurl is much different in nature than the usage now, and is at a more rudimentary level, so the hope is this won't complicate the build too badly. In most other cases in the future, agents will likely have ready access to such a client anyway. The development of the functionality in Java will be greatly aided by using HTTP by making this a plugin to the IdP and reusing the existing Spring Web Flow design.

Work will continue over the summer and fall to start to flesh out proof of concept code in a number of areas so that work on a refactored Apache agent can also get underway. Ironically, the last and least important work to do is actually implementing SAML itself because that's a very small part of what the SP actually does. The harder problems to solve are configuration, migration paths from the current software, sessions, and handling of attributes. Adding the SAML processing will be a relatively simple task during the later stages of work.

#### **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.

#### **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 % rate increase was agreed in April workshop.

## **6. Next Meetings:**

**Wednesday 12<sup>th</sup> June**

**Wednesday 10<sup>TH</sup> July**