Minutes of Shibboleth Consortium Board Meeting #95

12th January 2022 – Videoconference

Attendees

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

Apologies

Rhys Smith (RS)	Jisc	United Kingdom
Joe Steele (JS)	Jisc	United Kingdom

Minutes of the previous meeting on 8th December 2021 were approved.

1. Actions

Ref	Description	Owner	Complete by	Status
93.1	Creation of a Shibboleth survey to acquire future development options from the community.	All	2022	**Ongoing Jan 2022**

2. Financial and membership updates

During the call Emily reported that payments were still due from the below members from 2021: University of Wisconsin-Madison, Marist College , University of Washington, Cornell University, CANARIE, Aktia Bank PLC, and the University of Maryland.

Invoices are currently out with: University of Wisconsin - Madison, University of Maryland, University of Washington, Cornell University, ACOnet , Marist College , University of Oxford, GARR, Johns Hopkins University, Sheridan College, Southern Methodist University, KU Leuven University, Gjaldstovan Talgildu Foroyar, The Rector and Visitors of the University of Virginia, CANARIE, Aktia Bank PLC, SWITCH, Brandeis University, Ligo Scientific Collaboration, University of California Office of the President, Deakin University, DAASI International, Stanford University, University of Toronto, The Rector and Visitors of the University of Virginia, Brandeis University, Gjaldstovan Talgildu Foroyar, Avasad, SWITCH, University of California Office of the President, The University of British Columbia (21/22 Renewal) and HEAnet.

A report is yet to be provided by Credit Control to see if any of the outstanding invoices have been received since the new year.

All January 2022 renewals have been sent out and confirmed from: North-western University, Mind Mercatis, Temple University & MIT.

3. Development update

Scott's update:
https://shibboleth.atlassian.net/wiki/spaces/DEV/blog/2022/01/11/2905243654/January+2022+Update

All projects were impacted to some degree by the log4shell vulnerability, which triggered a wave of questionable bug reports to a lot of logging libraries and a lot of triaging and threat assessment. The Shibboleth Project migrated away from log4j a long time ago so was not directly impacted by the mess, but we kept tabs on discussions around a supposed logback vulnerability that didn’t really turn out to be one. Nevertheless the maintainer acted conservatively and issued a CVE and a number of quick updates, and we felt waiting for things to settle was the best path to take. The latest logback release actually removes a few riskier features, but they probably aren’t coming back, so in the interest of caution and avoiding surprises later, we’re going to incorporate logback 1.2.10 into the next IdP patch (V4.1.5).

We are in the process of preparing that patch release now, and it should be imminent. The other known third-party CVEs that are feasible to address should be dealt with in that patch. There’s not much else in the queue for that patch, only some minor fixes. While this patch will be built using our old “we host all the jars” process, we do have the new signature and dependency checking enforcement enabled on the branch, and we hope to be ready to move to using Maven Central for third party artifacts in the near future to reduce the burden of constantly uploading everything ourselves.

Work has started in parallel to stand up a development branch of the IdP on top of Spring 6 and Java 17, and we are identifying where we have dependencies at risk due to the transition that may have to be remediated out or become internally forked projects. The most serious of these is, as expected, Spring WebFlow, about which we are trying to get an official admission of it being end of life. We don't think, at this point, there will be much chance we can identify a practical alternative so some kind of stripped down fork with as much removed as possible is the most likely outcome here.

During development work on the previously described OAuth enhancements to the OP plugin, some vulnerabilities around the handling of JWT client authentication were noted and fixed over the holidays, with that patch going out early this year. This doesn't impact a lot of deployers at this point, but the JWT support probably should be more widely adopted, as it allows for public-key authentication of clients, which in turn (combined with our SAML metadata support for OIDC) essentially would open the door to practical federation of OIDC and OAuth.

Work continues on a number of parallel projects centered around OIDC and OAuth features that will require IdP V4.2, so all of those releases are likely coming sometime this quarter. This will hopefully include the initial support for proxying authentication to an OIDC OP (in the form of a new RP plugin), at worst shortly after we ship everything else. The OAuth enhancements aren't functional yet but support for extending client (RP) authentication using the IdP's login flow machinery is feature complete already. This allows for validating client secrets using all the pre-existing back-end options supported by the Password login flow (e.g., LDAP, Kerberos, JAAS, and local htpasswd files), and easily extending this to additional options. Use of client metadata and dynamic registration is still supported, but having secrets in files or in the clear in a database is not good, so this will allow them to be externalized seamlessly (though see above, public keys are certainly a much better way to go).

The work on the client_credentials grant and JWT access tokens should be close to feature complete this month, and a number of RFCs will factor into making that work as standardized as we can make it. It is likely that we will punt a lot of the deployer pluggability for this feature to the Attribute Resolver as a means of defining policy around scopes and resources when issuing tokens. The resolver is the most powerful way of abstracting that kind of functionality, though we may embed some kind of simple API around it to allow for other implementations.

Until we get a lot of this work done, continuing with the SP redesign will be more or less on hold until probably this summer so there's not much to report there, but we should have packages available for some additional RPM-based platforms in the interim.

4. Discussion of Development Roadmap and sustainability of Development team

The below remains the same regarding the roadmap. Additional pieces will be delivered once we receive feedback from both Domino's & the survey.

The development project roadmap has been updated, showing clearly what work is ongoing, committed, planned, under discussion and parked. This was included in Scott's monthly update so members and watchers of the project can see. Time will tell if there is input from the community on the roadmap and any requests to add or attend to particular items.

When the skills matrix is collated, this will help enable the Board to see where skills are required and a plan can then be made as to how best to acquire them. This could be through offering financial incentives whereby the Consortium pays for effort from its membership; off-setting membership fees; or approaching agencies who specialise in finding/providing development effort. In any case, expenditure will need to be weighed against the benefits of gaining extra effort vs the overall balance and financial health of the Consortium.

Scott noted that a larger Dev team than we currently have would need PM effort too, which would incur extra cost. He also noted that the safeguarding of skills currently held by team members who may retire or leave the project is more important than expanding the team.

Justin noted that with some uncertainty about budgets and membership renewals, it would be worth waiting another 3 months or so before considering any significant expenditure.

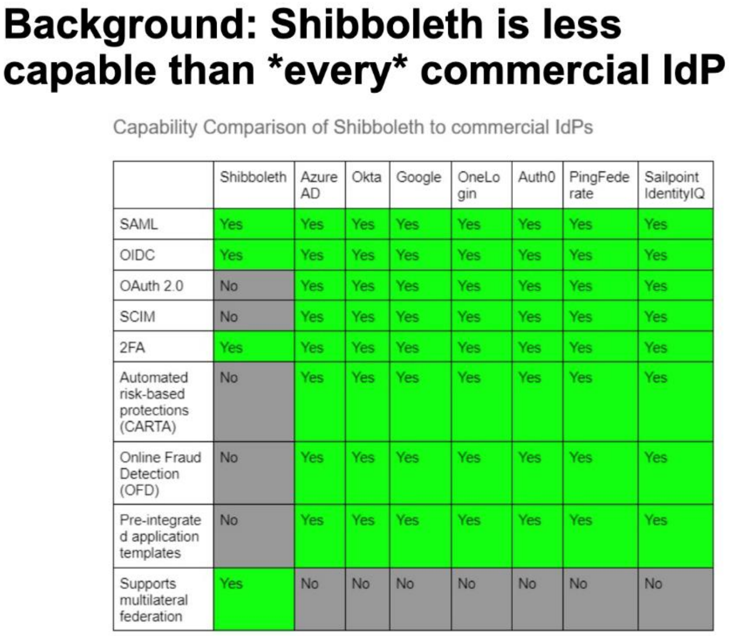
Regarding the above, Emily noted that the board had a discussion regarding an identity management portal for future development as well as a project manager to ease the growing workload and to aid future developments/ direction. The Consortium are in the financial position for this to happen. The board agreed that this should happen sooner rather than later.

Scott noted that the team are making sure the documentation regarding infrastructure/ onboarding/ are up to date and that he will continue to document this process.

5. AOB

The Board began the discussion surrounding the creation of a survey to collate a sound direction for the next 5 years of the Consortium. The board are currently in the early stages of brainstorming ideas.

Mannes chart below shows possible outreach opportunities that we could use to educate and provides the ability to expose certain conflicts of interests:



Background: Shibboleth is less capable than *every* commercial IdP

Capability Comparison of Shibboleth to commercial IdPs

	Shibboleth	Azure AD	Okta	Google	OneLogin	Auth0	PingFederate	Sailpoint IdentityIQ
SAML	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
OIDC	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
OAuth 2.0	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SCIM	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes
2FA	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Automated risk-based protections (CARTA)	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Online Fraud Detection (OFD)	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Pre-integrated application templates	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Supports multilateral federation	Yes	No	No	No	No	No	No	No

The Board members will come to the next meeting with a few questions regarding their specific inquiry needs in relation to their specific audiences.

Please see the below 2021 summary:

Summary 2021:

Where 2021 saw a continuation of the ongoing pandemic, we saw a continuation of prosperous development and growth in regards to the Shibboleth Consortium.

Early last year saw the launch of our new Shibboleth Consortium website re-design. This more modern and practical design has indeed proved beneficial in the increase of direct traffic towards the Consortiums membership. The new design has similarly provided those interested with access to all membership options as well as the newly added meeting minutes to stay up to date with the board's monthly discussions.

On the development front, our development team remain at a total of 9. The composition of the Consortium Board has also remained the same, with Internet2, NORDUnet and Jisc maintaining their roles as Principal members.

As the Consortium continues to increase its engagement, the board are in the process of creating a survey to collate information on our future agenda over the next 5 years. The audience for the survey will include current customers as well as those who may be misinformed and those who have veered away over time. The purpose of the survey will be to create an aligned position and guidance for the community for future development options.

Turning to development, we cannot overstate the significance of the changes in version 4.1 of the IdP. Released in early 2021, it introduces a plugin model and comprehensive OIDC OP support. The plugin model allows the core IdP to be smaller, and additional functionality to be added only if needed. It should help increase the speed of feature delivery and enhancements with greater security isolation. The OIDC OP plugin supports the majority of OP profiles and passed the OpenID certification tests in June. Other plugins provide support for Duo's strong two-factor authentication, and for ECMAscript support.

The lull after the release of IdP version 4.1 allowed the team to work on project infrastructure. Confluence and Jira server were migrated to the cloud. The team enhanced the scrutiny of third party components and improved the integrity of the build process.

Work on the SP continued. A new Docker-based build system gave the team space to consider the range of supported platforms. Rocky linux 8 and Amazon linux 2 have been added, and macOS and CentOS 8 are no longer officially supported. The re-design of the SP in Java is progressing.

In reference to the Consortiums finance and membership position, 2021 was a stable year. Overall , membership has risen to a total of 60 members, gaining a small 4 members this year and unfortunately losing 1. In a tough financial year we close 2021 on a balance of £720k. We are pleased to say that no membership fee increases are planned, maintaining the same fees that were introduced in 2017 and setting us up well for a promising year ahead.

Overall, the Consortium maintained its uniformed position with plans to enhance Shibboleth further to the needs of the community throughout 2022. We would like to thank all our members, partners and donors of the Shibboleth Consortium for another successful year. We are hugely grateful to everyone who has contributed to Shibboleth over the past 12 months, and look forward to working with you in the year to come.

For information on the Consortium, please email emily.brown@jisc.ac.uk or contact@shibboleth.net

6. Next Meetings:

Wednesday 9th February
Wednesday 9th March