



Minutes of Shibboleth Consortium Board Meeting #106 14th December 2022 – Videoconference

Attendees

Name	Organisation	Country
Scott Cantor (SC)	Developer Representative	United States
Kevin Morrooney (KM)	Internet2	United States
Grace Moore (GM) Temporary Secretary	Jisc	United Kingdom
Steve Zoppi (SZ)	Internet2	United States
Wolfgang Pempe (WP)	DFN – Member Representative	Germany
Alex Stuart (AS)	Jisc	United Kingdom
Manne Miettinen (MM)	NORDUnet	Finland
Davide Vagheti (DV)	GARR – Member Representative	Italy

Apologies

Emily Brown (EB) Secretary	Jisc	United Kingdom
----------------------------	------	----------------

Minutes of the previous meeting on 9th November meeting were approved.

1. Actions

Ref	Description	Owner	Complete by	Status
102.1	Emily & Grace to look to better present financial data	GM / EB	December 2022	Completed first draft. Revisions to be made moving into Jan 23 (Developer Contract & Hours Info).
102.2	Review Development Offer forwarded by Scott	Board	September 2022	Completed. Discussed in meeting – voted to push back on capped amount and reduced deliverables.
105.1	Renew Shibboleth.net	AS/JS	November 2022	Completed.
105.2	Survey: Next steps	AS/EB	November	Completed. Sent on 1 st December 2022. Discussion in meeting about new send dates + timeline.

106.1	Webinar on Advisory	Board	???	Discussed but not assigned in 14th Dec board meeting
106.2	Jisc advisory test on v4/4.1	AS	January 2023	If possible
106.3	Discussion about Privacy idea	SC	January 2023	Scott to contact author about potential for Privacy idea, whether tech or financial contribution
106.4	Scott to feedback on DAASI? Proposal	SC	January 2023	Scott to discuss statement of work and feedback to board
106.5	Confirm survey timeline and provide example email	GM	December 2023	Completed. Please see notes for AOB
106.6	Board to agree plan to discuss income generation, review of regulations and succession planning	Board	January 2023	As it says on the tin

2. Financial and membership updates

Outstanding payments to be confirmed ASAP after meeting. Awaiting a full list from Jisc's Credit Control of to confirm the debtors for 2022.

Renewal requests are out for everyone until the end of the year. Update to be provided ASAP after the meeting.

Focus was on presenting the 3 year financial update / position to the board and discussing the options paper for this. In essence – the Consortium is running at a deficit and will either need to increase income, or cut costs, if it wishes to sustain itself.

Reviewed following documents:

- High-level 3 Year Financial Update
- Options paper for increasing income, including commentary from this meeting

Agreed to revisit in next board meeting (11th January). Potential for board to run a half day workshop, to agree some 'quick wins'.

3. Development update

Talk at TechX, Denver

- No real feedback, appeared to go well. Not many questions
- One or two have raised concerns about the compressed timelines, i.e. getting off of Spring 5
- Scott has said that we'll do our best to get v4.3 live in January, with view to roll out v5 by end of quarter, so there's as small a gap as possible. v4.3 should be thought of as an interim release.
 - (Scott Ed Note: I screwed up the dates anyway, Spring 5 EOL is Dec 2024, not 2023, so we have time)

Security Issue – if it amuses you, this is my attempt to capture the technical discussion

Vendor reported issue to Apache who flagged to Santuario about a possible vuln. Issue relates to XML Encryption usage that is applicable to SAML.

<Executive Session Discussion of issue>

Advisory will be issued, and we are researching workarounds to help people on older IdPs, as current IdP appears unimpacted. Full scope of bug requires use of older, unpatched Java versions.

Steve wants to advocate for those with container deployments to just pull the container.

- Discussed that typically running an installer is enough, and that we need to bottom out why people don't think they can.
- Discussed that people 'don't know what they don't know' and there is likely a fear of unintended consequences. Suggested a webinar to give clarity on deployment advice.

Privacy idea

Raised by Davide Vagheti. Discussed an idea from SWITCH, which was signalled by DFN originally.

- <https://doku.tid.dfn.de/en:shibidp:plugin-fudiscr>
- Has been implemented by an Identity specialist at German university and is also being used by an Italian university
- Supports built in WebAuthn + Passkeys, amongst other things, but only for PrivacyIdea back-ends

Scott said he hasn't explored the code yet but has a concern from a support standpoint.

- Team don't use or know the PrivacyIdea solution, it 's complex software
- Would need to segregate that issue as can't support Privacy idea problems
- Another challenge is it's highly customised and uses lots of APIs, all doing things in a very abstract way This makes it hard to leverage more generally and isn't generic support for webAuthn
- Hasn't decided which way we want to go. Could use a version of it. Recommends this is a focus after v5 ships, which is when team is due to look at pass keys anyway.

Discussion around other ways to support this externally, such as signposting or even making financial contributions, if we do not wish to assign resource. No firm action agreed. Could be that we make a plug-in available, though don't want to takeover the code. Davide shared link for one:

<https://identity.fu-berlin.de/downloads/shibboleth/idp/plugins/authn/fudiscr/current/fudis-shibboleth-idp-plugin-authn-fudiscr-current.tar.gz>

Actions agreed:

- Scott to discuss with author(s) to see how we can work together, whether it be tech or financial contribution and update the board
- Phil Smart to review code from Switch/Duke/Carolina after v5 is shipped

DAASI Statement of Work

Statement of work has now been circulated. A little rough but captures the essence of conversations. Doesn't reflect wider conversations about future of the FedCM work though.

They want to test a log-out exercise with Google, examining the FedCM requirement and seeing if there is a way to make SAML log-out work. Currently we have no accurate reporting for logout,

which is not an issue based on current functionality and requirements. SAML log-out needs to make a request and get a response. Works differently to FedCM and is affected by 3rd party cookies.

Proposal is 16,000 EURO Total. It's around 10,000 EURO to develop the plug-in. This could be built into the Shibboleth software in time, if Google committed to the API.

May need more time for the bounce tracking changes, however this entails investigative work. Not looking at discovery – was hoping this might be in scope though not a priority.

Alex said that while the issue is primarily 3rd party cookies in log-out, item 4 is key. Timescales are much later than discussed and wondered whether this opportunity is exclusive to the Consortium, or if it's open to others too?

- Scott doesn't feel timelines are too far off (aiming for end of 2023)
- Reality is Google may not care and just break stuff
- Should get more feedback from them in early 2023
- Phil Smart may be good person to liaise with Google – discussed hackathon in Toronto in 2023

Alex raised the risk around deliverables and costs to the Consortium. This was echoed by other members of the board.

Discussed that Government customers are driving demand, but DAASI are looking to use partners like us to help finance the development.

Agreed that Scott will push back on the proposal a little to get it better defined in terms of the cap, and a reduced scope for deliverables.

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. Emily to provide details of individual developer's contracts and hours.

5. AOB

Member Survey

- This has now been circulated however is yet to be distributed to any individual mailing lists.
- GM to draft an example email and confirm timeline - circulate with meeting notes.
- Agreed to leave the survey open until Mid-February

- Agreed to send W/C 9th January onwards, leaving around 5 weeks for responses. Resends are optional.

Example Email:

Dear [First Name],

We hope you've had a fantastic start to the new year.

The Shibboleth Consortium are looking at ways to improve the quality of their free Identity Provider (IdP) and Service Provider (SP) software. They'd love to hear more about your experiences and thoughts.

Do you have 10 minutes to spare, to answer **this short survey?**

Participating allows you to have your voice heard. So, make sure to complete the survey if you've got a view on the future of the software.

The survey will close on 10th February 2023.

Thank you,

[Organisation]

6. Next Meetings:

Wednesday 11th January 2023

Weds 8th February 2023