**December 1, 2016 OpenID Executive Committee Call Minutes**

**Present:**

Don Thibeau, Executive Director

Nat Sakimura

Mike Jones

George Fletcher

John Bradley

Adam Dawes

**Visitors:**

Mike Leszcz, OpenID Foundation Staff

Tom Smedinghoff, Locke Lord LLP

1. **Executive Director’s Report**

Don sent a combined OpenID/OIX calendar for our review. We still need a host for the OpenID Summit before IIW on May 1st.

We’ll be having board elections in January. The elections will be for two community members – for seats currently held by John Bradley and Mike Jones – and for the corporate member position – for the seat currently held by Dale Olds of VMWare. Mike, as secretary, will work with Don and Mike Leszcz on the election schedule.

Don is planning for support infrastructure changes in 2017, which he will share with us at a future date.

1. **Certification Update**

Mike Jones reported on certification progress. Roland Hedberg has been working closely with both RP developers and Don, Mike Leszcz, and Mike Jones getting the RP Certification program ready to launch. At this point, there are at least 4 tested RPs (by Hans Zandbelt, Edmund Jay, Filip Skokan, and Roland Hedberg) that can be part of the initial launch. We’ve also sent pings to Janrain and Google asking them to participate. We anticipate RP Certification applications in December and a press release about certification progress during the RSA Conference (February 13th).

OP Certifications continue coming in several per month. We now have over 100 certifications. Don added that this is introducing us to new communities, such as Red Hat and Linux. Don also added that after all our work, it seems like we’ve gotten the pricing right.

Since the OP Certification launch, the testing code base has not stood still. Roland has made a number of improvements, some motived by the needs of the HEART. HEART’s testing work is based on Roland’s updated code base – not the frozen one deployed at op.certification.openid.net. We anticipate more kinds of tests to also eventually be added, for instance, from MODRNA, iGov, EAP, etc. As discussed by executive committee members, Roland, Justin Richer, and Debbie Bucci during CIS, the Foundation should have one unified certification suite that we expand to encompass these efforts – not a hodge-podge of different code bases that get increasingly out of sync with one another.

The OpenID Connect working group sees the need for several new kinds of certification profiles, among them, form post response mode tests, refresh token tests and logout tests.

From a business perspective, we agreed with Roland for him to take over the remaining deliverables from the Umeå contract. He has completed (and been paid for) 2 of the remaining 3. The remaining $3000 for the final milestone will be paid after two RP Certification applications have been received.

Mike Jones and Don asked Roland to create a proposal with fixed-price deliverables needed to keep our certification program strong and to expand its scope to meet additional developer needs. That proposal is attached. Mike discussed the need for the “Updating software version” deliverable and the two “Ongoing maintenance” deliverables. Mike also stated that he would review the other proposed deliverables for new tests with OpenID Connect working group before reporting back to the EC on them.

John pointed out that Justin Richer forked Roland’s code and is making changes to the fork. Mike reminded the EC of the discussion with Justin, Debbie, Roland, and the EC held at CIS. In that discussion, from which notes were circulated and agreed to, the EC members made it clear that the foundation wanted to have a single certification test suite, which would be extended as needed to accommodate the needs for additional certification tests. For instance, certification tests could be added for MODRNA, HEART, iGov, and EAP when their specifications and implementations reach appropriate levels maturity.

Of course, the test suite is open source software so anyone is free to use it in any way they see fit. But if enhancements are to be utilized as part of the foundation’s certification offering, they will need to be merged back into the certification code base. Per the discussion at CIS, the EC encourages Justin and HEART to pursue their enhancements in a manner that will enable all OpenID Foundation working groups to benefit from them. To be clear, if changes are being made that can’t be reintegrated, the EC agreed that that means that the authors are headed down a path that won’t lead to the software being used for OpenID Certification.

John said that a goal should be that the set of tests should be able to be expanded by third parties. Mike said that he viewed that mostly as being a documentation issue. Roland’s deliverables all include providing appropriate documentation so that others can use and maintain the software.

Mike reported that some of the enhancements made to the testing software since our certification launch have been to enable packaging it as a Docker container. Roland has reported that private installations of the software are in production use by at least four sites, including by at least one OpenID Foundation sustaining member.

Nat asked how to manage our risks in case Roland is hit by a bus. Don and Mike reported that Roland already is committed to writing down sufficiently detailed instructions such that others can do all the tasks that he does. This is part of the remaining deliverable from the existing contract. Mike pointed out that once these instructions are complete, it might be useful to have Hans Zandbelt or someone else try to use them to validate that they are actually complete.

We discussed approving the milestones in the new proposal to update the software to the current version and to perform ongoing maintenance. Don confirmed that we could pay for this out of existing general funds. Don said that PayPal has rejoined at the board level, which gives us some budgetary space to do this.

A decision was unanimously taken to fund updating the software version, ongoing maintenance from RP launch to RSA, and ongoing maintenance from RSA to IIW. Mike moved and Adam seconded.

Mike will take the additional proposed tests and profiles to the OpenID Connect working group for their review. After that review, we can consider authorizing work on those.

Adam discussed that there have been a range of RP implementations deployed of varying quality, problems in some of which have recently made the news. Adam sees RP testing as a tool to help improve the quality of RP deployments. When an RP is using a general-purpose library, we should definitely encourage them to be certified.

John pointed out that some of the problems identified in the media are sites not even using OpenID Connect but using home-brew protocols. Our tests would not help in cases where people aren’t even using Connect. In some of these cases, native apps sent ID tokens to a back-end and the back-end used them without validating the signature or audience.

Mike suggested that we move this discussion to the Connect working group. Nat suggested that a tiger team in the Connect WG be developed to make recommendations for use cases such as these. John said that before we have tests for functionality, we need a standard for it.

1. **BibXML for OpenID Specifications**

Axel Nennker has been talking to the xml2rfc folks about having authoritative BibXML files for OpenID specifications. Nat suggests that we offer authoritative BibXML files. Nat said that we could collate the XML references already in our specs and offer them. Mike said that we already require openid.net/specs/ to be stable so we could create another stable location on openid.net, such as openid.net/bibxml/.

Nat moved that we create a committee to do this. John seconded. Mike offered to participate. The motion passed unanimously.

1. **FAPI WG Report and Implementer’s Draft Votes**

Nat reported that the FAPI WG will be requesting Implementer’s Draft votes for specs in about a week. John said that there are similar votes being considered for MODRNA and iGov. Mike said that we should also have Implementer’s Draft votes soon for the Front-Channel and Back-Channel Logout specs soon, and that he would be discussing that in the Connect working group.