Draft Meeting Minutes 27 June 2013

Kantara Federation Interop Teleconference

Date and Time

- **Date:** 27 June, 2013
- **Time:** 13:00 PDT | 16:00 EDT | X UTC | 22:00 CEST

Attendees

- John Bradley, Ping Identity
- Scott Cantor, Internet2
- Rainer Hoerbe, Identinetics
- Nate Klingenstein, Internet2
- Colin Wallis, Internal Affairs, NZ Govt

Apologies

Agenda

1. Administrative - roll call : Minutes from May 2
2. OAuth Profile & Testing
3. SAML2INT updates Kantara
4. OIX and other meta-data aggregator projects.
5. AOB

Minutes

1. Administrative

Approval of minutes from May 30th: Any revisions to those? Hearing no objections, Nate moved, minutes are adopted.

2. OAuth Profile & Testing

John: Did not make any progress, had discussion with US Govmt on restarting work on profile. There is still a plan having an OAuth Test at MIT just before next IETF meeting, but I am not sure that will work.

3. SAML2INT updates Kantara

Renewed interest in the saml2int profile from various places, like the IRB based on some theory for FICAM interop testing. Possibly for some product selection guideline for FICAM SPs.

The SAML Test Harness project is related to this, because the current work on the AT eGov profile has a significant overlap with saml2int.

Leif: There was a recent discussion about saml2int on the REFEDs list, about who has the stewardship of saml2int. A question was who is actually running the saml2int site. However, Andreas is on paternal leave, so it will take some time until this is resolved.

John: Scott prepared some changes to the document.

Latest ARB discussion about comparability, technology profile that would allow inCommon-certified for Kantara LoA1.

Leif: At least it would be a training exercise.

John: Is that motivation enough to prepare a revision of the document? It is not clear to me what parts of the SAC relate to specific technology profiles.

Leif: I can dig it out. There are certain section regarding key management, and other requirements on encryption etc. These are not the most obvious items.

John: It sounds like we could have something for the SAC to reference as a SAML deployment profile that people can get certified against as part of their service assessment.

Leif: We have done it for LoA 1 and 2, but it would be useful to do it for the remaining levels.

John: We would not need difference saml2int profiles for different LoAs?

Leif: Certainly not. I will poke the guy who can do this to spend some time.

Scott: There are not to many change items to samle2int, I think some were metadata related, XML-encryption recommendation will be added. TLS will be made a MUST, which is currently MAY, and Response Signing a MUST.

John: If you do SSL, there is no point in encrypting, unless you are signing the message and doing all the appropriate checks.

Leif: The whole notion of when you should do encryption, and the value of end-to-end protection of assertions. It is probably something that has not be discussed very well. And the difference between Artifact and Post when it comes to end-to-end protection. I am not saying that we should change the normative text, but add the benefits and limits of TLS.

Scott: Yes, that should have been in the SAML2 Security and Privacy Considerations document.

Leif: We ran up against an implementation with broken encryption support, so badly, because people behind it thought without encryption it would make debugging much easier. We need a stable reference to point out what not to do, because it is stupid.

Scott: It become more difficult to dance around those issues when it was known that the XML encryption spec was completely blown. There was an opportunity to fix it with an HMAC CBC mode, but my proposal was not taken.

John: We could wrap the SAML assertion inside Jose ;-)

Scott: We could still take Simple Sign.

Scott: There are some good news. Redhat is upgrading OpenSSL to 1.0.1 RHEL 6.x for TLS 1.1 support, which has the side effect to add support for GCM.

John: Problem with any counter mode encryptions, if the caller does not change the nonce for each call, you could still have a plain text attack when you XOR the various bodies. Actually CBC is less vulnerable against poor initialization vectors than GCM.

John: We are doing a rev of saml2int, and mention these security considerations in addition e.g. for people using GCM.

Colin: It appears to me that SAML 2.1 is not really scoped for that, and XML Enc might not be regarded, because implementers might not pay attention to it because of its credibility.

Scott: Saml2int is a deployers, not an implementers profile. If developers do not read XML Enc, you have got a much bigger problem.

John: People ought to look at these issues in their deployments to look or test for some of these. Checking for different nonces to be used by CGM – which we recommend – could be a relatively simple test. So an appendix could list some things that people should look out for. As an example in OpenID the endpoint that checks signatures: according to the spec you are not supposed to check shared assertions, but if one implemented an endpoint that validated a shared assertion then potentially the security would go out of the window. Even it is written in the spec, it you do not test it, you may operate IDPs without security for years.

Rainer: Didn't we have a discussion that FI-WG should propose saml2int as a profile to the SSTC.

John: I think we did not make a decision; we might want to update the profile before we submit it. Scott, would it make sense to the SSTC to submit it as a deployment profile?

Scott: There was a discussion, but it was also the question if Chad would have enough time. If all things materialize, it would be pretty straightforward to do a conformance mode based on saml2int. In general I am more interested in a conformance mode for implementers than deployers.

Rainer: saml2int would have to come in a package with the eGov Interop profile.

Scott: Yes, I am making the assumption that the thing that has been done with the metadata document that references IOP would be done and references there. In summary, a better conformance mode is needed to reflect reality.

Rainer: Should the FI-WG take some action in the course of the SAML 2.1 work?

Scott: eGov is in some sense an implementers conformance profile that is a superset of what is needed for saml2int. Yes, I think when the time comes Kantara could submit a document for consideration.

John: It might make sense to annotate eGov to show what is required by saml2int. That is probably a step after we clean up saml2int. Let this put on the agenda for the next call.

4. Metadata Aggregator project

At refeds and other places we have been discussing the Account Chooser stuff to support IDP selection. The current status is that the OpenID foundation is looking into creating some metadata which can push information about trusted IDPs into Account Chooser without having to go into a user consent flow. The main concern is to avoid spam. Currently everybody can push information into Account Chooser, but the user has to agree. MS, Goolge and others want to out information for their own users into Account Chooser. It is still to be determined how to get IDPs on the naughty/nice list. Leif, where are we at with the refeds stuff for discovery?

Leif: It is actually published online at http://discovery.refeds.org. It does not mention Account Chooser. It is useful for academic account selection.

Actually, no one has tried to apply Account Chooser to SAML in practice. We need to try this.

Some SPs are concerned about giving the control for discovery away. Own discovery allows you to optimize the technical process, account chooser allows to optimize user experience using some costly UI components. Some people came to the conclusion that it is too focused on the graphics and probably not the right approach. The R&E community have not got that realization yet.

John: We should talk about a project to do some Account Chooser/SAML integration.

Leif: The simplest thing would be to do a kind of proxy.

John: In 2 weeks some people will be tied up with the cloud identity summit. We will discuss it on the list if we will have a meeting.

5. AOB

none

Next Meeting

- **Date:** Thurs, July 15, 2013
- **Time:** 13:00 PDT | 16:00 EDT | 22:00 CEST *(Time Chart)*
- **Dial-In:** Skype:+99051000000481 | Room Code: 178-2540
- (US Dial-In: +1-805-309-2350)

http://kantarainitiative.org/confluence/display/GI/Telco+Bridge+Info