eGov Meeting Minutes - 2012-02-06

Kantara eGov Working Group Teleconference

Date and Time | Attendees | Next Monthly Meeting:

Date and Time

- **Date:** 6. February 2012
- **Time:** 11:00 PDT | 14:00 EDT | 20:00 CET | 06:00 NZ(+1)

Attendees

Bob Sunday

Scott Cantor

Keith Uber

Thomas Gundel

John Bradley

Sal d'Agostino

Meeting Notes

1) Roll call for Quorum determination

Quorate. 6 of 9 voting members present.

2) eGov Membership Status

- No new members.

3) Review and approve December meeting draft minutes (attendees)

December minutes moved by Scott , Thomas seconded.

4) Status of eGov-WG for Kantara F2F Munich April 2012

- SLO topic to be discussed in Munich

- Keith, John and Thomas will take part. Afternoon time slots have been requested so that North American members can join by phone.

5) Update: Collaboration on Profile Management: REFEDS SAML2int, a subset" of Kantara eGov SAML2.0 implementation profile.

Discussion regarding proposed changes, including addition of TLS as a requirement

TLS 1.1, TLS 1,0 , SSL as a last resort
TLS 1.1 is difficult to roll out.
USA deployment profile states TLS 1.2 "using an approved algorithm"

Need to get a feel for what the requirements are in the field.
Strictness has always been a deployment profile issue

Higher ed has always had lower requirements. For example, due to bureaucratic difficulties implementing SSL/TLS, this is sometimes not implemented.

Scott invites members to join the OASIS calls in SAML2. The wiki is open for non-members.

Joni gave a note that she wanted to know what the workgroup's plans are for contributing to additional test.

Scott has added many metadata issues to the list.

Keith offered to review the current tests and contribute more test cases.

We don't have test cases for all of the profile.

Discussion of what is the current coverage of test cases.

We need a volunteer.

6) Work Item 2: SLO (including Global Idle Timeout) use case/requirements update (Rainer and Keith)

Page has been created at IDP idle timeout management using session refresh via isPassive

Keith to invite other IDP implementations to participate.

SLO to discussed during F2F in Munich in April.

This led into a long discussion of timeouts, third-party cookies and logout from shared machines:

Bob :

There is no idle session timeout at all in the canada
3 lifetimes:

- assertion lifetime
- authentication session lifetime
- saml session lifetime (how long the IDP could send an SLO request)

The timeout is so short for the SSO timeout

If you have too low a saml session timeout, SAML requires the SP to kill the security session at that time
SessionNotOnOrAfter (making the length of the authentication session).

Scott:

Using a tick box at initial login if the user is on a shared computer is one technique to deal with overzealous browsers that save cookies. SSO for that session would then be prevented.

Age old problem
Firefox's behavior has been the biggest problem with it's session restart behaviour - it restores SSL protected cookies
Not enabled by default (3.5 will)
The option is broadly enabled by default
Listed in Bugzilla as a Feature, which is not appropriate.

HTML5 local storage might be a way around the cookie storage issue.

Thomas: Denmark has timeout set at
IDP 60 minutes
SP 30 minutes
+ use user education for logout, but doesn't solve the firefox problem

----

Scott: If there are typical things that people are finding useful, that have real world experience, then we could capture these to feed back into implementation profiles or an update to the spec.
Logout is an issue in the openid space too, and they can learn from these.

Scott: there was some discussion about HTML5 features to make logout more effective without relying on third party cookies.

john- scale issues for google, are not front channel
HTML5 post message, cached javascript is the best approach
The sp is updated from a logout within 10th of a second
A closed tab reopened will get the logout situation

Using the relying party in an iframe which opens a connection to the IDP which has a standard javascript which inspects the IDP cookies. If there's a change in status at the IDP it sends a post message to the sp in the iframe.

3rd party cookies are rejected more often by default.

The entire concept of signed in is getting bigger and bigger.
The sites using this are using javascript already in the browser,
Loading a new page is no longer a suitable paradigm, there is no more page by page navigation as before.

Google's tests have shown that it turns out to be a disaster on a large scale (millions and millions of logins).

Next Monthly Meeting:

- **Date:** Monday, March 5, 2012
- **Time:** 11:00 PDT | 14:00 EDT | 20:00 CET | 06:00 NZ(+1)