eGov Meeting Minutes - 2012-04-02

Kantara eGov Working Group Teleconference

Date and Time | Attendees | Next Monthly Meeting:

Date and Time

- **Date:** 2. April 2012
- **Time:** 11:00 PDT | 14:00 EDT | 20:00 CET | 08:00 NZ(+1)

Attendees

Bob Sunday – Fed Canada

Colin Wallis – NZ Govt, Internal Affairs

John Bradley - Individual

Rainer Hörbe - Kismed

Sal d'Agostino – ID Machines

Keith Uber - Ubisecure Solutions

Thomas Gundel - IT Crew

1) Roll call for Quorum determination

Quorum reached with 7 out of 11

2) eGov New Membership Status

No new eGov members. Recent Kantara members include Exostar, Unboundid.

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

March minutes moved by John, Sal seconded.

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

From the people on this call Colin, John, Rainer will participate; Ken will make it dependent on recovery of injury.

Rainer, colin, keith and John Bradley will be at F2F Thomas will be at EIC from Tuesday.

Others are invited to join by teleconference, please advise if desired. Time slots have been chosen for afternoon to accommodate US callers. Scott advised

Colin arrives on wednesday. Rainer/Colin are in Ibis. Keith to send Colin Teclo meeting details for the Wednesday before the event.

The work we have for the F2F is important with this in mind. FIWG will join us.

Registrations are low for the F2F.

There will be a technical stream (egov and fiwg working together) A second group on privacy assurance criteria for the identity assurance framework

The summit on the Monday at EIC has better registration.

Plan was to discuss the implementation profile and various deployment profile. TO discuss static test harness.

David Simonson, through Rainer, has been proposed as a good speaker, regarding the economics of a federation network. Joni is waiting for an agreement from this group to offer the time to David. He would take the major part of the egov slot. We could then present a summary of our work items during a wrap up. Keith to send Sal a link to a presentation, so that he can make a judgement. Thomas, Rainer, Keith, Colin support the plan, thus majority support.

5) Update: Collaboration on Profile Management: REFEDS SAML2int, various other eGov deployment profiles (US, CA, NZ, DK, FI) and the eGov SAML2.0 conformance profile

Emerging UK Gov SAML2 Profile

UK gov has produced a profile (steven dunn) for saml2. Is seeking comments from John and Colin. Colin would like to have him share the document with a wider audience.

Security chapter is light for a complex deployment.

John B met with Steven Dunn last week in London, also regarding the matter.

Perhaps the document is not yet ready for wider sharing /eg oasis sstc review/ We will have yet another deployment profile which will be useful for many reasons.

May have new SAML use cases. AQ is in use.

AOB

SAML security discussion

Long conversion after reviwe of the minutes regarding encryption two best options were BXX and Galois/Counter Mode (GCM) is the best for saml but has zero interop GCM is not in openssl which most crypto products rely on. Artifiact binding is an option or stronger TSL requirements.

Denmark encrypt attributes within an encrypted assertion - Scott: this is vulnerable to same style attacks as well. John: may be better but no guarantee, as a general rule, don't send data through the browser for best protection. AQ will mitigate the attack as well, if all sensitive data is kept out of authnrequest.

Thomas - the attacks require an oracle, which leaks error responses.

The complexity of trying to double encrypt will cause more interop problems than for example a better TSL or etc

Call adjourned 20.47

Next Monthly Meeting:

- **Date:** Monday, May 7, 2012
- **Time:** 11:00 PDT | 14:00 EDT | 20:00 CET | 06:00 NZ(+1)