eGov Meeting Minutes - 2012-11-04 -(pending approval)

Kantara eGov Working Group Teleconference

Date and Time

- **Date:** 4. Nov 2012
- **Time:** 11:00 PDT | 14:00 EDT | 20:00 CET | 07:00 NZ(+1)

Attendees

John Bradley, Ping

Sal D'Agostino, ID Machines, USA

Allan Foster, ForgeRock

Rainer Hoerbe, Kismed, Austria

Denny Prvu, CA

Bob Sunday

Keith Uber, Ubisecure

Colin Wallis, DIA NZ Govt, NZ

Apologies

Thomas Grundel, IT Crew, Denmark

1. Agenda review/Minutes approval

Minute taker: Keith.

Quorate call: 7 of 13 voting members. Bob is currently non-voting.

June 4th minutes approved. Colin moved, Denny seconded.

2. eGov Charter Repositioning

An e-vote of the eGov members was held at the end of September (and approved the new Charter), after which this should have gone to LC for approval. There was no time on the 10 Oct LC Call. The LC will vote on the 7 Nov call.

3. eGov Membership Invitation Letter

- Status report from Colin

Rainer sent the letter already to a Dutch representative. No response back yet.
Add Jaap Kuiper (sp?) to Dutch list.
Colin to dig up the Dutch ebook author.
Kick Willemse (OpenID Board Member - NL)
The letter won't be sent until the Charter is approved by LC.
More names are required. List of contacts is not for redistribution or publication.
Letter will be sent by Joni under her name.

Note: The LC call is scheduled to be on the same day and time as the next NSTIC call.

4. Face to Face meeting, Washington DC, 31stOct/Nov 1st

Meeting was postponed due to Hurricane Sandy and will be rescheduled soon.

5. Privacy Enhanced WebSSO

Proposal of a new work item from Rainer: CA, NZ and now UK have extended SAML WebSSO or are in the process to do so to implement a non-traceability requirement for identity and attribute providers. A collection and comparison of approaches, architectural designs and extensions of SAML profiles would be useful in particular for private-public federations.

Colin presented the requirements of NZ

- you can't move personal information from one domain to another without specific user consent.
- the best way in their opinion is to get consent at the time of the event
- SAML AQ profile was ideal, but is backchannel.
- NZ had requested a browser-based binding for Attribute Query

John Bradley:
AQ (or was this the BAE profile of AQ?) is broken in a few ways. It does not support actually support evidence of consent. The consent is collected by the wrong party (SP, not the IDP).

In the UK, they had a similar requirement (according to Matt Trigg, Standards Manager for the IDAP)
NZ uses a mix of back and front channel techniques based on the use case, including use of WS-Trust.
The Change Notify protocol from OASIS SSTC (Phil Hunt, Oracle) works in the front channel. The title belies the actual content of the document, but the flow seems to work for front channel interactions
David Simonsons of WAYF.dk can do front (SpringFicker) and back channel attribute exchange. Front channel was a proposal in a TERENA pilot project. It was found to be unstable in the case of when multiple attributes need to be queried in sequence.

Q. How many use cases have more than one Attribute Provider in addition to the IDP?

NZ is building a user centric consent service to get around the drawbacks of a provider centric centralized consent register.
There are issues in getting the consent information and the user information needed for the transaction that consent is being asked for at the same time.

John Bradley: Most people are doing this with OAuth.
Colin: The current architecture is SAML in NZ (and in the UK's matching service too?) but this likely to be the last major refresh before developing in OAuth for future implementations.

Allan:
Discussion of IDP with two AAs (attribute authority)

Q. Is it possible to standardize this in any way so that it would a solution used across multiple governments? Or become a standard product feature?

A: No response but mention made of Internet2 winning a contract to provide a privacy-enhanced solution - along the lines of the Swiss "uApprove style"

User experience discussion: 10 dialogs vs one

How do you have multiple consent services, which could provide a common consent dialog?

It depends on what is the relationship between the attribute provider and the consent service.

1. UMA-like consent service
2. Attribute provider manages consent on their own

OIX attribute exchange network is looking at attribute release (Postscript: noting Kantara's Attributes in Motion WG is looking at attribute exchange best practice with a view to assessment criteria being developed).

Colin: Would it not be better, to see what the funding possibilities are from offshooting from the NSTIC pilots - are those projects which have got funding usable in this case?

This new work item proposal is sufficiently overlapping with the NSTIC pilots - perhaps it's better to wait for them?

The work item would include:
Couple of stakeholders, privacy requirements, solutions and discussion
Not a standardization activity, rather a review of current solutions and needs with a view for interoperability and standardization

Given that XML and JWT are not too technology dependent and would be used in Attribute exchange work can start now.

Brief UK Report - JB: Stephen Dunn, UK IDAP developer
processed their first SAML assertion 3 or 4 weeks ago
building a proxy using OpenSAML to proxy basic SAML assertions
DWP will be deploying
Creating good practice guide for proofing on several dimensions

AP: Agreed to collect the use cases and solutions on the eGov wiki.
If we can do that before the next call, great.

The UK is willing to release documents/information
CA specs are already open
NZ solution overview presentation for its PPP play (RealMe) has been posted on the eGov wiki (more coming)

We need some ways to compare approaches.

We will collect material
AP: Rainer: create wiki page for page use cases and solutions

Next Monthly Meeting:

- **Date:** Monday, December 3, 2012
- **Time:** 11:00 PDT | 14:00 EDT | 20:00 CET | 08:00 NZ(+1)
- Please use Skype or US local access numbers where possible.