Promising developments in the Australian Access Federation

At the eResearch Australasia conference last week I attended a Birds of a Feather session, Authorisation community developments run by Markus Buchhorn (Intersect), Lyle Winton (Victorian eResearch Strategic Initiative), Clare Sloggett (Intersect) and Neil Witheridge (ARCS). Clare asked me to come along, possibly because she knew I had been critical of some aspects of the Australian Access Federation machinery and how it is supposed to work. I am pleased to report, though that it sounds like some things have changed for the better.

About a year ago, I addressed the ARROW repository community about the then-new Object Reuse and Exchange (ORE) standard. I started with a slightly belligerent rant about another standard, XACML (eXtensible Access Control Markup Language). XACML was supposed to be a part of how the Australian Access Federation (AAF) was supposed to allow all of us in the Australian Higher-Education and research community to access each other's stuff based on our *roles*.

Back then I noted the difficulty with defining role attributes in a way that would work cross-institution:

> I was always vaguely worried about how XACML policies were going to work but one day I met Kent Fitch who really nailed it. On the subject of these use cases for XACML where you, an anthropologist want to grant access to a repository to other anthropologists, he asked “What’s an anthropologist?”
>
> This is a very, very good question. Does an academic working in the education faculty who self-identifies as a visual ethnographer qualify? What if she’s got an honours degree in anthropology? […] [fixed a spelling error]

(I finally have an answer for Kent about what an anthropologist is. Read on.)

My previous understanding of how the AAF would work was that my host organisation would have to be solely responsible for asserting stuff about me, who I was and what roles I had, because there was no publicly shareable identifier to allow other people to assert things about me, such as that they trusted me to look at some data or edit a document. This meant that simple, obvious use-cases like a group of ethnographers setting up a collaboration space by asking each other for their login names would not be possible; due to privacy concerns there would be a unique ID for each AAF person but **there would be no sharing**.

I'm pleased to report that things have changed and the AAF now **does encourage the use of public shareable IDs**. So a few points occur to me. The first couple I raised at the BoF, the last one came later.

1. This means we can **let people self-organise** by adding white-lists of known IDs to their systems. An institution might not be a reliable way to sort the anthropologists from the ethnographers, but they can sort themselves out all right and form whatever working groups they want.
2. It was noted at the BoF that some people would have more than one AAF ID, I suggested that it might be good to **register these in the new researcher ID system** that I believe is being set up at the National Library as part of the ANDS infrastructure. I think this new NLA system will be what Nick Nicholas calls an Identifier Assertion Hub.
3. There was some talk of **systems that could manage groups of AAF users**. This answers the bigest problem I had with the AAF not being able to work with ad-hoc or user-defined communities, only with role attributes assigned by the home identity provider.

   Following from this I finally worked out how to answer Kent's question “what's an anthropologist”. An

(Australian) anthropologist is someone who's a member of the he Australian Anthropological Society.

In an identity federation that does include public, shareable identifiers, societies could publish lists of members or run a group-server that could be used by other services.

Finally, I can't help commenting that if we're going to have a federation where a lot of the trust relationships are devolved to the users, allowing them to assemble groups, or to societies like the AAS then maybe we should consider allowing the use of OpenId as well as or instead of Shibboleth. I bet not everyone in the AAS has an institutional login at an AAF member, even once the AAF is fully operational with wall to wall Shibboleth, but anyone can get an OpenId.

This post was written in OpenOffice.org, using templates and tools provided by the Integrated Content Environment project and published to WordPress using The Fascinator.