UC Santa Barbara HR Payroll and IAM

The following is the response to Stevan's document. This is verbatim from our response to the list.

Page 4 HCM Data Interface Strategy
Identity is one of potentially multiple interfaces, or it is a fork in a single unified interface. As an example, if message queuing is used, a single stream can be used for all destinations - Identity, DW, whatever.

I understand there are many variations on the need to place a datum from the campus into the transaction creating a person within HCM. Our particular need is to place a (for us) global key that we have identified with this person as an existing principal in our IAM. A student for example now becoming an employee. We do not, however, have a process that creates a principal on our end before that entry has been created in PPS (HCM).

Matching is, for us, a symmetric process. Whether we match a student becoming an employee on the upward flight or not, we will be doing a reconciliation matching process on all entries coming towards us from external systems of record such as PPS (HCM).

UCSB Profile Comments
As regards our specifically documented profile, looks reasonably accurate. Our IAM data of record is in a single data repository that we do not allow external access. Authentication has traditionally been ldap, and to that end, we provision active identities, as distinguished from all identities, into the ldap for simple authentication purposes. We are also in the process of pushing identities towards a Microsoft Forefront complex of software utilizing message queuing technology. It will likely be fully functional by Spring. There is nuance in all of this that I am not describing, but it will be fully Silver compliant (old standard, not the newer easier one).

We have ***many*** global keys, among which the UCnetID. It was not designed to be a global foreign key, and we are very negative about attempts to back it into that posture. If we were to do a round trip on a single identifier used for all principals, regardless of origin, it would be the UUID we use as the campus internal key for all principals. If all of us scoped our campus internal keys, we would be unique. Those who are using UUID / GUID algorithms don't even need to scope.

We are clearly headed to Silver. No question there. However, we see no linkage between the the PPS(HCM) requirements and Silver. UCTrust Basic, in every way, satisfies the security requirements of PPS, and we see it as co-requisite scope creep to make it part of the project. Obviously not my problem. We are wave 3 and designed to support Silver.

SMG (subject matter guru) required on the Oracle SAML2 statement. I know what Cantor says, but I'm a bit wary of the complete SAML2 compatibility statement due to my lack of that deep expertise. I don't
recall ever hearing about an Oracle IAM / Shibb 2 at the yearly interoperability lab, but then I don't recall quite a number of things :)

Section 5 Questions for UCSB
As mentioned previously, our process does not depend on pre-provisioning a principal within our IAM prior to instantiation in PPS(HCM). If we place our campus UUID in the input screen for external data, it will initially be for the student employee process. Its conceivable this might be leveraged for other activities at some future date, but there are no current plans. The character representation of our UUID is 32 bytes in length.

We support the current crop of SAML1 and SAML2 handlers in the metadata. Nothing is turned off.

UCTrust Basic is the same as Silver in our IAM design. Nobody is provisioned with Basic (Silver). They will have to go through a person to person help desk process that uplifts their account to the Silver level. We do not currently support that. Probably towards the end of 2012, but by no means scheduled yet. For a wave 3 campus, this is not on any critical path.

Yes. Our data is published with InCommon. As was asked of us, we are not members of any other federation.

Observations

The call we had provided a bit more illumination on the nature of the Oracle SP end. I would be interested in our group's views on addressing the logout process.

Since the nature of these systems is that there is a complex of internal authorization and provisioning tools, we can ask questions about the business processes because the technology is already in place. I'm wondering what the campus vs. UC Service Center responsibilities will look like as regards these routine processes?

If some aspect of provisioning is boot strapped, and by that I mean higher level authorizations at the campus level create lower level authorizations, then we would need to conceptualize what identity tools are needed. In our local case, the IAM has pretty much every datum about any particular individual stored within it. How does a new individual that is populated by some fraction of this data materialize within the HCM? Obviously we can type it in. What better, but inexpensive, other possibilities are there? Alternatively, perhaps the Service Center handles it.

I included my original response verbatim, but from the call it sounds like Oracle is committed to their software inter-operating appropriately with our Shibboleth IdPs. Nothing to do beyond testing when the time comes.

Do we want to discuss or say anything about a common IdP version of Shibboleth? Supposedly 2.3.3 is the stable IdP version at the moment. Perhaps there is leverage in everyone having the same code base?

At present, I see no InCommon Silver issues from an authentication perspective. From a business process perspective, the more the HRIS process can automatically inform Identity processes, the easier it will be for us to instantiate Silver. I am expecting the detailed design to spell out the exact nature of the attribute exchange for the authentication aspects of this.

I would like there to be a minimum of two authentication levels because it seems inappropriate to require the highest level of assurance for the self-service updates of minor information. If it was a single monolithic approach, all 6000 of our employees would need to have the highest levels of assurance. That would drive an increased campus expense within local IAM services.

In all of this, the decisions that wave 1 campuses make can be highly influential on the rest of us, particularly if we are trying to keep local costs under control.