Notes from 1-10-2012 UCPath, Oracle, UCTrust meeting

These notes refer to the UC Path/Oracle **Identity Management -- Strategy** PowerPoint document that was used as the outline for the meeting's agenda.

Slide names are boldfaced

- Questions and requested additions/corrections are captured in first-level bullets
    - *Answers about current plans (where available) are noted in second-level, italicized text.*

Meeting notes

Security Strategy/Summary UC Campus Responsibilities

- Add SAML2 to requirements (not just Shibboleth 2)

Use Cases

- Capture the process of user transitions from campus 1 to campus 2: user provisioning, data entry and data reconciliation processes.
- How do you deal with InCommon Silver/UCTrust Basic certification of an individual during a transition from one campus to another? (E.g., we may need to generate a new validation code for the second campus to use)
- Users being provisioned in advance (e.g., like UCSC DivData, future appointments)
- Are users ever required to log in prior to being provisioned to a campus? E.g., prospects. How would logging those people in be handled.
- Campuses should consider DR options (see campus responsibilities note, below)
- Existing campus user (e.g., consultant, student) needs access to PeopleSoft; how can data entry be done to simplify match with local campus IDM after entry into PeopleSoft.
    - *Entry of student ID, etc during account creation.*
    - *Oracle intent is to allow campuses to have more than one "external id" per user.*
- What is the process for merging UCPath records, to correct errors in data entry/data duplication?
- Employee returns to a different campus after 10 years of separation (so user is not currently in UCPath, but does have a local "ex-employee" identity at first institution)

InCommon Silver

- Is there possibility for some sort of retroactive assertion process; e.g., postal mail validation codes to home address of some such, to allow all campuses to meet InCommon Silver
- PS SP should be configured to accept either UCTrustBasic or InCommon Silver IAQ

UC Trust Federation Interface

- Assertions should not be signed with PKI certs, but rather the self-signed certs that are part of the metadata
- What support of SLO endpoints can we provide? Can Oracle accept an out-of-band SLO endpoint ID?
- forceAuthn: Do we want this? Can all campuses support this? Can this be configured per campus? Is UCPath seen as being sensitive enough to require this to be set? Oracle assumption is that forceAuthn should not be set.
    - *Probably requires a risk matrix of some sort, to be handled by UCOP/Oracle project team.*

Data Sync Strategy

- "Standards based message queue" implies something like a JMS Queue
- Feed will include the message when entered, not on effective date.
- IDM will have our own account and access to whatever mechanism we have. So if IDM wants a message queue, Oracle/UCOP will publish an IDM-specific message queue separate from any other queues.
- Can we have access to the database at the DB Link level (rather than flat file)?
    - *No, at least not initially.*
- In flat files, can we have the data encrypted at rest? Encrypted file systems (probably not in the Oracle DataCenter)? Etc.
- Oracle/UCOP is looking for mechanisms for managed file transfers.
- The ESB for IDM feeds could (likely would) be hosted by Oracle; the local IDM clients would only need to subscribe to this bus.
    - *Could be useful to have campuses collaborate on defining clients.*
- Upload interface may be a web service. Needs definition on where in process the data is collected (e.g., can it be part of the PS data entry).
    - *March timeframe to try and spell this out.*
- Functional team is clear that there are campus identifiers and potentially multiple identifiers. It's their issue to ensure there's a way to do this.
    - *Oracle is thinking there would be one id per campus, but limited to only allow updates where there's a campus association for that user. E.g., a UCSC student (no job in UCPath) has an employee role at UCD. Should UCSC be able to add their campus ID to the identity record? Current answer is tentatively "no".*
- *_External search match: PS provides this, with one external repository. How would PS be able to call out to one system to do that external repository for all campuses? _*
    - *Another option is to have new identity created and published to ESB, then UCLA could have a BPEL process that does additional reconciliation. Expected process is something like:*

- *# *## user is entered in UCPath, and a UCPath-wide search match is done.*
    1. *## when a user is later associated with a campus (via job entry), that user is published to the campus.*
        a. *### May look like a new user to the campus person repository, even if not a new user to PS.*
        b. *Local processing of record (via ESB, Queue, etc) would do match against local person repository, kick any "fuzzy matches" out for review.*
        c. *after review, complete processing prior to actually provisioning information to local campus IDM*
- Berkeley/SF are looking at developing a search match system that could potentially be used to support step (c).
- What about creating a unique ID per user/per campus and storing it in a system somewhere?

UC Campus Responsibilities

- Would be nice to have a corresponding "Summary UCOP/Oracle responsibilities" slide
- Conversion will have data for employees from the last two years. Older employees will essentially lose their EIDs, and we (UCOP UDIR? campuses?) will be required to add the value back in.
- Assuming someone is active, with old (>2 years) affiliation with a different campus, will the conversion have both sets of employee info (e.g., EID) or, just the data from one of the PPS systems?
    - *UCOP will discuss using UDIR matching to get old EIDs added for current employees*
- What SAML attribute name/OID/URN should be used for transmitting with the emplid? Does Oracle have a standard OID for emplid? Should we use inetOrgPerson/employeeNumber?
- Work with the UCPath PMO and Oracle to review their DR plans to make sure IP infrastructure and support are consistent with the DR requirements of the Peoplesoft investment

Central LDAP

- Discussion on hold for now. Discussed a little bit what the scope should be.

Data Conversion

- Will we load *all employees* and employee data from the last 2 years, or is it all employee data for employees who are "Active" at the time of the conversion?
    - *Randy will clarify.*