When the active directories are consolidated, it would be nice to have WatIAM manage user accounts. However, many system administrators feel the present WatIAM needs enhancement or documentation before it is ready for use.

(DK) General note: Additional documentation is one of the items in Connie's transition plan as she moves over to Finance and Research in the next couple of months.

user interface. The user interface is clumsy. There are buttons to press that one is instructed to not press.

(DK) The look and feel used in the present implementation relies on out-of-the-box functionality within the SUN Identity Management module. It is somewhat rigid, but we have tried to remain within its framework and not do customizations unless absolutely necessary. It is admittedly not as friendly as we might like. Changes to some aspects are more complex than they should or appear to be (e.g. some objects reside in compiled code that can't be readily replaced). It should be possible to prioritize some of the areas of most concern.

renaming a userid (people get married), joining a userid (when two different sources have created different userids).

(DK) The initial implementation for these types of changes involved some relatively limited functionality. A new process for merging accounts was introduced to L1 administrators this month. Account renaming still requires some manual intervention due to dependencies outside WatIAM (e.g. home directories where system administrators are not comfortable with that level of automation as there is a potential for "orphans" to be created and services become unavailable). One possible solution would be to expand on the decoupling notion where the ID becomes disentangled from the name or service (e.g. UW ID versus email alias/name).

accounts should be created at hire date, not on first day on job. This is particularly true of faculty, who often have to move many resources to UW before their first day of employment. But it would also be good for staff – they need working computer accounts on their first day, not the day after as presently done

(DK) Changes have just been introduced to WatIAM and in HR to assist with this process. A delegated administrator can now create a new entry and flag the record indicating that an incoming record from HR is pending. There is a subsequent approval process for when the HRMS event occurs. There are other related changes and workflow for the process. This should result in a considerable improvement in the timeframe and initial provisioning.

web service interface (so we can submit requests from scripts). Eg. LDAP, XML/SOAP, etc. so we can set UID, GID, home directory, profilepath, etc.

(DK) This is available now and is known as SPML. There is a Java based client available and a PHP client is in testing. This is the technology currently being used for Joberloo, in the promissory note application supported by Client Services and on "ego" for processing email changes from the Faculties. It is also the technique planned for use with RaisersEdge for alumni and also proposed for the registration system used in DCE.

bulk account manipulation (passwords, home/profiles, creation) for generic accounts for conferences, camps, etc.

(DK) Bulk loads are possible (and routinely run), but currently require a resource in IST to be imported. It is possible to roll this out to a broader community of delegated administrators with minor changes to the security model and overall interface. This is in the development queue.

"Ownership" of data. Right now, if I edit an entry I become the owner. This is not ideal.

(DK) Agreed. At present, there is limited granularity; any change to a record does result in the maintainer becoming the most recent authority. This logic is customizable, so it would be possible to establish rules that would look at the type of change and appropriateness of transferring ownership. I would need to investigate further on whether we can separate the notions of "last maintainer" versus "authority/owner" on an individual record.

Expiry. Right now, expired accounts go into an Expired department. This does not make sense; they should stay with their department but have an expired status.

(DK) Also agreed. The use of expired as an OU/orgunit/dept was intended as a temporary measure. This is being looked at as part of the overall lifecycle review being started this month.

We should also be able to set reasonably long expiry dates, or perhaps none at all, for faculty/staff. This expiry should only be triggered by some event, e.g. termination for faculty/staff, or graduation/drop out (maybe) for students. In WatIAM, nobody gets notified if an account expires. The user, at least, needs to know.

(DK) One of the key issues noted by the auditors in their IdM review was that accounts were rarely if ever removed from the old UWdir. WatIAM uses a "rolling forward" idea where expiry dates are set for some reasonable future date, which is extended when there is any relevant activity noted on one of the authoritative sources. The actual process and specific details on the dates and timing can be reviewed as requirements expand with the AD reorganization.

Department names - still a bunch of redundancy, e.g. "ENG/Electrial and Computer" (for students) vs. "Electrical & Computer Engineer" for faculty/staff. A useless and confusing distinction carried over from UWdir. Now we have fields to distinguish roles.

(DK) This is being considered along with the overall discussion about departments, their communication and maintenance in campus systems and publications. The specific example noted is the result of different information that may be received from Quest as a result of the mapping of plan/program

information to an "academic affiliation" as compared to what HR might send WatIAM in the form of a "department" (which is largely derived from financial org units).

"Generic" accounts, e.g. for guests, etc. There are tons of them in WatIAM. Do they need to be there? If so there should be a field in the DB that says they are not a person. How should expiry be handled?

(DK) Many, though not all, of these guest accounts are created to enable wireless access. Jason Testart is investigating a "netid" approach which would reduce the need for these generic or guest accounts. There are other generic accts, typically associated with helpdesk or other shared situations and do need to be part of WatIAM.

Need some checking on format of data entered, e.g. for phone numbers.

(DK) There is some limited filtering of input for bad characters, etc. which might cause issues on update. WatIAM does not attempt to edit information that comes from authoritative sources. Additional checking can be created for self-service and other manual entries. This is in the development queue.

Better handling of roles, e.g., students can be both students and employees. These should all show up with the primary role identified, e.g. "staff" for a full-time staffer taking some courses, "student" for a full-time student on co-op here. We should also know when a person is an active employee, vs. was a co-op here two years ago. Right now, I believe, we don't see two roles for current co-ops; they show up only as students. Some thought should be put into what correct roles info can do for us too.

(DK) WatIAM doesn't actually track a history per se. It does, for example, track changes for audit purposes, but doesn't employee an "effective date" principle as might be seen in PeopleSoft applications. It does not know, for example, if a student was on a coop term last year, only that they are currently a student (and if applicable, part of a coop program). It does assign multiple roles (e.g. staff, student) and these determine which resources are provisioned, which OU and security groups they belong to, etc. There are precedence rules in place that help determine what the authoritative source is for specific fields or objects. There is no "primary" role currently assigned, but if needed for future provisioning, logic could be added (significant discussion required due to the possible combinations and potential downstream uses).

We may need some extensions to AD Schema and WatIAM. RFC-2307 attributes (UID, GID, home directory, Unix groups) are used by different faculties, so we may need one for CS environment, Math environment, Engineering, Electrical & Computer, and possibly others as some users will have accounts in multiple areas. There are other possible solutions to this problem.

(DK) Definitely. We would need to know more about the entities to be populated, rules and generally implement much finer grained provisioning. Most of the work required for WatIAM to take on the role of primary provisioning agent would be involved here. Close coordination would be needed with the AD group as plans there unfold.