

## Access Provisioning Subgroup

11/6/08

### Discussion Items

D1) Recommendation to Streamline the Provisioning of Access to University Systems – draft dated 10/20/2008

- a. Dan recapped the last meeting which he had to miss; the original purpose was to document use cases and processes for access provisioning (looking at HRMS flowchart). Part of the meeting then went into the recommendations for “Role-based” Access. This document is targeted at how we might do things here at IU. Currently everything is based on an individual so that whenever a person comes and goes, their access must be set up from start to finish.
- b. Dan led a discussion on the draft document; Alan Walsh indicated that he could build a system based on this type of recommendation. It is harder on the application side; creating a list of all user roles. Once this is defined, it is not difficult from a technical standpoint. Dennis noted that it might be difficult to start with something like SIS which is so huge.
- c. The main purpose of this document was to get something written; are there any red flags? Dan wondered about taking a few users and see what a profile might look like in this situation.
- d. Kevin asked about piloting a particular area and how that would work. Could you create a framework? Must focus on user, rather than application. Dan posed the problem of dealing with hourly and student workers if we use position as the driving profile. Maybe we need another type of hourly type – Dan Rives. Maybe if you took some of the administrative offices, you could create profiles and document all new positions that come up.
- e. Who would own such a service? Dan answered that he doesn’t know the answer to that. Dan would like to send this forward to the full Committee of Data Stewards. His hope would be that if we can get this endorsed by CDS, it could get an implementation plan attached to it within the new Strategic Plan. Alan noted that Action Item 39 fits directly into this (see item at end of minutes). It would be a specific recommendation under Item 39.
- f. Lora used a faculty member as an example; one of his roles might be access to e-Docs or ERA. Those would then be the only two items on his/her profile. Beth asked if it was going to be by position, and Dan felt that would be the case. Dennis noted that this doesn’t simplify the number of people having access, but streamlining the process to grant or change access.

D2) Access Provisioning processes for HRMS, SIS and Library

- a. The SIS has a data supervisor role which is different from other systems. This person is to coordinate across the various modules (see diagram distributed prior to meeting and stored

- in OnCourse**). Unlike HRMS, SIS stores the documentation for access in ARMS, not just in Falcon. Within ARMS, they verify that a new user has completed steps 5 – 8 before granting access. Alan asked if step 14 is a manual process; Dan indicated that it would be good to automate this step. ARMS does have roles defined within it; this led to a question as to whether or not this could be used as an example in developing “Role-based” access. ARMS is a web application written in Cold Fusion that is the Access Request Management System for SIS across all campuses. It reads data from PeopleSoft.
- b. Phyllis walked through the HRMS flowchart (**distributed with agenda and in OnCourse**)– Dennis noted that HRMS also had the same requirement for Safeword Cards. Phyllis will add this.
  - c. Carolyn walked through the Library processes (**distributed to group and in OnCourse**).
    - a. Unicorn/Symphony Workflow – all IU
    - b. At hiring – sign computer use agreement
    - c. Supervisor completes web form requesting access submits to the LIT staff person. These are set up based on profiles.
    - d. Access granted based on supervisor request network ID access.
- Dan asked if it would be fairly easy for the library to document their roles, and Carolyn felt that could be rather easily done.
- d. Dan asked if these documents are helpful; the group felt they are. Dennis noted that all of the systems have similar processes, so it would be helpful to generalize them and see where there is overlap. Carolyn asked about the term “enterprise systems”. Do we need to consider access to library electronic resources (databases, journals, etc.) as a part of this discussion? The group felt this would be helpful to also document.
  - e. Alan noted that there is a theme of prerequisites for what a person needs to do whatever they need to do. For instance, these need to be electronic and stored in the same place, same process (such as Workflow) and included within each role. Then it doesn’t matter if we have multiple use agreements, or different agreements for different roles or systems.
  - f. We should be able to look at these processes and see where there are opportunities for simplifying them and what we’d like to recommend for next steps.

D3) We reviewed the task list, and Phyllis will update it with comments from the group.

### **Action Items**

A1) Take the recommendation above forward to CDS as a draft requirements document for their approval and recommendation to UITS.

A2) Phyllis will add safeword card requirement to HRMS diagram.

A3) Phyllis will put all of these documents in OnCourse for easy access by all members of committee.

A4) Dan and Phyllis will try to capture all of these processes in some coherent fashion.

## **Addendum**

The second major component of identity management is a robust ability to manage fine-grained access and restrictions to distinct resources – or authorization. Authorization presents an even greater challenge as it requires revision in each system to seek and make use of more details than simple authentication. Systems must understand who has access to which resources or services at what points in time. As the university becomes increasingly connected and partnered in its core missions of research and education, it will need a more sophisticated means to manage authorizations in a world of federated identity.

**Action 39: IU should provision a robust and secure ability to support fine-grained authorization to specific systems and data utilities across a range of internal users and trusted partners.**