INDIANA UNIVERSITY

42 – Authorization Systems

Action Item Template Response

General Action Item Information

Lead Division/Office: EI
Action Item Number: 42
Action Item Short Name: Authorization Systems
Dependencies with other EP Action Items: 58
Implementation leader (name & email): Alan Walsh (alwalsh@indiana.edu)

I. DESCRIBE YOUR PLANS FOR IMPLEMENTING THIS ACTION.

In late 2007 the committee for data stewards was reconstituted after an extended hiatus. The initial effort of the committee focused on an assessment of the current state of affairs with respect to the management of data at Indiana University. One of the areas that quickly jumped to the forefront was access provisioning, or how individuals gain access to enterprise applications and data. Today access is currently granted on a case-by-case basis, individually, for each information system. The process is decentralized, and it is difficult for employees and their supervisors to know how to proceed with requesting access to each information system, and cumbersome for the data managers to process access requests.

Another area identified was the process for de-provisioning access to certain systems and the inherent risk in not immediately identifying and deleting access that is no longer required. A sub-committee was quickly formed to investigate the existing processes and to pursue opportunities for improvement.

The initial result of that work is a recommendation to pursue a role-based access and provisioning strategy to manage and control access to data and applications. More specifically, the goal is to create a central repository of roles and access to information about all users. That repository would drive provisioning and de-provisioning of access in various applications. The repository would also provide reporting and auditing, allowing anyone to see the access that a person has, and why. When individuals change roles, their access will adjust accordingly and automatically. Although still in the early stages, the subcommittee has a good head start in laying the foundation for an infrastructure capable of efficiently managing fine-grained access to existing enterprise applications.

On a parallel front, Indiana University continues to move towards a wide-scale implementation of Kuali, including modules for financial systems, research, and workflow. A core component of the underlying platform is an access-control system known as Kuali Identity Management (KIM). This service manages and controls access to applications within Kuali using a flexible and open model. Any solution for addressing access control and fine-grained authorization at Indiana University must be integrated with KIM. And there may be opportunities to leverage the capabilities of KIM, perhaps as part of the broader access-management solution.

Looking beyond the enterprise, the ability to manage access at a fine-grained level must be extended to federated scenarios. There will be numerous use-cases, particularly in research, where access will have to be managed on behalf of external users. There is early work happening within Internet2 to address this challenge, most notably the COmanage project. The work in that area should be closely watched and thoroughly investigated, and if it proves to be viable, it can be incorporated into an overall solution. Most importantly, our strategy must take into account the need for fine-grained access beyond just enterprise or other internal applications and support those scenarios.

The single most important element of the strategy for managing fine-grained access will be the use and adoption of broadly supported standards. Authorization information should be widely accessible, using technologies that lower the costs of entry as well as dependencies on non-standard or proprietary technology. Only by adhering to standards-based solutions will we be able to succeed in implementing a truly robust solution capable of effectively managing access in every use case across the institution.

II. WHAT ARE THE POLICY AND PRACTICE IMPLICATIONS OF YOUR PLANS?

There will be decisions regarding authorization data, especially the definition of roles and the access granted for a given role.

III. IDENTIFY STAKEHOLDERS.

- Research Technologies
- Enterprise Software
- Networks Support
- Information and Infrastructure Assurance
- Data Stewards
- Internal Audit
- Human Resources
- Foundation
- Clarian SchoolofMedicine
- Regional campuses
- Libraries
- Identity Management Taskforce
- Financial Management Systems.