

Identity and Access Management Meeting

Minutes

April 4, 2007, 1:30 P.M.

In Attendance:

Lisa German, Renee Shuey, Joel Weidner, Jackie Babcock, Rick Ramsey (for Scott Bitner), Jae Shin (for John Gorman), Steve Selfe, Dan Sickles (for Tom Moore), Vince Timbers, Tom Irwin, Cheryl Seybold, Ken Forstmeier, Bob Quinn, Janice Pearce, Karen Schultz, Jim Smith, Steve Shelow, Debbie Meder, Donna Neideigh, Mark Sherburne, Judith Getz, Kevin Morooney, Steve Kellogg, Judy Goetz, Rand Allison

Introduction

Kevin Morooney opened the meeting with introductions of those present and a brief PowerPoint presentation about the importance and necessity of the University developing an Identity and Access Management (IAM) roadmap. Kevin reviewed some of the past history related to IAM at Penn State and future challenges which include the need for a strong institutional identity that will meet needs both internal to Penn State as well as external agencies such as other educational institutions and the Federal government.

The charge to the group will be to identify University's needs to support the management of identity and access control and develop a roadmap for managing identity and access.

Kevin encouraged the group to think strategically and to consider what other people or departments are not represented that need to be part of this effort. Kevin will use the roadmap developed by this group to "sell" the plan to University executives and muster the resources required to implement the plan.

Discussion Centered Around Proposed Case Study

Renee Shuey began a group discussion by asking the group to consider what would have to take place for the University to create the required employee credentials and access rights in a single day

The following are bullet points taken from the discussion. Many of the bullets are questions that were posed by the group in thinking through the broad issues of IAM at Penn State.

- We need to understand better the current process for assigning identity to both employees and students
- Where do employees go to establish their credentials? It seems like they need to visit multiple locations.
- How do we vet identity now? Are employees asked to prove their identity multiple times?
- We have the challenge of creating an identity and allowing limited access to systems before the employment and/or enrollment process is complete (before the official relationship begins).
- What about employee/students who are not physically located on a Penn State campus (World Campus, Extension offices)?
- Are multiple level of certainty needed? If so, how many levels?
- Level of access may be linked to certainty of identity
- Recognizing the difference between certainty of identity and level (or right) to access information. In some cases you may have no access rights to information regardless of how certain we are who you say you are.
- Identity proofing and management of access levels are related by distinct issues
- In order to properly grant access to data or digital assets we must understand the value and sensitivity of the data/assets
- Digital rights management – assigning rights to both persons and objects (assets).
- Speedy creation of credentials and access to data may have a negatives side-effect in that users have access to data before they have been properly trained and educated as to how the data should be used (or not used)
- We must separate entitlements from privileges

- What are all the ways in which an individual becomes part of the University and needs credentials?
- How will the new role management, workflow system fit into the IAM landscape?
- What constitutes a digital identity (user ID, password, digital photo, biometrics, SSN, PSU ID... others)?
- Where does CIDR fit into the roadmap?
- How would the right type of central person file facilitate IAM?
- Person naming convention issues. Who owns a particular name or nickname?
- How do second factor authentication devices (SecureIDs, biometrics) fit into the roadmap?
- What are the special challenges for a research institution like Penn State (federal issues, multi-institution collaboration efforts, international research projects)
- How does physical access (as opposed to logical) fit into the roadmap?

Wrap-Up

Renee wrapped up the discussion by proposing that the group break into sub-groups to study and work on different area of focus. Based on the discussion she proposed the five following areas:

Identity Life Cycle and Affiliations

Vetting, Proofing, and Registration Authorities

Levels of Assurance

Risk Assessment (Legal/Physical)

Governance & Policy for Managing Identity and Access

There was general agreement surrounding these broad topics. It was further agreed that smaller working groups would be formed around each one of these area. Descriptions of each group will be sent out and committee members were asked to volunteer to lead a group. Others, not on the central committee could be invited to participate in the working groups.

Future Meeting Schedules

Joel and Renee asked the group about meeting every other month over the next 9 months. The group felt that monthly meetings may be needed. It was decided that we would meet again in two months to give some time for the smaller working groups to get started. At that point we would revisit the monthly meeting schedule .