Identity and Access Management

IAM and Central Person Registry Overview

Contents
IAM and Central Person Registry Overview ................................................. 1
Purpose of this Paper .................................................................................. 2
What is IAM? ............................................................................................. 2
IAM Central Person Registry Overview ...................................................... 4
Policy and Governance ........................................................................... 6
Operations .................................................................................................. 6
Stewardship .............................................................................................. 7
Affiliations .................................................................................................. 7
Guidance ...................................................................................................... 8
Reflect and Join ........................................................................................... 9
University Identity Management ............................................................... 10
Delivery ....................................................................................................... 11
References ................................................................................................... 12
Conclusion .................................................................................................... 12
Purpose of this Paper

- Provide an overview of Identity and Access Management and the Central Person Registry.

Target Audience

- Participants in the Student Admissions Identity Integration Project

What is IAM?

Fundamentally, Identity and Access Management (IAM) is about aligning University business processes, policies, and technologies to support the delivery of a rich and diverse array of online services for faculty, staff, and students. At Penn State, individuals gain access to such resources and services through their respective digital identities.

Managing digital identities at Penn State includes many factors:

- the processes responsible for the registration and credentialing of digital identities
- managing relationships of individuals and objects within the University
- the assertion of these digital identities both internal and external to the University
- the technology to support the management securely and efficiently, as well as protocols for authentication and authorization.

IAM crosses all boundaries at Penn State and in the higher education community at-large.

The IAM Charter

Recognizing the importance of developing a comprehensive, forward-looking strategy to deal with Identity and Access Management, Kevin Morooney, vice provost for Information Technology Services (ITS), formed the IAM initiative in April of 2007. The primary Identity and Access Management committee and related sub-groups is comprised of forty individuals who span many administrative areas at the University.
Identity and Access Management

The group's primary charge was to create an IAM road map (or strategy) for Penn State. A secondary goal was to establish a community of people and organizations from across the University who understand each others' pressures, needs, and desires for developing an IAM infrastructure that will support and enhance academic, research, business, and collaborative processes.

Four overarching goals were defined by the IAM Committee:

- Increase collaboration and innovation
- Improve customer service
- Increase efficiency and productivity
- Improve security of digital assets

Eight recommendations were offered to advance the above goals:

- Create a Comprehensive Policy for Identity & Access Management
- Develop a Plan for a Formal Risk Assessment
- Create a Central Person Registry (CPR)
- Add Level of Assurance Component to Accounts and Access Decisions
- Promote Single Sign-On, Federated Identities, and Control of University Digital Credentials
- Streamline Vetting, Proofing, and the Issuance of Digital Credentials
- Streamline and Automate the Provisioning (and De-provisioning) of Access
- Promote Awareness and Education of the Importance of Identity & Access Management

For more information on the committee's work and final recommendations, please see the "IAM Final Report" available on our community space, [https://iam.psu.edu/](https://iam.psu.edu/).

The Identity and Access Management (IAM) Technical Architect Group (TAG)

TAG is charged with furthering Penn State's vision for a comprehensive IAM solution. This group's mission is to support the University's goal to expand access and opportunities while preserving privacy for the Penn State community. In collaboration with IAM stakeholders, the group will evaluate, prototype and recommend identity and Access Management solutions that provide the appropriate access to enterprise resources.
TAG members include:

- Renee Shuey, Lead, rshuey@psu.edu
- Jim Vuccolo, Technical Manager, jvuccolo@psu.edu
- Richard Dumm, Process Manager, RichardDumm@psu.edu
- Lynn Garrison, Lead Programmer Analyst, Ilg5@psu.edu
- Karen Hackett, Communications Coordinator, kmh@psu.edu
- Ed Hayes, Lead Programmer/Analyst, emh1@psu.edu
- Randy Hegarty, Security Systems Analyst rhegarty@psu.edu
- Sue Jones, User Access Analyst, sjj2@psu.edu
- Michael Pelikan, Information Architect, mpp10@psu.edu
- Bob Walters, Lead Technologist/Architect, raw121@psu.edu
- Ann West, Consultant (Internet2), ahw11@psu.edu
- Charlotte Wilusz, Lead Systems Analyst/Architect, cjw1@psu.edu
- Sherry Tirko, slk24@psu.edu
- Emily Brokering, Database Administrator, ehb3@psu.edu

IAM Central Person Registry Overview

What is the Central Person Registry?

A centralized person registry is a directory or database that consolidates identity information currently stored in separate and non-integrated sources throughout the University. Integrity rules will be applied that will ensure the validity of the identity data---resulting in a complete and up-to-date person record for each individual University member or affiliate.

Creating a CPR was the first recommendation that TAG has undertaken in support of the overarching goals of the IAM committee. Detailed project scope and time lines around the CPR is found in the "Resources" section of the IAM Online Community site at https://iam.psu.edu/resources/.
IAM Central Person Registry Diagram

The diagram below is a high level overview of the components, functions, data inputs, and services around IAM and the new CPR. The diagram is followed by a contextual description of its components.
Policy and Governance

The IAM Governance council was formed in late 2009, and it is co-chaired by the vice provost for Information Technology and vice provost of Undergraduate Education and with University-wide representation that includes The Dickinson School of Law, Penn State Milton S. Hershey Medical Center, Auxiliary and Business Services, Penn State campuses, University Outreach, and Police Services. The goals and guiding principles for the IAM Governance Council are to provide oversight for IAM that will:

- Define the future of IAM at Penn State.
- Establish criteria for making decisions, resolving conflicts, and sharing information with all University constituents.
- Involve all major stakeholders in governance process and decisions.
- Gather input from all campus constituencies and engage campus-wide technical experience when necessary.

Policies impact the development and deployment of IAM services as services will need to incorporate the University business rules developed around federal, state, local, University, and departmental policies.

Although there currently is not a comprehensive IAM policy at Penn State, various policies exist that address specific aspects of IAM, such as network security, ID cards, or Penn State Access Accounts. However, there are inconsistencies between existing policies and related procedures. As IAM services and processes mature, there will be a need to modify existing policies and/or create new policies.

Operations

IAM will recognize and incorporate the operational functions of business rules, policy, roles and security into the operations of the identity management system.

Business rules will originate from many sources including, but not limited to, stakeholder defined requirements and identity related business processes (for example the business rules that are discovered during the student and non-student on-boarding processes).
University security, policy and federal, state, and local regulations that require IAM compliance will be operational inputs into the functionality of identity-related services.

The provisioning of IAM services will recognize the application of roles as they are applied to the University’s operations. For more information on roles, please refer to University Policy AD63 Workflow Policy.

Federating allows users to access resources external to the University using his/her credentials. For example: A Penn State faculty member collaborating on a research project with Michigan State University (MSU) would federate to MSU with his/her Penn State credentials to access research materials (and vice versa).

Stewardship

The stewardship of the identity management system should be the combined management of IT (for the service), Data Stewards (for the data), Process Stewards (for the process), and Registration Authorities (for the identity on-boarding). Additional players may include risk managers and auditors, online service providers, application champions, and system users.

Affiliations

- Affiliation is the combination of one's relationship with Penn State (which may allow access to electronic services) and some form of trusted (may not be Penn State) identity.
- At Penn State, affiliations are not roles.
- A person may have more than one affiliation with the University. For example, a staff member who is also enrolled in classes as a student.
- Student affiliations include potential students (prospects), applicants, student and former student.
- Other University affiliations include:
  - Employee (All Penn State regular and non-regular employees as defined in OHR Policy HR05)
  - Contractor (A person or organization who contracts with Penn State to perform work at a certain price or rate)
  - Partner (A person or organization who has some degree of involvement with Penn State)
Identity and Access Management

- Customer (A person or organization that purchases or receives goods and services from Penn State and has no other affiliation with Penn State)
- IAM will include an identity framework for managing University affiliations.

Guidance

The key identity management inputs that will guide the access, authorization and provisioning of services include:

Identity On-boarding

- On-boarding refers to the addition of a new employee, faculty, staff, or affiliation to the University's IAM system. The term is also used if a University entity (faculty, staff, student, or affiliate) changes roles within the University and/or is granted new or expanded access privileges.
- Conversely, off-boarding refers to the IAM processes surrounding the removal of an identity for an employee who has left the University. The term may also be used to describe the restriction of certain access rights when an employee has changed roles within the University.

Group Membership

- Group membership refers to the many institutional and personal groups at the University. Group management puts the control of groups in the hands of its steward and enables users to manage group membership and what resources it can access.

Privileges

- Privileges refer to the rights University affiliations have for accessing services. Individuals across campus manage their users’ privileges, which are then supplied to the identity management system and used by applications and services to make authorization decisions.

Accounts

- A Penn State Access Account is a user ID and password that enables Penn State students, faculty, and staff to use the full range of the
University's Internet services, on or off campus, at computer labs or on personal computers. For example: xyz5000 (a sample user ID) plus a password equals an Access Account.

- Once a user's Access Account is active, it provisions for authentication (user ID/password), an entry in Penn State's Directory Services, e-mail services, and file storage space known as Penn State Access Storage Space (PASS). Penn State Personal Web space may also be obtained by taking and passing a short quiz (upon successful completion of the quiz, Web space is created within one's PASS folder).

- These entitlements noted above in the second bullet item are associated with a full Access Account. Slim Access Accounts may also be issued, which provide only for authentication.

- Currently the Kerberos realm name for Access Accounts is dce.psu.edu.

- Accounts and account management are inputs to the identity management system and used by applications and services in the provisioning of services.

Data

- Today, the main source of identity related data for the identity management system are sourced from student data (Integrated Student Information Systems/ISIS), business data (Integrated Business Information Systems/IBIS), the Office of Human Resources, the Central Identity Repository (CIDR), Hershey Medical Center, and the World Campus information system.

Reflect and Join

- The identity management inputs from on-boarding, groups, privileges, accounts, affiliations, stewardship, business rules, policy, roles, security, governance and systems of record are reflected and joined into the University Identity Management system.
University Identity Management

Rules

- A business rule defines or constrains one aspect of University business that is intended to assert business structure or influence the behavior of our business.
- Business rules often focus on access control issues, for example, professors are allowed to input and modify the marks of the students taking the courses they instruct, but not the marks of students in other courses.
- University business rules may also pertain to business calculations, for example, how to convert a percentage mark (for example, 91 percent) that a student receives in a course into a letter grade (for example, “A”)
- Some business rules focus on the policies of our organization, for example, a University policy maybe to expel for one year anyone who fails more than two courses in the same semester.
- IAM services should reflect the business rules that have been defined for the University.

Services

The initial set of IAM services will be centered on the Central Person Registry and will include:

- Applications and systems access to the CPR information.
- Management services for maintaining:
  - identities
  - contact information
  - affiliations
  - PSU IDs
  - Penn State Access Account user IDs
  - Sponsored Accounts
  - Identity Assurance Profiles
- Matching services (with the goal of minimizing duplicate identities in central systems).
- Address validation services.
- Batch interfaces for maintenance of the CPR data from other entities.
- Management services affiliation assignments from systems of records.

Additional IAM services will be developed as the project matures.
Delivery

The implementation of IAM combined with policy and data stewardship, will provide the infrastructure and tools necessary to provision University services that are aligned to an individuals affiliation, role, identity policy, and their rights or privileges.

Authenticate

- The process of validating the identity of user; the user is who he/she says they are. Typically, this is accomplished through a username/userID and password pair.
- For example: Has the user specified the correct password for their digital identity?

Authorize

- The process of deciding if a user should have access to a service. The authorization check may be as simple as verifying that the user is in a list of users or as complex as checking for membership in a group.
- Authorization decisions may be based on a user’s affiliation with the University, their role and related role attributes, and their identity assurance profile.
- For example: A student is registered for Economics 101, and as such is authorized to participate in Penn State's Online Learning Management System (ANGEL) for this particular class.
- For example: A staff member has been granted access to the Business Information Systems in their security profile, and as such is authorized access to IBIS.

Federate

- With an enterprise identity management system, rather than having separate credentials for each system, a user can use a single digital identity to access all resources to which the user is entitled. Federated identity management permits extending this approach above the enterprise level, creating a trusted authority for digital identities across multiple organizations. It results in greatly simplified administration and streamlined access to resources; eliminating the need to replicate databases of user credentials for separate applications and systems offers improved security. Federated identity management puts the
focus on users of information and services rather than on entities that house those resources.

- For more information about federation and federating initiatives within the higher education community, please visit the InCommon site, [http://www.incommonfederation.org/](http://www.incommonfederation.org/).

### Applications

- Examples of applications that are enabled through the deployment of IAM services include, but are not limited to University services like e-mail, ANGEL, eLion, and ESSIC; Departmental applications like MyPennState, PennState Online, and The Graduate School Admissions Portal; and, Cloud and Federated applications like out-sourced e-mail, iTunes U, and TeraGrid.

### References

- IAM Online Community Site, [https://iam.psu.edu/](https://iam.psu.edu/).
- The IAM Technical Architecture Group e-mail address: iam@psu.edu
- A glossary that provides more detailed definitions of IAM terminology will available soon at [https://iam.psu.edu/](https://iam.psu.edu/)
- Facebook: [http://facebook.com/PennStateIAM/](http://facebook.com/PennStateIAM/)
- Twitter: @PennStateIAM

### Conclusion

- Identity and Access Management (IAM) is about aligning University business processes, policies, and technologies to support the delivery of a rich and diverse array of online services for faculty, staff, and students.
- The Penn State CPR will be a directory or database that consolidates identity information currently stored in separate and non-integrated sources throughout the University. Integrity rules will be applied that will ensure the validity of the identity data---resulting in a complete and up-to-date person record for each individual University member or affiliate.
The IAM CPR services will provide access to the CPR data, as appropriate and within the guidelines of policy, that will enhance the vetting, proofing, on-boarding, and business processes of the University.

Additional IAM services for access management, directory, and groups will be developed as the IAM project matures.