Access Management
Software Requirements Specification
Review Session

28 July 2010
Agenda

• Introduction
• Software Requirements Specification
• Summary
• Contact Information
Introduction

• Terms and Abbreviations
• What is IAM?
• What is the Central Person Registry?
# Terms and Abbreviations

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>IAM</td>
<td>Identity and Access Management</td>
</tr>
<tr>
<td>CPR</td>
<td>Central Person Registry</td>
</tr>
<tr>
<td>SRS</td>
<td>Software Requirements Specification</td>
</tr>
<tr>
<td>FPS</td>
<td>Friends of Penn State</td>
</tr>
<tr>
<td>CIDR</td>
<td>Central ID Repository</td>
</tr>
<tr>
<td>CACTUS</td>
<td>Central Accounts Coordination Tracking of User Services</td>
</tr>
<tr>
<td>LoA</td>
<td>Level of Assurance</td>
</tr>
<tr>
<td>SoR</td>
<td>System of Record</td>
</tr>
<tr>
<td>RA</td>
<td>Registration Authority</td>
</tr>
</tbody>
</table>
## Terms and Abbreviations

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group</td>
<td>Collection of people who exist in the Penn State Directory.</td>
</tr>
<tr>
<td>Role</td>
<td>An identity attribute that is defined to facilitate assignment of privilege for the purposes of access management. Roles may also be implemented with the user of groups.</td>
</tr>
<tr>
<td>Attribute</td>
<td>Information associated with a digital identity record. Attributes may be general or personal. A subset of all attributes defines a unique individual.</td>
</tr>
</tbody>
</table>
What is IAM?
IAM Defined

“An administrative process coupled with a technological solution which validates the identity of individuals and allows owners of data, applications, and systems to either maintain centrally or distribute responsibility for granting access to their respective resources to anyone participating within the IAM framework.” - NYS Forum
In a nutshell, it’s about aligning policies, processes, and the technologies to support managing identities and access to information.
Identity and Access Management

- Access to Protected Library Resources
- Library Staff Access to Integrated Library System
- Access to Library Public Workstations
- HMC Affiliate
- Access to Library Resources
- Access to Alumni Library Resources
- Access to Electronic Theses and Dissertations Web Site
- Graduate School Exit Survey Federating to blogging hosted Services
- Prospective students applying for financial aid
- Employee Confidentiality
- Provisioning of an employee's digital Identity
- Student early access to residence hall requests and immunization records submissions
- Grouper Auditing Use Case
- Continuing Education and Adult Students
- New Students Applying for Admissions and On-campus Housing
- Prospective Students Visiting Penn State New Kensington
- New Faculty and Access to ANGEL and Other Class Resources
- Adjunct Faculty Activating Access Account
- New Faculty & Staff Selecting Benefits
- Terminated Faculty Member Maintains Access
- Physicians at the Hershey Medical Center and Access to Library Resources
- Patients, Family Members, and Visitors at the Penn State Hershey Medical Center
- Alumni Donors
- Local Community Member and Short Term Access Accounts
- Registrar Relationships
- Student Lifecycle
- New Students Applying for Undergraduate Admissions
- Provision of Access to Course Work For Students at a Distance
- Library Resources
- ITS Computer Store Access
- CIC CourseShare Deprovision User content after graduation or resignation
- Google Cache Updates
- Access to user content after graduation and or resignation
- Emergency Rehire
- Multiple IDs
- Deceased Employee Outreach Registration
- Updating ISIS Security Profile
- Multiple Security Realms, Same Userids but Different Passwords
- ROTC Instructor Affiliation
- Instructor with Independent Contractor Status
- Name change switching in the directory
- Special Affiliates (for example Religious Affiliates)
- Father and son who is a JR
- Cloning ISIS Security Profiles
- New PSUId assigned for new PSU affiliation
- Student Football Tickets
- Department Identity
- DSL Use Case Interview
- Police Services Use Case
- Police Log
- Alumni Association
What is Access Management?

- Access Management is a system that includes the following components:
  - Groups Management
  - Roles Management
  - Attributes Management
  - Risk Assessment
  - Provisioning/De-provisioning of Services
  - Auditing
  - Policy Engine
  - Subscription Services
Software Requirements Specification

• What is an SRS?
• Requirements
What is an SRS?

• “A complete description of the behavior of the system to be developed.” - wikipedia

• “A deliverable that describes all data, functional and behavioral requirements, all constraints and all validation requirements for software.” - Software Testing Glossary
Requirements
Definition

“A requirement is a singular documented need of what a particular product or service should be or perform.” - wikipedia
Requirement Types
Functional Requirement: “defines a function of a software system or its component.” - wikipedia

Non-Functional Requirement: “is a requirement that specifies criteria that can be used to judge the operation of a system, rather than specific behaviors.” - wikipedia
Requirement Sources

- Existing Registries
  - CACTUS, CIDR, FPS
- Existing Groups, Roles, and Attributes
- Regulations and Legislation
- University Sources
  - Survey
  - Interview Sessions
  - Use Cases
- External Sources
Functional Requirements
Registries

- All interfaces to the system shall be done via a secure access method.
- The system shall provide Web services to interact with its features.
- The system shall dynamically generate entitlement strings for all of the courses an instructor teaches.
- The system shall dynamically generate entitlement strings for all of the courses a student takes.
Existing Groups

- The system shall support the establishment and maintenance of standing groups based on data from System(s) of Record (SoR).
- The system shall maintain student and instructor groups.
- The system shall provide a delegated group service.
- The system shall provide Web services to access and maintain group membership.
Existing Roles

• The system shall provide a facility for the management of roles.
• The system shall provide Web services to access and maintain role information.
• The system shall support published views of role information.
• The system shall support the creation, modification, and deletion of roles.
Existing Attributes

• The system shall provide an attribute service. Attributes may be single or multi-values.
• The system shall support public and sensitive (limited access) attributes.
• The system shall support official and user-modifiable attributes.
• The system shall provide Web services to access attributes.
• The system shall support a Web-based search facility.
• The system shall provide a Web-based page for updating user-modifiable attributes.
Regulations and Legislation

- University Policies
  - AD11 - University Policy on Confidentiality of Student Records
  - AD19 - Use of Penn State Identification Number and Social Security Number
  - AD20 - Computer and Network Security
  - AD23 - Use of Institutional Data
  - AD35 - University Archives and Records Management
  - AD22 - Health Insurance Portability and Accountability Act (HIPAA)
- HEOA - Higher Education Opportunity Act
- Red Flag Rules
- PCI - Payment Card Industry
Regulations and Legislation

- The system shall distinguish between directory and non-directory information in accordance with FERPA.
- The system shall include protection for privacy of information.
- Data elements shall be classified as confidential and non-confidential in accordance with law and University policy.
- The system shall protect local storage of data with the same granularity of security control provided by the originating host system.
University Sources

• A formal risk assessment shall categorize data, based on its sensitivity.
• Policy should be established or updated to revoke access to sensitive resources when an employee is terminated or changes positions.
• The provisioning and de-provisioning of access rights shall be automated.
• The system shall support the capability to nest groups.
• The system shall support the capability to generate dynamic groups.
University Sources

• The system shall provide a metadata facility for groups, so that users can identify groups without having to know their names.
• A mechanism shall be developed to enable authorized support personnel to view various aspects of a user’s role information.
• The system shall support the concept of proxy roles.
• A common access method shall be developed for accessing attributes.
• Web services shall be developed to support REST and/or SOAP.
University Sources

• The system shall support the periodic review of a user’s privileges as defined by policy.
• The system’s policy engine shall allow for search of existing rules for possible reuse.
• IBIS and ISIS information shall be sharable with other Penn State applications that serve up academic, financial, and human resources data.
External Sources

• The system shall provide controls on access and changes to critical data.
• The system shall log date, time, nature, and outcome of all significant events. The logs must be kept for 6 months.
Non-Functional Requirements
Non-Functional Requirements

- The system shall be available 24/7/365.
- The system shall support multiple factors of authentication.
- The system shall be open, extensible, and scalable.
- Physical access to data centers is restricted and all access to the data centers shall be logged.
- Continuity of Operations Plan shall be in place.
To Summarize…

• Access SRS contains all of the requirements gathered for the components of Access Management
  – Functional - describing a function or behavior
  – Non-functional - describing the operation of the system
• The SRS is a living document and will be updated with new requirements as they become available
Contact Information

• E-Mail: iam@psu.edu
• Web Site: https://iam.psu.edu/
  – Access Management Forum
• Other places (PennStateIAM):
  – Del.icio.us
  – Twitter
  – Facebook
  – YouTube