To protect the confidentiality and privacy of information at Penn by:

- Uniquely identifying entities associated with Penn
- Providing access to appropriate facilities, services and systems
- Preventing unauthorized access to facilities, services and systems
Current identity management components

- Penn Community – central repository for a person’s bio/demo data as fed by disparate systems (SRS, HR/Payroll, UPHS) and entered directly for ancillary affiliates
- Penn Directory – place that holds the preferred identifying and contact info for all Penn affiliates.
- Penn Card – system used to generate the physical ID card that is used for physical access across the university.
- PennNames - system used to associate a unique username to each individual at Penn, providing a common and consistent University namespace for online services.
- PennKey – unique identifier for our central authentication system. When accompanied with their password provides an electronic means to identify an individual and provide access to systems across the university
PennAccess

Penn’s Identity Management Strategy

HR
SRS
UPHS
Ancillary Affiliates
(Temp, VFAC, CHOP, etc.)

Penn Community

Penn Card

Penn Directory

Penn Names

Central Authorization

PennKey

4/20/08
Central Authorization at the University of Pennsylvania
Currently a missing link in Penn’s identity management strategy

- PennKey authentication, tells us who you are
- There is no comprehensive means to control and distribute access privileges across the university.
Proposed Central Authorization

- Build a central authorization system that could be utilized by applications across the University
- Utilize Penn Community data and school/center created lists to facilitate authorization decisions
- Allow Schools and Centers to build and reuse authorization information across applications
- Provide sophisticated group management capabilities, such as subgroups and composite groups, to support access management needs.
Facilitate consistent application of University business rules
  - Managed through a common UI and standard API

Streamline maintenance of authorization data
  - Bring scattered redundant groups together for re-use
  - Allow useful actions on these groups -- group math, group nesting, exclusion criteria

Leverage Penn Community data for accurate, up to date authorization decisions
  - Can leverage existing attribute information

Support the creation of new groups
  - By schools, departments, and individuals!
  - Distributed/delegated model of control
Proposed Approach

- Reach out to the university community to understand need and develop requirements
- Leverage open source software where it is in alignment with our objectives
- Design and develop a central authorization solution based on industry accepted standards
  - Schools and centers can integrate authorization into new applications
  - New applications no longer have to build their own authorization system
  - Existing applications can be modified to capitalize on the features and benefits of a central system
Challenges

- Adoption
- Maintenance – naming conventions
- Authority to create groups
- Clean up – dormant or obsolete groups
- Automation of groups
- Existing applications – no plan to retrofit