Identity Services @ MIT

a strategic view for IS&T/ISDA

Version 1.2
June 9, 2008

Identity Services (IdS) Defined

- Information used to maintain a profile of a person is "Identity" data. Identity data is used to allow access to online resources and maintain individual and institutional brand.
- Identity Services are sets of capabilities to allow identities access to online resources. Applications use IdS to manage online communities.
- Identity Services include Authentication, Authorization, Groups, Privileges (Roles), Identity lifecycle, Directories, Federations and federating technology.

Identity Components Defined

- Identity = a collection of attributes used to define any entity (e.g. person)
- Authentication = Act of proving someone is who they claim to be
- Privileges (Roles) = Statements of who is allowed to do what
- Authorization = Act of determining if someone is allowed to perform a function usually based on Privilege information
- Groups = Collections of identities; providing capabilities to manage them and allowing applications to use them
- Identity lifecycle = From creation to expiration and all possible states between making up the life of an Identity
- Directories = Repositories of identity information where applications rely for real-time access
- Federations = Collections of organizations linked by identity services agreeing upon rules of engagement to exchange identity information
- Federating Technology = Software used to implement federations such as Shibboleth which MIT Touchstone is based

Vision

1. Enables internal and external collaborations
   Federated access for faculty, researchers & students
2. Transparent and easy to use; reduced support
3. Improved and timely access to MIT services
4. Improved security via better identity control
5. Respect privacy of users and community
6. Easy integration for Apps and developers
7. Near real-time (de-)provisioning to Apps
8. Services built on technology used globally

Goals

1. All IS&T applications use common Identity Services
2. Majority of MIT uses Identity Services
3. MIT active in Federated services
4. Federated access beyond the web browser (such as N-Tier problem, mobility)
5. Provide federated capability to HPC platform
6. Alignment of IdS and business processes
7. Reliable services (24x7 infrastructure)
8. Support needs of MIT Next Generation Student System Services project

Value/Benefits of IdS

- Reduce duplication of effort for developers
- Developers concentrate on Apps; not IdS
- Increased choice of Apps to community
- Insulate Apps from evolving IdS technology
- More rapid App integration into MIT infra
- Consistent user experience for App access
- Increase importance/value of MIT brand

MIT having been a leader in IdS …

Enjoyed benefits of Kerberos for non-web SSO
Unique groups, roles & certificate capabilities
Good understanding of IdS processes
But…
- Limited abilities hosting non-MIT users
- Increased App integration complexity
- Only some Apps distinguish AuthN & AuthZ
- Need to evolve some IdS to be more current
- And better integrate IdS processes (tech + biz)

Gaps (functional)

- Not yet federated with other institutions
  - NSF/NIH want collaborative cyber-infrastructure
- Current technology web browser oriented
  - No effective solutions for N-Tier problem (portals) and non-browser applications
- Identity business processes not fully aligned with technology capabilities or other business needs
- Kuali Student App needs not fully defined, yet

Approach

- Identify MIT-only assets viable/needed for global usage
- Identify MIT-only assets where non-MIT solutions are more appropriate or viable. Contribute back to community.
- Make change wisely – demonstrate value as we go
- Characteristics of Services & Software
  - standard protocols and data formats
  - Real time updates and access (data feeds only where required)
  - 24x7, scalable, reliable, modular, serviceable
  - Integrates easily with vended and OSS products
  - SDKs for developers
  - used by others, especially in higher education
  - Audit-ability

Trends & Drivers

On the Internet, it's all about Identity (Burton Group)

Some existing MIT technology is 10-20 years old, MIT-specific, hard to integrate

Federation – Collaboration with external organizations preserving credentials, affiliation and control

Sourcing – Apps moving inside to outside and back again. Identity needs to be consistent

Identity theft on the rise !!

Real criminals now on the net, not just hackers

Conceptual Architecture

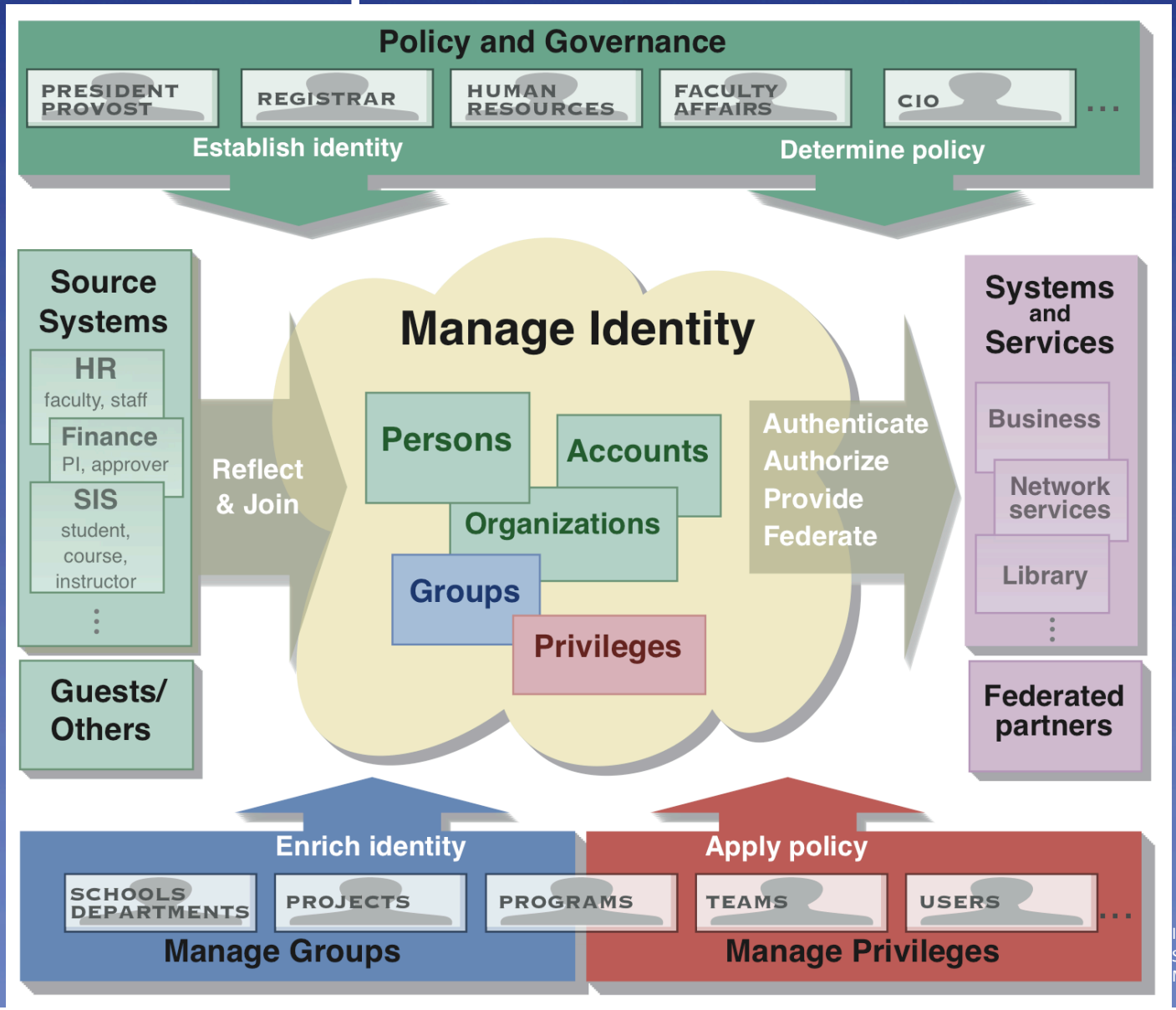

Image courtesy of National Science Foundation Middleware Initiative

Dependencies & Assumptions

MIT wishes to preserve its prominent identity

MIT wishes to collaborate in global science

IdS shall be a managed resource for most of MIT

IdS shall be as reliable as power, water & phone

Emerging Applications like Kuali Student and DOS will help define needs for evolving IdS

Risks (*of providing IdS*)

- Centralization concerns:
  - Single point of failure (if IdS breaks then access to relying services may be interrupted)
  - DLCs might perceive IS&T as obstacle or overseer
- If not seen as good enough, the community will do its own thing
- Perceived fear: Standardization sometimes stifles innovation
- Business processes not aligned for near real-time delivery of identity data

Risks (*of **not** providing IdS*)

- The Balkanization of identity in the community
- Administrative inefficiencies will increase
- Significant overhead and complexity for users
- Duplication of IT effort & development
- Institutional identity lost (i.e. goes to ~Google)
- MIT becomes lead story in the news because of
  - Privacy Spills or increased identity theft

Summary

Identity Services are

- Critical cyber-infrastructure
- Essential to enable collaboration for research & education according to NSF, NIH and other funding bodies
- Fundamental to representing MIT brand, globally
- Key to securing MIT electronic assets
- Evolving and addressable in the next 3 years

IS&T/ISDA is the appropriate locus to develop IdS