

How Identity and Access Management Can Help Your Institution Touch Its Toes

Renee Woodten Frost
Internet2 and University of Michigan

Kevin Morooney
The Pennsylvania State University



Agenda

- Evolution of Identity and Access Management efforts: bridging to Security
- Potential benefits for future Enterprise Infrastructure and Architecture from the perspective of a CIO

Evolution of Identity and Access Management: Bridging to Security

Copyright Renee Woodten Frost 2008. This work is the intellectual property of the author. Permission is granted for this material to be shared for non-commercial, educational purposes, provided that this copyright statement appears on the reproduced materials and notice is given that the copying is by permission of the author. To disseminate otherwise or to republish requires written permission from the author.

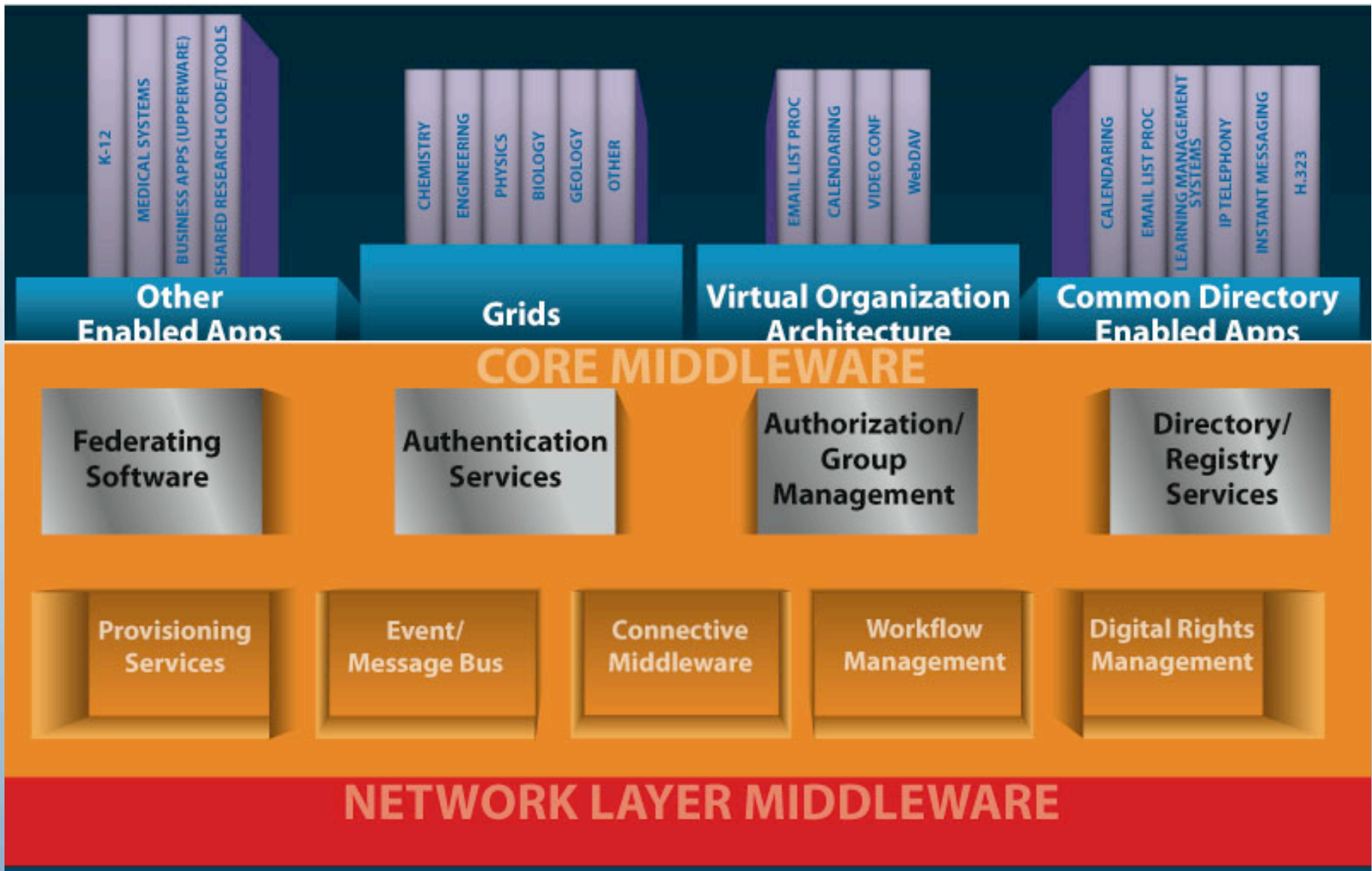
Enterprise Challenges

- Wondering how your campus will comply with the growing number of state and federal privacy requirements?
- Struggling to keep up with the increase in the number of applications and ensuring that their security and access requirements adhere to your policies?
- Concerned about using outsourced services and the need to supply personally identifiable information to third-party providers for access control?

Identity and Access Management (IAM)

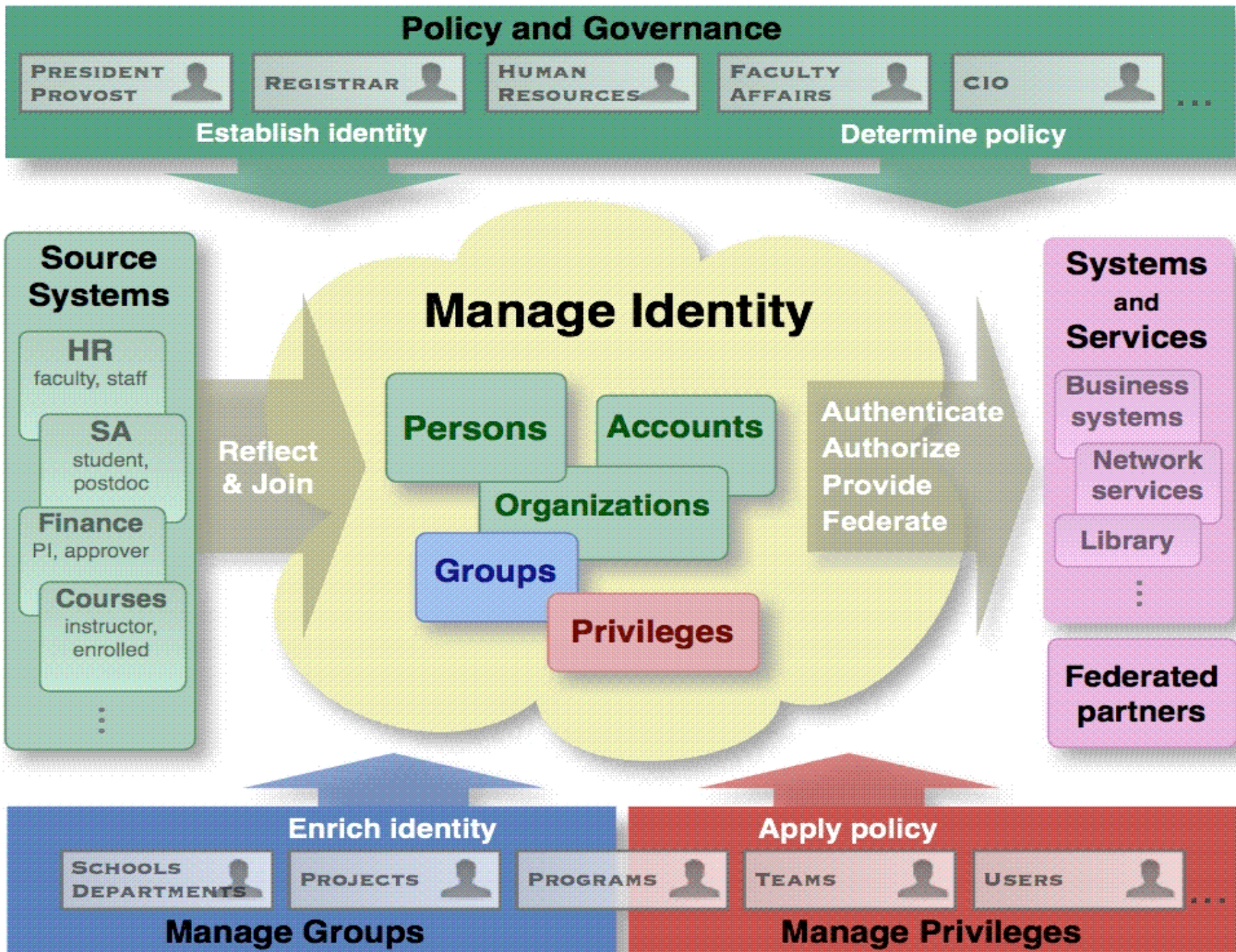
How IAM infrastructure helps

- Supports increased electronic interactions
- Reduces incremental cost to implement new online services
- Increases security
- Assists with regulatory compliance
- Enhances end user experience
- Integrates web services
- Offers flexible, largely scalable, privacy-preserving access via federating software



Identity and Access Management Survey

- Have enterprise directory?
- Have a unique identifier for campus members? Affiliates?
- Have implemented EDUPERSON?
- Have a WEBISO (pubcookie, CAS, Cosign, your own)?
- Have implemented Shibboleth?
- Are a member of InCommon?

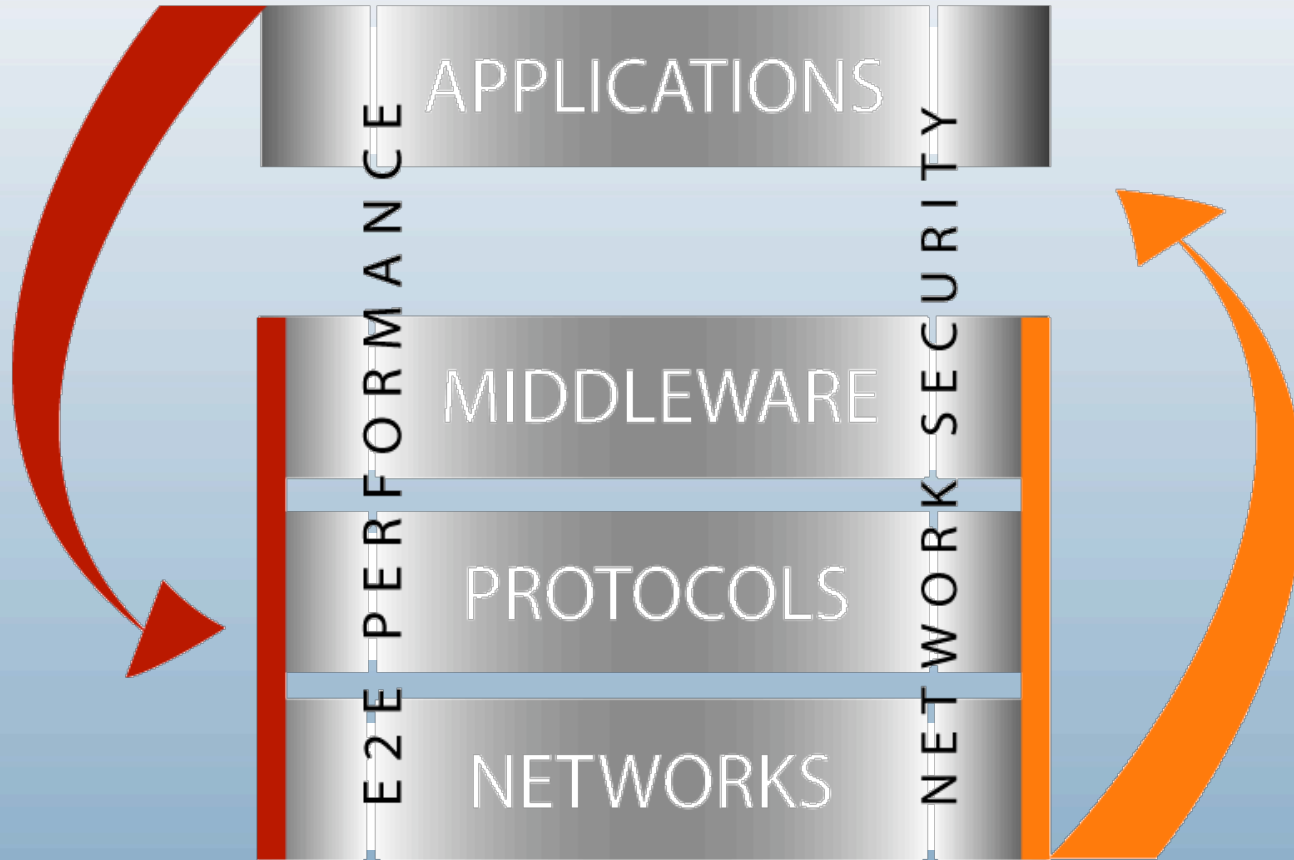


Convergence of Challenges and Intersection of IAM, Security, Policy

- NMI-EDIT Middleware/IAM
- EDUCAUSE/Internet2 Security Task Force

Integrated Systems Model

Motivate



Enable

Relationship between Middleware/IAM and Security

Physical infrastructure:

Middleware/IAM: well-defined infrastructure layer

Security: not crisply defined, spans all layers

Goal:

Security staff want to keep the bad guys out and
IAM folks want to let the good guys in.

“Bridging Security and Identity Management” CAMP Workshop – Feb 2007

To explore overlap in challenges and possible opportunities for interactions for:

- privacy and compliance
- threat and risk mitigation
- scalability

each of which would benefit from a bridge between security and identity management

Pre-Workshop Survey: IAM and Security Attendees' Concerns

- Provisioning and de-provisioning
- Implementing access policy across enterprise systems
- Using IAM as a basis for security architecture
- Managing sensitive data across the institution
- Enabling users outside the firewall for services inside the firewall
- Integrating IAM and security planning and staffing
- Using IAM for risk mitigation
- Achieving compliance with privacy obligations

“Bridging Identity Management with Security” Workshop Themes

- Current and near-term drivers bringing these areas together
- Looming ERP challenges
- Thinking differently: how linking IAM and security provides new flexibility for solutions
- Opportunity to extend “securing our campuses” to “protecting the privacy of users”

IAM and Security Drivers in ERP

- Managing access and security often requires multiple full-time staff, represents hidden cost
- Complex business systems provide little support for auditing and compliance. Certifying key business records, such as required by Sarbanes-Oxley, is extremely difficult, time consuming and expensive
- Compliance requires ensuring policy, procedure, and technical operations are followed
- SOA is going to require this be integrated with IAM

Ensuring Audit Compliance

- At core of auditing: ensuring orgs have adequate policy + procedures and adhere to them
- Challenge for IT: often policies do not map well to technical infrastructure - difficult to validate adherence - results in significant staff time for oversight/review or creates gaps
- Single signon created situation where some apps drive draconian authentication policies. IAM + Level Of Assurance allows authentication policies based on services we provide
- Vision: A policy-driven enterprise security architecture that verifies compliance with policy

Managing Access with Privacy

- Privacy protection **MUST** become central to our thinking – must move from securing computers to protecting privacy
- Federations are essential to building a common contractual definition of trust and . . . privacy
- With R&E now a global enterprise, we must take into acct privacy rules elsewhere

Key IAM Points: Privacy & Compliance

- To address privacy, identity and access management (IAM) is used to reduce exposure of personally identifiable information and other important resources and services.
- To address compliance, IAM and related functions of logging, tracking, and provisioning access are critical to achieving this goal.

Key IAM Points: Threat & Risk Mitigation

- To address threat and risk mitigation, IAM can be used to properly handle sensitive attributes such as PII (personally identifiable/identifying information) including SSN and those needing protection in Sunshine/Open Records challenges

Key IAM Points: Scalability

- To scale all of this requires an eye toward reducing complexity, which IAM does by correlating identity and access across campus applications and systems and enabling the consistent application of institutional policy.

Key Points from Security Panel

- Delegation of certain control functions is often required and needs special care to ensure adequate controls.
- Compliance & audit requirements are frequently the driver for security becoming more important to the organization. Security point solutions are not adequate; strong IdM is really required. Organization needs to be able to demonstrate the controls are effective.
- Competing & overlapping regulations make for a complex environment. ISO 27001 is turning out to be an effective approach that addresses the other requirements well.

More Key Points from Security Panel

- Resources are never sufficient; a risk assessment/management approach is useful in prioritizing for executives.
- The risks of a particular path need to be explored, enabling decisions by management about budget priorities.
- Goal is reducing “unintentional risk.” Deliberate choices need to be made to reduce/eliminate risk. Business officers should be the ones to make the final risk decisions

Identified Possible Intersections

- Integration of campus card with IAM
- Emergency communication
- Rethinking password resets
- Location aware WebISO
- Firewall access control
- Dynamic VPN access to resources
- Password change requirements and Level of Assurance
- Federated access

Some Approaches and Techniques

- Balance use of access control methods at application and network layers
- Define roles and groups for managing access to systems
- Build Web applications using the right identity-based approach for your security requirements
- Leverage IAM principles for authenticated guest access to your wireless network
- Use a risk assessment to drive your authentication infrastructure
- Use IAM to abate your use of Social Security numbers

Relationship Findings

IAM is key enabler and fundamental to Security; very few business processes have this level of impact on security; understanding links critical to planning future infrastructure