Identity Management Brief

Presentation to the
Executive Management Team
November 26, 2007
What is Identity Management?

“the management of information required to identify who a particular user is and to determine what enterprise resources they can access”.

An authoritative place to store identities
A system to synchronize the identities with other systems
Systems to leverage the identities for single-sign-on
Systems to facilitate internal and external entities’ integration and access to the identities
Identity Management architectures must be dedicated only to storing and distributing identities
Identity Management is not data management
Identity Management is not choosing a unique identifier
Current State

- We have a provisioning system in place and running
- We have an identity store in place and running
- Many applications currently authenticate to the identity store (UGAMail, WebCT, UGA Payroll)
- Many applications use their own proprietary identity store to authenticate users (UGA Calendar, mainframe applications)
- Externally hosted applications have no way to integrate with the identity store (external email accounts, iTunesU)
- Process to create and remove an identity is labor-intensive, error-prone, and insecure
- Administration and engineering of the identity management systems is not dedicated to those systems
Our Strategy

- Embrace the diversity of how identity stores are currently managed
- Architect with decentralized management of identities in mind
- Automate the workflows involved in creating and removing a identity
- Leverage currently in place systems where industry trends and support is strong
- Leverage a functional committee to make human interface and workflow decisions
- Leverage a technical committee to provide decision support for the functional committee (provide options for them)
- Don’t create any dependencies on a particular unique ID number
- Don’t allow any other functionality besides managing identities to enter any requirements (will not store grades, will not store salary)
Risks

• **Securing Sensitive Data**
  Continuing in insecure process exposes UGA to significant legal risk (DMCA, FERPA, HIPAA)

• **Productivity**
  Continuing in inefficient process exposes UGA to productivity loss
  Continuing without a authoritative identity store exposes UGA to productivity loss (within IT functions)

• **Federation**
  Continuing without a coherent strategy and architecture exposes UGA to risks when wanting to collaborate with others on research and academic scholarship
Next Steps

• Approval by the EMT of functional and technical committee scope
• Communications plan for the identity management strategy
• Funding for a requirements analysis effort for the scope provided in executive brief involving collaboration with the functional committee and customers
• Request for funding for detailed plan will follow requirements analysis