IDENTITY MANAGEMENT OVERVIEW

…for the University of Alaska System

7/8/2009

Paul Caskey, U.T. System

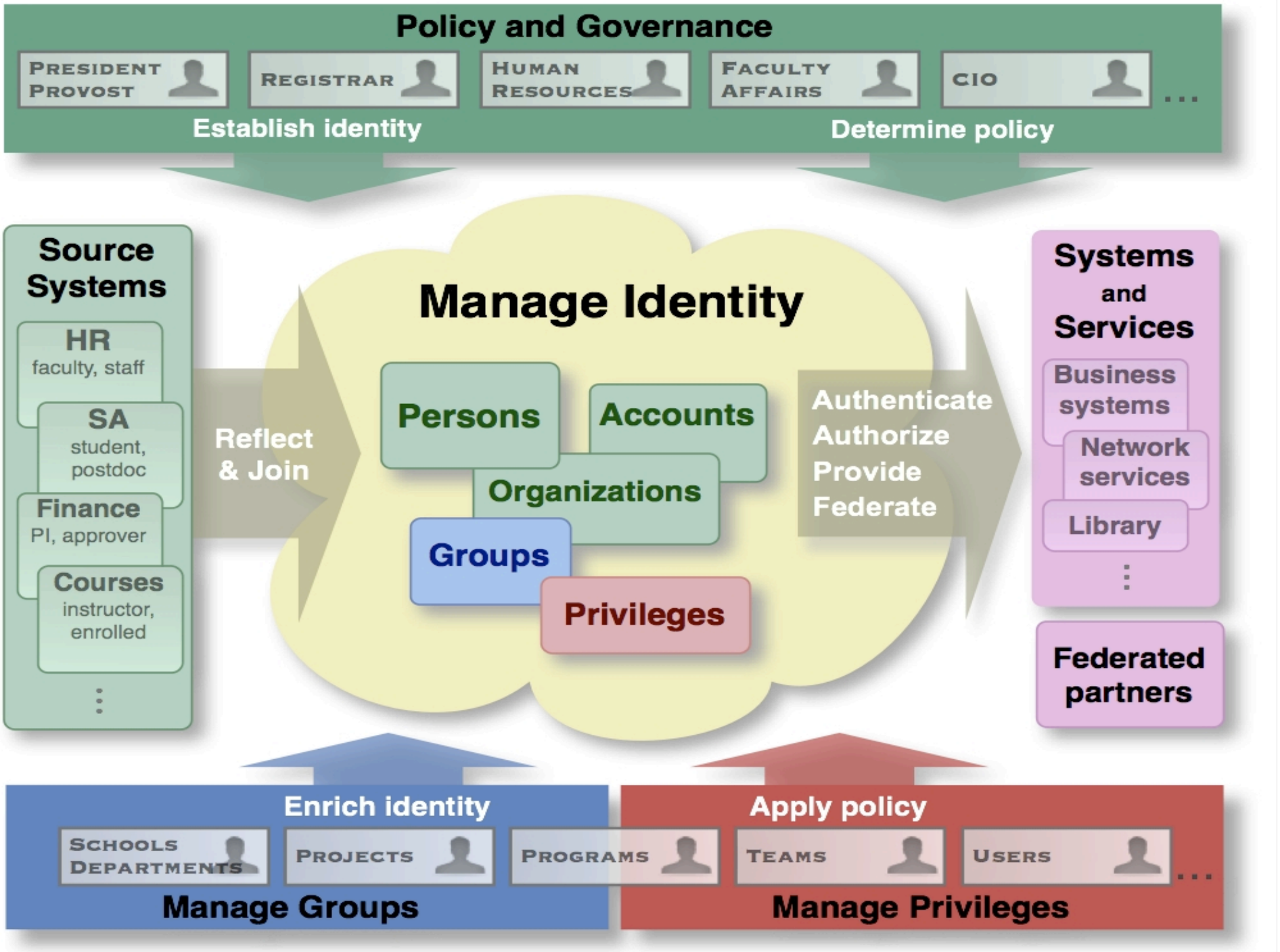
INTRO / IDM OVERVIEW

- What is Identity Management?

  "A set of processes, and a supporting infrastructure, for the creation, maintenance, and use of digital identities." *(Burton Group)*

- It is more than account creation, more than directories, authentication, access controls, etc.

- It includes policy, process, governance, trust, and new ways of thinking about I.T.


Policy and Governance
President
Provost
Registrar
Human Resources
Faculty Affairs
CIO
...
Establish identity
Determine policy
Source Systems
HR
faculty, staff
SA
student, postdoc
Finance
PI, approver
Courses
instructor, enrolled
Reflect & Join
Manage Identity
Persons
Accounts
Organizations
Groups
Privileges
Authenticate
Authorize
Provide
Federate
Systems and Services
Business systems
Network services
Library
Federated partners
Enrich identity
Schools
Departments
Projects
Programs
Manage Groups
Apply policy
Teams
Users
Manage Privileges

FIRST, A FEW TERMS…

- Authentication – “The process by which you prove your identity to another party…” (Cornell University)
- Authorization – “The process of determining a user's right to access a resource.” (the MAMS project - Australia)
- Credential – “An object that is verified when presented to the verifier in an authentication transaction.” (Webopedia, OMB)
- Federation – “A collection of organizations that agree to interoperate under a certain ruleset.” (SWITCH)

A FEW *MORE* TERMS…

- Identification/Vetting – "The process by which information about a person is gathered and used to provide some level of assurance that the person is who they claim to be." (NMI-EDIT)

- Level of Assurance (LoA) – "Describes the degree of certainty that the user has presented an identifier (a credential in this context) that refers to his or her identity." (NMI-EDIT)

- Reflect & Join – "Accumulating, maintaining, and refreshing data of interest from authoritative source systems and consolidating it into a cohesive whole that represents an established identity."

SOURCE SYSTEMS

- These are the enterprise systems which contain authoritative records for various people throughout the institution.
  - HR
  - SIS
  - Finance/Research
  - Guest Mgmt System
  - Graduate/Post-doctoral
- These systems provide information to the IdM system about who is affiliated with the institution.

SOURCE SYSTEMS (CONT.)

Questions to ponder:

- Who is considered a student/employee/etc?
- How are guest credentials created and delivered?
- How does the IdM system learn about these various people?
- How/When do deactivations flow from these systems to the IdM system?

POLICY AND GOVERNANCE

- This area includes the various stakeholders that provide input to the effective operation of the IdM system.
- These stakeholders establish the policies that specify how IdM should work across the institution and the governance structure that provides the oversight and direction needed to operate in the manner intended (and what to do when it doesn't.)

POLICY AND GOVERNANCE (CONT.)

Questions to ponder:

- Who decides/develops the policies that need to be established or revised to govern IdM?
- What groups will approve IdM policies?
- Who owns the IdM function?
- What is the role of internal audit?
- With whom will you federate?
- What dispute resolution mechanisms will be put in place?

GROUPS/PRIVILEGES

- This is where a person's interactions and affiliations with the institution are established.
- There are several sources of information for the IdM system that determine to what schools, projects, research teams, V.O.s, etc. a person belongs.
- These entities determine not only groups/affiliations, but also an individual's role within the institution.
- Groups, Roles, and Privileges together form a distributed access management system that application owners can utilize to control access to their systems.
- There are a variety of collaborative tools that can take advantage of a distributed access management system to allow seamless collaboration.

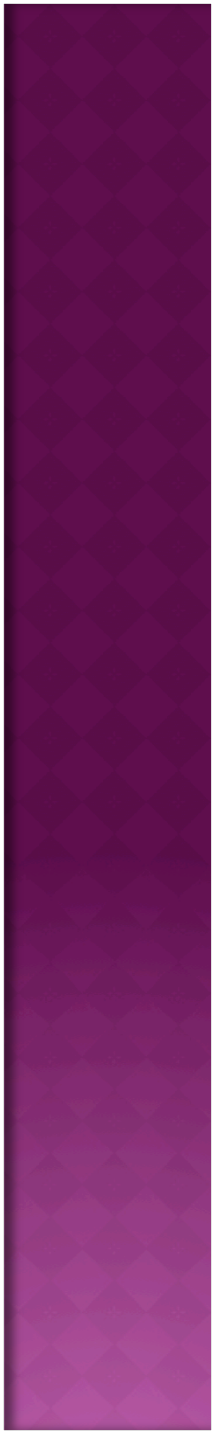
GROUPS/PRIVILEGES (CONT.)

Questions to ponder:

- How are multiple affiliations handled (e.g., student-employees, etc)?
- How does a person transition from one affiliation to another?
- How does the IdM system learn about groups, roles, and privileges?
- How do new groups/roles/privileges get established?
- How will applications use group/privilege information?

MANAGE IDENTITY

- This is where accounts are provisioned, bound to identities, populated with other information, joined to groups, and given privileges.
- This is where identifiers are established and credentials are issued.
- Authentication, authorization, provisioning, and federation all happen in this area.



MANAGE IDENTITY (CONT.)

Questions to ponder:

- What types of credentials will be given to various people?
- What identifiers will be used on your campus?
- How will people be identified/vetted?
- How will credentials be delivered?
- What happens when they lose/forget their credentials?
- How/When will credentials be de-activated/ revoked?

SYSTEMS AND SERVICES

- These are the downstream consumers -- applications and services -- of the IdM system.
- Of course, these include all the applications on a typical campus but increasingly include external applications (e.g., library content providers, grid computing, collaboration tools, and a host of shared applications and services.)

SYSTEMS AND SERVICES (CONT.)

Questions to ponder:

- How do you decide what applications are integrated into the IdM system? What review and approval process will exist?
- What technologies and protocols will the IdM system support?
- What risks are associated with various applications?
- What data will be provided to applications?
- Are there any privacy implications with these applications?
- What types of logging capabilities are applications expected to provide?

SO, HOW DOES THIS ALL WORK TOGETHER?

- A “new-hire” example… The goal is for a newly hired faculty member to gain access to grid computing resources at another institution (like Teragrid, etc).
- A new faculty member is hired.
- He/She is entered into the source system (HR) with an appropriate effective date.
- At some point prior to starting work, according to account provisioning policy, the new faculty member is “seen” by the IdM system and is added to the person registry and all basic accounts are provisioned automatically, based on data fed from the HR system.
- Groups and Roles are also defined at this point.
- The new faculty member shows up on campus in their new department/ college.
- New faculty member goes to the account activation agent in their department.

SO, HOW DOES THIS ALL WORK TOGETHER? (CONT.)

- The new faculty member is asked to sign the AUP.
- The registration agent verifies identity, according to establish policy, and records appropriate information.
- The registration agent records the identity verification event in an account activation system (temp password is retrieved)
- The new faculty member logs on for the first time using the temporary password and is forced to change to a "real" credential/password, based on established policies (LoA is increased at this point).
- Optionally, if the faculty member will work with high-risk apps and sensitive data, they will also be issued a dual-key digital certificate and token (via an online system).

SO, HOW DOES THIS ALL WORK TOGETHER? (CONT.)

- To request an allocation of time on grid resources, the new faculty member simply navigates to the grid portal, logs on via shibboleth, and clicks on a button that says "Request Allocation".

- The 'Request Allocation' button would not even be visible, had 3 key things not been communicated to the grid portal:

1. he/she authenticated successfully with their home institution
2. there is a higher level of assurance with this authentication, and
3. he/she is PI-eligible.

DO WE *REALLY* NEED TO DO IDM - AREN'T OUR CURRENT PRACTICES "GOOD ENOUGH"?

- Well, maybe they are today, but…. The world is changing!
- Effective IdM is critical to holistic I.T. Security!
- Effective IdM is critical to legal compliance (HIPAA, FERPA, SOX, GLB, etc).
- Increasingly, we are not alone in our own little sandboxes. Secure collaboration requires effective IdM and possibly higher LoAs!

HOW DOES FEDERATION FIT IN?

- When you have your own house in order, you're ready to go play nicely with others!
- Trust is the key. Without effective IdM, it's very difficult to convince others to trust you!
- Level of Assurance (LoA) becomes critical to developing trust. It gives us a standardized way to discuss the parameters of trust.
- LoA compliance requires good IdM governance.

BENEFITS OF FEDERATED SSO

- Secure collaboration – across the world as easily as across campus
- Access to a growing list of online services
  - https://spaces.internet2.edu/pages/viewpage.action?pageId=11484
- Ease of use, consistent interface for users
- Improved application development/lower costs
- Improved application security (no “islands of identity info”)
- Easier to share apps and services (Ex: Selfscan)
- Maintains local autonomy in a distributed world (can support differing technologies/infrastrucutres in a common framework)

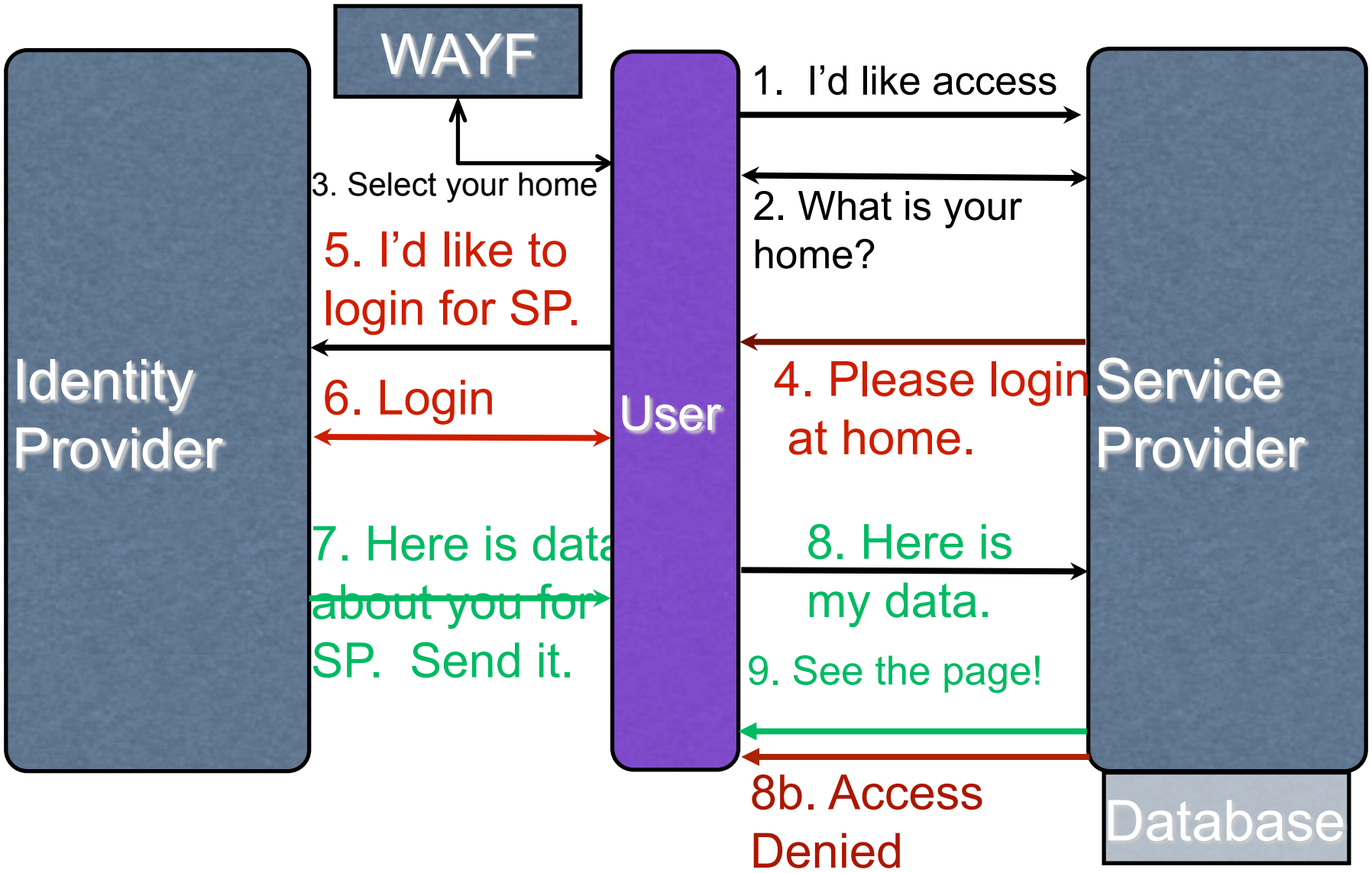
WHAT SORT OF IDM PRACTICES ARE IMPORTANT TO FEDERATIONS (LOA)?

- Identity verification (vetting)
  - Ideally, in person
  - Remote vetting procedures do exist (notary, etc)
  - See NIST sp 800-63
    - http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63V1_0_2.pdf
- Password policy
  - A good standard to use is the federal government's password entropy score (at the level 2 standard). The spreadsheet for scoring a password policy can be found here:
    - http://www.cio.gov/eauthentication/documents/CommonCAP.xls (use the "Password Calculation" tab)
- Credentials
  - Username/password, certs, tokens, etc. and the issuance process

WHAT IS SHIBBOLETH?

- It is **THE** open-source software product developed by Internet2 (The shibb authors are lead contributors of the SAML specification from OASIS)
- An implementation of the SAML specification (OASIS)
- A single sign-on solution, akin to Pubcookie, CAS, CA-Netegrity, etc.
- Federating software (software that enables identity federation)

SHIBBOLETH 2 DEFAULT FLOW



WHAT WE'VE DONE IN TEXAS

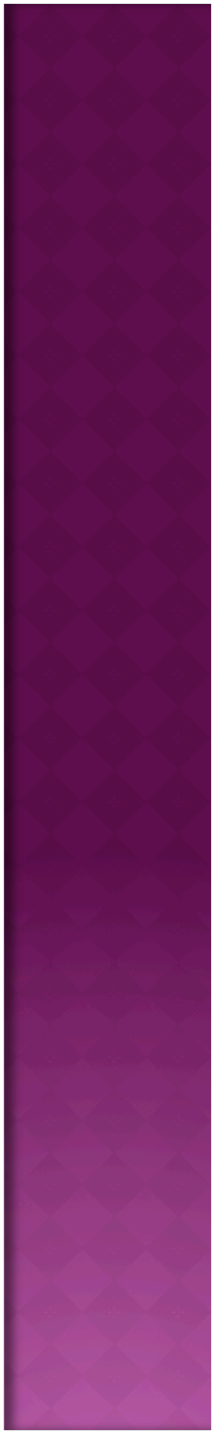
- UT System Federation
  - 16 legally independent institutions (9 academic, 6 health, 1 admin)
  - Secure collaboration is a key goal
  - Started federation in pilot mode by holding a shibb-fest in 9/2004, helped immensely from a small EDUCAUSE/ NSF grant (*"Extending the Reach"*)
  - Grew number of IdPs to where all campuses were up and running (16) over next 2 years
  - Federation entered production status 9/1/2006
  - ~40+ applications, including vendor services (Cayuse, Avatar) and commercial apps (Blackboard, Adobe Connect, etc)

WHAT WE'VE DONE IN TEXAS (CONT)

- The LEARN Federation
  - Lonestar Education and Research Network (RON)
  - 30+ member institutions
  - Research and collaboration a key mission
  - Federation is in its infancy, but growing
  - Microsoft DreamSpark was the first app
  - Envisioning a collaborative portal
    - Grid computing portal
    - *Texas Digital Library*
    - *Collaborative Funding Network*

POTENTIAL ISSUES

- Authorization
  - Federated or locally managed?
  - Attributes?
  - Role changes?
  - EX: “Application Admin” app
- Identifiers / Privacy
- Attribute definitions
- Test accounts
- Test pages
- Required LoA (risk assessment)
- Audit (who, when)



BEST PRACTICES/LESSONS LEARNED

- Using shibb for internal apps makes it very easy to share them across a broader audience and gives users a consistent UI
- Authorization is hard, plan early, start small
- Provisioning is a key challenge
- Policy work is hard, takes consensus, buy-in from all levels
- Support can be a challenge since there are more pieces and players involved

THE FUTURE…

- eGovernment
  - Federal government already doing federation (NIH, NSF, GSA, etc)
  - Several states are looking keenly at federation
- Inter-federation
  - UT System pursuing inter-fed with InCommon
  - InCommon peering with UK Federation
  - Transitive trust? Membership issues?
- Vendors becoming more SAML-aware
  - We now write this into our contracts
  - Mixed results, so far
- Microsoft activity in this space…
  - Geneva
    - http://www.microsoft.com/forefront/geneva/en/us/
  - Cardspace
    - http://www.microsoft.com/windows/products/winfamily/cardspace/default.mspx

A FEW DEMOS….

- Wireless
- Blackboard
- SelfScan
- Compliance Training
- Application Admin