

# Identity Management and Shibboleth at MSU

Jim Green

Manager, Identity Management  
Michigan State University  
Academic Technology Services



MICHIGAN STATE  
UNIVERSITY

# Identity Management

- Definition: “Identity management is the set of business processes, and a supporting infrastructure, for the creation, maintenance, and use of digital identities.” -- The Burton Group
- MSU’s centrally-supported IdM infrastructure:
  - Digital credentials
  - Authentication
  - Single Sign-on
  - Directory Services
  - Middleware
  - Federation

# Organizational Structure

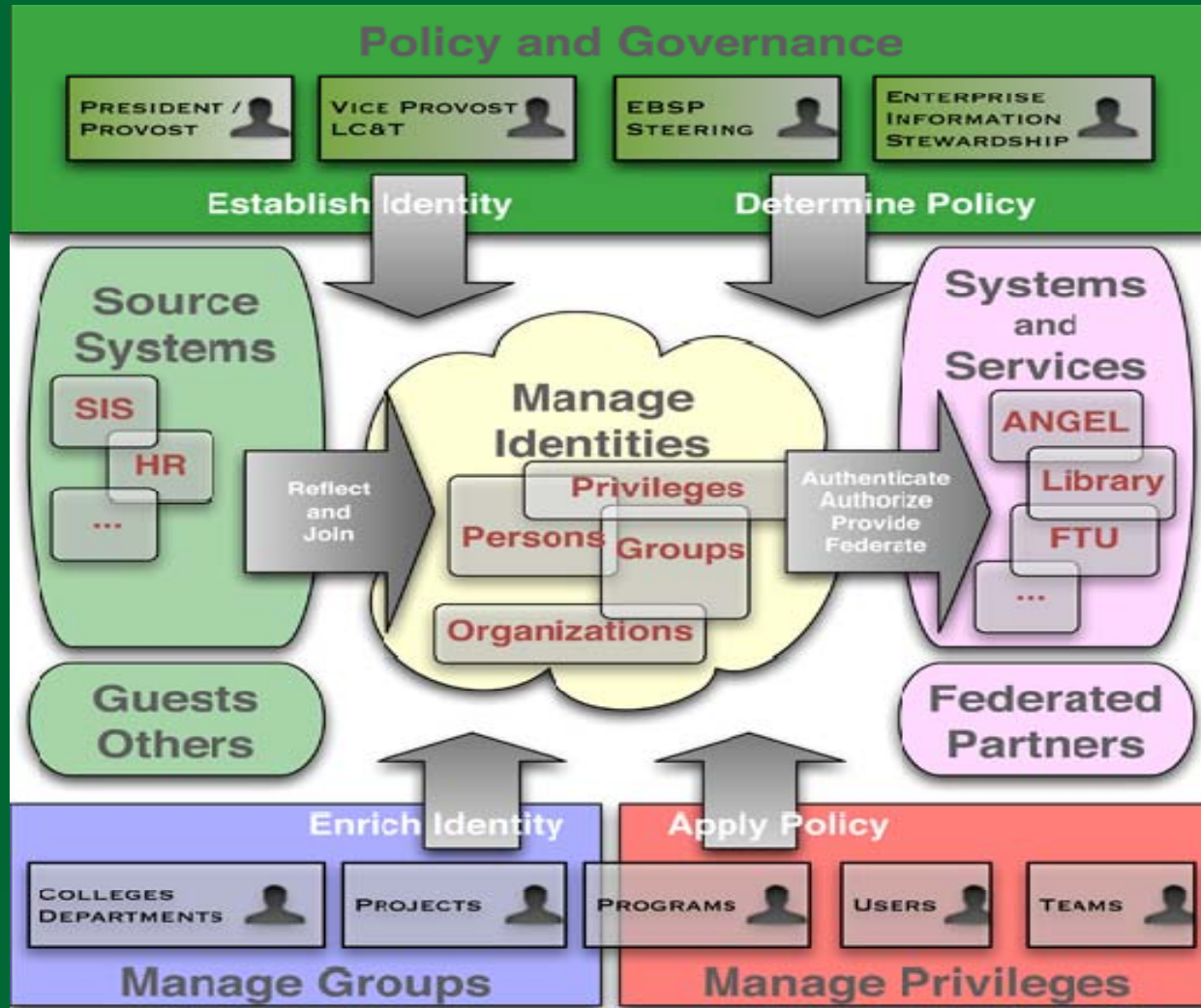
- Libraries, Computing and Technology
  - Academic Technology Services (ATS)
  - Administrative Information Services (AIS)
  - Broadcast Services
  - Enterprise Business Systems Project (EBSP)
  - Enterprise Information Stewardship (EIS)
  - University Libraries
  - University Archives & Historical Collections (UAHC)
  - Virtual University Design & Technology (VUDAT)

# How IdM fits in

- EIS – IT governance
- EBSP – new HR, financial, BI, research administration
- AIS – Enterprise data/systems of record, administrative systems
- ATS – Network, LMS, mail, web, computer labs
  - IdM
- Requires partnership – EIS, EBSP, AIS
- Stakeholders – data stewards
  - Registrar’s office
  - Human Resources
  - ID Office
  - Internal Audit
  - Others

# Guiding Organizations

- Internet2/MACE (Middleware Architecture Committee for Education)
- NMI-EDIT (National Science Foundation Middleware Initiative Enterprise and Desktop Integration Technologies)
- Educause/Internet2 CAMP (Campus Architecture and Middleware Planning) workshops
- Educause net@EDU Identity Management Working Group
- InCommon



# MSU IdM technology

- Central authentication service – Kerberos
- Intra-institutional single sign-on – Sentinel
- Federated authentication – Shibboleth
- Directory services – OpenDS
  - msuEduPerson, eduOrg, eduPerson
- CommunityID
  - Provisioning
  - Web services
  - Self service account creation/management
- NetID – legacy provisioning system

# InCommon

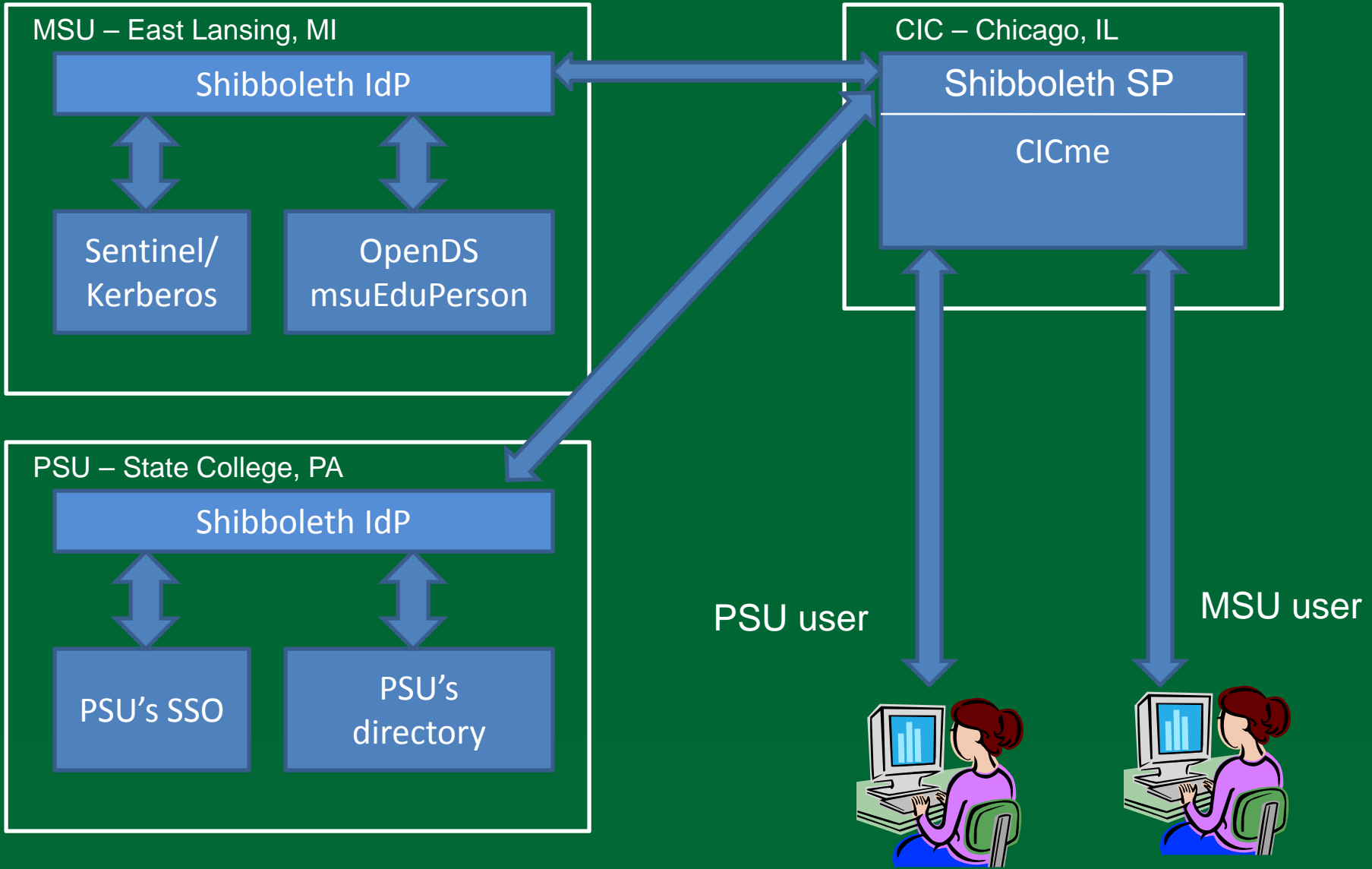
- Trust fabric between federation members
  - Higher Ed
  - Government – NIH, NSF
  - Sponsored participants -- Apple, EBSCO, OCLC, ...
- Shibboleth and SAML
- Participant Operating Practices statement
- Federation membership not necessary

# Shibboleth introduction

- An Internet2/MACE initiative
- Open source
  - Apache 2.0 license
  - Strong community
- Standards-based -- SAML
- InCommon – other federations
- Authentication and Authorization Infrastructure
  - Simplify inter-organizational access to resources
  - Intra-organizational applications, too

# Shibboleth components

- Identity provider (IdP)
  - Java/Tomcat
- Works with authentication/SSO and enterprise directory systems
  - Can also be configured to provide its own SSO capability, eliminating the need for an external SSO system
- Service provider (SP)
  - Java – works with Apache or IIS
  - Where are you from? (WAYF)



# Shibboleth at MSU

- IdP – Shibboleth v. 1.3
  - 1.x twilight June 30, 2010
  - Authentication – Kerberos
  - SSO – Sentinel
  - Attribute server – OpenDS-based private LDAP directory
  - msuEduPerson, eduPerson, eduOrg
- SPs – Versions 2.x and 1.3 supported
  - Interest as a local SSO solution
  - Federation capability – “icing on the cake”

# MSU Shib SPs

- ANGEL – course management system
- EZProxy – access to library-licensed electronic resources
- Storemedia – media server
- forums.msu.edu – campus-wide discussion forums
- photos.msu.edu – UR's stock photo store
- Departmental:
  - ATS's Confluence wiki
  - Biochemistry
  - Chemistry
  - HPCC's wiki
  - Supported as an authentication method in our web hosting service

# Partner projects

- Penn State – ANGEL course
- Microsoft DreamSpark – student software downloads
- CIC's CICme Sharepoint site
  
- In the works:
  - Tower travel -- travel portal
  - Aliquant – benefits portal – SAML 1.1
  
- Proposed:
  - StudentsOnly/StudentUniverse.com – student travel portal

# Issues

- Adoption
  - Application integration required
  - Limited (but growing?) support for Shibboleth or SAML among external entities
  - Trust relationship required
- Policy infrastructure – internal and external
- Identity verification and levels of assurance
- Questions about SSO and authentication in general
- Centralized vs. distributed IdM, access control

# Plans

- Implement Shibboleth for more applications
- Begin to leverage federation capability by establishing partnerships
- Identity verification and InCommon Silver LOA
  - Considering how to implement support for additional factors to allow stronger authentication for higher security applications
- Provisioning modernization/middleware
- Build out the Shibboleth attribute server

# Resources

- Shibboleth
  - <http://shibboleth.internet2.edu>
- InCommon
  - <http://incommon.org>
- MSU's Participant Operating Practices
  - <http://www.msu.edu/~identity/incommonpop.pdf>
- Internet2/MACE
  - <http://middleware.internet2.edu/MACE/>
- NMI-EDIT
  - <http://www.nmi-edit.org/>
- SWITCH Federation AAI info:
  - <http://www.switch.ch/aai/about/>

# Resources, cont'd

- Educause net@edu Identity Management Working Group
  - <http://www.educause.edu/IDMworkinggroup>
- Educause/Internet2 CAMP Workshops
  - <http://net.educause.edu/camp>
- NIST SP 800-63
  - [http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63V1\\_0\\_2.pdf](http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63V1_0_2.pdf)
- InCommon Identity Assurance Framework
  - [http://www.incommonfederation.org/docs/assurance/InC\\_IAAF\\_1.0\\_Final.pdf](http://www.incommonfederation.org/docs/assurance/InC_IAAF_1.0_Final.pdf)

# Contact Info

- Jim Green
  - Manager, Identity Management
  - Email: [jfgreen@msu.edu](mailto:jfgreen@msu.edu)
  - Phone: (517) 432-7239