Bronze and Silver Identity Assurance Profiles for Technical Implementers

Tom Barton
Senior Director for Integration
University of Chicago

Jim Green
Manager, Identity Management
Michigan State University

Academic Technology Services

Michigan State University

Toward InCommon Silver Certification at MSU

Jim Green
Manager, Identity Management
MSU – Academic Technology Services
jfgreen@msu.edu

Academic Technology Services

Michigan State University

Why?

- Use cases – research, government, sensitive data
- Shibboleth proliferation
- CIC sharing
- Opportunity to influence the process
- Worth doing
- Can be a driver

What we've done so far

- Study IAP and related documents
- Establish a weekly meeting with IdM, ATS, and Internal Audit
- Participate in CIC InC Silver conference calls
- Presented project proposal to ATS management
- Use a spreadsheet (based on InCommon checklist) to tally gap analysis bullets
- Summarized issues for Phase 1 report by answering Tom Barton's questions

Academic Technology Services

MICHIGAN STATE UNIVERSITY

IAP areas

- Policy
  - Privacy policy
  - Policy on disabling netids
- Business processes
  - Netid provisioning process
- Technical infrastructure
  - Network security

Issue categories

- Documentation lacking
  - Policy, process, or infrastructure probably OK
- Policy lacking or doesn’t comply
- Process lacking or doesn’t comply
- Technical infrastructure lacking or doesn’t comply

Documents lacking

- 4.2.1.5 appropriate staffing
- 4.2.2.3 identity proofing
- 4.2.4.3 credential issuance process
- Many, many examples of processes that are not well documented

Policy lacking or doesn’t comply

- 4.2.1.3 – privacy policy
- 4.2.4 – credential issuance and management --policy on disabling netids, end of lifecycle management of netids
- 4.2.5.7 – mitigate risk of sharing credentials

Process lacking or doesn’t comply

- 4.2.1.8 – IT audit
- 4.2.3.4 – strong resistance to guessing shared secret – our password complexity rules likely do not rise to Silver level
- 4.2.1.9 – Risk management methodology
  - Background checks not retroactive
  - Strong digital credentials (?)

Technical infrastructure lacking or doesn’t comply

- 4.2.5.2 – end-to-end secure communication
- 4.2.4.5.2 – 10 or more successive failed authentication attempts in 10 minutes
- 4.2.8.3 – physical security – log entrance and exit

Approaches

- New ID Office will manage physical ID cards and digital credentials – reports to central IT
- Considering two factor authentication
- Affiliates system in development
  - System of record for non-HR, non-SIS
  - Owned by Enterprise Information Stewardship
  - Operated by Identity Management

Academic
Technology
Services

Michigan State
University