Monday April 26, 2010
Tom Dopirak, Paul Hill, Chad La Joie, Harold Teunissen

MACE-PACCCMAN WORKING GROUP
Agenda

• Why are we here? History repeats itself.
• Review Progress against Charter
• Surfnet Authorization Strategy - Harold Teunissen
• Virtual Organizations – Chad La Choie
• MIT’s perMIT update – Paul B Hill
WHERE WE STARTED

Username & password managed inside application; each application has separate access management.

<table>
<thead>
<tr>
<th>Application A</th>
<th>Application B</th>
</tr>
</thead>
<tbody>
<tr>
<td>Username &amp; Password A</td>
<td>Access Mgmt.</td>
</tr>
<tr>
<td>Username &amp; Password B</td>
<td>Access Mgmt.</td>
</tr>
</tbody>
</table>
WHERE WE ARE

Phase 2
Username & password managed outside application (single sign-on), but access management performed within application.

Username & Password C

Application A
Access Mgmt.

Application B
Access Mgmt.
FEDERATED IDENTITY

Phase 3
Access management still resides within application, but can handle authentication from different domains.

Institution 1 Username & Password
Institution 2 Username & Password

Application A
Access Mgmt.

Application B
Access Mgmt.
Federated Authentication and Authorization

Diagram:
- Federated authentication and authorization
- Federated Username & Password
- Federated Access Mgmt.
- Univ. #1 Application
- Univ. #2 Application
- Univ. #3 Application
- Univ. #4 Application
Not So dreamy, but Still Good

Privilege, Role, Group
Metastore

Authorization Service
Directory of Attributes
Application-based authorization
Working Group Outcomes

• Frameworks and Roadmaps for executives and architects
• Documentation of common requirements, concepts, and terminology.
• Documentation of capabilities and features of leading-edge products and implementations.
• Documentation of "lessons learned" from access management software projects
• Proposals for new software development, new architectures, and new standards.
• Smaller contributions such as recipes, techniques, tips, position papers, demos, proofs-of-concept, etc of practical value to the community.
Things we have

• A nice glossary

• A library of use cases

• Some idea how to implement the use cases using
  • MIT perMIT
  • Grouper
  • Kuali KIM Authorization Service

• Some engagement with important applications in Higher Education and research
Where are we going next?

1. Publish reference-able use cases
2. Examine the problems of federated access management
3. Access Management for Mortals published
4. Clarity of attributes vs groups vs privileges
5. Standard APIs for asking authorization questions?
6. Anything commercial worth examining?
So now what
For more information
visit http://middleware.internet2.edu/paccman/
Working Group Charter

**Internet2 Intellectual Property Framework**
- Friday 11AM EST call, http://middleware.internet2.edu/paccman
- Indefinite timeframe, yearly assessments

**Operational**
- Part of the MACE/Internet2 Middleware Program
- Coordination with Grouper
- Knowledge of commercial offerings and open source efforts
- All of Higher Ed is the beneficiary
- Business, policy and technology issues are in scope

**Principles**
- Frameworks and Roadmaps for executives and architects
- Documentation of common requirements
- Proposals for software development and new standards
- Recipes, techniques, position papers
- Conferences, workshops and frameworks
- Lessons learned from Signet
- Broadly understood use cases

**Outcomes**
- Higher education
- Grid Authentication and Authorization with Reliably Distributed Services (GAARDS)
- SurfNet
- research
- iplant collaborative
- ligo scientific collaboration
- JA-SIG
- Kuali
- Sakai
- OCLC

**Concepts**
- Authorization
- Federated Authorization
- roles
- privileges
- permissions
- groups
- policy
- XACML
FEDERATED AV ENHANCEMENT

http://tinyurl.com/3xe73v6