Joining the Club: e-Authentication and Authorization in an NHIN World

Presentation to HIMSS
Thursday, February 28, 2008
9:45 AM - 10:45 AM
Co-presenters:
Richard Moore
President, eHealth Ohio
and
John Fraser
CEO, MEDNET USA

Talk Outline
1. Identity Management – the problem
2. HIMSS/GSA: Phase One
3. GSA/Internet2/Liberty: Phase Two
4. Role Based Access and Controls
5. Role scenarios
6. Formation of the HIMC Group
7. International Expansion / Liberty Alliance

Identity Management – the problem
• How many passwords do you keep now?
  – Is more better ??!
• Health care professionals work in multiple places, access multiple systems
• They need simplified sign-ons by using a shareable identity – but HOW?
Shareable Identities

- One doctor = one identity
- Identity stored on-line in Identity Providers (IDP)
- IDP provides identity information when asked
- IDP authenticates users when asked
- So – Providers need only one identity for multiple applications

How do we get there??

HIMSS/GSA eAuthentication Project:
Phase One - 2006
HIMSS/GSA eAuthentication Project

- **Who:** HIMSS and The General Services Administration (GSA)
- **When:** 2006, early 2007
- **Purpose:** Demonstrate federally approved authentication services
- **Pilot Participants:** Seven Regional Health Information Organizations (RHIOs)/health information exchanges (IHEs) and ORC, Inc. Federal Certificate Authority.

Phase One - Participants

1. ORC, Inc. ACES Certificate Authority
3. Michigan: Michigan Data Sharing & Transaction Infrastructure Project
4. Texas: CHRISTUS Health, Health eCities of Texas Project
5. Minnesota: Community Health Information Collaborative
6. Ohio: eHealth Ohio/OSC Bioinformatics
7. Ohio: Virtual Medical Network
8. Nevada: Single Portal Medical Record Project
Phase One - Results

- Multiple RHIOs can agree and implement a common framework for the policies, procedures, and standards for federated identity authentication across multiple use cases.
- The Federal e-Authentication infrastructure is relevant and applicable to use cases for RHIOs in diverse operational environments.
- PKI, as a standard for strong authentication, can be deployed uniformly across multiple RHIOs.
- The Federal PKI and its trusted Federal Credential Service Providers can be leveraged for use in multiple use cases across multiple RHIOs.
- For RHIOs, local registration authorities and local enrollment are viable for larger scale deployments to provide for strong authentication using Federal e-Authentication components.
- Hardware tokens (i.e., smart cards, flash drives) are viable for RHIO deployment of level 4 authentication assurance.

Phase Two – 2007/2008

2. Minnesota: MEDNET, USA
3. Minnesota: Community Health Information Collaborative (CHIC)
4. Ohio: eHealth Ohio
5. Ohio: Virtual Medical Network

Participants in Phase 2
Phase Two - Guiding Principles

- Use National and International standards for HIT and RHIO/NHIN solutions.
- Provide a Federated Single Sign-on solution with Third-party Certification.
  - Wherever possible utilize Open Source tools (e.g. Shibboleth)
  - Maintain platform independence.
- Provide connectivity to all, even proprietary RHIO solutions.
- Publish/Present discovery of solutions to inform healthcare stakeholders.

Phase Two - Extended Testbed

Shibboleth “Club”

- Shibboleth software has the concept of a “Club”
- A “Club” is a group of companies that support single sign on between themselves.
- Club is common security and operational policies
- Simplifies trust between members
- Clarifies SAML assertion management
- Directory information can then be exchanged and trusted between companies regarding identities.
Directories

- Large networks require directories
- Directories contain users, machines and their attributes.
- Lightweight Directory Access Protocol (LDAP) used in conjunction with X.500 directory standards
- Internationally supported

Defining Role Based Access and Control (RBAC) using Directories

- Well established and accepted standards exist for group policy administration for network access of resources at the local and wide area network level.
- Middleware RBAC is working to bridge and integrate group policy to establish regional, national and international user administration.

RBAC Directory Contents

- Standardized attributes: Object Identifiers (OIDs)
- OIDs registered with the Internet Assigned Number Authority (IANA).
- LDAP attributes define roles and access controls using RBAC.
Academic RBAC Model

- Universities began implementing roles for users in the academic setting in 2000.
- Specific models for accessing library collections by authorized personnel.
- Middleware is configured to authenticate and authorize a user into a federated multi-university, multi-library system. Only authorized personnel can reserve specific collections.

Academic RBAC Model

- Internet2, the Middleware Architecture Committee for Education (MACE) and the eduPerson task force have defined an LDAP object class that includes widely-used person attributes in higher education.
- These attributes are then utilized to control access to resources on the institution’s network and other interconnected networks.

Example Academic Directory OIDs

<table>
<thead>
<tr>
<th>Attribute</th>
<th>OID</th>
</tr>
</thead>
<tbody>
<tr>
<td>eduPerson</td>
<td>1.3.6.1.4.1.5923.1.1.1.2</td>
</tr>
<tr>
<td>eduPersonAffiliation</td>
<td>1.3.6.1.4.1.5923.1.1.1.1</td>
</tr>
<tr>
<td>eduPersonNickname</td>
<td>1.3.6.1.4.1.5923.1.1.1.2</td>
</tr>
<tr>
<td>eduPersonOrgDN</td>
<td>1.3.6.1.4.1.5923.1.1.1.3</td>
</tr>
<tr>
<td>eduPersonOrgUnitDN</td>
<td>1.3.6.1.4.1.5923.1.1.1.4</td>
</tr>
<tr>
<td>eduPersonPrimaryAffiliation</td>
<td>1.3.6.1.4.1.5923.1.1.1.5</td>
</tr>
<tr>
<td>eduPersonPrincipalName</td>
<td>1.3.6.1.4.1.5923.1.1.1.6</td>
</tr>
</tbody>
</table>

The Middleware Architecture Committee for Education and the EDUCAUSE/Internet2 eduPerson task force have the mission of defining an LDAP object class that includes widely-used person attributes in higher education. There currently are 10 OIDs defined. Not shown are eduPersonAffiliation, eduPersonPrimaryOrgUnitDN, eduPersonScopedAffiliation and eduPersonTargetedID.
Healthcare Directory Research

• Instead of using the Academic eduPerson attributes, investigating ISO standards, specifically: ISO/TS 21091:2005(E)
  – Directory services for security, communications and identification of professionals and patients
  – Supports these types of directory entries:
    – regulated health care professionals
    – non-regulated health care professionals
    – employees of health care organizations and supporting organizations
    – health care consumers

ISO/TS 21091 Directory Design

O=Mayo Clinic
L=MN
C=US

OU=Issuing Authority
  (i.e. Pharmacists, MDs, Dentists)
  CN=Practitioners

CN=Organizational Role

CN=Devices

CN=Practitioners

CN=Patients

Selected ISO Directory OIDs

<table>
<thead>
<tr>
<th>OID</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0.21091.2.1.1</td>
<td>HcConsumerID (e.g. security number, health insurance number, medical record number, and driving license number)</td>
</tr>
<tr>
<td>1.0.21091.2.0.2</td>
<td>HcIdentificationService</td>
</tr>
<tr>
<td>1.0.21091.2.1.2</td>
<td>HcMPILocation (location of Master Patient Index system)</td>
</tr>
<tr>
<td>1.0.21091.2.1.2</td>
<td>HL7PatientDeathDateAndTime (everybody's final entry :)</td>
</tr>
<tr>
<td>1.0.21091.2.0.5</td>
<td>HcRole</td>
</tr>
</tbody>
</table>
(more) Selected ISO Directory OIDs

<table>
<thead>
<tr>
<th>Role</th>
<th>OID</th>
</tr>
</thead>
<tbody>
<tr>
<td>HcProfessional</td>
<td>1.0.21091.1.2</td>
</tr>
<tr>
<td>HcEmployee</td>
<td>1.0.21091.1.3</td>
</tr>
<tr>
<td>HcPayer</td>
<td>1.0.21091.1.5</td>
</tr>
<tr>
<td>HcStandardRole</td>
<td>1.0.21091.1.8</td>
</tr>
<tr>
<td>HcLocalRole</td>
<td>1.0.21091.1.9</td>
</tr>
<tr>
<td>HcDevice</td>
<td>1.0.21091.1.11</td>
</tr>
</tbody>
</table>

Middleware RBAC

- Define the roles broadly using existing standards, but model a few most common exchanges of health information.
- Start now with small workable model to test the authentication and authorization solutions.
- Convene a large advisory group for discussing and refining the big picture using the results of the phase 2 modeling.
- Present results to the Healthcare community.
- Avoid Analysis-Paralysis. Just do it.

Phase Two: Roles Development

- Start Roles list with Provider Taxonomy defined under HIPAA using ASTM and NUCC specifications for providers and expand to include all healthcare stakeholders including consumers, employers, payers, etc.
- Use the VA RBAC Taskforce functional definitions that apply to the restricted scenarios.
- Define the LDAP objects for the test cases and step through the model scenarios.
Phase Two: Role Scenarios

- All scenarios are defined unambiguous “need to know” accesses of health information to avoid consent issues.
- Provider A is a Primary Care Physician sending a patient to Provider B, a specialist, for a consultation. Provider B receives the consultation request and is linked electronically to a view of the related medical history. Provider B finishes examination and leaves/messages consultation results back to Provider A.
- Emergency Physician sees patient of Provider A and is granted emergency access to a view of the patient’s medical history.

Phase Two: Shibboleth Testbed

- Shibboleth IdP
- Shibboleth SP
- WAYF

MEDNET USA

VMN

Phase Two: Users & Roles

<table>
<thead>
<tr>
<th>User</th>
<th>Role from IdP</th>
<th>@MEDNET</th>
<th>@CHIC</th>
<th>@VMN</th>
</tr>
</thead>
<tbody>
<tr>
<td>Brett D Jones</td>
<td>Physician A</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Richard Moore</td>
<td>Physician B</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>John Doe</td>
<td>First Responder</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Health Identity Management Consortium

- Collaborative effort by multiple organizations
- Goal to improve community health and safety
- Objective: secure exchange of clinical info between federated (shareable) identities
- Objective: develop standardized, federated security model and directory standards

- Define the roles, level of access, security, and data elements required in a federated identity management system (FIMS).
- Implement the FIMS using national standards and wherever possible open source software to allow identity management and authentication system for access to diverse sources of health information.
- Develop a security and policy framework to support community-wide participation of the health stakeholders within HIPAA guidelines. This includes development of the security architecture, FIPS-201 standards and the federal public key infrastructure (PKI) with certification authorities (CAs).
- Test the utility of the patient identity management system that includes a “look-up” process and an ATM-type card based identity system for patients across health information systems.
- Test the scalability of this model to support a national identity management service by supporting multiple independent identity providers to have access to summary patient medical information from diverse EMRs for emergency care.
- Measure quality indicators for improved safety and quality of care in emergency departments based on the use of this technology.

Health Identity Management Consortium

<table>
<thead>
<tr>
<th>Member</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wells Fargo</td>
<td>Connecticut e-Health</td>
</tr>
<tr>
<td>MEDNET USA</td>
<td>Virtual Medical Network (VMN)</td>
</tr>
<tr>
<td>RSA</td>
<td>BBN Corporation</td>
</tr>
<tr>
<td>HIMSS</td>
<td>Univ. of Texas Medical Center</td>
</tr>
<tr>
<td>Liberty Alliance</td>
<td>Colorado HIE</td>
</tr>
<tr>
<td>Internet 2</td>
<td>Vangent Inc.</td>
</tr>
<tr>
<td>CHIC</td>
<td>AAFP</td>
</tr>
<tr>
<td>eHealth Ohio</td>
<td>SALT</td>
</tr>
<tr>
<td>University of Minnesota</td>
<td>ePCRN Research Project – U of MIN</td>
</tr>
<tr>
<td>HealthNet</td>
<td></td>
</tr>
</tbody>
</table>
Phase 2 Results

• Federated single sign-on works
• Demonstrated multiple systems using third-party authentication and Middleware access control.
• Initial list of roles were defined using the HIPAA Taxonomy and other established sources.
• LDAP directory objects prototyped for RBAC solution.
• Authentication and Authorization Models for provider referral/consultation and emergency access were tested using the Middleware solution.

Global Expansion / Liberty Alliance

• As of December, 2007, HIMC group discussing a Liberty Alliance membership transition.
• Liberty is global, multi-industry group
  – Focus on federated identity management
• Goal is globally recognized healthcare federated identity management system
• Please join!

Thank You!

• Rick Moore
  – eHealth Ohio
  – +1 877.813.9750
  – rkmoore@ehealthohio.org
• John Fraser
  – MEDNET USA
  – +1 612.435.7602
  – john.fraser@mednet.org