Lori Reed-Fourquet, MS
Consultant, e-HealthSign
Co-Chair E31.20 Health Information Security and Privacy
ASTM E31 Health Informatics Executive Committee
HL-7 EHR Technical Committee Expert Panel on Security & Privacy Functions
Vice-Convener ISO TC215 Health Informatics WG4 Security
ISO TC215 Health Informatics Executive Council
Member IHE IT Infrastructure Technical and Planning Committees
HIMSS Standards Task Force

IHE Cross-enterprise User Authentication Profile,
and e-authentication in the Federated Environment
Liberty Alliance e-Health Workshop
Wednesday April 26, 2006
Goals of IHE

• Increase the rate and quality of integration in healthcare environments.
• Foster communication among vendors.
• Prove that integration is attainable through the use of standards.
• Improve the efficiency and effectiveness of clinical practice.
What is IHE?

A joint initiative to improve systems integration

• Clinicians define system integration needs
• Vendors use a well-defined process to develop standards-based solution profiles – the IHE Technical Framework.
• HIMSS/RSNA/ACC supervise documentation, testing, demonstration, and promotion.
Connecting standards to care

• Care providers work with vendors to coordinate the implementation of standards to meet their needs
  – Care providers identify the key interoperability problems they face
  – Drive industry to develop and make available standards-based solutions
  – Implementers follow common guidelines in purchasing and integrating systems that deliver these solutions

What is the effective way to establish those “standards” for how to implement standards?
IHE 2006 – Nine Active Domains

Over 100 vendors involved world-wide, 5 Technical Frameworks
37 Integration Profiles, Testing at Connectathons
Demonstrations at major conferences world-wide
What IHE is NOT!

A standards development organization

- Uses established standards (HL7, DICOM, others) to address specific clinical needs
- Activity complementary to SDOs

Simply a demonstration project

- Demos are only one means to the end: Adoption
- Backed up by documentation, tools, testing, and publication of information
What is IHE NOT?

- Not a standard, *although it leverages them*
- A vendor initiative, *although they participate*
- Not a certifying authority, *although IHE provides testing that should be leveraged by certification*
- Not simply a demonstration project
  - Demos are only one means to the end: *Adoption*
  - Backed up by documentation, tools, testing, and publication of Technical Frameworks and Product Integration Statements.
IHE IT Infrastructure – Plan for 2005-2006

- **IT Infrastructure Development Plan:**
  - 2006/2007 Planning Meeting: November 2005
  - IHE Planning Committee decision: January
  - Issue Public Comment version: June 2005
  - Public Comment Due: July 2005
  - Issue Trial Implementation version: August 2006
  - IHE Connectathon: January 2007
  - HIMSS Demo: February 2007
IT Infrastructure Security Profiles

2004
  Consistent Time (CT)
  Enterprise User Authentication (EUA)

2005
  Audit Trail and Note Authentication (ATNA)
  Personnel White Pages

2006
  Cross-Enterprise User Authentication (XUA)
  Document Digital Signature (DSG)

2007
  Risk Management
  Cross-Enterprise User Authentication (XUA)
  Patient Consent
Introduced at HIMSS in 2005: IHE-XDS

**Community or sub-network**

- Hospital Record
- Clinic Record
- Specialist Record
- Repository of Documents

- Reference to records
- 3-Records Returned
- 4-Patient data presented to Physician

**Sharing System**

- Clinic
- Aggregate Patient Info
- Index of patients records (Document-level)
- 2-Reference to Records for Inquiry
Cross-Enterprise Document Sharing (XDS)

Standards Used

Two “categories” of standards used

XDS Doc Content
- Medical Summaries (HL7 CDA/CRS+V3)
- Imaging (DICOM)
- ECG Reports (PDF+)
- Next lab, nursing, etc.

XDS Infrastructure
(Document sources, consumers, registries, repositories)
Consistent Time (CT)

- Network Time Protocol (NTP) version 3 (RFC 1305)
- Actor must support manual configuration:
  - Manual IP address or hostname for time server
  - Preferably 3 or more servers should be supported
  - Automatic discovery and broadcast will not be tested
- Required accuracy: 1 second
- Optional Secure NTP may be tested
- Required for use of ATNA, EUA, XUA. All time tags must be time synchronized.
- See [http://www.ntp.org](http://www.ntp.org) for extensive technical details on the protocol, and your vendor documentation for installation and configuration.
ATNA
Audit Trail and Note Authentication

• IHE makes cross-node security management easy:
  – Only a simple manual certificate installation is needed, although more sophisticated systems (LDAP, PKI) can be used.
  – Implementations should separate the authentication, authorization, and accountability functions to accommodate the needs of different locations.
  – Enforcement is driven by ‘a posteriori audits’ and real-time visibility, not detailed access controls.
XDS Scenario + use of ATNA & CT

XDS Affinity Domain (NHIN sub-network)
XDS Scenario + use of PIX & PDQ

- PDQ Query to Acquire Affinity Domain
- Patient Identity Feed
  - Physician Office
  - Community Clinic
  - Lab Info. System
  - PACS
  - XDS Document Repository
  - ATNA Audit record repository
  - CT Time server
  - Teaching Hospital

- Patient Identity XRef Mgr
- Affinity Domain Patient Identity Source
- Patient Identity Feed
- Document Registry
  - PIX Query
  - PIX Query to Acquire Affinity Domain Patient ID
  - M8354673993
  - A87631
  - L-716
- M8354673993
- M8354673993
- L-716
- A87631
- M8354673993
- XDS Document Repository

- ED Application
- PACS
- EHR System
- Provide & Register Docs

XDS Affinity Domain (NHIN sub-network)
Federation of XDS and non-XDS Domains
Leverage Connecting for Health RLS – 2006-2007 Development

Cancer Treatment

Cross-state IDN
Registry Locator service

NHIN Backbone

State RHIO

State RHIO

Registry Locator service

Which registry holds records for a patient?

Sub-Network

Sub-Network

Sub-Network

Sub-Network

Integrated Delivery Network
IHE Integration Profiles for Health Info Nets
What is available and has been added in 2005 and is for 2006

- **Patient Demographics Query**

- **Patient Identifier Cross-referencing** Map patient identifiers across independent identification domains

- **Consistent Time** Coordinate time across networked systems

- **Audit Trail & Node Authentication** Centralized privacy audit trail and node to node authentication to create a secured domain.

- **Document Digital Signature** Attesting "true-copy and origin"

- **Audit Trail & Node Authentication**

- **Cross-enterprise User Authentication**

- **Cross-enterprise User Authentication & Auditing:**
  Enhanced Access Control

- **Consistent Time**

- **Cross-Enterprise Document Sharing** Registration, distribution and access across health enterprises of clinical documents forming a patient electronic health record

- **Cross-enterprise Document Interchange** Media-CD/USB & e-mail push

- **Imaging Information**

- **Medical Summary** (Meds, Allergies, Pbs) Format of the Document Content and associated coded vocabulary

- **Cross-enterprise User Authentication**

- **Patient Created Summaries**

- **ECG Report Document**

- **Lab Results Document**

- **Scanned Documents**

- **Emergency Referrals**

- **Notification of Document Availability** Notification of a remote provider/health enterprise

- **Notification of Document Availability**

- **Notification of Document Availability**

- **Notification of Document Availability**
Use Case Definition

HITSP Technical Committees:
Biosurveillance
Consumer Empowerment
Electronic Health Records
Description

• EHR - Goals
  – Improve quality by informing clinician of comprehensive patient data at the point of care
    • Informed Decision
    • Shorter Timeframe
  – Lower Cost
    • Streamline data collection
    • Decrease likelihood and cost of medical errors
    • Reduce resources for duplicative/unnecessary testing

• Consumer Empowerment Goals
  • Involvement of consumers in managing their health care
  • Registration/family history capture
  • Current medications and allergies

• Biosurveillance Goals
  • Ability to detect events rapidly
  • Manage the events
  • Appropriately mobilize resources in response
  • Save lives
HITSP Building Blocks

• **IP1 Authenticate User Across Enterprises**
  – Assures the claimed identity of a user across enterprises, i.e., verify the user is who he says he is.
  – Standards and best practices are emerging:
    • OASIS/WSS
    • SAML
    • Liberty-Alliance
    • IHE XUA
    • ISO (non-health informatics-focused standards)
    • ISO IS17090 Healthcare Informatics: PKI
    • ITU (X9, X.509, X.500, etc)
    • FIPS (140-2)
HITSP Building Blocks

- **IP1 Authenticate User Across Enterprises**
  - Assures the claimed identity of a user across enterprises, i.e., verify the user is who he says he is.
  - Standards and best practices are emerging:
    - OASIS/WSS
    - SAML
    - Liberty-Alliance
    - IHE XUA
    - ISO (non-health informatics-focused standards)
    - ISO IS17090 Healthcare Informatics: PKI
    - ITU (X9, X.509, X.500, etc)
    - FIPS (140-2)
The following Building Blocks have been identified by HISTP

<table>
<thead>
<tr>
<th>ID#</th>
<th>Title</th>
<th>#</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Authenticate User across Enterprises</td>
<td>21</td>
<td>Manage Patient Communications across Enterprises</td>
</tr>
<tr>
<td>2</td>
<td>Collect and Communicate Audit Trail</td>
<td>22</td>
<td>Maintain Consistent Time across Enterprises</td>
</tr>
<tr>
<td>3</td>
<td>Provide Secure Data Messaging</td>
<td>23</td>
<td>Notify Document Availability across Enterprises</td>
</tr>
<tr>
<td>4</td>
<td>Digitally Sign Documents</td>
<td>24</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>Share Medical Summaries across Enterprises</td>
<td>25</td>
<td>Provide Node Authentication and Secured Communication</td>
</tr>
<tr>
<td>6</td>
<td>Share Diagnostic Images across Enterprises</td>
<td>26</td>
<td>Manage User Credentials</td>
</tr>
<tr>
<td>7</td>
<td>Share Lab Reports across Enterprises</td>
<td>27</td>
<td>Communicate Scheduling and Appointment Information across Enterprises</td>
</tr>
<tr>
<td>8</td>
<td>Identify a Patient across Enterprises</td>
<td>28</td>
<td>Communicate Batch Data</td>
</tr>
<tr>
<td>9</td>
<td>Share Patient Demographics across Enterprises</td>
<td>29</td>
<td>Communicate Eligibility Benefit and Coverage Information</td>
</tr>
<tr>
<td>10</td>
<td>Manage and Control Data Access</td>
<td>30</td>
<td>Communicate Treatment Authorization Information</td>
</tr>
<tr>
<td>11</td>
<td>Share Clinical Decision Support Info across Enterprises</td>
<td>31</td>
<td>Communicate Referral Information</td>
</tr>
<tr>
<td>12</td>
<td>Share Order Info across Enterprises</td>
<td>32</td>
<td>Communicate Claim, Encounter, or EOB Information</td>
</tr>
<tr>
<td>13</td>
<td>Communicate Real-time data</td>
<td>33</td>
<td>Communicate Claim Status Information</td>
</tr>
<tr>
<td>14</td>
<td>Verify Patient Consent, Authorizations and Advance Directives</td>
<td>34</td>
<td>Communicate Claim Payment or Payment Advice Information</td>
</tr>
<tr>
<td>15</td>
<td>Share Patient Medication History across Enterprises</td>
<td>35</td>
<td>Communicate Healthcare Attachment Information</td>
</tr>
<tr>
<td>16</td>
<td>Access Terminology Service</td>
<td></td>
<td></td>
</tr>
<tr>
<td>17</td>
<td>Anonymize and Pseudonymize Data</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Cross-Enterprise User Authentication

Value Proposition

• Extend User Identity to Affinity Domain
  – Supports any cross-enterprise transaction
  – Federated or Centralized
• Provide information necessary so that XDS actors can make Access Control decisions
  – Does not include Access Control mechanism
• Provide information necessary so that XDS actors can produce detailed and accurate Security Audit Trail
Cross-Enterprise User Authentication

Standards Used

• Employs SAML 2.0 Profiles
• Specifies use of SAML Browser SSO Profile and Enhanced Client/Proxy Profile
• Specifies SAML Profile to use with XDS (ebXML Registry)
  – Consistent with ebXML 3.0 use of SAML
• Extends SAML 2.0 Profiles into HL7
  – future DICOM
Problems

- SAML v2 is very new
- Toolkits are not yet readily available
- Short timeframe till Jan connectathon & HIMSS
- Very new technology to healthcare
- Other gaps in standards (e.g. WS-*)
- ASTM/ISO still working on PMI
- HL7, DICOM are very early works that need OASIS review
IHE IT Infrastructure Roadmap for Security

• Stage 0 - 2003 profile development for 2004 Connect-a-thon

• Profiles
  – Enterprise User Authentication (EUA)
  – IHE ITI Consistent Time profile (CT)

• Standards & Prerequisites
  – CCOW v 1.4 User Context
  – Kerberos - IETF RFC 1510
  – Network Time Protocol – IETF RFC 1305
  – Simple Network Time Protocol - IETF RFC 2030
IHE IT Infrastructure Roadmap for Security

Stage 1 – 2004 profile development for 2005 Connect-a-thon

• Profiles
  – Audit Trail Node Authentication (ATNA)
  – Personnel White Pages (PWP)

• Standards & Prerequisites
  – IHE Radiology Basic Security
  – Stage 0 IHE ITI security profiles
  – RFC 3881 (Audit record schema)
  – LDAP (RFC 2251-2256)
  – RFC 2798 (inetOrgPerson schema)
IHE IT Infrastructure Roadmap for Security

Stage 2 - 2005 profile development for 2006 Connect-a-thon

• Profiles
  – Cross-Enterprise User Authentication and Accountability
    • PKI (identity management only)
    • Multi-enterprise-scope
    • UsersPatients?
  – Digital Signature

• Standards & Prerequisites
  – Stage 1 IHE ITI security profiles
  – Liberty Alliance Identity Management Framework
  – SAML
  – ISO/TS 17090
  – Public Key Infrastructure (PKI) for user identify management
IHE IT Infrastructure Roadmap for Security

Stage 3 - 2006 profile development for 2007 Connect-a-thon

• Profiles
  – Preliminary Security White Paper
  – Role Based Access Control (RBAC) –
    • Consideration for consumption of authorization
  – XUA Experimental Pre-profile
    • "Experimental Federated Identity Coordination"
  – Risk Management White Paper

• IHE PCC domain
  – Patient consents
    • Privacy – Access to medical information
    • Medical procedures (out of scope for 2006)
  – Advance directives (out of scope for 2006)
IHE IT Infrastructure
Roadmap for Security

Stage 4 - 2007 profile development for 2008 Connect-a-thon

• Profiles
  – Role Based Access Control (RBAC)— multi-enterprise scope
  – Wide-area patient access
  – Mobile applications
    • Wireless
    • Patient active homecare
    • Mobile providers

• Standards & Prerequisites
  – Stage 3 IHE ITI security profiles
  – Stable standards for mobile access security
  – Stable standards for patient identification
IHE IT Infrastructure Roadmap for Security

Stage 5+ - 2008+ profile development for 2009+ Connect-a-thon and beyond

• Profiles
  – Remote service access
  – Anonymization
  – Pseudoanonymity
  – Patient-controlled access

• Standards & Prerequisites
  – Stage 4 IHE ITI security profiles
  – Stable healthcare data model standards
  – Stable standards for labeled data access rules
Next Steps

• Participate in May 1 IHE XUA call for Experimental Implementation pre-profile
• 1-877-352-0183, Passcode 622075#, Intl 1-602-462-1021
For more information contact:

Lori Reed-Fourquet,
E-HealthSign
1056 Durham Road
Wallingford, Ct. 06492
phone: (203)294-0479
Cell: (203)435-4348
Fax: (203) 294-9623
e-mail: lori.fourquet@sbcglobal.net