

Health Information Exchange (HIE) Cookbook Leveraging Open Source and CDC Products

August 28, 2007

PHIN Conference 2007 (PHINMS)

Vaughn McMullin - PHINMS Technical
Development Lead
Vanguard Consultant to CDC

Tim Morris – PHINMS Project Sponsor
CDC/NCPHI Director, DISS

The findings and conclusions in this presentation are those of the author and do not necessarily represent the views of the Centers for Disease Control and Prevention/the Agency for Toxic Substances and Disease Registry.



Overview

- Ground Rules
- Network Topology
- Basic Framework for Health Information Exchange Node
- Publishers and Subscribers
- Transport and Service Directory (Resource Management)
- Security Management (Protecting Resources and PKI)
- Federated Identity Management (SAML)
- Support Plan
- Conclusion (The Recipe)
- Questions & Answers

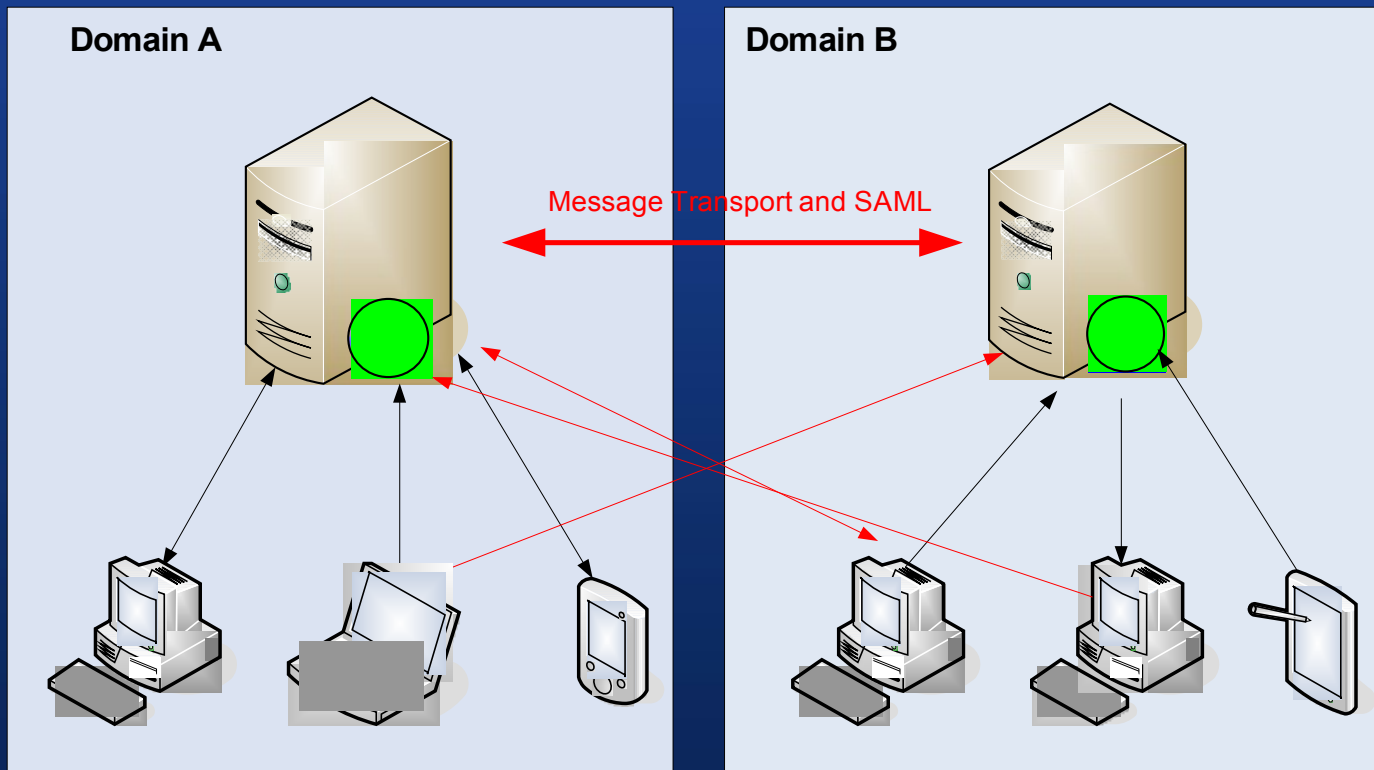


Ground Rules

- Technical approach by illustrating a basic framework
- Open Source Licensing – Deployment friendly and access to source code: Examples (Apache, LGPL, BSD)
- Interoperability and Standards Driven – (OASIS: ebXML, SAML, UDDI) (Sun: JSR, JAX-WS, JAAS)
- Build towards a Service Oriented Architecture (Plug and Play)
- Access to support and professionals
- Integration (Multi-Platform and Web Server Proxy)
- Drive Cost Down

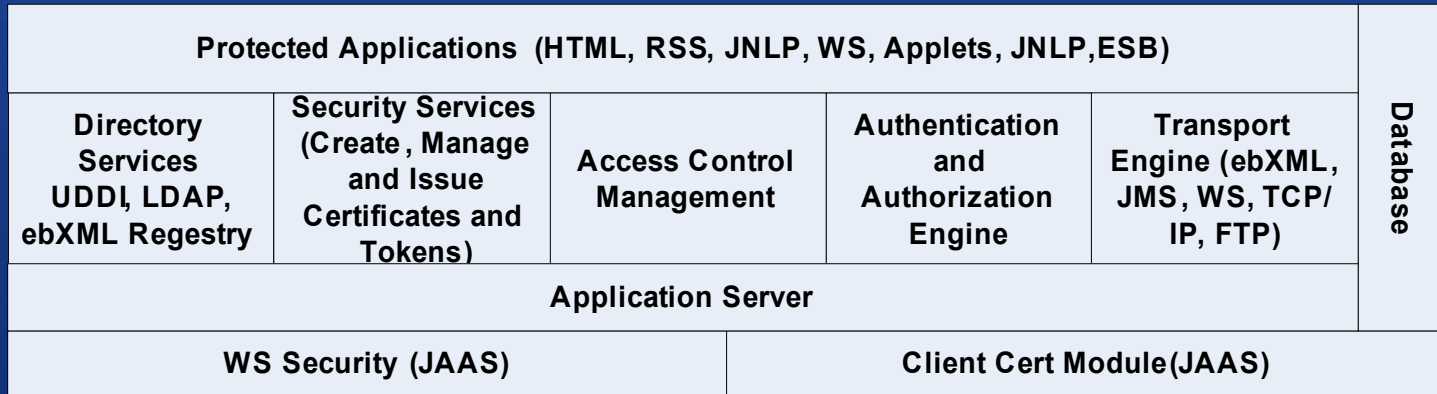


Network Topology – Connecting Devices

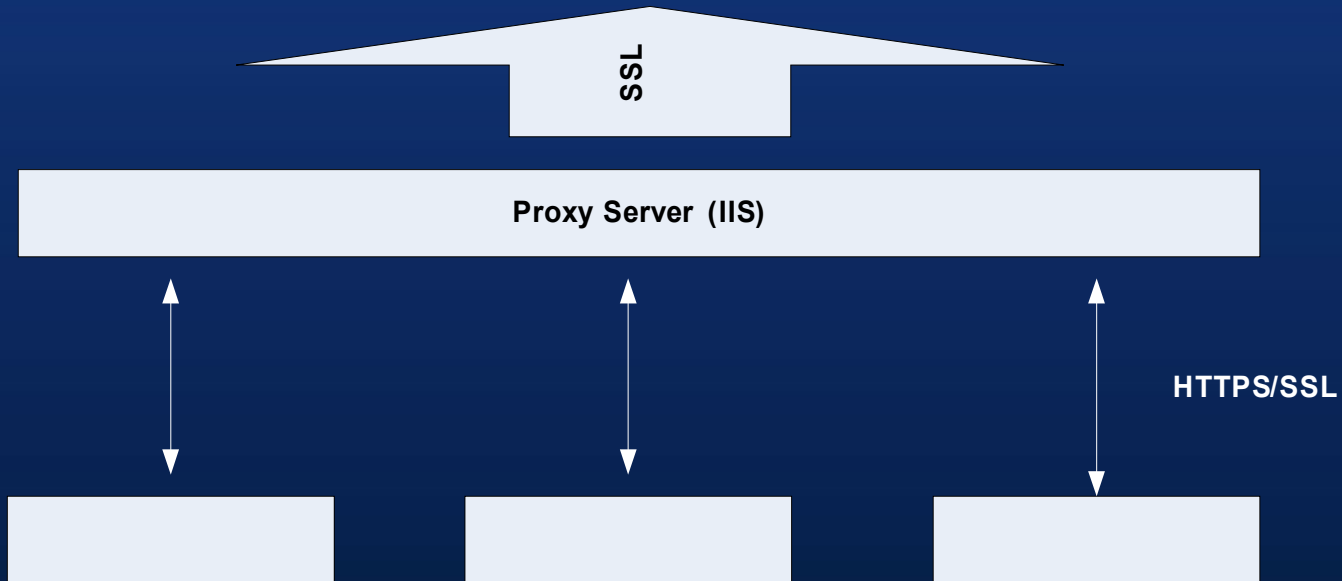


- Network Architectures should support B2B and B2C communications.
- Homogeneous authentication schemes will simplify support.

Basic HIE Framework



Pluggable Authentication Modules (Manages request from proxy server)



Publishers and Subscribers

Publishers and Subscribers

- User and Group Classifications
 - Ability to develop a client
 - Leverage purchased product that interoperate with your protocol
 - Utilize products that are supplied by the your system
- Service Classifications
 - Applications: HTML, Applets, JNLP
 - Protocols: WS, LDAP, ebXML, JMS
- Connecting and trusting devices not users
- Users control several devices
- Identity Management should be granular to specific device: Possible ID Combinations (MAC and Time created UUID, Domain Name and assigned user id)



Security Management (PKI)

- Select a transport mechanism that fits the PKI Architecture
- X509 Certificate Management Components should have the ability to generate, revoke and renew
- Authentication and Authorization (SAML extendable and Policy Driven)
- Access Control
- SAML Tokens for federated security models

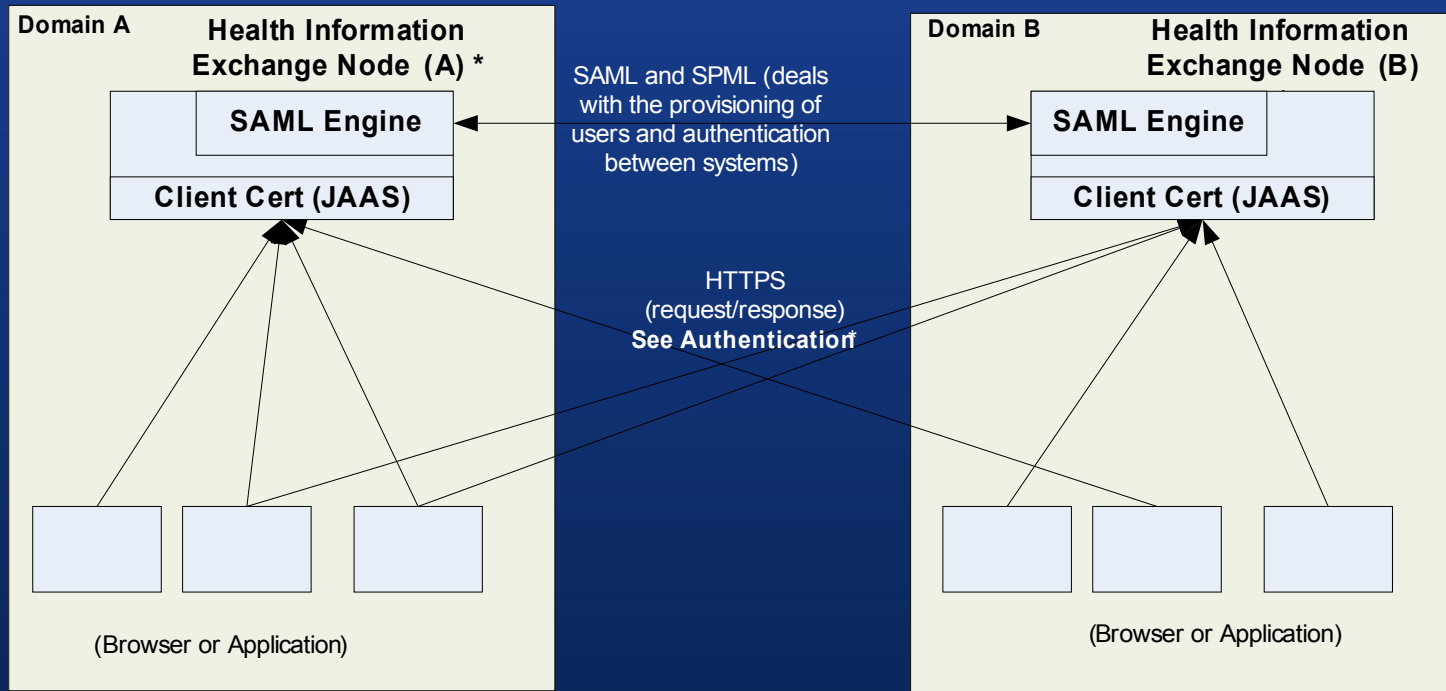


Transport and Service Directory

- Transport Choices
 - ebXML Transport (PHINMS)
 - Web Service Transport (JAX-WS)
 - JMS (Java Messaging Service over HTTPS)
 - FTP (File Transfer Protocol)
- Directory Services Choice
 - UDDI (Universal Description, Discovery and Integration- jUDDI)
 - ebXML Registry (freebXML)
 - LDAP (Lightweight Directory Access Protocol- OpenLDAP)
 - LDAP is a good bases to support security models



Federated Identity Management



Health Information Exchange Node *: Combined Identity provider and WS-Server – this just indicates that this will be considered one entity but does not mean the architecture of this component resides all on one server. There are trust, authentication and authorization considered for this approach. All of the components are standards based and interoperable. Some of the standard protocols to consider are (DSML or Identity provider communication and SASL for authentication components)

Authentication * - Clients will still utilize Client-Cert authentication. The certificates can be obtained from the elected Identity Provider for the network. Once the certificate is received a custom JAAS module can transform the certificate to a SAML assertion to submit to the Identity Provider. This approach allows the usage of legacy products.

Support Plan

- Communicate your work flow to publishers and subscribers.
- Publisher and Subscriber initiation and tracking process definition.
- Service notifications for creation, updates and deletions
- User friendly interfaces for both administrators and users.
- Group coordination via role assignment and well defined process flow
- Trouble ticket response plan
- Training (Web based)



Conclusion (The Recipe)

- Development Language – Sun Java 1.5 or above
- Application Server (JBoss or Geronimo)
- Secure Transport that Supports a PKI (ebXML – PHINMS)
- Directory Services (LDAP-ApacheDS and UDDI -jUDDI)
- X509 certificate generation and management (PKI) – (OpenSSL or EJBCA)
- Access Control -Java Open Single Signon (JAAS Modules available from various sources)
- Federated Authentication (SAML – OpenSAML and JAAS Modules)
- Multidiscipline Personnel: Architect, Developers, Integrators
- Support Plan – There are several cost effective tools available
- Interoperable with purchased products.
- More details available in the White Paper
- Questions and Comments about this approach
 - Vaughn McMullin – vaughn.mcmullin@vanguardcg.com





Questions & Answers

The findings and conclusions in this presentation are those of the author and do not necessarily represent the views of the Centers for Disease Control and Prevention/the Agency for Toxic Substances and Disease Registry.

