



Federated Identity Management and the GRID

***Presented at the:
HIMSS 6th Annual Health Information Technology Institute
The Future of IT, Implementation of Technology
University of Minnesota, Carlson School of Management***

Thursday, May 17, 2007

***Presented by:
John Fraser, CEO
MEDNET USA***

What is a GRID?

From Wikipedia:

Grid Computing is an emerging computing model that treats all resources as a collection of manageable entities with common interfaces and accessibility via open protocols.

Grid computing originated in the early 1990s as a metaphor for making computer power as easy to access as an electric power grid

GRID History

Fathers of the Grid:

Ian Foster, Carl Kesselman(*) and Steve Tuecke

Grids can help solve “Grand Challenges”:

1. DNA analysis
2. Protein Folding
3. Financial Modeling
4. Earthquake simulations
5. Climate/weather (global warming) modeling
6. Health care services??

Common GRID Definition:

1. Computing resources not administered centrally
2. Open standards used
3. Non-trivial quality of service achieved.

GRID Types:

1. Compute Grids
2. Data Grids
3. Science Grids
4. Access Grids
5. Knowledge Grids
6. Bio Grids
7. Sensor Grids
8. Cluster Grids
9. Campus Grids
10. Tera Grids
11. Commodity Grids

***A grid for every
grant writer 😊***

GRID and Federation:

A Grid is built from multi-purpose protocols and interfaces that address such fundamental issues as authentication, authorization, resource discovery, and resource access.

Authentication and authorization need to be federated, or shared. Hence the need for federated identity management.

GRID and Federation:

Several large Federated efforts:

- Shibboleth
- GridShib

Shibboleth:

- Provides Web Single SignOn (SSO)
- Funded by Internet2
- Standards-based, open source middleware
 - Across or within organizational boundaries
- Interoperable with commercial vendor software
- Uses SAML attribute exchange



SAML – Security Assertion Markup Language:

- An **OASIS** standard
- Supports XML exchanges of:
 - authentication
 - authorization
 - attributes (from LDAP directory in Shibboleth)
- SAML is often part of a complete security solution, but rarely the only part
- Liberty Alliance, Shibboleth, GridShib, Sun, IBM, other solutions all using **SAML**..

SAML Example:

- ◆ **<Assertion>**
- ◆ `<!-- Conditions may include optional XML attributes defining a time period for validity -->`
<Conditions NotBefore="dateTime" NotOnOrAfter="dateTime">
 `<!-- limit who can rely on this assertion -->`
 <AudienceRestrictionCondition>
 <Audience>http://www.example.com/Members</Audience>
 </AudienceRestrictionCondition>
</Conditions>
- ◆ `<!-- Optional Advice used to include supporting evidence, proofs, assertions, pointers to updates etc. -->`
 <Advice>
 </Advice>
- ◆ `<!-- Authentication - example: SSL client certificate authentication -->`
<AuthenticationStatement AuthenticationMethod="urn:ietf:rfc:2246"
 AuthenticationInstant="dateTime">
- ◆ <Subject>
 <NameIdentifier
 Format="urn:oasis:names:tc:SAML:1.0:assertion#emailAddress">
 john_doe@example.com
 </NameIdentifier>
</Subject>
</AuthenticationStatement>
- ◆ **<ds:Signature>**
 XML Digital Signature for assertion
</ds:Signature>
- ◆ **</Assertion>**

GridShib:

GridShib leverages use of SAML/Shibboleth

- Bridges Shibboleth and GRID
- Adapts SAML attribute methods to work with standard Grid certificate authentication
- Shib extensions to support X.509 naming

Example GridShib: caBIG / caGRID

- Grid for sharing cancer research
- Very large scale bioinformatics project
- Based on Grid technology
- Working with Globus, Internet2, others
- caGrid technology using PKI, federation, attributes, using GridShib

RHIOs, GRIDs and Federation:

1. How can I trust that my personal health information remains private and only used when needed by an authorized professional?
2. Emerging health information exchanges, Regional Health Information Organizations (RHIOs), and the National Health Information Network (NHIN) all require security and privacy infrastructure **before a single transaction or health information exchange can take place**



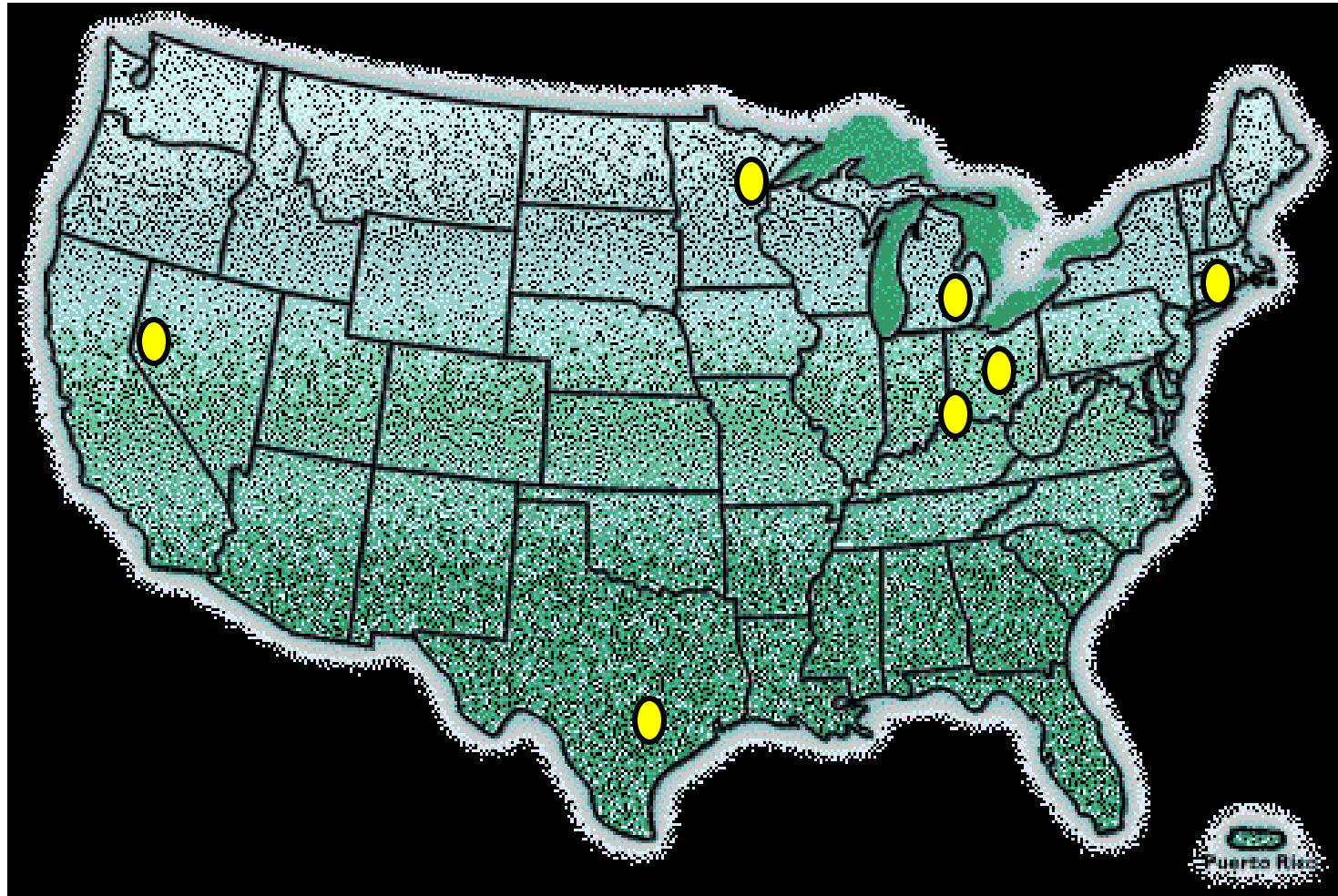
HIMSS e-Authentication Project

1. HIMSS and the General Services Administration (GSA) collaborated on a pilot project to demonstrate the use of the Electronic Authentication Service Components.
2. Pilot participants consists of seven Regional Health Information Organizations (RHIOs) and health information exchanges (IHEs) that are members HIMSS.

HIMSS Participants:

1. e-Health *Connecticut*
2. Michigan Data Sharing & Transaction Infrastructure
3. CHRISTUS Health of Texas
4. Community Health Information Collaborative (Minnesota)
5. Nevada Single Portal Medical Record
6. e-Health Ohio
7. Ohio Supercomputer Center Bioinformatics
8. Virtual Medical Network (Cincinnati, Ohio)

HIMSS e-Authentication Project



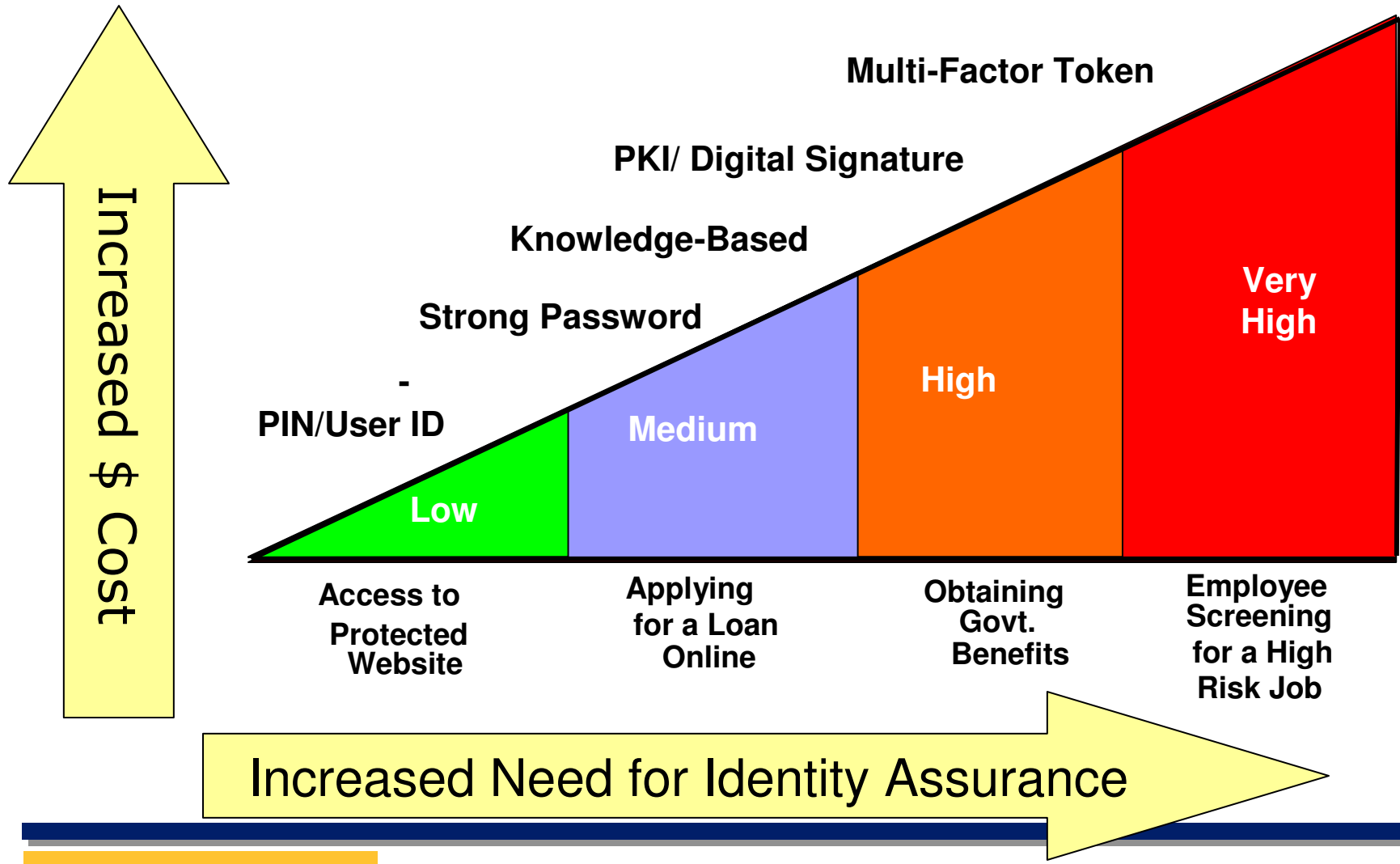
Constrains on National System:

- No National ID
- No National unique identifier
- No central registry of personal information, attributes, or authorization privileges
- Different authentication assurance levels are needed for different types of transactions
- Authentication – not authorization

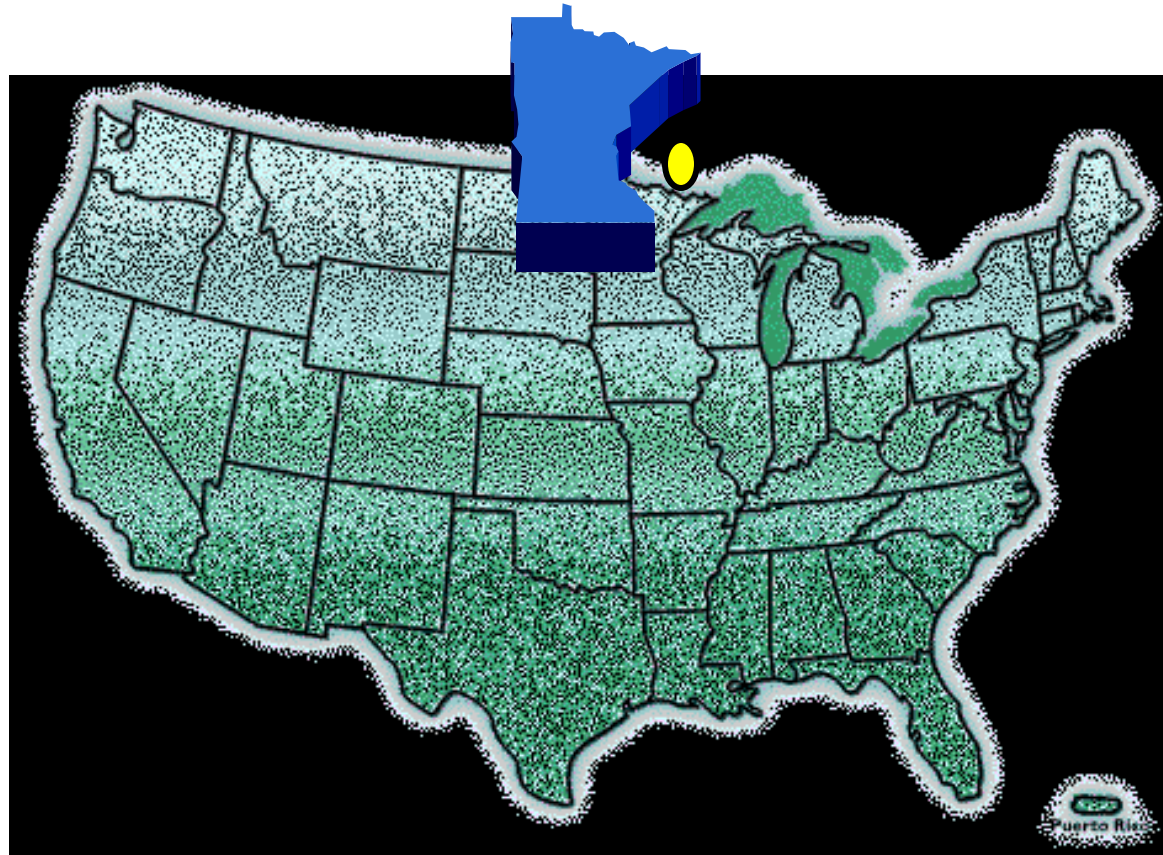
Technical approach:

- No single proprietary solution
- Deploy multiple COTS products – user's choice
- Products must interoperate together
- Controls must protect privacy of personal information
- Common Identity Assurance Levels

Security Considerations: Four Identity Assurance Levels



Minnesota HIMSS Project



Minnesota Goals

- ◆ **Develop single sign-on service with several Duluth hospitals**
- ◆ **Use High or Very High Assurance Level Security**
- ◆ **Test usage of Federal Government ACES PKI certificates**
- ◆ **Test concept of “Federated Identity Management”**
- ◆ **Test an open-source solution called “Shibboleth”**
- ◆ **Test access via Citrix web front end**

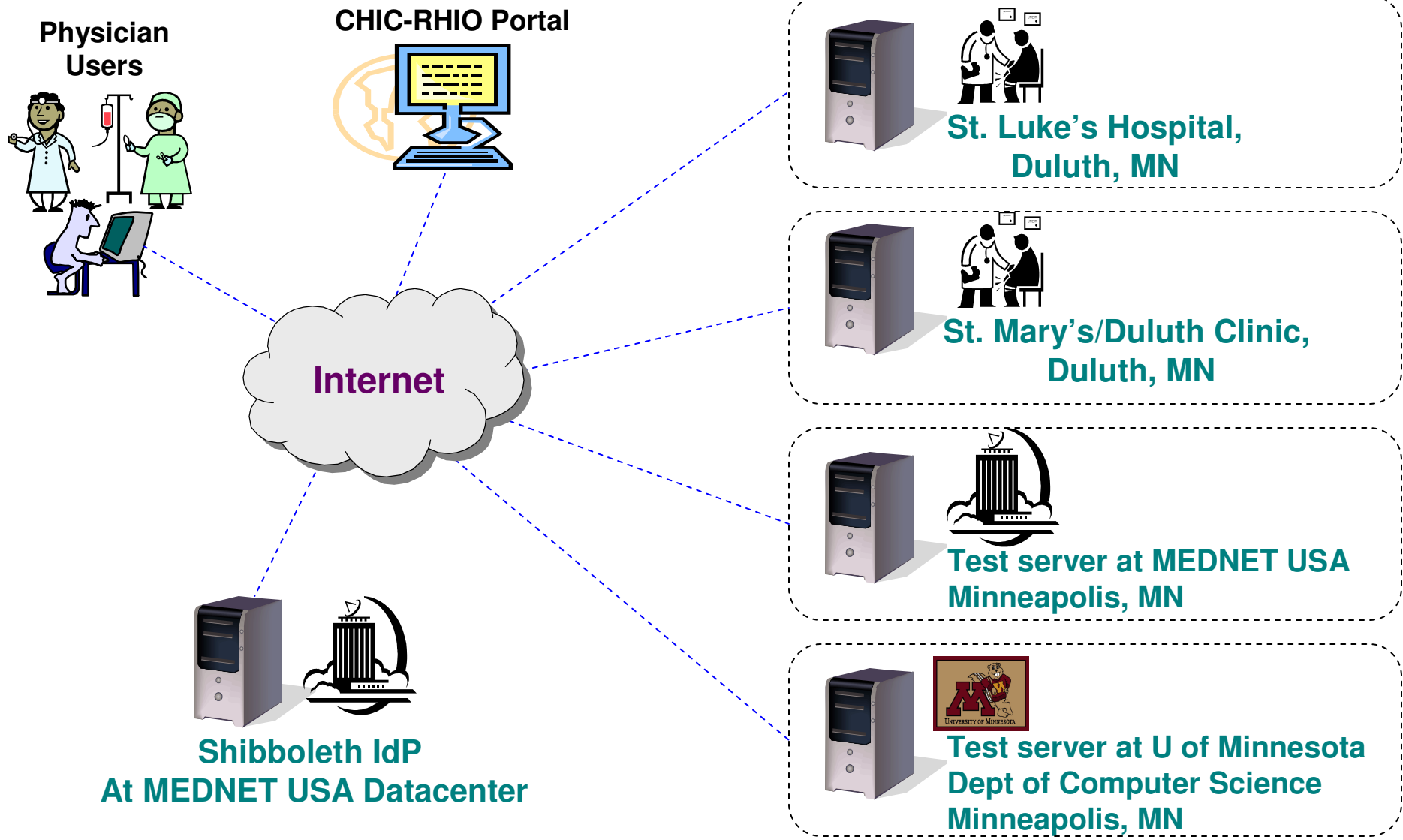
Team:

- ◆ Cheryl Stevens - CHIC
 - Executive Director of CHIC – Co-project lead
- ◆ Melinda Machones
 - College of St. Scholastica, Center for Healthcare Innovations
 - CHIC – Co-project lead
- ◆ John Fraser – MEDNET USA
 - Technical Project Manager
 - National PKI / Infrastructure expertise
- ◆ Dr. Jon Weissman, U of M
 - Associate Professor of Computer Science
 - Oversees Shibboleth planning / Seonho advisor
- ◆ Seonho Kim, MEDNET USA
 - Ph.D Student in GRID Computing, Dept of Computer Science
 - Installation and Config - Shibboleth installation

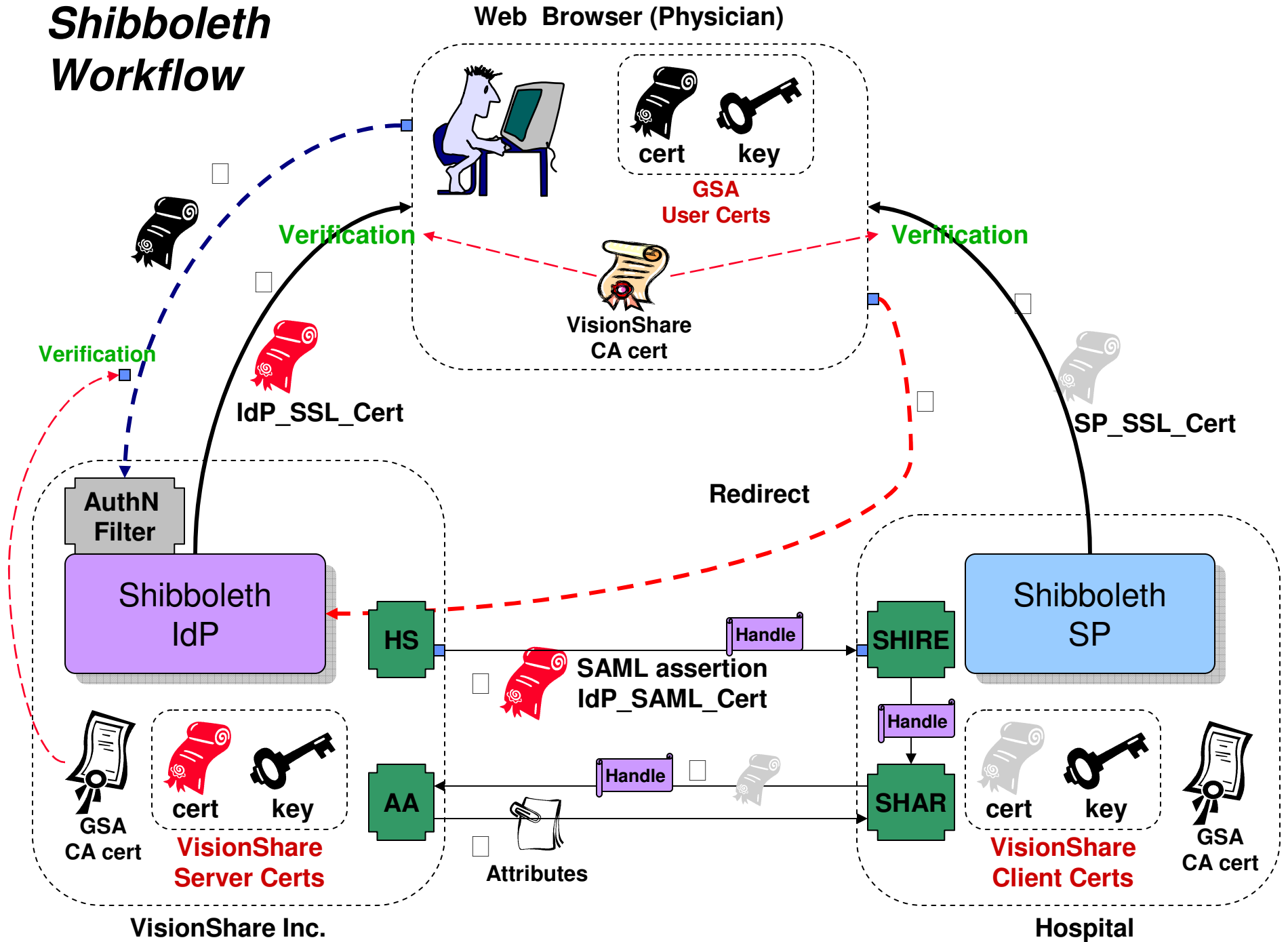
Current Progress

- ◆ Two Hospital Participants:
 - St. Luke's
 - Saint Mary's Duluth Clinic (SMDC)
- ◆ Common Web Portal up
- ◆ Shibboleth Federated Identity System Operational
- ◆ Test certificates issued by VisionShare
- ◆ All testing completed

MEDNET USA - Shibboleth Testbed



Shibboleth Workflow



Shibboleth Workflow:

- 1. A physician tries to access a Shibboleth service provider. Then SP's SHIRE (Shibboleth Indexical Reference Establisher) service sends the server certificate SP_SSL_Cert to the user browser and the browser verifies it**
- 2. The SHIRE asks IdP HS (Handle Service) to create a handle for this physician and redirects the browser to the IdP HS (No WAYF service)**
- 3. The user browser verifies the IdP server certificate IdP_SSL_Cert**
- 4. The Apache HTTP server authentication filter (AuthN Filter) asks the user browser a valid certificate for authentication and verifies the user certificate (Or asks a valid user name/password)**
- 5. The IdP HS returns a handle with SAML Authentication Assertion to the SP SHIRE. The SP SHIRE hands over the handle to SHAR (Shibboleth Attribute Requestor)**
- 6. The SP SHAR asks the IdP AA (Attribute Authority) for attributes by sending the user handle and Shibboleth SP client certificate**
- 7. The IdP AA verifies the SP client certificate and returns the attributes according to the ARP (Attribute Release Policy) to the SP SHAR**
- 8. The SHAR performs basic checks on attributes according to AAP (Attribute Acceptance Policy)**

Minnesota: Lessons Learned

- Community ready
- Digital Certificates acceptable
- Want High or Very High Assurance Levels
- Federated Identity Management System Possible

HIMSS e-Authentication Project Outcome:

MEDNET USA

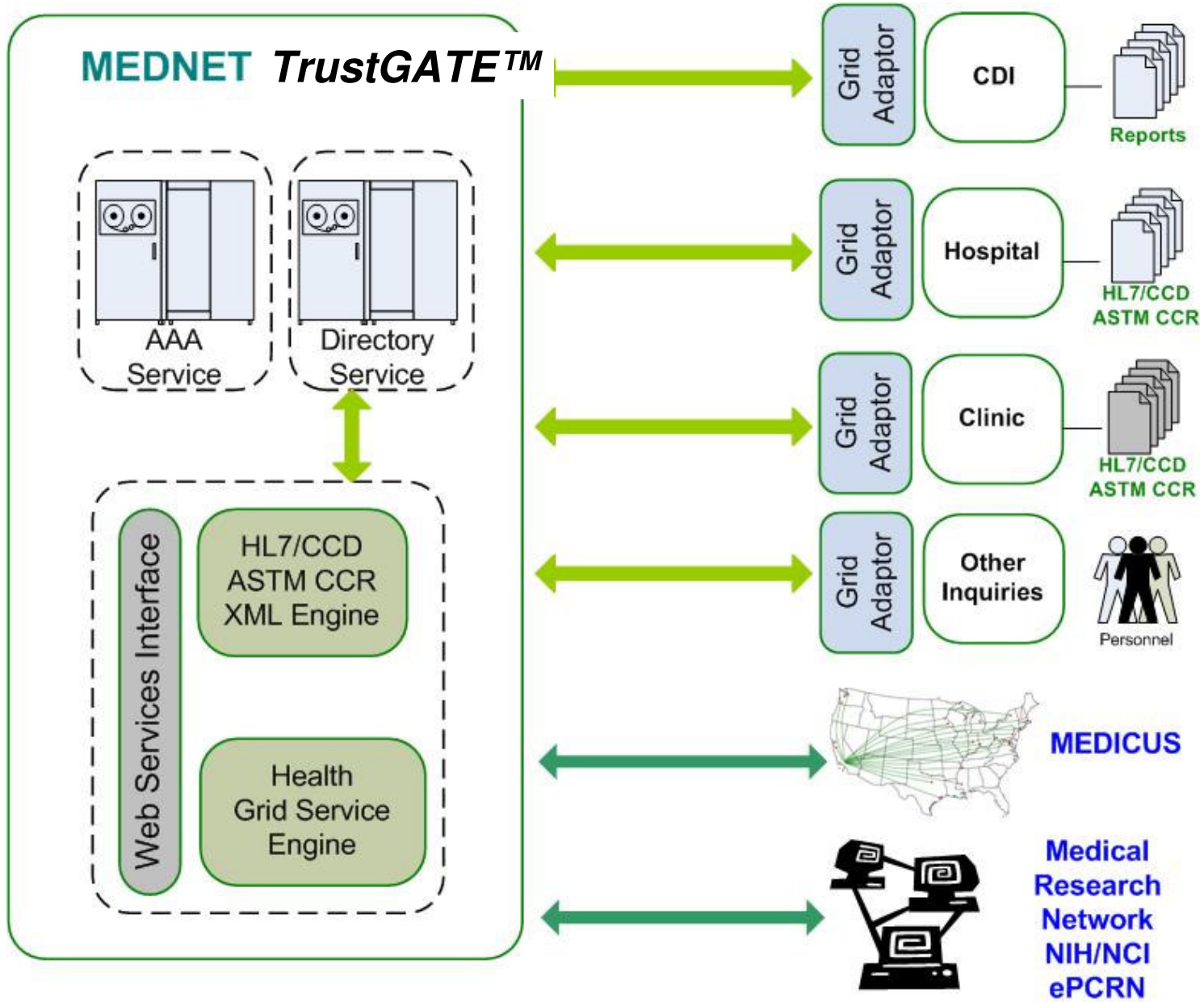
MEDNET SERVICES:

- TrustGATE™ Shibboleth Service
- Digital Certificate Support
- National Patient Directory
- National Patient Card Service

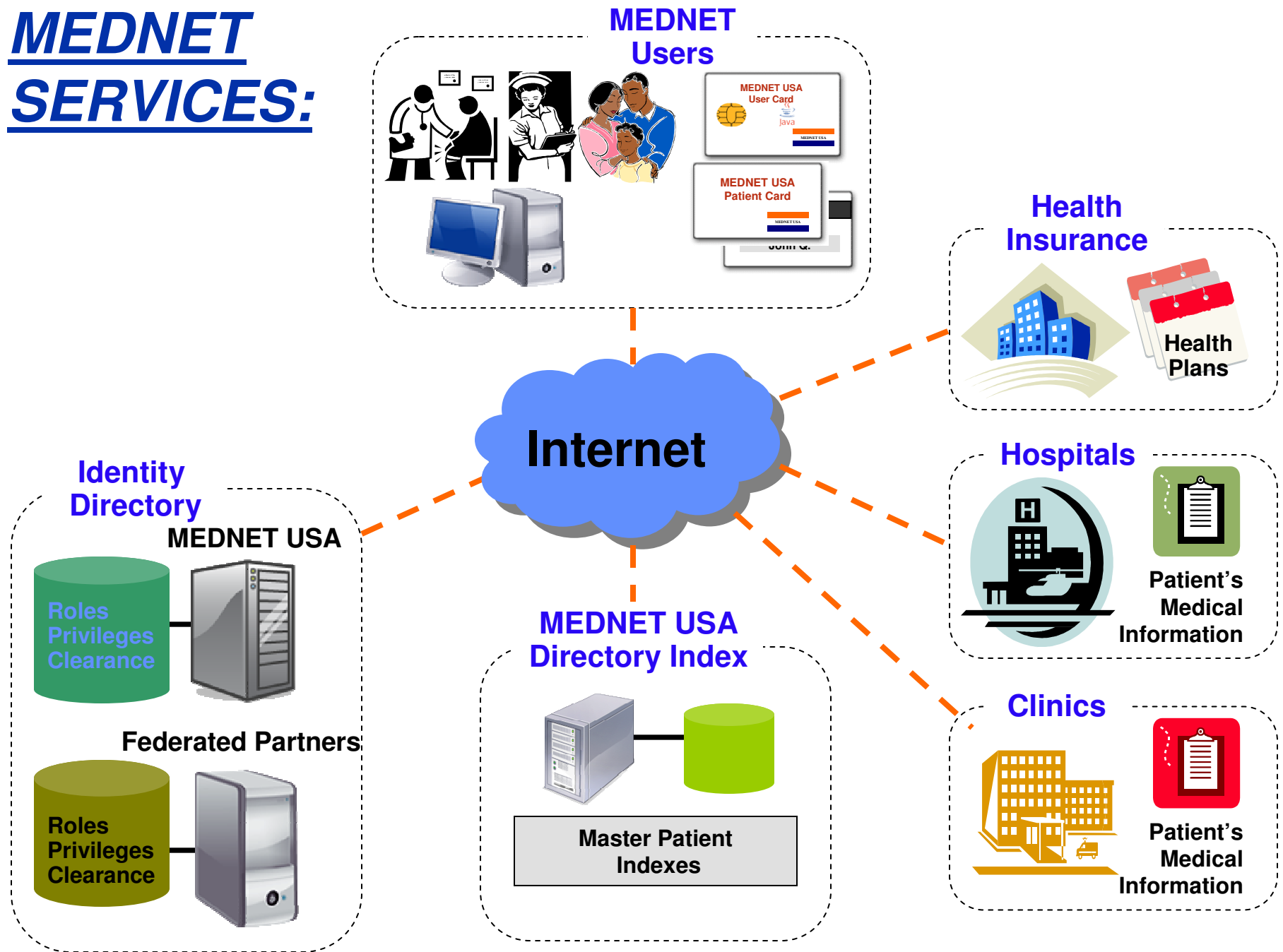
MEDNET SUPPORTS:

- Community Single Sign On
- Medication Reconciliation
- e-Prescribing
- Emergency Services
- Public Health Services
- Insurance verification
- Medical Record Exchanges

MEDNET ARCHITECTURE:

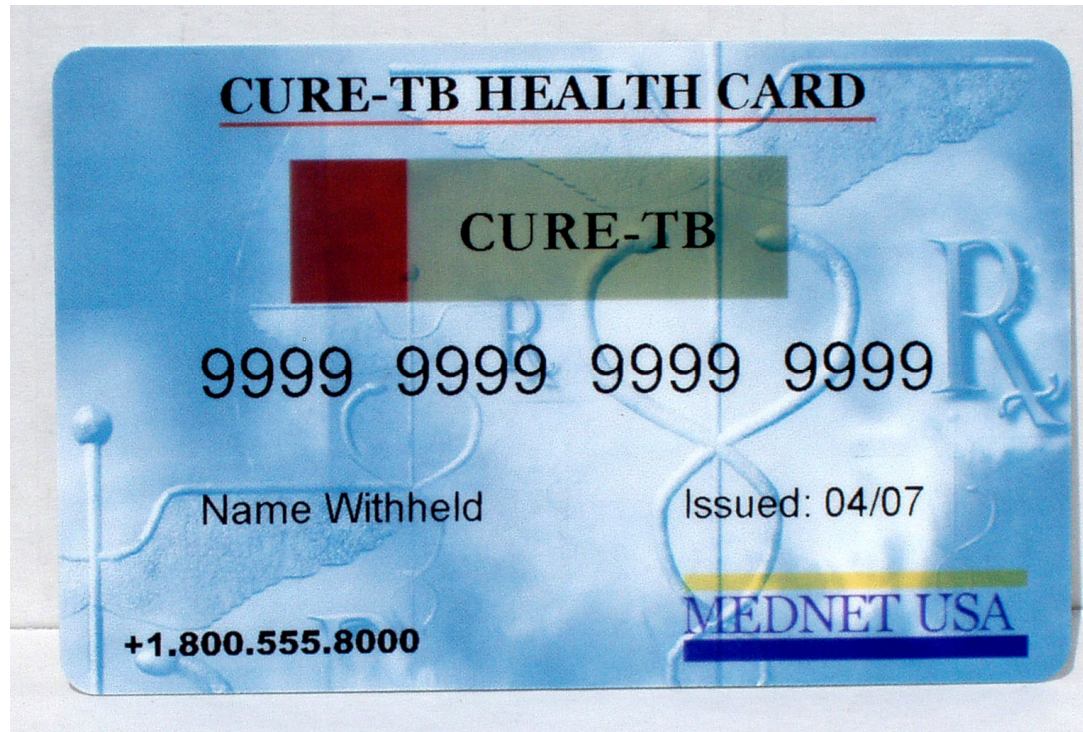


MEDNET SERVICES:

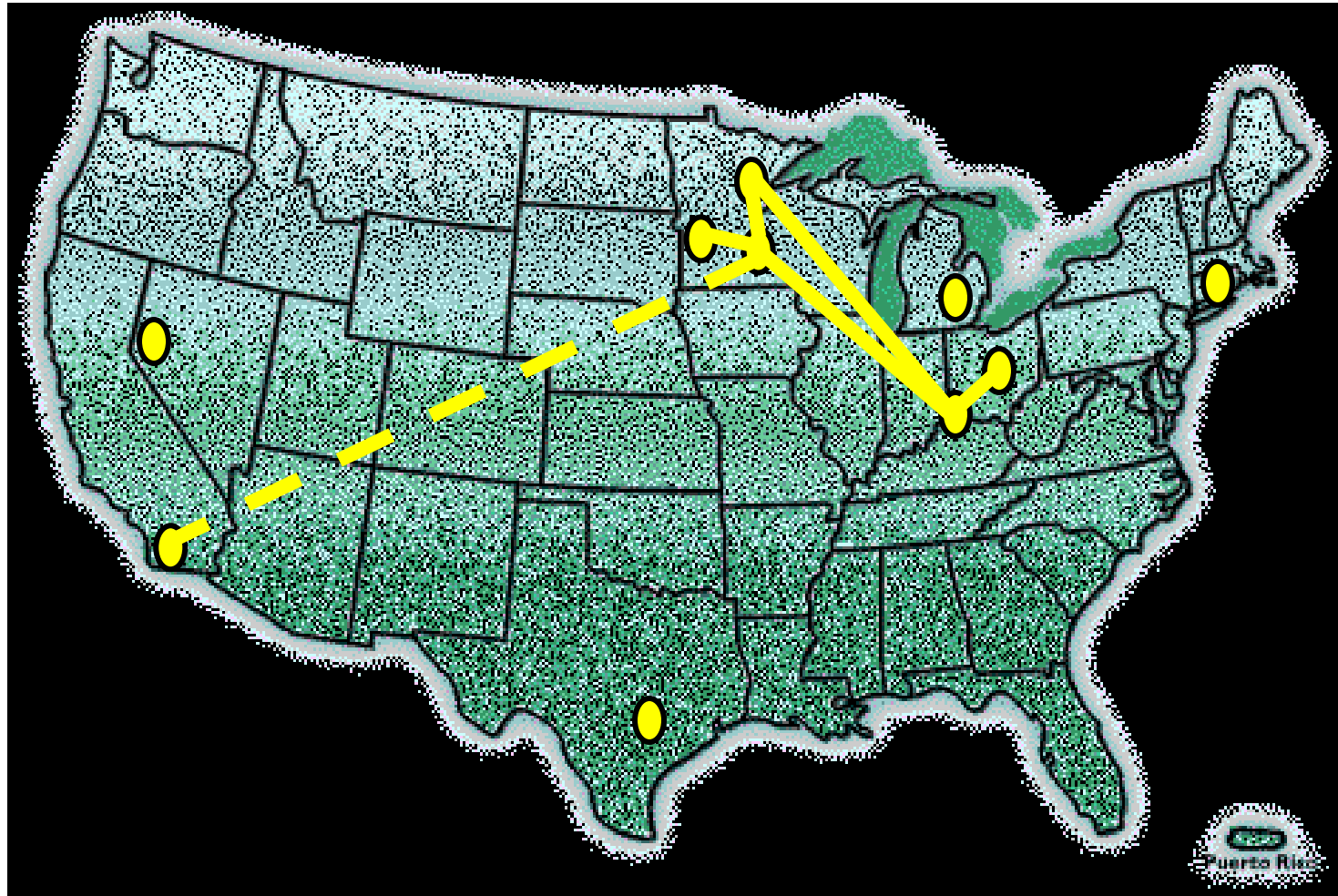


MEDNET SERVICES:

Example Patient Card



Federation Testbed - Building!



Please Join the Federation!

THANK YOU!

Contact Information

John Fraser

CEO, MEDNET USA

Email: john.fraser@mednet.org

+1 612.435.7602