OASIS-HITSP

Privacy Consent and Access Control

Advanced Technology Demonstration

13 Apr 2009

Duane DeCouteau (Edmond Scientific)
Duane.DeCouteau@VA.gov

Organization for the Advancement of Structured Information Standards

John "Mike" Davis (DVA)
Mike.davis@va.gov

Healthcare Information Technology Standards Panel

EHT's Emerging Health Technologies Advancement Center (EHTAC)

- **Leadership**

- EHT operates under the leadership of its Director, Jim Demetriades who sets overall objectives and approves all EHTAC projects.

- **Mission**

To investigate requirements suggested by emerging technology, not currently implemented by VA, that offers promise of improving support to VHA's healthcare line of business. EHTAC seeks to answer the healthcare equivalent of the fundamental question:

> ***"If I had a tractor instead of a horse would my farming business be any different?"***

Operations

EHT operates the EHTAC lab and other services on behalf of VHA and VHA stakeholders. The Lab provides simulations and feasibility experiments to understand their potential for future requirements generation in the healthcare environment. If feasible and shows potential, the information obtained is used for community review through requirements steering committees or validation through management and ESM processes. EHTAC does not recommend or endorse any particular vendor product or technology solution. While EHTAC does not implement Class I projects for VA enterprise-wide deployment, it does support the development of Class III software.

EHT Approved/Funded Demonstrations

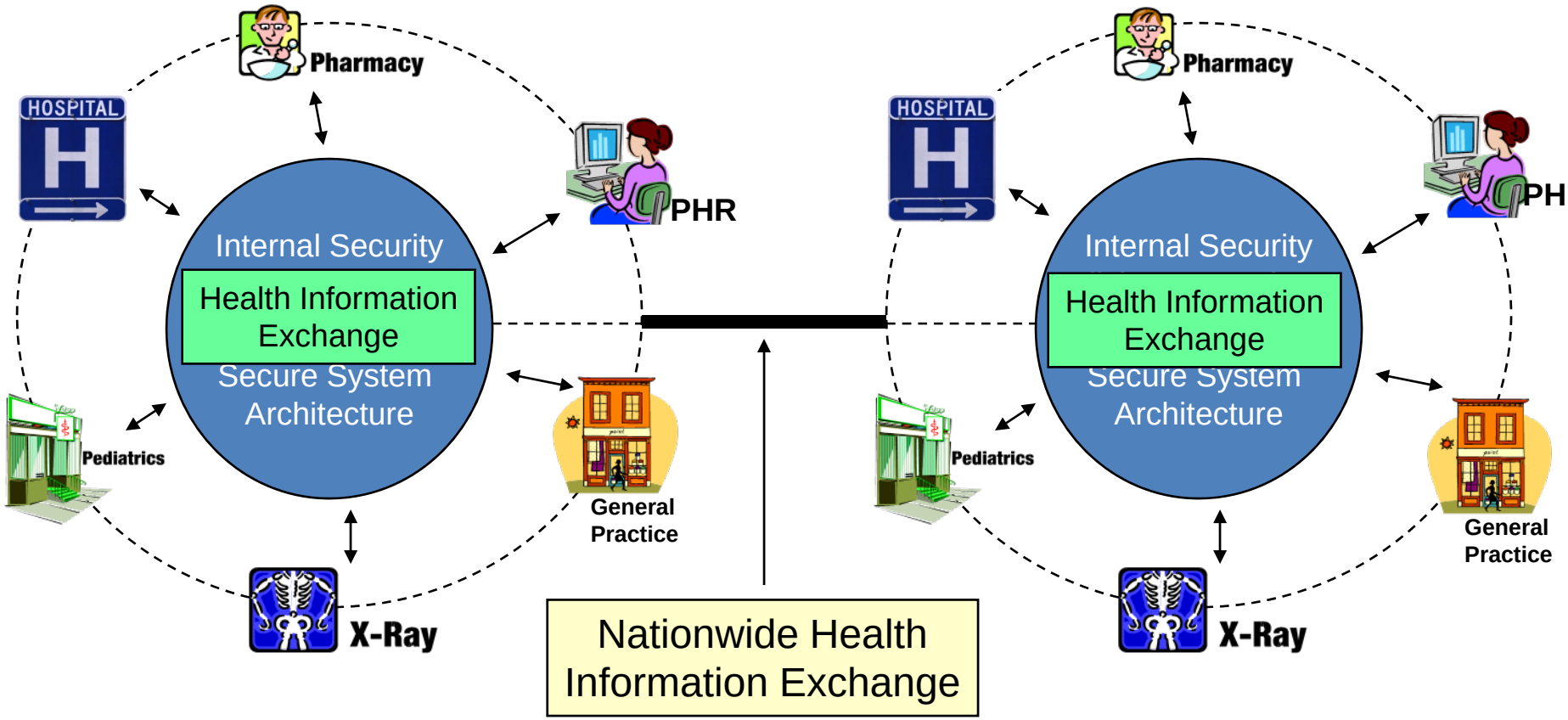
1. Advanced technology demonstrations in support of Health and Human Services ONC recognized privacy and access controls for the secure electronic exchange of healthcare information (HITSP TP20/30).
2. Support for VHA Standards and Interoperability Initiatives (San Diego Project)

RSA Conference April 2008
Multi-vendor demonstration of OASIS XACML supporting HITSP TP20

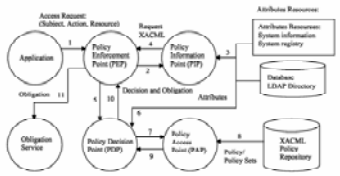
London Conference Oct 2008
Extensions to the RSA demonstration

HIMSS Apr 2009
End-to-end demonstration of OASIS SAML/ XACML/ WS-Trust supporting HITSP TP20/30

Interoperability – The Focus of HITSP

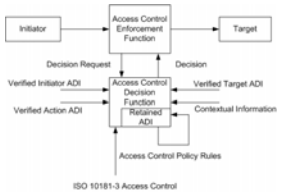


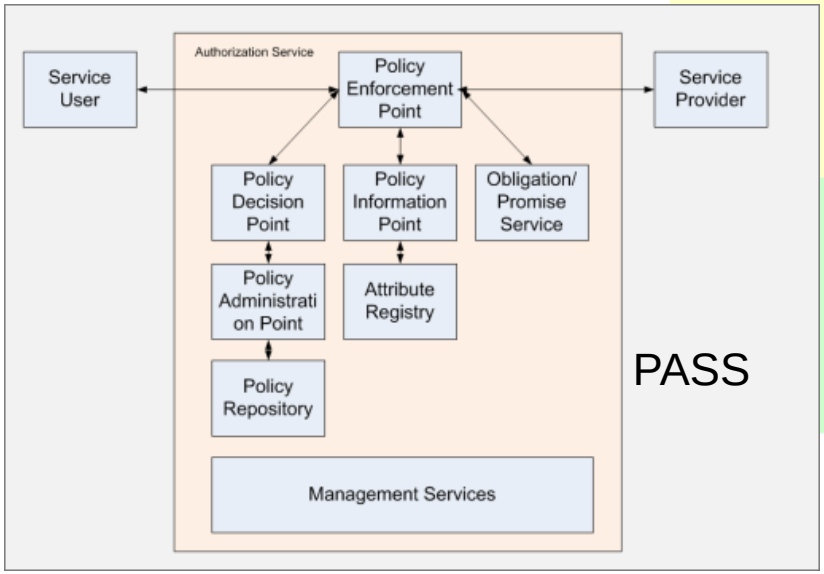
Authorization SOA Models



OASIS

ISO





PASS

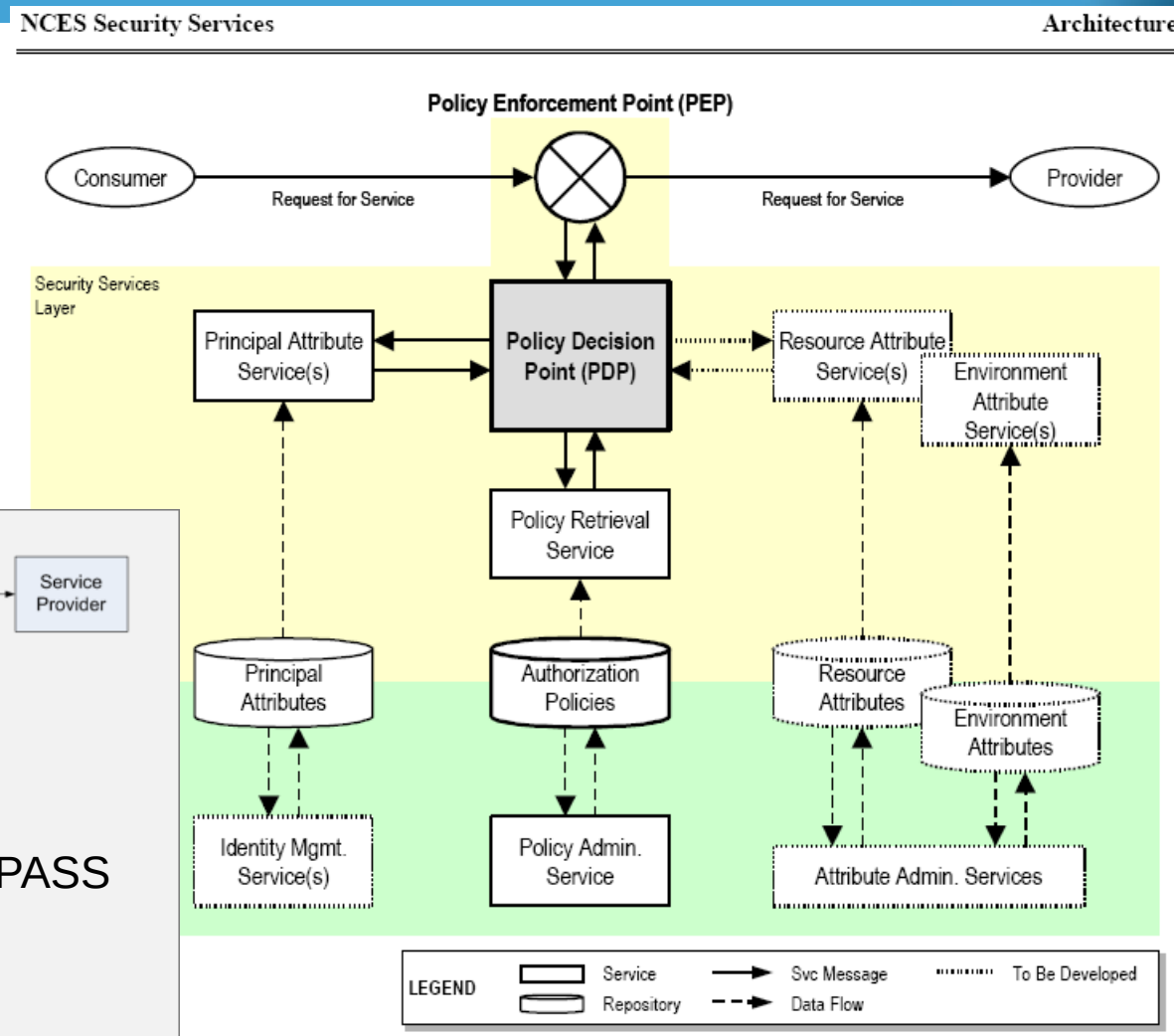
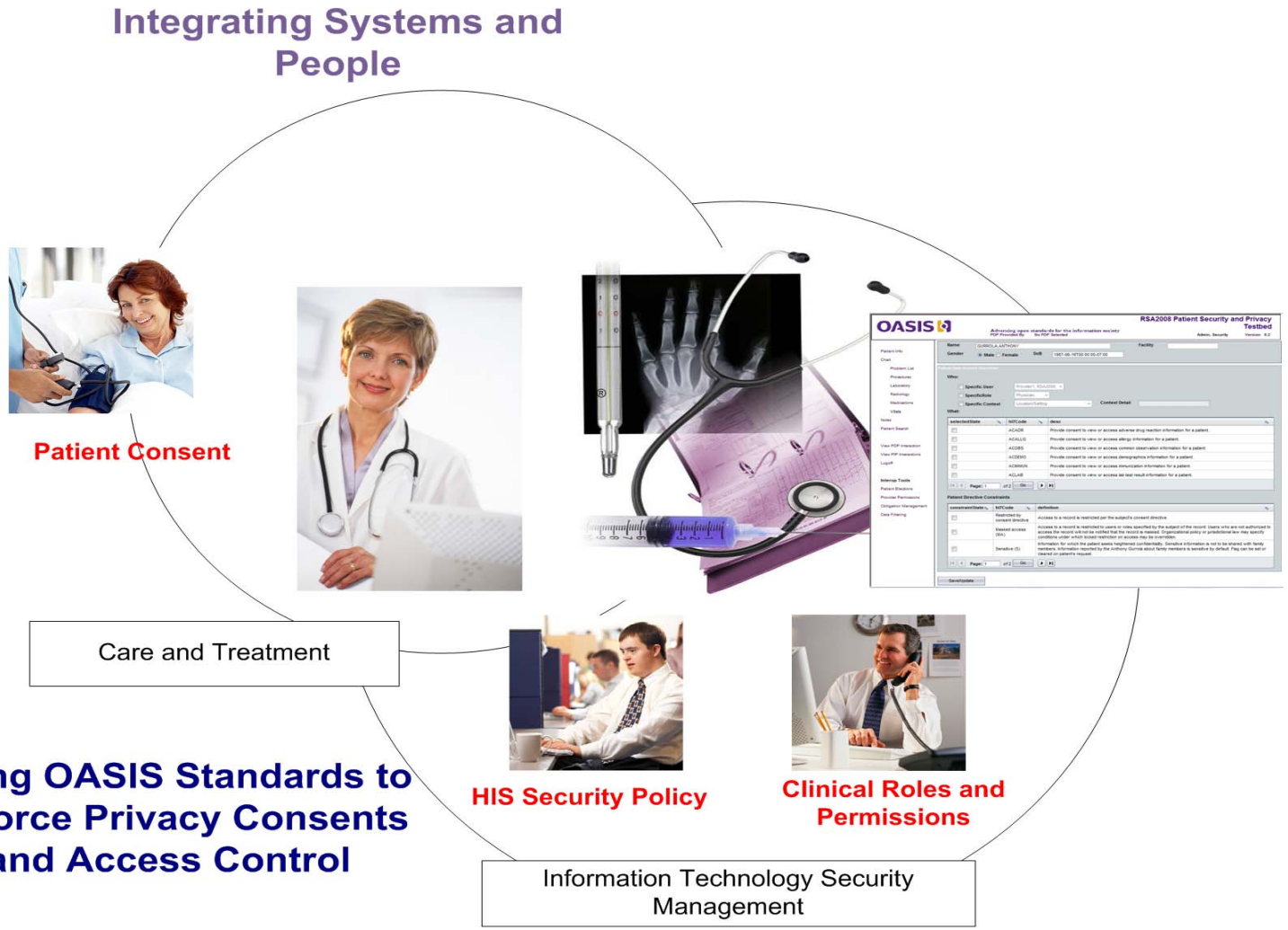
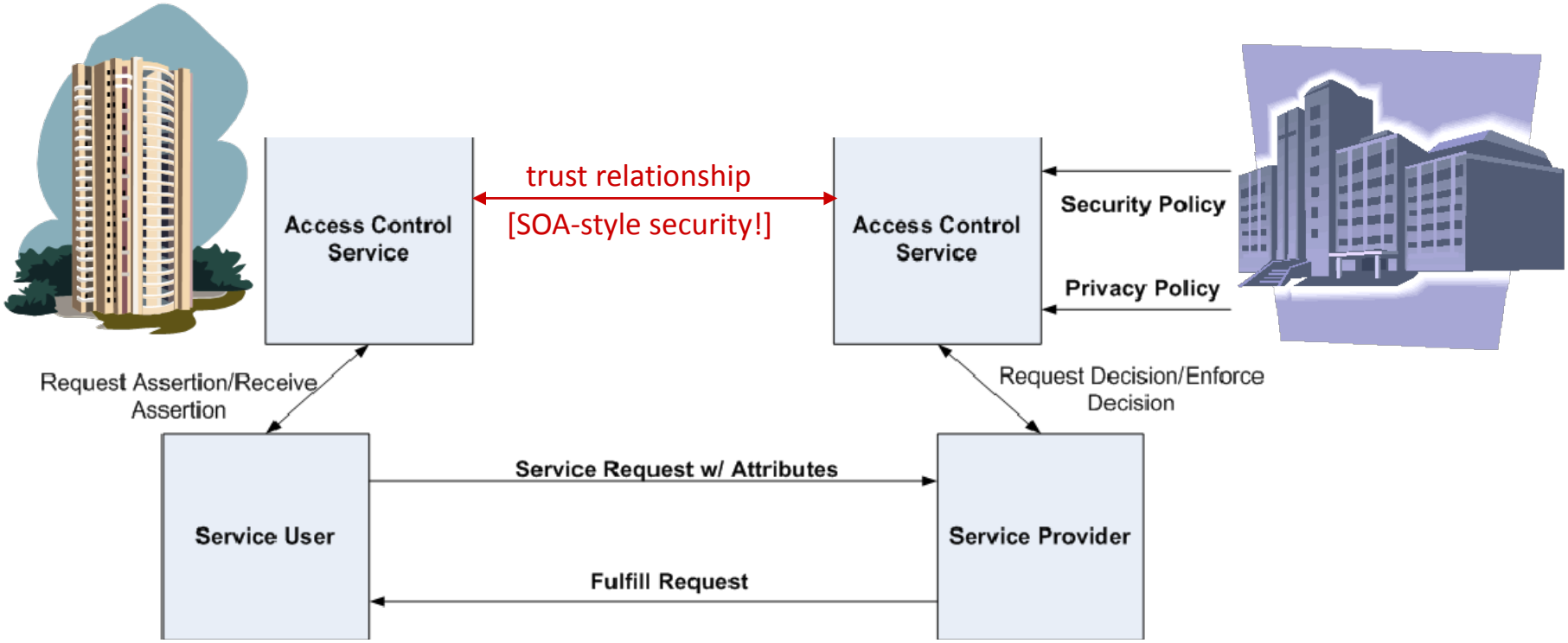


Figure 12 - Authorization Architecture

Security and Privacy Demonstration Overview: Provision of Care



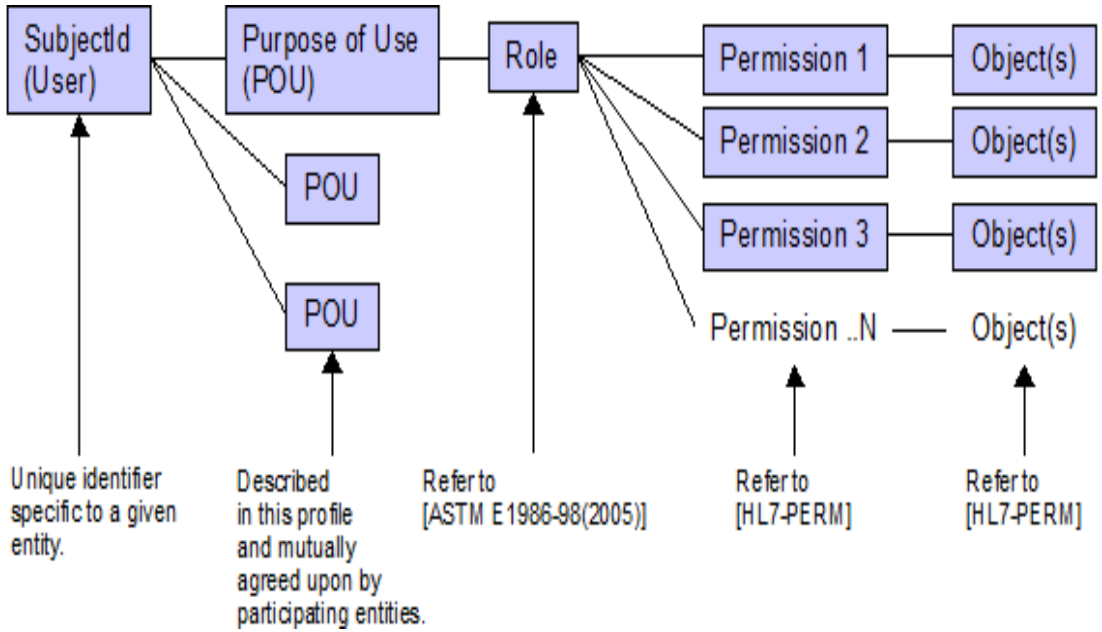
Security and Privacy Demonstration Overview: Cross Enterprise Data Sharing



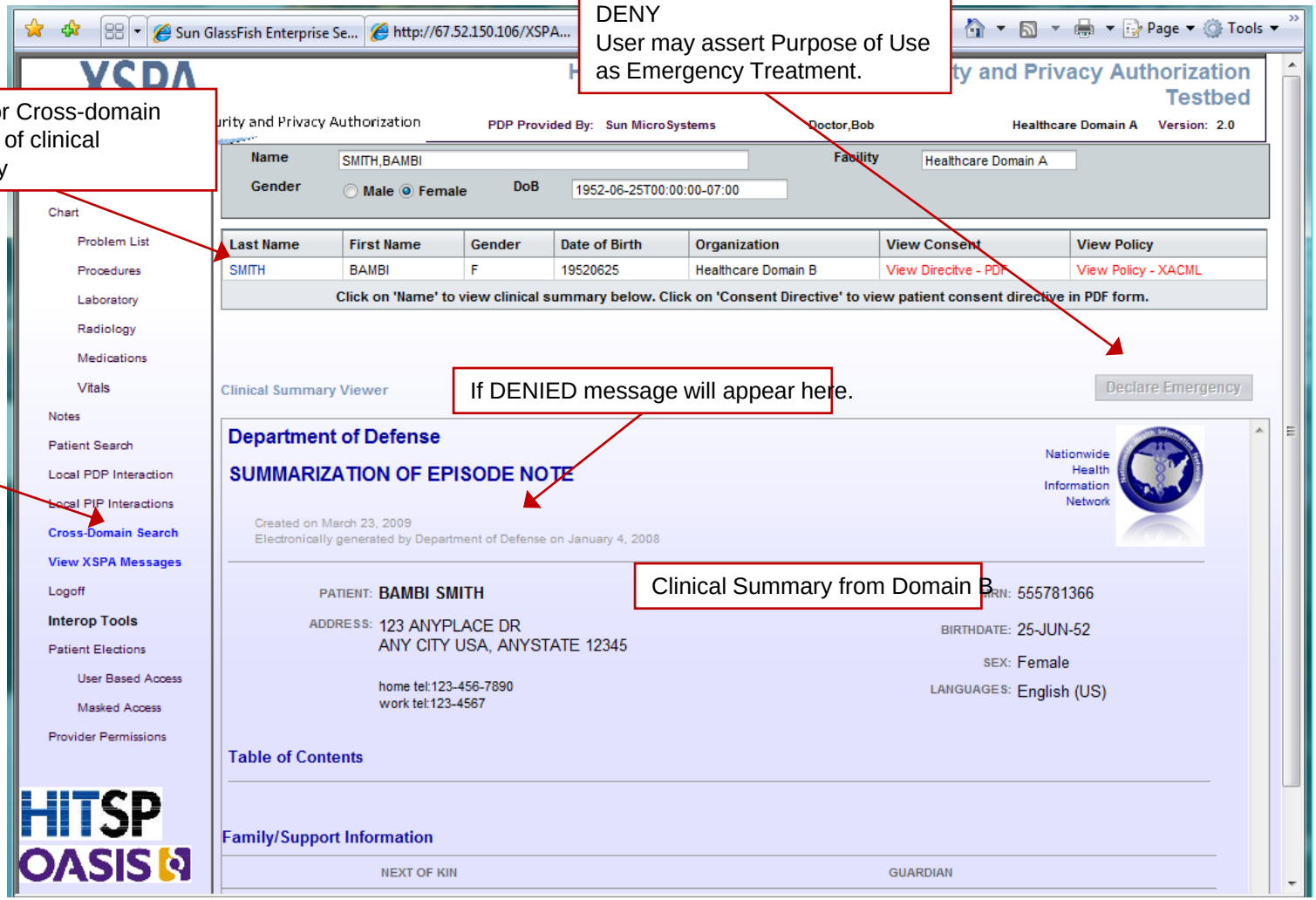
XSPA SAML Profile / HITSP TP20 High-Level Interactions

Security and Privacy Demonstration Overview: Behind the Scenes

Relationship between subject and permissions to specific objects under POU



Service User



Security and Privacy Demonstration Overview:

Use Cases

- Demonstrate the Enforcement of Patient Consent Directives
  - Opt-In / Opt-Out
  - Allowed Organizations
  - Confidentiality Codes (Consent Directive Template)
  - Deny Access based on Role and Purpose of Use
  - Deny Access to Specific Providers
  - Masked Results based on Role
  - Masked Results for Specific Providers

- Demonstrate the Enforcement of Organizational Policies
  - Limit access to specific organizations
  - Limit access during specific hours of the day
  - Require certain roles based on purpose of use and service requested
  - Require certain permissions based on purpose of use and service requested

Summary of Technical Features

- DHHS approved HITSP IS, standards, constructs (TP20/TP30)
- DHHS Security and Privacy Framework Compliant
- HIPAA Security and Privacy Compliant
- Extends Security and Privacy technologies for NHIN
- Standard Clinical Roles (ASTM, ANSI, HL7)
- Standard Patient Consent Directives (HL7, IHE BPPC)
- Standard Web-Service Protocols (OASIS SAML, XACML, WS-Trust)
- Federation of authenticated identities (OASIS SAML, IHE XUA, C19)
- Standard Interoperability Profiles (OASIS XSPA, IHE)
- Implementation-ready without change to legacy systems
- Polices managed centrally, enforced locally (ASTM, ISO PMI)
- Vendor supported solutions

IS = Interface Specification
NHIN = Nationwide Health Information Network
PMI = Privilege Management Infrastructure

SAML=Security Assertion Markup Language
XACML= eXtensible Access Control Markup Language
C19 = HITSP Entity Identity Assertion Component

Conclusion

Health and Human Services Security and Privacy Framework is realizable

We are Ready

- Vendor security/privacy products are available
- HITSP Constructs are mature (DHHS Accepted)
- OASIS – HITSP demonstrations since April 2008
- Interoperability Standards/Profiles are there