OASIS-HITSP

Privacy Consents and Access Controls

Advanced Technology Demonstration

Chicago
McCormick Place
April 4-8 2009

Technology Showcase

Presents

An

Advanced technology demonstration of Health and Human Services recognized privacy and access controls for the secure electronic exchange of healthcare information.

Booth 7750

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

Privacy—Security's Point of Pain

- **Privacy Traditionally not a Security concern-Now it is**
  - Security administrators unfamiliar with Privacy
  - Privacy Coordinators unfamiliar Security systems
- **Health Information Exchange "Opt in/Opt out"**
  - Too coarse
  - Patients want more options and control
- **DURSA-Privacy complicates, conflicts with traditional rules**
- **HIPAA Privacy Rule-Too complex for information systems?**
- **Managing and enforcing patient Consent Directives, Preferences, Constraints**
  - To what granularity?
  - Impact of patient decisions on provision of care?

Status of Security and Privacy

Things are Good Enough

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

Healthcare Scenarios

Clinician asserted rights and permissions

- Clinical Roles and Permissions, least privilege, credentialing, separation of duty

Purpose-based access

- Emergency Access: Granting extraordinary access during events involving risk of potential death or injury

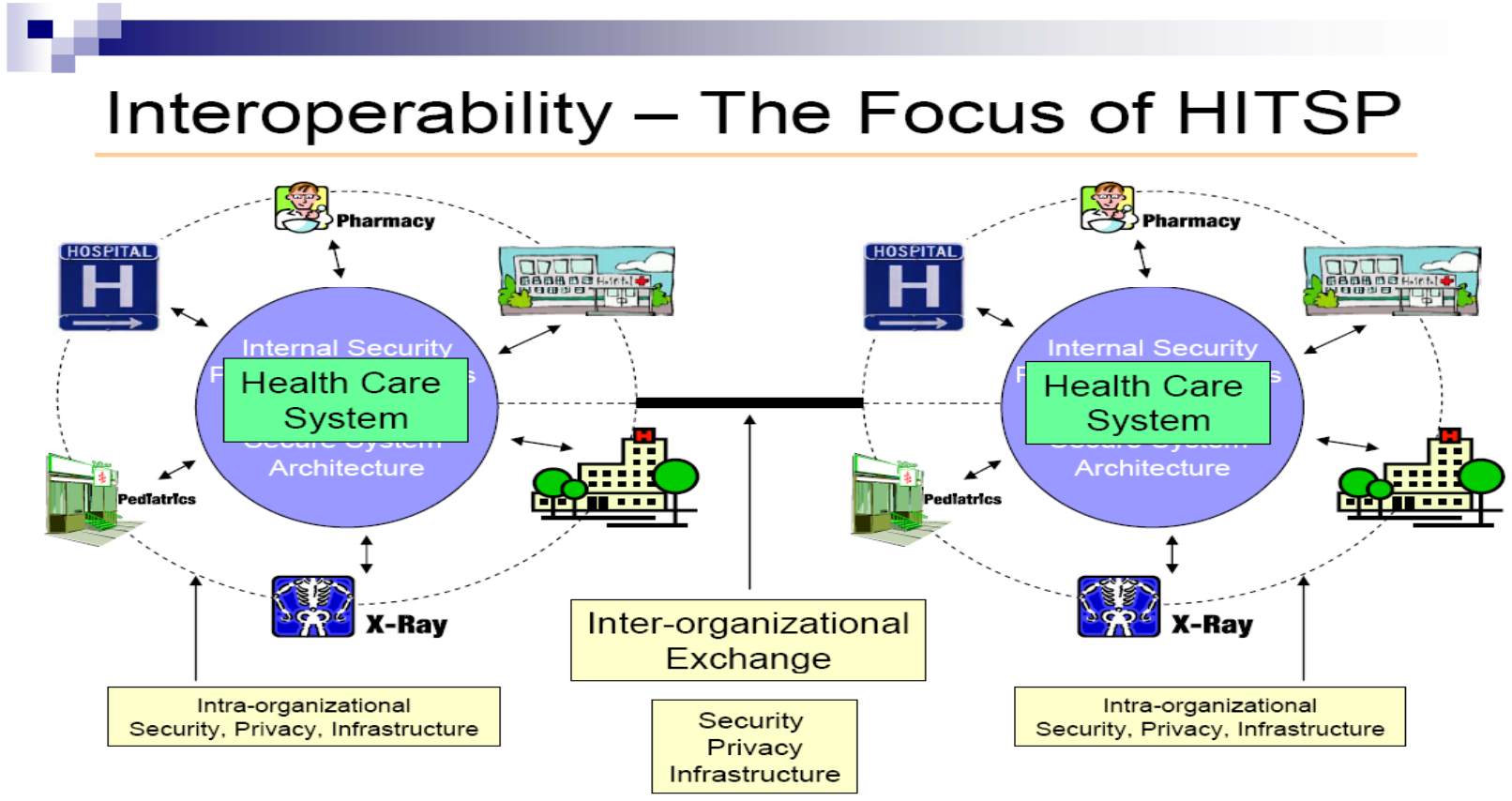
Patient Privacy

- Data Filtering: Patient directed masking of some data
- User Based Access: Patient directed access for persons or roles

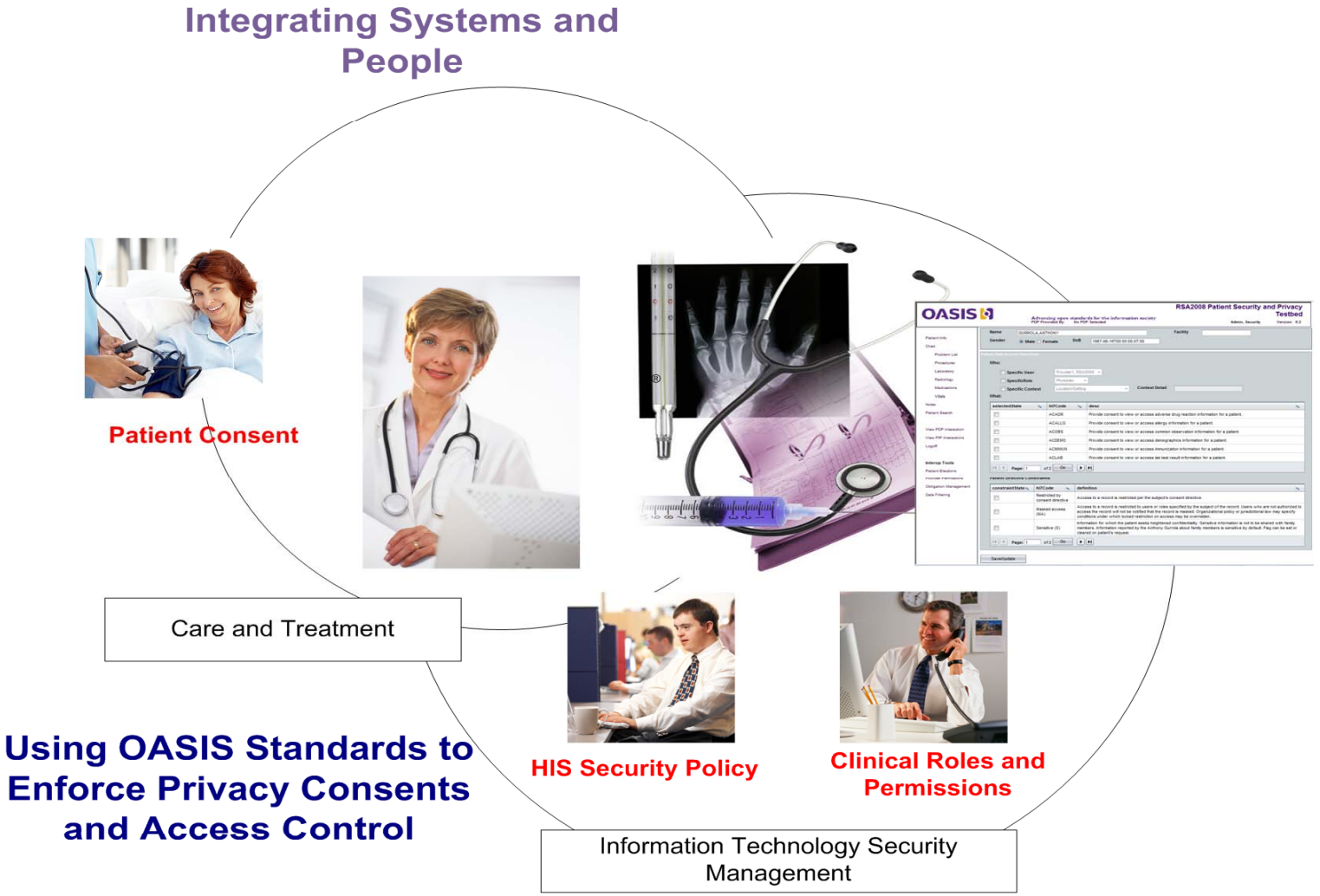
Organization specific policy

- Organizational Security Policy: Healthcare specific business rules for application behavior and patient safety

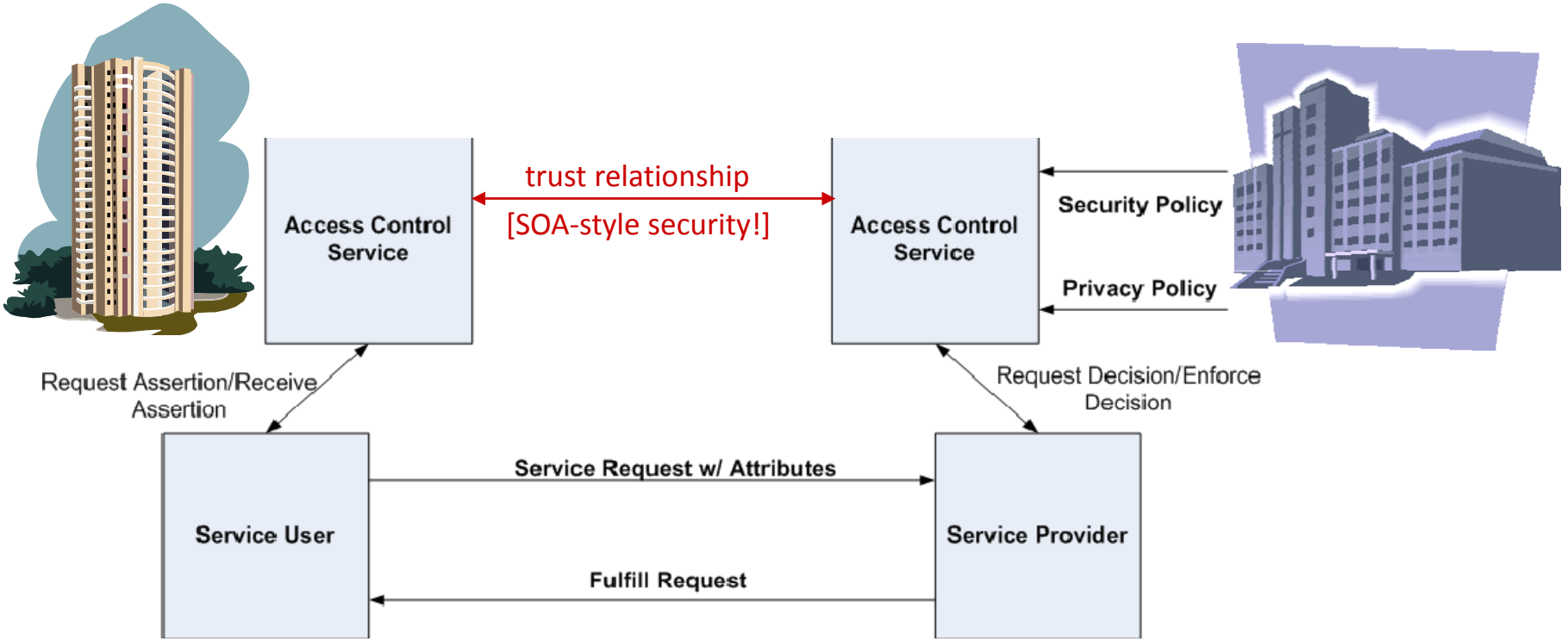
Interoperability – The Focus of HITSP



Security and Privacy Demonstration Overview: Provision of Care



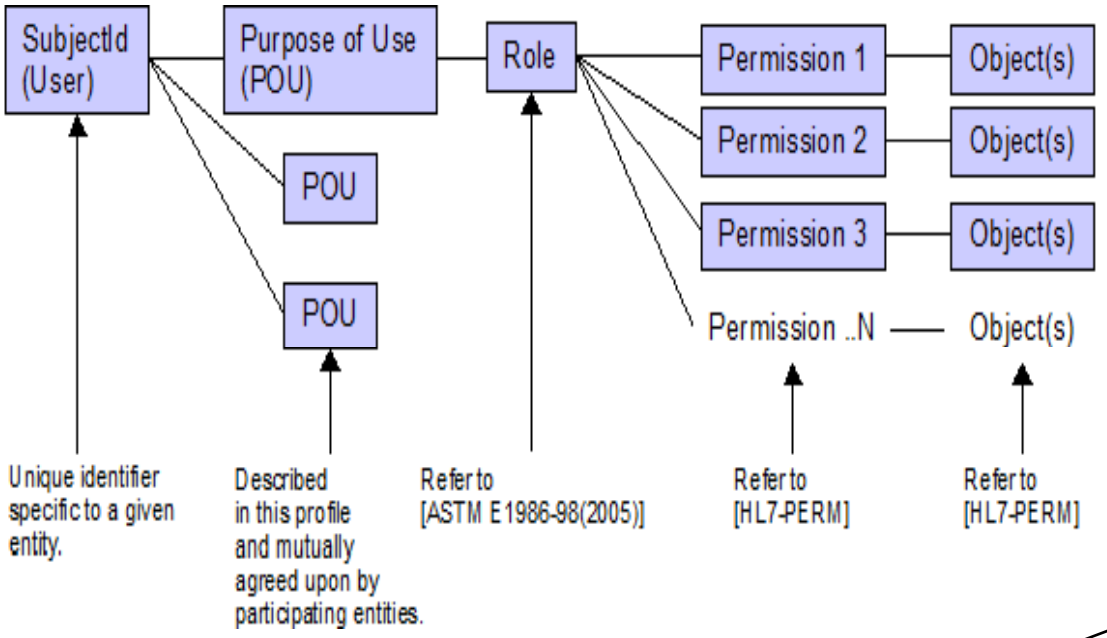
Security and Privacy Demonstration Overview: Cross Enterprise Data Sharing

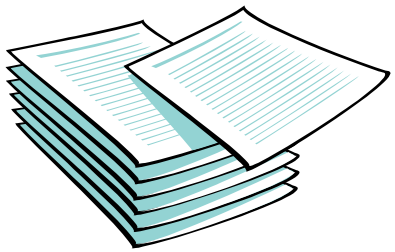


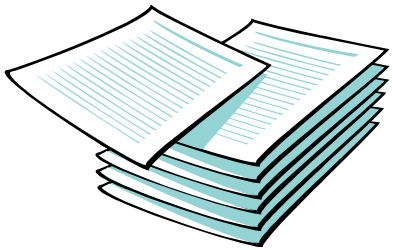
XSPA SAML Profile / HITSP TP20 High-Level Interactions

Security and Privacy Demonstration Overview: Behind the Scenes

Relationship between subject and permissions to specific objects under POU

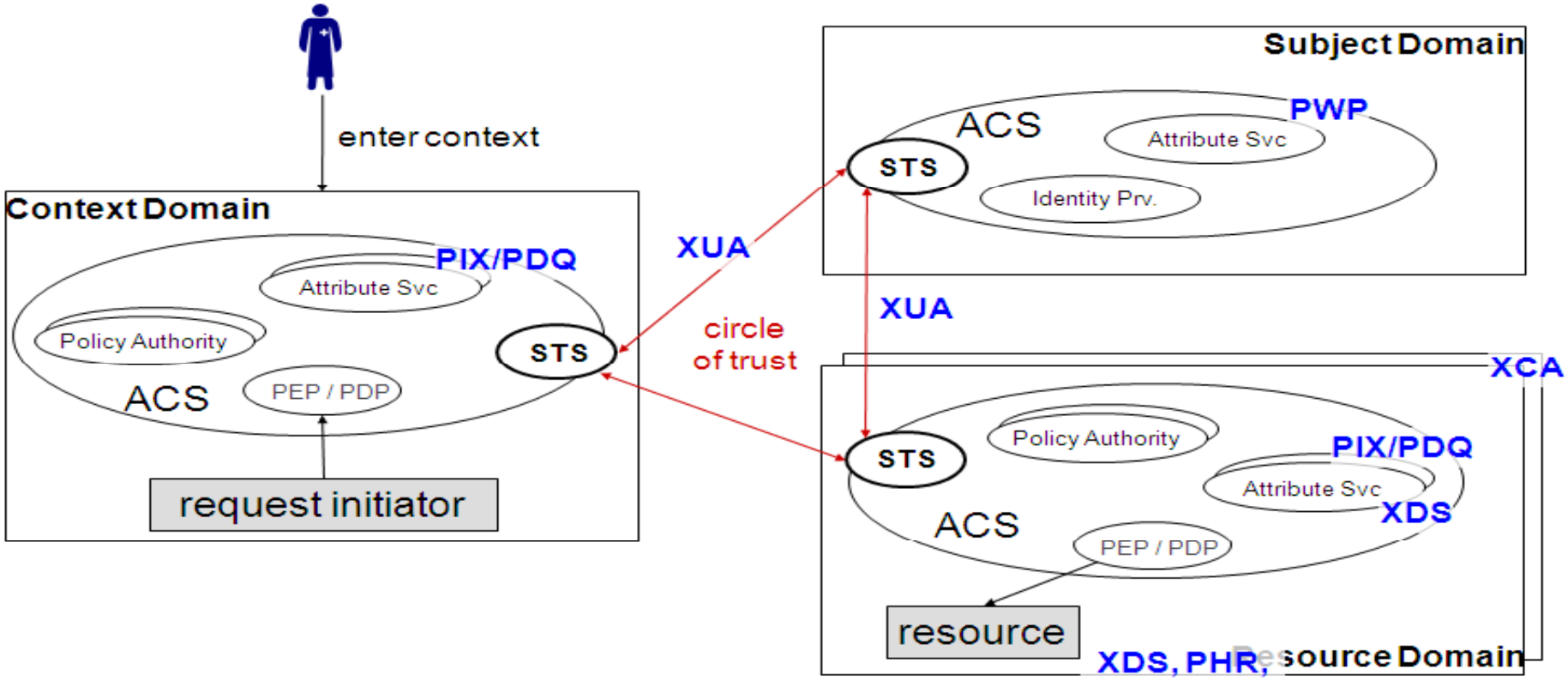






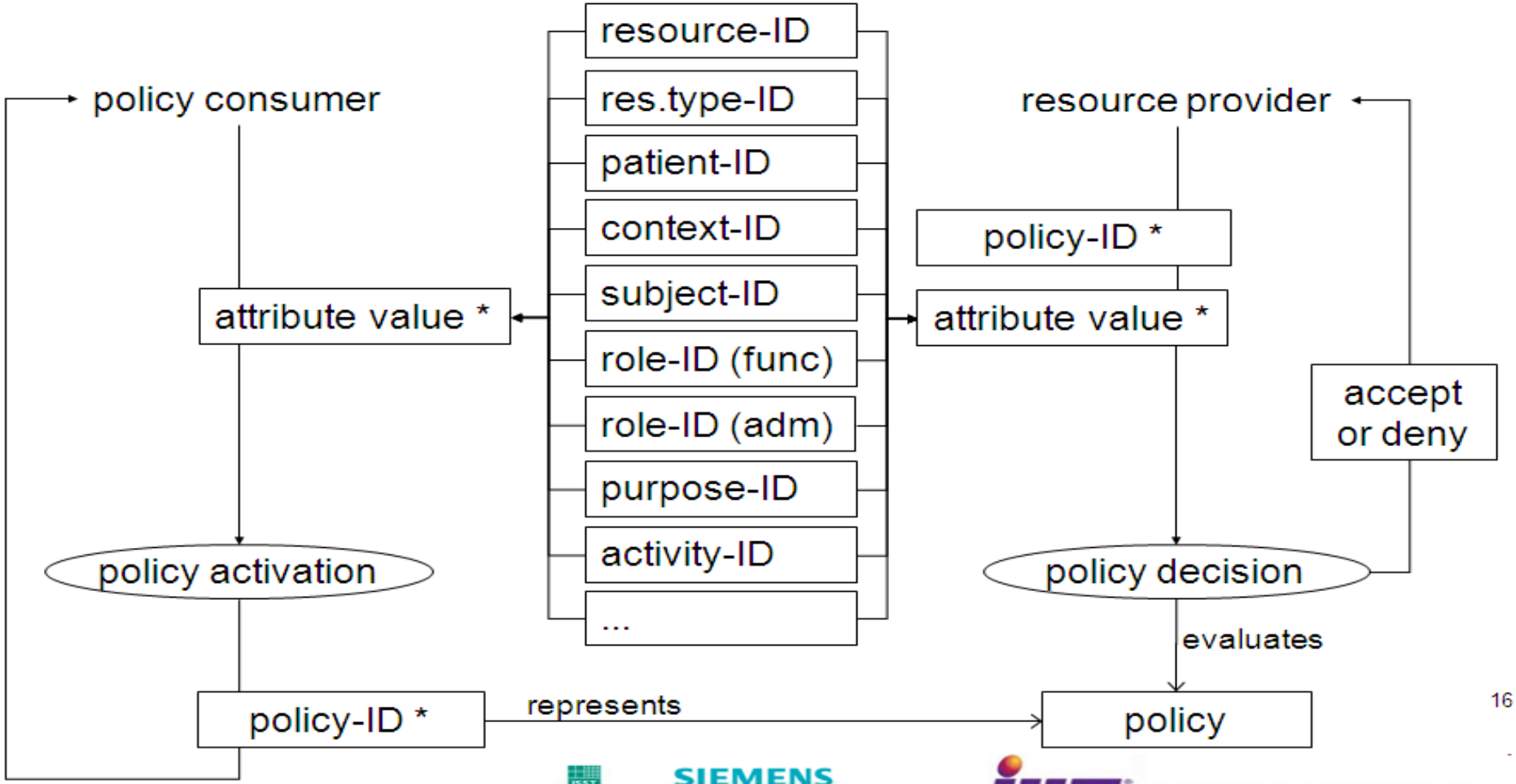
ACS= Access Control Service
PEP=Policy Enforcement Point
PDP=Policy Decision Point
PDQ=Patient Data Query
PIX=Patient Identity Exchange
PWP=
STS=Security Token Service
Svc=Service
XDS=Cross Enterprise Data Service
XSPA= Cross Enterprise Security and Privacy Authorizations
XUA=Cross Enterprise User Authentication

Core Model (XSPA + externalized IdP)



Fraunhofer ISST Institut Software- und Systemtechnik
SIEMENS
Sun microsystems
IHE changing the way healthcare connects www.ihe.net

Shared Policies and Attributes



Fraunhofer ISST Institut Software- und Systemtechnik
SIEMENS
Sun microsystems
IHE changing the way healthcare connects www.ihe.net
OASIS
HITSP

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 BPPA)
- Standard Web-Service Protocols (OASIS SAML, XACML, WS-Trust)
- Standard Interoperability Profiles (OASIS XSPA, IHE)
- Implementation-ready without change to legacy systems
- Polices managed centrally, enforced locally (ASTM, ISO PMI)
- Vendor supported solutions

Roadmap to the Future

- **HL7 Standards**
  - Update to Roles (adding new vocabulary from SNOMED CT, LOINC, IDC-10)
  - Joint Security and Privacy Information Models
  - Update to Consent Directives
- **OASIS**
  - XSPA Profiles
  - WS-Federation
- **SOA/Web Services**
- **Conformance Testing through IHE**

Conclusion

Secretary Health and Human Services Security and Privacy Framework is realizable

Things are Good Enough

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

Booth 7750

Participants

Booth 7750

Working to Meet the Privacy Needs of the Nation Today

- Jericho
- Red Hat
- Sun
- U.S. Department of Defense
- U.S. Department of Veterans Affairs