

XSPA

Cross-Enterprise Security and Privacy Authorization

HIMSS 2009 Playbook

TP/20 describes framework for cross-enterprise authorization interoperability in healthcare data exchange.

XSPA Profiles describe a minimum set of subject and resource attributes necessary to perform a cross-enterprise access control decision between two Healthcare organizations.

- Demonstrate the Enforcement of Patient Consent Directives
 - Opt-In / Opt-Out
 - Allowed Organizations
 - Confidentiality Codes (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
 - Required certain roles based on purpose of use and service requested
 - Require certain permissions based on purpose of use and service requested

SERVICE USER (REQUESTOR)

- Domain A – the TP20 Service User (Requestor), is not a production system but is representative of a light Electronic Health Record or Provider Portal
- The requestor is representative of a legacy implementation that has been TP20 enable and supports the cross-domain dialogue between healthcare organizations as described by the XSPA profiles of SAML and WS-TRUST
- It has its own internally roles and permissions and Access Control System based on XACML Interops of RSA2008 and Ditton Manor London England (Sun Microsystems provide ACS)

SERVICE PROVIDER (RESPONDER)

- Domain B – the TP20 Service Provider (Responder), is representative of a production implementation at a component level, i.e., Service Provider, Assertion Handler, PEP, PIP, PDP, Attribute Services, and Data Masking Subsystem
- Domain B – Understand how to consume and produce an access control decision based on the XSPA Profiles of SAML and WS-TRUST
- It offers 2 services – patient discovery and getMedicalRecord which returns the opted-in clinical summary
- The Domain B Service provider wraps, or TP20 enables, a DoD developed Document Assembler from the December demonstrations of NHIN (this was an implementation specific decision, the Service provider could just as easily wrap the NHIN Federal Adapter)

Participant Technologies

Jericho Systems and Red Hat

- 1) Implement the XSPA Profile of XACML
- 2) Control all aspects of PHI data delivery outside of the Domain B Healthcare Enterprise
- 3) Share and consume a common XACML Policy

Sun Microsystems

- 1) Delivers standard based interface libraries to produce XACML request and consume its response
- 2) Provide Circle of Trust for PDPs that conform to the XSPA Profile of XACML

Dept. of Veterans Affairs

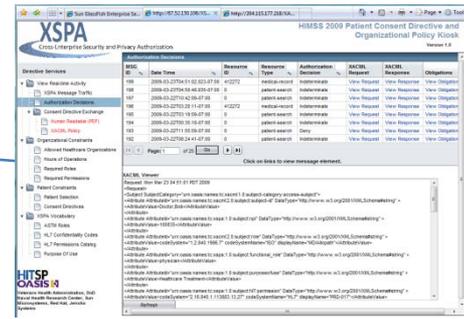
- 1) Delivers the TP20 Service Provider wrapper/enabler
- 2) Provides ability to consume a Subject and Resource assertion as described by XSPA Profiles of SAML and WS-TRUST
- 3) Provides ability to augment Subject and Resource assertion with organizational policies and patient consent directives
- 4) Provides Enforcement of PDP decision
- 5) Delivers Obligations to Service Provider

Dept. of Defense Naval Health Research Center

- 1) Integrate with TP20 Service Provider
- 2) Generate and deliver NHIN C32 Compliant Clinical Summary
- 3) Consume and Enforce Data Masking obligations from TP20 Service Provider



XSPA Profiles
of
SAML and WS-Trust



XSPA Profile
of
XACML

HITSP TP/20 – Service User

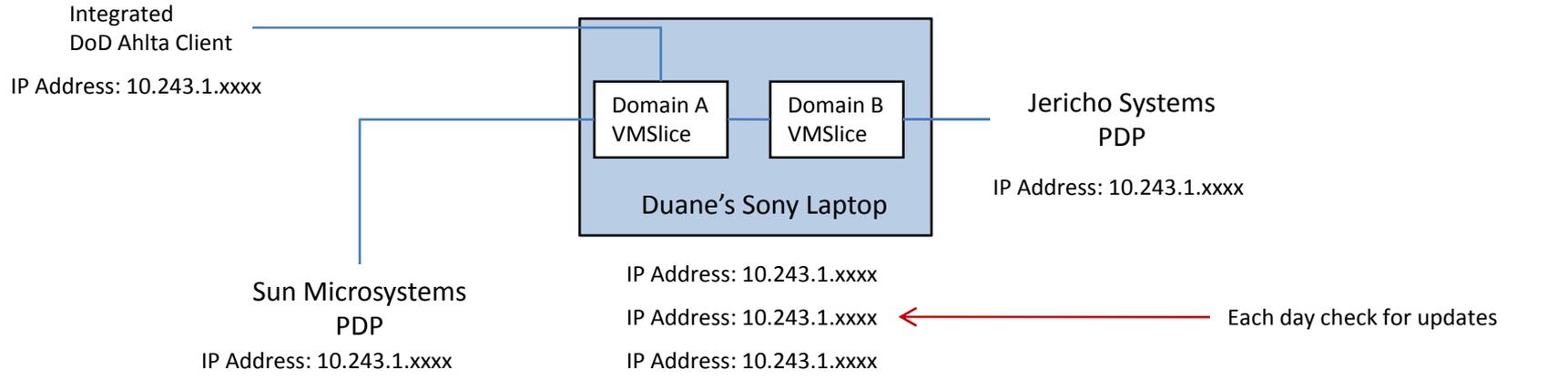
<http://10.243.1.xxx/XACMLPatientPrivacy>

HITSP TP/20 – Service Provider

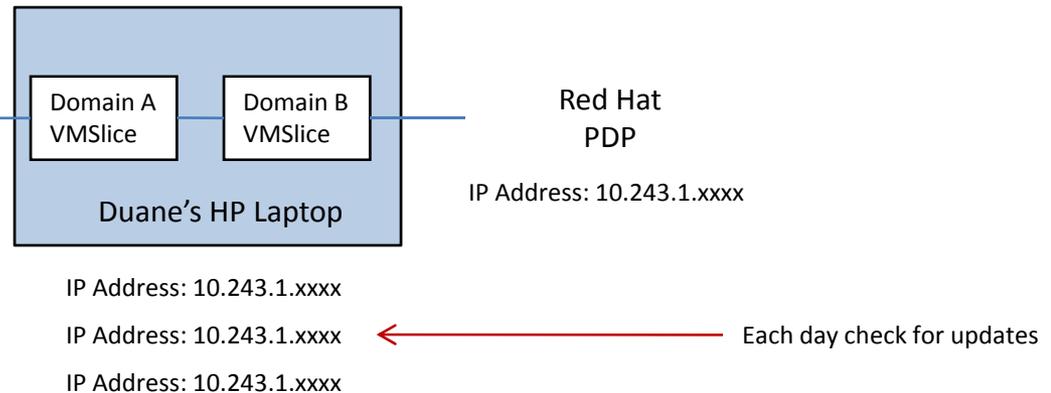
<http://10.243.1.xxx/XSPASecurityServices>

TESTBED TOPOLOGY

Testbed A

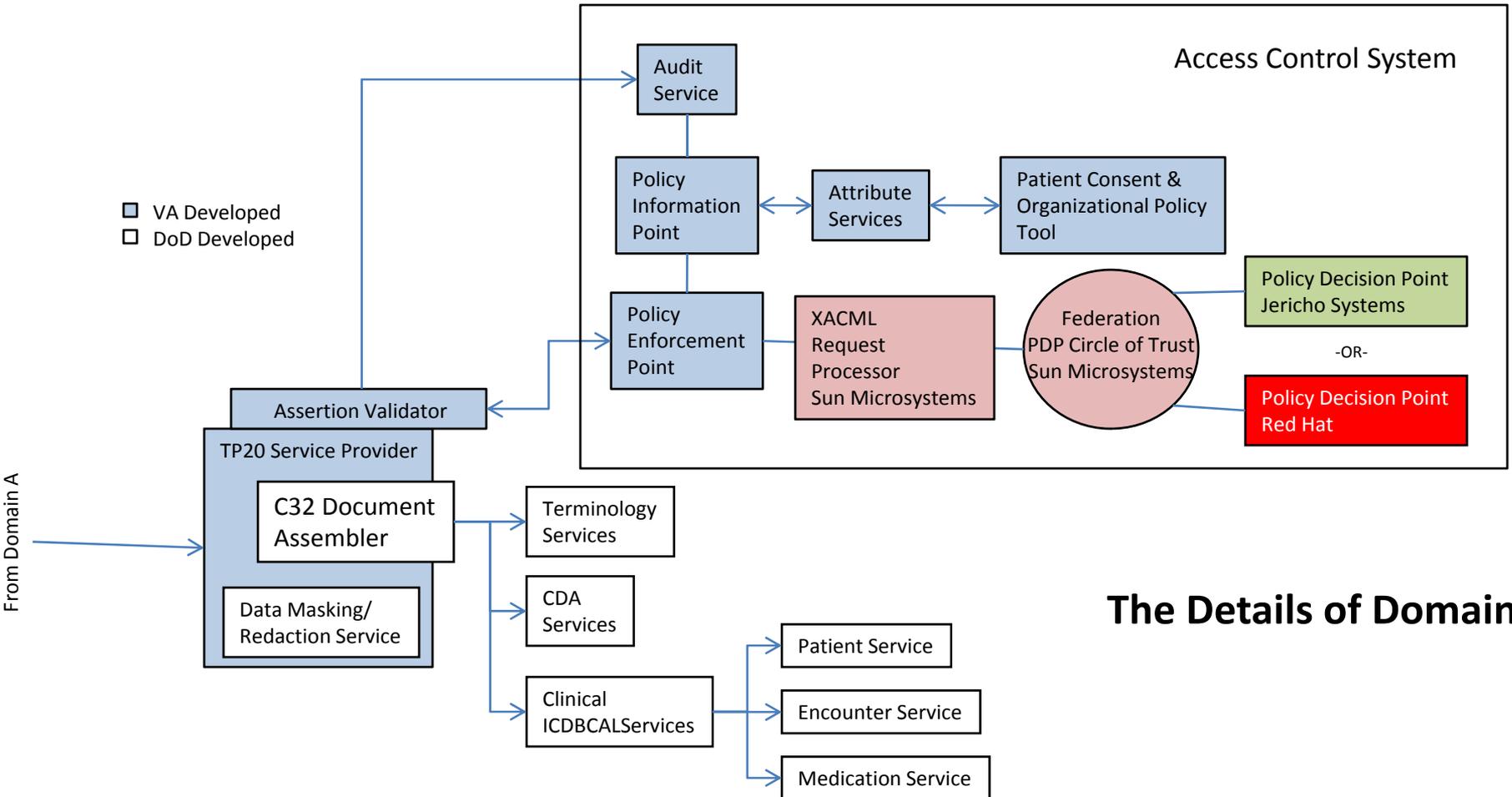


Testbed B



Schedule:
April 4-7 XSPA Profile of SAML
April 8 XSPA Profile of WS-TRUST

TESTBED TOPOLOGY



The Details of Domain B

XSPA
Cross-Enterprise Security and Privacy Authorization

HIMSS 2009 Patient Consent Directive and Organizational Policy Kiosk
Version 1.0

Name: SMITH, BAMBI Facility: Healthcare Domain B
Gender: Male Female Date of Birth: 19520625

Directive Services

- View Real-time Activity
 - XSPA Message Traffic
 - Authorization Decisions
 - Consent Directive Exchange
 - Human Readable (PDF)
 - XACML Policy
- HL7 Confidentiality Codes
- HL7 Permissions Catalog
- Purpose Of Use

Consent Options:

- Patient wishes to participate in Cross-Enterprise exchange of their health record.
- Patient DOES NOT wish to participate in Cross-Enterprise exchange of their health record.

Consent Options (highlighted in red box):

- Patient Must Opt-In To be visible to Patient Discovery Service
- Patient Can Constrain access to Healthcare domains that Domain B exchanges with
- Patient Can Set High Level Constraints through use of HL7 Confidentiality Codes
- Patient Can Control Access to Specific Roles based on Purpose of Use, or Constrain Access of Specific Provider
- Patient Can MASKED results of Clinical Summary based on Role or a Specific Provider

HITSP OASIS
Veterans Health Administration, DoD
Naval Health Research Center, Sun
Microsystems, Red Hat, Jericho
Systems

- 1) Click on the "Patient Consents" tree node a list of those patient who have opted-in will appear.

The screenshot shows the XSPA web application interface. The browser address bar displays the URL <http://10.243.1.42/XSPA...>. The page title is "HIMSS 2009 Patient Consent Directive and Organizational Policies" for the "Healthcare Domain B".

The left sidebar contains a "Directive Services" tree with the following nodes:

- View Real-time Activity
 - XSPA Message Traffic
 - Authorization Decisions
- Consent Directive Exchange
 - Human Readable (PDF)
 - XACML Policy
- Organizational Constraints
 - Allowed Healthcare Organizations
 - Hours of Operations
 - Required Roles
 - Required Permissions
- Patient Constraints** (highlighted)
 - Patient Selection
 - Consent Directives
- XSPA Vocabulary
 - ASTM Roles
 - HL7 Confidentiality Codes
 - HL7 Permissions Catalog
 - Purpose Of Use

The main content area is titled "Patients Constraints" and displays a table of "Patients who have Opted-In".

| Patient MPI | Last Name | First Name | Gender | DoB | Opt-In Date |
|-------------|-------------|------------|--------|----------|-------------|
| 97371 | DAVIS | BAMBI | F | 19430120 | 03/25/2009 |
| 661856 | DURHAM | LARRY | M | 20030209 | 03/23/2009 |
| 359324 | JOHNSON | ANNA | F | 19852108 | 03/12/2009 |
| 595259 | JONES | BAMBI | F | 19700504 | 03/11/2009 |
| 525872 | JONES | ELLIOT | M | 19781011 | 03/23/2009 |
| 476770 | JONES | HAROLD | M | 19700605 | 03/16/2009 |
| 498016 | NHINPATIENT | JOSEPH | M | 19761212 | 03/27/2009 |
| 412272 | SMITH | BAMBI | F | 19520625 | 03/24/2009 |
| 362122 | SMITH | JERRY | M | 19951012 | 03/16/2009 |
| 184749 | THOMAS | BAMBI | F | 19250505 | 03/15/2009 |
| 302259 | THOMAS | LARRY | M | 19721507 | 03/13/2009 |

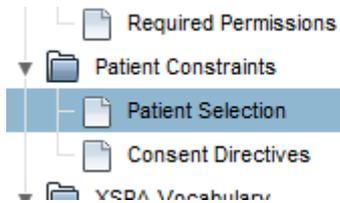
Below the table is a "Refresh" button and a note: "Click on Patient MPI to select and navigate to consent directive screens." A red arrow points from the "Patient Constraints" tree node to the table, and another red arrow points from the "Patient MPI" column header to the table.

At the bottom left, the HITSP OASIS logo is displayed, along with the text: "Veterans Health Administration, DoD Naval Health Research Center, Sun Microsystems, Red Hat, Jericho Systems".

At the bottom right, a small watermark reads: "Microsoft PowerPoint non-commercial use (Trie...".

- 2) Select PATIENT by clicking on Their MPI link. This will direct you To the Patient Consent Directive Screens.

Add New Patient Consent Directive Opt-In - #1



1) Click on PATIENT SELECTION

2) ENTER IN LASTNAME AND FIRSTNAME CLICK ON SEARCH

Form fields for patient search:

Lastname Firstname

| Patient MPI | Name | Gender | Date of Birth | Address |
|------------------------|-------------|--------|------------------------------|--|
| 412272 | SMITH,BAMBI | F | Wed Jun 25 09:21:46 PDT 1952 | 123 ANYPLACE DR null ANY CITY USA ANYSTATE 12345 |

Click on MPI to select patient.

3) CLICK ON MPI, THIS SELECTS PATIENT AND NAVIGATE YOU TO PATIENT CONSENT DIRECTIVE SCREENS

Add New Patient Consent Directive Opt-In - #2

- 1) Click on Option "Patient wishes..."
- 2) Click on Save Changes to commit
- 3) Note: the inverse is true to Opt-Patient out. Their patient consent directive if it exist is not deleted, so opting back in restore previous state.

The screenshot displays the XSPA web application interface. The browser window shows the URL <http://10.243.1.107/X...> and <http://10.243.1.42/...>. The page title is "HIMSS 2009 Patient Consent Directive and Organizational Policies" for "Healthcare Domain B".

The main content area shows a form for a patient named "WANICKI, HAROLD" with facility "Healthcare Domain B", gender "Male", and date of birth "10/28/1946". The "Patient Participation" tab is active, showing two radio button options:

- Patient wishes to participate in Cross-Enterprise exchange of their health record.
- Patient DOES NOT wish to participate in Cross-Enterprise exchange of their health record.

A "Save Changes" button is located below the options. The left sidebar contains a tree view of "Directive Services" with "Patient Selection" selected. Red arrows point from the text in step 3 to the "Patient Selection" folder and the "Save Changes" button.

HIMSS 2009 Patient Consent Directive and Organizational Policy Kiosk
Version 1.0

Name: SMITH, BAMBI Facility: Healthcare Domain B
Gender: Male Female Date of Birth: 19520625

Directive Services

- View Real-time Activity
 - XSPA Message Traffic
 - Authorization Decisions
- Consent Directive Exchange
 - Human Readable (PDF)
 - XACML Policy
- Organizational Constraints
 - Allowed Healthcare Organizations
 - Hours of Operations

Organizations Patient Wishes to Allow Access

| Patient Selected | Organization Name | Contact Name | Phone Number | Is Available For Exchange |
|-------------------------------------|-------------------------|-----------------|--------------|-------------------------------------|
| <input checked="" type="checkbox"/> | Healthcare Domain A | Duane DeCouteau | 4065551212 | <input checked="" type="checkbox"/> |
| <input checked="" type="checkbox"/> | DoD Healthcare Domain A | CDR Emory Fry | 8585551212 | <input checked="" type="checkbox"/> |

Click on Organization name to select.

Select Organization: Healthcare Domain A

Save Changes Delete Permission Reset Selections

HITSP OASIS
Veterans Health Administration, DoD
Naval Health Research Center, Sun
Microsystems, Red Hat, Jericho
Systems

Patient can limit access based on requesting organization, only organizations Domain B that have been setup at the in "Organizational Constraints" are available to patient.

XSPA
Cross-Enterprise Security and Privacy Authorization

HIMSS 2009 Patient Consent Directive and Organizational Policy Kiosk
Version 1.0

Name: SMITH, BAMBI Facility: Healthcare Domain B
Gender: Male Female Date of Birth: 19520625

Directive Services

- View Real-time Activity
 - XSPA Message Traffic
 - Authorization Decisions
 - Consent Directive Exchange
 - Human Readable (PDF)
 - XACML Policy
 - Organizational Constraints
 - Allowed Healthcare Organizations
 - Hours of Operations
 - Required Roles
 - Required Permissions
 - Patient Constraints
 - Patient Selection

Confidentiality

- By default the patient will participate in normal healthcare operations (N).
- Patient wishes to limit access to specific providers and/or structured roles (UBA).
- Patient wishes to limit access to certain healthcare objects, i.e., medication, lab results, diagnosis etc., (MA).
- Patient requires heightened access controls on sensitive results (S).

Save Changes

HITSP OASIS
Veterans Health Administration, DoD
Naval Health Research Center, Sun
Microsystems, Red Hat, Jericho
Systems

Confidentiality is based on the HL7 Confidentiality Codes
NOTE: If a PATIENT chooses "S" for Sensitive control it will result in immediate DENY as masking service for hiding data base on results is Not implemented on our testbed...this however is not to say it could not be done..

Patient Consent Directive – UBA Constraint Based on Role and Purpose of Use

Limit Access by Role
Allows patient ability to DENY Access
Based on a users ASTM Role and Purpose of Use.

HIMSS 2009 Patient Consent Directive and Organizational Policy Kiosk
Version 1.0

Name: SMITH, BAMBI Facility: Healthcare Domain B
Gender: Male Female Date of Birth: 19520625

Patient Participation | Allowed Organizations | Confidentiality | Control Access to Providers | Control Access to Objects | View Directive

Limit Access by Role | Limit Access by Provider

| Structured Role | Purpose of Use |
|-----------------|----------------------|
| Pharmacist | Healthcare Treatment |

Click on Structured Role to select.

Purpose of Use: Healthcare Treatment
Structured Role: Administration - Health Records (Medical Records)/Health Information Management Department

Add Delete Reset

HITSP OASIS
Veterans Health Administration, DoD
Naval Health Research Center, Sun
Microsystems, Red Hat, Jericho
Systems

These are evaluated in the XACML policies as;
urn:oasis:names:tc:xspa:1.0:resource:patient:dissenting-role

Patient Consent Directive – UBA Constraint Based on a Specific Provider

Limited Access by Provider
Allows patient to DENY
access
To a specific provider.

HIMSS 2009 Patient Consent Directive and Organizational Policy Kiosk
Version 1.0

Name: SMITH, BAMBI Facility: Healthcare Domain B
Gender: Male Female Date of Birth: 19520625

Directives: Patient Participation | Allowed Organizations | Confidentiality | Control Access to Providers | Control Access to Objects | View Directive

Limit Access by Role | **Limit Access by Provider**

| NPI | Provider Name | Primary Location |
|--------|-----------------|---------------------|
| 100017 | Doctor, Alice O | Facility A |
| 100035 | Doctor, Bob | Healthcare Domain A |
| 400000 | Doctor, Alice | Healthcare Domain A |

Click on NPI to select.

Provider Name: Doctor, Bob H NPI: Location:

Add Delete Reset

These are evaluated in the XACML policies as;
urn:oasis:names:tc:xspa:1.0:resource:patient:dissenting-subject-id

Patient Consent Directive – MA Constraint Masking Based on Role

Deny Object Access by Role
Allows patient to DENY access
To a specific healthcare object based
On the requestors structured ASTM role.

The screenshot shows the XSPA web application interface. At the top, there is a navigation bar with the XSPA logo and the text "HIMSS 2009 Patient Consent Directive and Organizational Policy Kiosk Version 1.0". Below this, there is a patient information form with fields for Name (SMITH_BAMBI), Facility (Healthcare Domain B), Gender (Female), and Date of Birth (19520625). The main content area is divided into several tabs: Patient Participation, Allowed Organizations, Confidentiality, Control Access to Providers, Control Access to Objects, and View Directive. The "Control Access to Objects" tab is active, showing a sub-tab for "Deny Object Access by Role". Below this, there is a table with two columns: "Structured Role" and "Healthcare Object". The table contains one entry: "Pharmacist" under "Structured Role" and "Problems" under "Healthcare Object". Below the table, there is a button labeled "Click on Structured Role to select." At the bottom of the page, there is a form with a "Structured Role" dropdown menu (set to "Administration - Health Records (Medical Records)/Health Information Management Department") and a "Healthcare Object" dropdown menu (set to "Alerts"). There are also "Add", "Delete", and "Reset" buttons. A red box highlights the "Deny Object Access by Role" sub-tab and the table entry. Another red box highlights the text "These are evaluated in the XACML policies as; urn:oasis:names:tc:xspa:1.0:resource:patient:masked:'healthcareobject':dissenting-role".

| Structured Role | Healthcare Object |
|-----------------|-------------------|
| Pharmacist | Problems |

Click on Structured Role to select.

Structured Role: Administration - Health Records (Medical Records)/Health Information Management Department

Healthcare Object: Alerts

Add Delete Reset

These are evaluated in the XACML policies as;
urn:oasis:names:tc:xspa:1.0:resource:patient:masked:'healthcareobject':dissenting-role

Patient Consent Directive – MA Constraint Masking Based on Specific Provider

The screenshot displays the XSPA web application interface. The top navigation bar includes the XSPA logo and the title "HIMSS 2009 Patient Consent Directive and Organizational Policy Kiosk Version 1.0". The main content area is divided into several sections:

- Directive Services:** Includes "View Real-time Activity" and "XSPA Message Traffic".
- Organizational Constraints:** Includes "Allowed Healthcare Organizations", "Hours of Operations", "Required Roles", and "Required Permissions".
- Patient Constraints:** Includes "Patient Selection", "Consent Directives", "XSPA Vocabulary", "ASTM Roles", "HL7 Confidentiality Codes", "HL7 Permissions Catalog", and "Purpose Of Use".

The "Patient Constraints" section is currently selected, showing a form for "Deny Object Access by Provider". The form includes fields for "Name" (SMITH, BAMBI), "Facility" (Healthcare Domain B), "Gender" (Male/Female), and "Date of Birth" (19520625). Below the form is a table with the following data:

| NPI | Provider Name | Primary Location | Healthcare Object |
|--------|-------------------|---------------------|-------------------|
| 100027 | Doctor, Charlie S | Facility B | Medications |
| 100036 | Doctor, Alice | Healthcare Domain A | Problems |

Below the table is a text box containing the XACML policy evaluation string: `urn:oasis:names:tc:xspa:1.0:resource:patient:masked:"healthcareobject":dissenting-subject-id`. At the bottom of the form are "Add", "Delete", and "Reset" buttons.

Deny Object Access by Provider
Allows the patient to DENY access to specific Healthcare objects to specific Providers.

These are evaluated in the XACML policies as;
`urn:oasis:names:tc:xspa:1.0:resource:patient:masked:"healthcareobject":dissenting-subject-id`

Patient Consent Directive – TP30 Viewing Directive

The screenshot displays the XSPA web application interface. The browser's address bar shows two URLs: `http://67.52.150.106/XS...` and `http://204.115.177.218/XA...`. The application header includes the XSPA logo and the text "Cross-Enterprise Security and Privacy Authorization". On the right side of the header, it says "HIMSS 2009 Patient Consent Directive and Organizational Policy Kiosk" and "Version 1.0".

The main content area is divided into a left sidebar and a main panel. The sidebar, titled "Directive Services", contains a tree view with the following items: View Real-time Activity, XSPA Message Traffic, Authorization Decisions, Consent Directive Exchange (highlighted with a red circle), Organizational Constraints, Patient Constraints, and XSPA Vocabulary. Under "Consent Directive Exchange", there are two sub-items: "Human Readable (PDF)" and "XACML Policy", both also circled in red. A red box labeled "PART of Future HITSP TP30 demonstration" has arrows pointing to these two items.

The main panel shows patient information for "SMITH, BAMBI" at "Healthcare Domain B". Below this, there are tabs for "Patient Participation", "Allowed Organizations", "Confidentiality", "Control Access to Providers", "Control Access to Objects", and "View Directive" (circled in red). The "Deny Object Access by Provider" tab is active, displaying a table with the following data:

| NPI | Provider Name | Primary Location | Healthcare Object |
|--------|-------------------|---------------------|-------------------|
| 100027 | Doctor, Charlie S | Facility B | Medications |
| 100036 | Doctor, Alice | Healthcare Domain A | Problems |

Below the table, there is a note: "Click on NPI to select." At the bottom of the main panel, there are input fields for "Provider Name" (set to "Doctor, Bob H"), "NPI", and "Location", along with a "Healthcare Object" dropdown (set to "Alerts"). There are also "Add", "Delete", and "Reset" buttons.

At the bottom left of the application, there is a logo for "HITSP OASIS" and the text: "Veterans Health Administration, DoD Naval Health Research Center, Sun Microsystems, Red Hat, Jericho Systems".

Organizational Constraints

Allowed Organizations

Provides control over which participating organizations.
This is evaluated in the XACML policies as;
`urn:oasis:names:tc:xspa:1.0:resource:org:allowed-organizations`

The screenshot shows the XSPA web application interface. On the left is a navigation tree with 'Organizational Constraints' expanded to 'Allowed Healthcare Organizations'. The main area displays a table of participating organizations:

| ID | Name | OID | Active | Contact | Phone Number |
|----|-------------------------|-----------|-------------------------------------|-----------------|--------------|
| 1 | Healthcare Domain A | 1.0.0.0.1 | <input checked="" type="checkbox"/> | Diane DeCouture | 405551212 |
| 3 | DoD Healthcare Domain A | 1.0.0.0.2 | <input checked="" type="checkbox"/> | CDR Emery Fry | 656551212 |

Below the table is a form for adding a new organization with fields for Name, Organization ID, OID, Contact, and Phone #, along with an 'Active' checkbox and 'Add', 'Update', 'Delete', and 'Reset Form' buttons.

Hours of Operation

Provides control over when services are available
This is evaluated in the XACML policies as;
`urn:oasis:names:tc:xspa:1.0:resource:org:hoursofoperation:start`
`urn:oasis:names:tc:xspa:1.0:resource:org:hoursofoperation:end`

The screenshot shows the XSPA web application interface. On the left is a navigation tree with 'Organizational Constraints' expanded to 'Hours of Operations'. The main area displays a table of hours of operations:

| Operations ID | Day of Week | Start Time | End Time |
|---------------|-------------|------------|----------|
| 1 | Sunday | 00:00 | 23:59 |
| 2 | Monday | 00:00 | 23:59 |
| 3 | Tuesday | 00:00 | 23:59 |
| 4 | Wednesday | 00:00 | 23:59 |
| 5 | Thursday | 00:00 | 23:59 |
| 6 | Friday | 00:00 | 23:59 |
| 7 | Saturday | 00:00 | 23:59 |

Below the table is a form for adding a new operation with fields for Operations ID, Day of Week, Start time, and End time, along with 'Add', 'Update', 'Delete', and 'Reset Form' buttons.

Organizational Constraints

Required Roles

Allows organization to control who has access to specific Services based on their structured role and purpose of use. These are evaluated in the XACML policies as;
`urn:oasis:names:tc:xspa:1.0:resource:org:role`

The screenshot shows the XSPA web interface with the 'Required Roles' configuration page. The left sidebar contains a tree view with 'Required Roles' selected. The main content area features a table of roles and a form below it.

| Rule ID | Service Provider Object | Purpose of Use | Structured Role |
|---------|-------------------------|----------------------|-----------------|
| 1 | patient-search | Healthcare Treatment | MDA/IpPath |
| 2 | medical-record | Healthcare Treatment | MDA/IpPath |
| 3 | patient-search | Healthcare Treatment | Pharmacist |

Below the table, there is a form with the following fields:
Rule ID:
Purpose of Use: Healthcare Treatment (dropdown)
Service Provider Object: Patient Discovery (dropdown)
Structured Role: Administration - Health Records (Medic) (dropdown)
Buttons: Add, Copy, Reset Form

Required Permissions

Allows organization to set required permissions for a specific service. These are evaluated in the XACML policies as;
`urn:oasis:names:tc:xspa:1.0:resource:org:hl7:permission`

The screenshot shows the XSPA web interface with the 'Required Permissions' configuration page. The left sidebar contains a tree view with 'Required Permissions' selected. The main content area features a table of permissions and a form below it.

| Rule ID | Purpose of Use | Service Provider Object | Required Permission |
|---------|----------------------|-------------------------|---------------------|
| 2 | Healthcare Treatment | medical-record | PRD-003 |
| 3 | Healthcare Treatment | medical-record | PRD-010 |
| 4 | Healthcare Treatment | medical-record | PRD-005 |
| 6 | Healthcare Treatment | patient-search | PRD-006 |
| 7 | Emergency Treatment | patient-search | PRD-006 |

Below the table, there is a form with the following fields:
Rule ID:
Purpose of Use: (dropdown)
Service Object: Patient Discovery (dropdown)
Permission: PRD-003 (dropdown)
Healthcare Object:
Action:
Buttons: Add, Copy, Reset Form

The screenshot shows the XSPA web application interface. The top navigation bar includes the XSPA logo, the title "HIMSS 2009 Cross-Enterprise Security and Privacy Authorization Testbed", and user information: "PDP Provided By: Sun Microsystems", "Doctor, Bob", "Healthcare Domain A", and "Version: 2.0".

The main content area is divided into two sections. The left section, titled "Patient Info", contains a form with the following fields:

- Name: SMITH, BAMBI
- Gender: Male Female
- DoB: 1952-06-25T00:00:00-07:00
- Facility: Healthcare Domain A

The right section, titled "Recent Cross-Enterprise Messages", displays a list of messages. The most recent message is expanded, showing its XML content. A red box highlights the "View XSPA Messages" link in the left sidebar, with an arrow pointing to the expanded message content.

```
<?xml version="1.0" encoding="UTF-8"?><saml2:Assertion xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion" xmlns:ds="http://www.w3.org/2000/09/xmldsig#" xmlns:exc14n="http://www.w3.org/2001/10/xml-exc-c14n#" xmlns:xenc="http://www.w3.org/2001/04/xmenc#" xmlns:xs="http://www.w3.org/2001/XMLSchema" ID="1237809060783" issueInstant="2009-03-23T04:51:00.783-07:00" Version="20"><saml2:Issuer Format="urn:oasis:names:tc:SAML:2.0:nameid-format:X509SubjectName">CN=Doctor, Bob, OU=Healthcare Domain A, O=Veterans Health Administration, L=San Diego, ST=CA, C=US</saml2:Issuer><saml2:Subject><saml2:NameID Format="urn:oasis:names:tc:SAML:2.0:nameid-format:X509SubjectName">CN=Doctor, Bob, OU=Healthcare Domain A, O=Veterans Health Administration, L=San Diego, ST=CA, C=US</saml2:NameID><saml2:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:holder-of-key"><saml2:NameID Format="urn:oasis:names:tc:SAML:2.0:nameid-format:X509SubjectName">CN=Doctor, Bob, OU=Healthcare Domain A, O=Veterans Health Administration, L=San Diego, ST=CA, C=US</saml2:NameID><saml2:SubjectConfirmationData><ds:KeyInfo><ds:KeyValue><ds:RSAKeyValue><ds:Modulus>vYxVZKlzVdGMSBKw4bYnV80MV/RgQKV1bfDoMTX8laMO45P6rEarxQIOYrgzuYp+snz22XM0S6o3JGQtXQuzDwccwPkH55bHFwHgtOMzxG4SQ653a5Dzh04nsmJvxbncNH/XaWfhaC0JHBEINCMwRebYocxYM92pq/G5OGyE=</ds:Modulus><ds:Exponent>AQAB</ds:Exponent></ds:RSAKeyValue></ds:KeyInfo></saml2:SubjectConfirmationData></saml2:SubjectConfirmation></saml2:Subject><saml2:Conditions NotBefore="2009-03-23T03:51:00.783-07:00" NotOnOrAfter="2009-03-23T05:51:00.783-07:00"/><saml2:AttributeStatement><saml2:Attribute Name="urn:oasis:names:tc:xacml:2.0:subject:subject-id"><saml2:AttributeValue xmlns:ns6="http://www.w3.org/2001/XMLSchema-instance" xmlns:ns7="http://www.w3.org/2001/XMLSchema" ns6:type="ns7:string">Doctor, Bob</saml2:AttributeValue></saml2:Attribute><saml2:Attribute Name="urn:oasis:names:tc:xacml:1.0:subject:np"><saml2:AttributeValue xmlns:ns6="http://www.w3.org/2001/XMLSchema-instance" xmlns:ns7="http://www.w3.org/2001/XMLSchema" ns6:type="ns7:string">100035</saml2:AttributeValue></saml2:Attribute><saml2:Attribute Name="urn:oasis:names:tc:xacml:2.0:subject:locality"><saml2:AttributeValue xmlns:ns6="http://www.w3.org/2001/XMLSchema-instance" xmlns:ns7="http://www.w3.org/2001/XMLSchema" ns6:type="ns7:string">Healthcare Domain A</saml2:AttributeValue></saml2:Attribute><saml2:Attribute Name="urn:oasis:names:tc:xacml:2.0:subject:role"><saml2:AttributeValue xmlns:ns6="http://www.w3.org/2001/XMLSchema-instance" xmlns:ns7="http://www.w3.org/2001/XMLSchema" ns6:type="ns7:string">codeSystem="1.2.840.1986.7" codeSystemName="ISO" displayName="MD/Allopath"</saml2:AttributeValue></saml2:Attribute><saml2:Attribute Name="urn:oasis:names:tc:xspa:1.0:subject:functional_role"><saml2:AttributeValue xmlns:ns6="http://www.w3.org/2001/XMLSchema-instance" xmlns:ns7="http://www.w3.org/2001/XMLSchema" ns6:type="ns7:string">physician</saml2:AttributeValue></saml2:Attribute><saml2:Attribute Name="urn:oasis:names:tc:xspa:1.0:subject:purposefuse"><saml2:AttributeValue xmlns:ns6="http://www.w3.org/2001/XMLSchema-instance" xmlns:ns7="http://www.w3.org/2001/XMLSchema" ns6:type="ns7:string">Healthcare Treatment</saml2:AttributeValue></saml2:Attribute><saml2:Attribute Name="urn:oasis:names:tc:xspa:1.0:subject:hl7.permission"><saml2:AttributeValue xmlns:ns6="http://www.w3.org/2001/XMLSchema-instance" xmlns:ns7="http://www.w3.org/2001/XMLSchema" ns6:type="ns7:string">codeSystem="2.16.840.1.113883.13.27" codeSystemName="HL7" displayName="PRD-017"</saml2:AttributeValue><saml2:AttributeValue xmlns:ns6="http://www.w3.org/2001/XMLSchema-instance" xmlns:ns7="http://www.w3.org/2001/XMLSchema" ns6:type="ns7:string">codeSystem="2.16.840.1.113883.13.27" codeSystemName="HL7" displayName="PRD-003"</saml2:AttributeValue></saml2:Attribute></saml2:AttributeStatement></saml2:Assertion>
```

Selecting View XSPA Messages
Will display the most recent request
Including the assertion of it's profiles
Attributes.

Example Interaction Between Domains

PDP delivers
Obligation to mask
medications

| MSG ID | Date Time | Resource ID | Resource Type | Authorization Decision | KACML Request | KACML Response | Obligations |
|--------|-------------------------------|-------------|----------------|------------------------|---------------|----------------|-----------------|
| 477 | 2009-03-28T01:43:27:574-07:00 | 490016 | medical-record | Permit | View Request | View Response | View Obligation |
| 478 | 2009-03-28T01:42:26:67-07:00 | 490016 | medical-record | Permit | View Request | View Response | View Obligation |
| 476 | 2009-03-28T01:24:54:57-07:00 | 490016 | medical-record | Permit | View Request | View Response | View Obligation |
| 475 | 2009-03-28T01:22:26:07-07:00 | 490016 | medical-record | Permit | View Request | View Response | View Obligation |
| 474 | 2009-03-28T01:21:58:07-07:00 | 0 | patient-search | Permit | View Request | View Response | View Obligation |
| 473 | 2009-03-28T01:09:39:07-07:00 | 490016 | medical-record | Permit | View Request | View Response | View Obligation |
| 472 | 2009-03-28T01:08:30:07-07:00 | 0 | patient-search | Permit | View Request | View Response | View Obligation |
| 471 | 2009-03-28T01:04:26:07-07:00 | 412272 | medical-record | Permit | View Request | View Response | View Obligation |

Redaction service removes the
Medications section and Service
Provider (responder) delivers
updated document

PDP Provided By: Sun Microsystems

PATIENT: JOSEPH

Female DoB: 1976-11-15T00:00:00-08:00

| Name | Gender | Date of Birth | Organization | View Consent | View Policy |
|--------|--------|---------------|---------------------|--------------------------------------|-------------------------------------|
| JOSEPH | M | 19761212 | Healthcare Domain B | View Directive - PDF | View Policy - XACML |

Name to view clinical summary below. Click on 'Consent Directive' to view patient consent directive in PDF form.

Clinical Summary Viewer

Problems

| TYPE | DESCRIPTION | DATE |
|---------|---|-----------|
| Problem | Depression | 04-JAN-08 |
| Problem | Crushing Injury Of Foot | 04-JAN-08 |
| Problem | Concussion With Brief Loss Of Consciousness | 04-JAN-08 |
| Problem | Traumatic Brain Injury (TBI) | 04-JAN-08 |

Allergies, Adverse Reactions, Alerts

| SUBSTANCE | EVENT TYPE | REACTION | SEVERITY | STATUS |
|------------|--------------|------------------|----------|--------|
| Penicillin | drug allergy | Eruption of skin | Mild | Active |

Family/Support Information

NEXT OF KIN: GUARDIAN

MOTHER: BARBARA NHINPATIENT
100 SOMEWHERE STREET
CHEROKEE, NC 28719

```
[#|2009-03-28T01:43:36.538-0700|INFO|sun-appserver2.1|javax.enterprise.system.core_1|ThreadID=18; ThreadName=httpWorkerThread-4980-0|  
***New CSZ - DOCUMENT_HASH=11cc4a2ec14e25807f5fde45e620b9931e4c1b|#|  
[#|2009-03-28T01:43:36.556-0700|WARNING|sun-appserver2.1|javax.enterprise.system.core_1|ThreadID=14; ThreadName=httpWorkerThread-80-1; RequestID=0ca57620a-421b-9215-fa01d34ed825|  
XSPAAttributeService:getPatientMostRecentObligation  
Exception Description: No transaction is currently active|#|  
[#|2009-03-28T01:43:36.564-0700|INFO|sun-appserver2.1|javax.enterprise.system.core_1|ThreadID=14; ThreadName=httpWorkerThread-80-0|  
Found section with id: 2.16.840.1.113883.10.20.1.11|#|  
[#|2009-03-28T01:43:36.566-0700|INFO|sun-appserver2.1|javax.enterprise.system.core_1|ThreadID=14; ThreadName=httpWorkerThread-80-0|  
Found section with id: 2.16.840.1.113883.10.20.1.2|#|  
[#|2009-03-28T01:43:36.564-0700|INFO|sun-appserver2.1|javax.enterprise.system.core_1|ThreadID=14; ThreadName=httpWorkerThread-80-0|  
Found section with id: 2.16.840.1.113883.10.20.1.0|#|  
[#|2009-03-28T01:43:36.566-0700|INFO|sun-appserver2.1|javax.enterprise.system.core_1|ThreadID=14; ThreadName=httpWorkerThread-80-0|  
<<text>This data was masked per patient consent directive.</text>|#|
```

In this example, the Domain B patient privacy policy restricts access so that Dr. Bob (by name or role) cannot see meds report information for patient “X” even though he is asserting authorizations granted by Domain A.

- Partners establish trust relationships between organizations
- Information owner establishes data access policies
- Patient makes policy preferences known (consent directives)(POU, UBA, MA)
- Policy and attribute stores are provisioned

- Clinician searches for patient
- Submits a request
 - Includes authorizations
 - Includes credentials
- Receives Data

- Receive request+Authn+Authz
- Determine POU and applicable policy set
- Return the response masked based on patient consent directive
- We will see the request granted.

In this example, the Domain B patient changes their privacy policy to deny all Nurses access to their medical record. Nurse Charley cannot see the patient's record even though he is asserting authorizations granted by Domain A. Nurse Charley asserts a medical emergency from Domain A and subsequently is able to see the patient's record from Domain B.

- Partners establish trust relationships between organizations
- Information owner establishes data access policies
- Patient makes policy preferences known (consent directives)(POU, UBA)
- Policy and attribute stores are provisioned

- Clinician searches for patient
- Submits a request
 - Includes authorizations
 - Includes credentials
- Receives Data
- Declares an Emergency
- Receives Data

- Receive request+Authn+Authz
- Determine POU and applicable policy set
- Return the response masked based on patient consent directive
- We will see the request granted
 - POU normal: no access to nurses in domain A
 - POU emergency: allow access to nurses in domain A