



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 internal 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

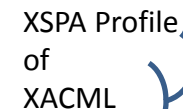
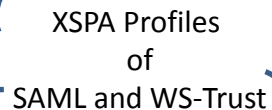
- 1) Delivers standard based interface libraries to produce XACML request and consume its response
- 2) Provide Circle of Trust for PDPs that conform to the XSPA Profile of XACML

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

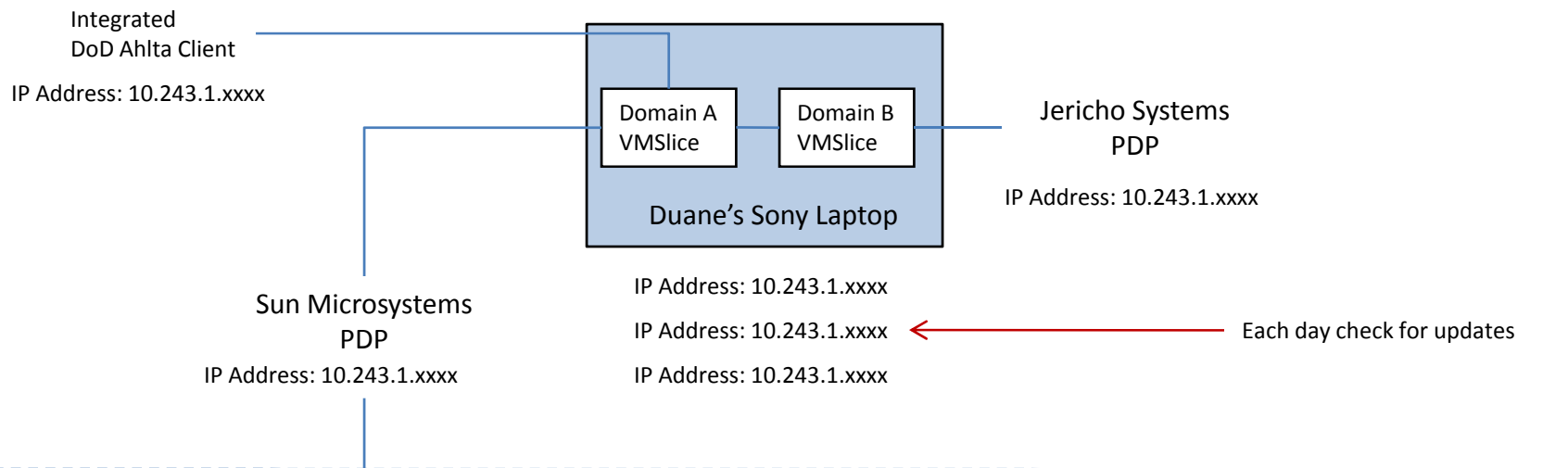
- 1) Integrate with TP20 Service Provider
- 2) Generate and deliver NHIN C32 Compliant Clinical Summary
- 3) Consume and Enforce Data Masking obligations from TP20 Service Provider



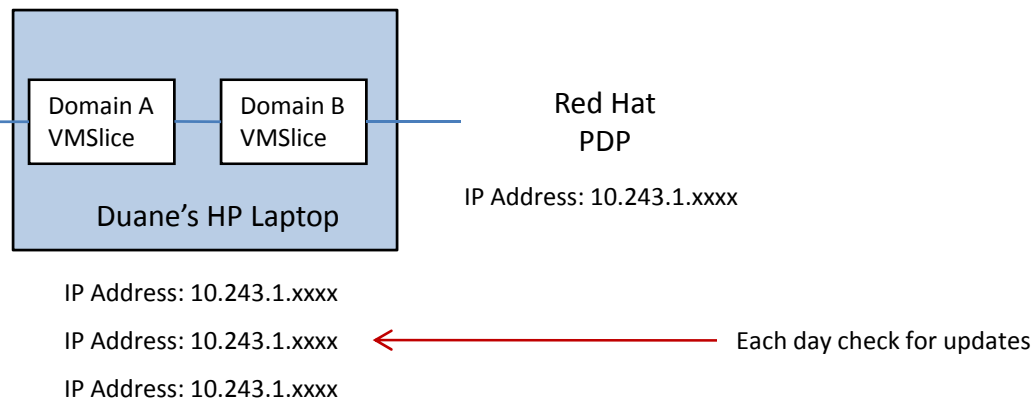
http://10.243.1.xxx/XSPA_SecurityServices

TESTBED TOPOLOGY

Testbed A



Testbed B

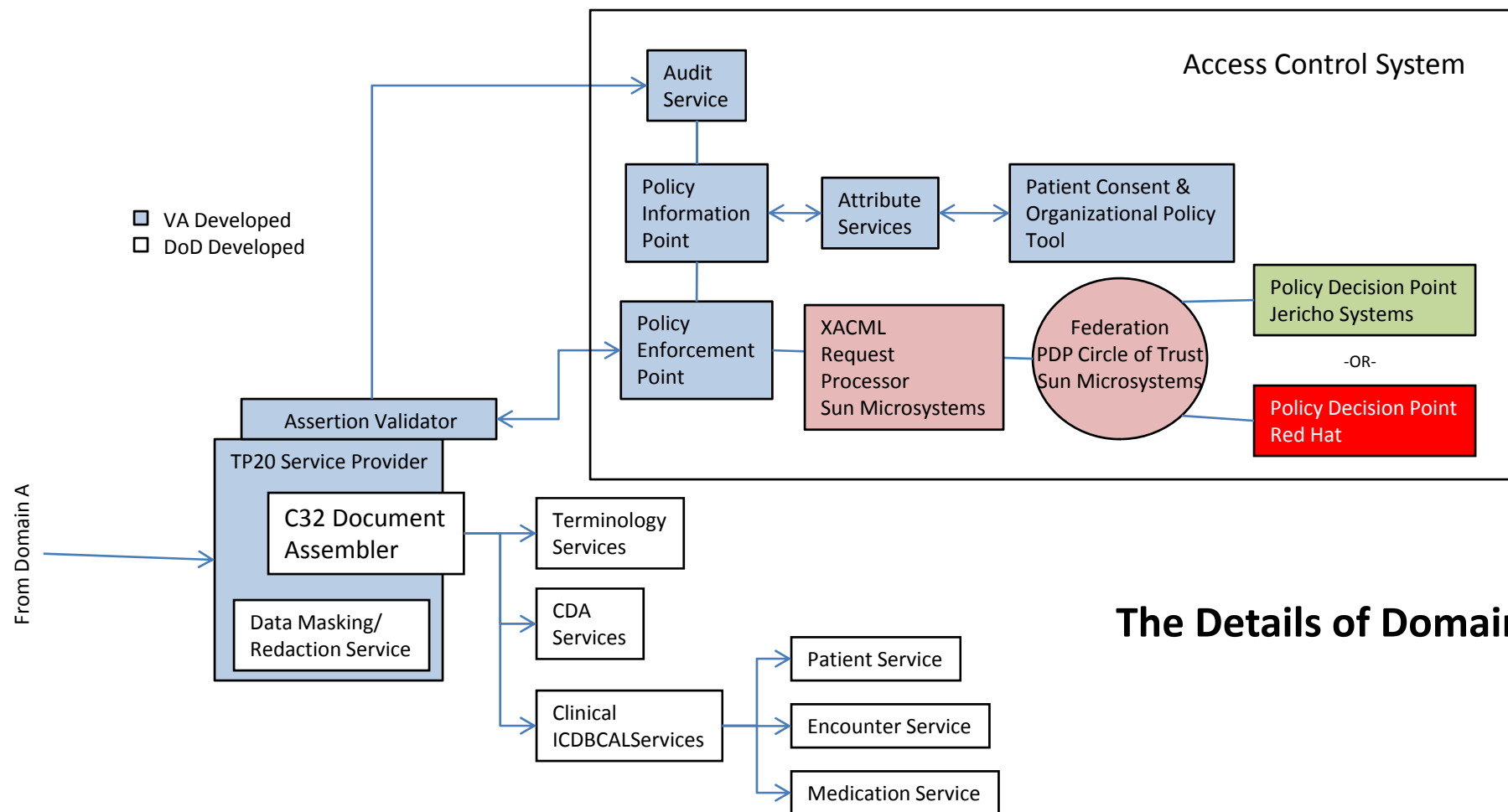


Schedule:

April 4-7 XSPA Profile of SAML

April 8 XSPA Profile of WS-TRUST

TESTBED TOPOLOGY



The Details of Domain B

Patient Consent Directive

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

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

☒ 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.

HL7 Confidentiality Codes
 HL7 Permissions Catalog
 Purpose Of Use

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.

PATIENTS WHO ALREADY OPTED-IN

HIMSS 2009 Patient Consent Directive and Organizational Policies
Healthcare Domain B

Patients Constraints

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

Click on Patient MPI to select and navigate to consent directive screens.

Refresh

Directive Services

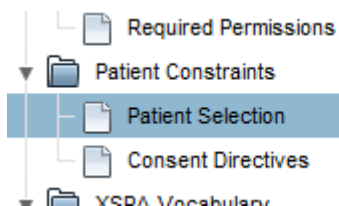
- View Real-time Activity
 - XSPA Message Traffic
 - Authorization Decisions
- Consent Directive Exchange
 - Human Readable (PDF)
 - XACML Policy
- Organizational Constraints
 - Allowed Healthcare Organizations
 - Hours of Operations
 - Required Roles
 - Required Permissions
- Patient Constraints**
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

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

Microsoft PowerPoint non-commercial use (Tri

- 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.

XSPA
Cross-Enterprise Security and Privacy Authorization

HIMSS 2009 Patient Consent Directive and Organizational Policies
Healthcare Domain B

Name: Facility:
 Gender: ☒ Male ☐ Female Date of Birth:

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**
 - Consent Directives
- XSPA Vocabulary
 - ASTM Roles
 - HL7 Confidentiality Codes
 - HL7 Permissions Catalog
 - Purpose Of Use

Patient Participation Allowed Organizations Confidentiality Control Access to Providers Control Access to Objects [View Directive](#)

☐ 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.

HITSP OASIS

XSPA
Cross-Enterprise Security and Privacy Authorization

HIMSS 2009 Patient Consent Directive and Organizational Policy Kiosk
Version 1.0

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

Patient Information

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**

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

Buttons: 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.

Patient Consent Directive

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

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

☒ 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.

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: Real-time Activity, A 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, Consent Directives

XSPA Vocabulary: ASTM Roles, HL7 Confidentiality Codes, HL7 Permissions Catalog, Purpose Of Use

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.

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

Provider Name: Doctor, Bob H NPI: Location:

Add Delete Reset

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

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.

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

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

Deny Object Access by Role Deny Object Access by Provider

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

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

Patient Consent Directive – MA Constraint Masking Based on Specific Provider

The screenshot displays the XSPA web application interface. The browser window shows the URL `http://67.52.150.106/XS...` and `http://204.115.177.218/XA...`. The application title is "HIMSS 2009 Patient Consent Directive and Organizational Policy Kiosk" with "Version 1.0".

Left Navigation Panel:

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

Main Content Area:

Name: SMITH,BAMBI **Facility:** Healthcare Domain B

Gender: ☐ Male ☒ Female **Date of Birth:** 19520625

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

Deny Object Access by Role | **Deny Object Access by Provider**

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

Click on NPI to select.

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

Form Fields:

Provider Name: Doctor, Bob H **NPI:** **Location:**

Healthcare Object: Alerts

Buttons: Add, Delete, Reset

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

Patient Consent Directive – TP30 Viewing Directive

XSPA
Cross-Enterprise Security and Privacy Authorization

HIMSS 2009 Patient Consent Directive and Organizational Policy Kiosk
Version 1.0

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
 - Consent Directives
- XSPA Vocabulary
 - ASTM Roles
 - HL7 Confidentiality Codes
 - HL7 Permissions Catalog
 - Purpose Of Use

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

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

Control Access to Objects **View Directive**

Deny Object Access by Provider

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

Click on NPI to select.

Provider Name: Doctor, Bob H **NPI:** **Location:**

Healthcare Object: Alerts

Add **Delete** **Reset**

PART of Future HITSP TP30 demonstration

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 'Allowed Healthcare Organizations' section of the XSPA application. It features a table with columns: ID, Name, OID, Active, Contact, and Phone Number. The table lists two organizations: Healthcare Domain A (OID 1.0.0.0.1) and DoD Healthcare Domain A (OID 1.0.0.0.2). Below the table is a form to add a new organization with fields for Name, Organization ID, Contact, and Phone Number, and an 'Active' checkbox. Buttons for 'Add', 'Update', 'Delete', and 'Reset Form' are at the bottom.

ID	Name	OID	Active	Contact	Phone Number
1	Healthcare Domain A	1.0.0.0.1	<input checked="" type="checkbox"/>	Duane DeCouteau	4055551212
3	DoD Healthcare Domain A	1.0.0.0.2	<input checked="" type="checkbox"/>	CDR Emery Fry	6565551212

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 'Hours of Operations' section of the XSPA application. It features a table with columns: Operations ID, Day of Week, Start Time, and End Time. The table lists seven operations for each day of the week, all with a start time of 00:00 and an end time of 23:59. Below the table is a form to add a new operation with fields for Operations ID, Day of Week, Start time, and End time, and buttons for 'Add', 'Update', 'Delete', and 'Reset Form'.

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

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

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

Click on Rule ID to view and edit.

Rule ID:
 Purpose of Use: Service Provider Object: Structured Role:

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

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

Click on Rule ID to select.

Rule ID:
 Purpose of Use: Service Object: Permission:
 Healthcare Object: Actions:

Viewing Clinical Summary

Select for Cross-domain Request of clinical summary

Select to Perform Cross-domain patient discovery

In access control decision is DENY
User may assert Purpose of Use as Emergency Treatment.

If DENIED message will appear here.

Clinical Summary from Domain B

Department of Defense
SUMMARIZATION OF EPISODE NOTE

Created on March 23, 2009
Electronically generated by Department of Defense on January 4, 2008

PATIENT: **BAMBI SMITH**
ADDRESS: 123 ANYPLACE DR
ANY CITY USA, ANYSTATE 12345
home tel:123-456-7890
work tel:123-4567

MRN: 555781366
BIRTHDATE: 25-JUN-52
SEX: Female
LANGUAGES: English (US)

Table of Contents

Family/Support Information

NEXT OF KIN
GUARDIAN

Viewing XSPA Request

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 first message is selected, and its XML content is shown in a text area. A red arrow points from the "View XSPA Messages" link in the left sidebar to the XML content.

The XML content is as follows:

```
<?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:RSAKeyValue><ds:Modulus>vYxVZKlZVdGMSBKW4bYnV80MV/RgQKV1bfDoMTX8laMO45P6rEanxQIOYrgzuYp+snz2XM0S6o3JGQdXQuZDwcwPkH55bHFwHgtOMzxG4SQ653a5Dzh04nsmJvxybncNH/XNaWfhaCQJHBEfNCMwRebYocxYM92pq/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 Name="urn:oasis:names:tc:xspa: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 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 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="1.2.840.10888.1.1.1.1" codeSystemName="HL7" displayName="MD/Allopath"</saml2:AttributeValue><saml2:Attribute Name="urn:oasis:names:tc:xspa:1.0:subject:hi7: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:Attribute Name="urn:oasis:names:tc:xspa:1.0:subject:purposeofuse"><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: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	RACML Request	RACML Response	Obligations
477	2009-03-20T01:43:27:07:00	400016	medical-record	Permit	View Request	View Response	View Obligation
476	2009-03-20T01:27:06:07:00	400016	medical-record	Permit	View Request	View Response	View Obligation
475	2009-03-20T01:22:05:07:00	400016	medical-record	Permit	View Request	View Response	View Obligation
474	2009-03-20T01:19:04:07:00	0	patient-search	Permit	View Request	View Response	View Obligation
473	2009-03-20T01:08:39:07:00	400016	medical-record	Permit	View Request	View Response	View Obligation
472	2009-03-20T01:06:30:07:00	0	patient-search	Permit	View Request	View Response	View Obligation
471	2009-03-20T01:04:26:07:00	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: 1959-11-15T00:00:00-08:00

Name	Gender	Date of Birth	Organization	View Consent	View Policy
JOSEPH, M	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

```

[2009-03-20T01:43:36.538-0700]INFO[sun-appserver2.1]java.enterprise.system
ream.out|ThreadID=13; ThreadName=httpWorkerThread-8080-0;
***New C32 - DOCUMENT HASH=110c42ec4d25807f5fde45c620b9931e4c1b1#}

[2009-03-20T01:43:36.556-0700]WARNING[sun-appserver2.1]java.enterprise.syste
ream.err|ThreadID=13; ThreadName=httpWorkerThread-80-1; RequestID=4ca5762
0a-42b-92f5-fa01334d258;
XSPAAttributeService:getPatientMostRecentObligation
Exception Description: No transaction is currently active!#}

[2009-03-20T01:43:36.564-0700]INFO[sun-appserver2.1]java.enterprise.system
ream.out|ThreadID=14; ThreadName=httpWorkerThread-80-0;
Found section with id: 2.16.840.1.113883.10.20.1.11#}

[2009-03-20T01:43:36.566-0700]INFO[sun-appserver2.1]java.enterprise.system
ream.out|ThreadID=14; ThreadName=httpWorkerThread-80-0;
Found section with id: 2.16.840.1.113883.10.20.1.2#}

[2009-03-20T01:43:36.566-0700]INFO[sun-appserver2.1]java.enterprise.system
ream.out|ThreadID=14; ThreadName=httpWorkerThread-80-0;
Found section with id: 2.16.840.1.113883.10.20.1.0#}

[2009-03-20T01:43:36.566-0700]INFO[sun-appserver2.1]java.enterprise.system
ream.out|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 sill 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