HIMSS Interop Scenarios – Demonstration of XSPA Profile of SAML

Table of Contents

1 Introduction

The OASIS Cross-Enterprise Security and Privacy Authorization (XSPA) Technical Committee was created by OASIS membership in support of the work of the Healthcare Information Technology Standards Panel (HITSP). Specifically, the Access Control Transaction Package, TP20. As part of that support, the XSPA TC has created this document describing a set of use cases for demonstrating the (XSPA) Profile of Security Assertion Markup Language (SAML) v2.0 for healthcare. TP20 and HITSP Security and Privacy Technical Note TN900 provide additional details in the protection of security and privacy in interactions between parties in the exchange of healthcare information.

An overview of interactions between parties in the exchange of healthcare information taken from TP20 is presented in Figure 1.

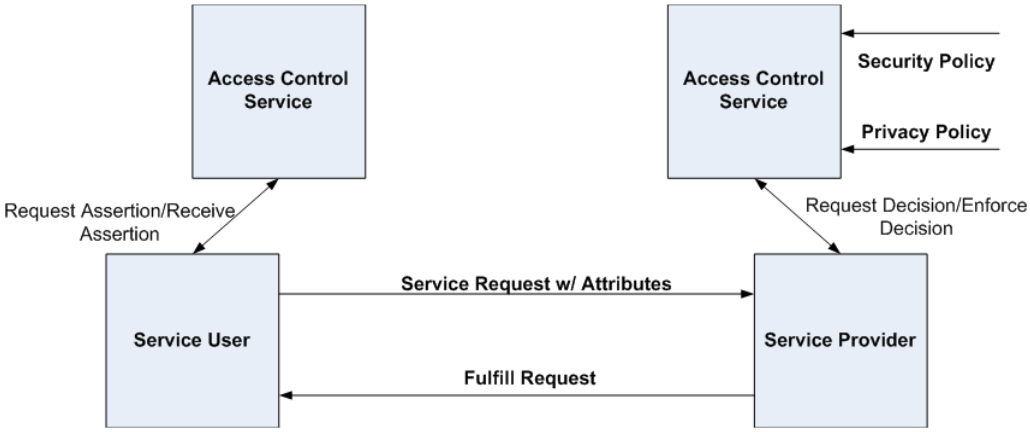

Figure 1: Interaction between Parties

Access Control Service (Service User)

The XSPA profile of SAML supports sending all requests through an Access Control Service (ACS). The Access Control Service receives the Service User request and responds with a SAML assertion containing user authorizations and attributes. To perform its function, the ACS may acquire additional attribute information related to user location, role, purpose of use, and requested resource requirements and actions.

Access Control Service (Service Provider)

The Service Provider ACS is responsible for the parsing of assertions, evaluating the assertions against the security and privacy policy, and making and enforcing a decision on behalf of the Service Provider.

Attributes

Attributes include access control information such as user location, role, purpose of use, data sensitivity, etc. necessary to make an access control decision.

Security Policy

The security policy includes the rules regarding authorizations required to access a protected resource and additional security conditions (location, time of day, cardinality, separation of duty purpose, etc.) that constrain enforcement. Matching the user attributes against the security policy provides the means to determine if access is to be permitted.

Privacy Policy

The privacy policy includes the set of patient preferences and consent directives and other privacy conditions (object masking, object filtering, user, role, purpose, etc.) that constrain enforcement. Privacy policy constraints may narrow allowable access otherwise permitted by entities complying with the security policy.

The remainder of this document describes an environment capable of supporting exchange of healthcare information consistent with TP20 and a set of use cases for demonstrating the XSPA Profile of SAML.

2 Use Case – SAML Interop

2.1 Interactions between Parties

In order to demonstrate the use cases, an environment capable of supporting exchange of healthcare information consistent with TP20 must be created. A high-level diagram of this environment is provided in Figure 2 and discussed in the following section.

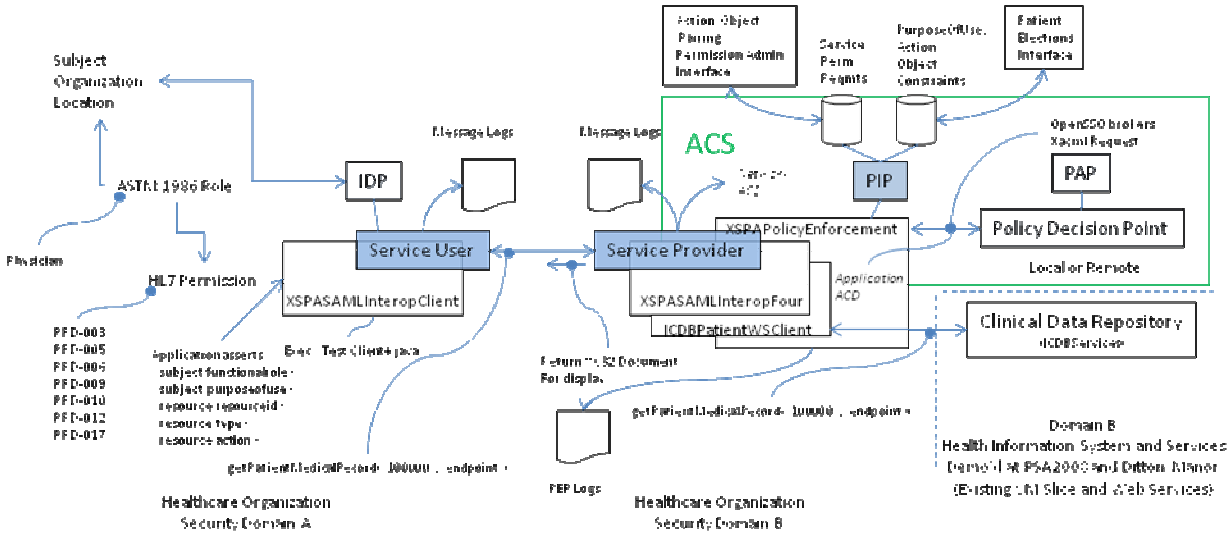

Figure 2: Topology of Participants

2.2 Pre-Conditions

- A trust relationship exists between DOMAIN A(Security Domain A) and DOMAIN B (Security Domain B).
- Both organization have agreed to use the XSPA Profile SAML.

2.3 USE CASE – Structured Roles

Structural roles provide authorizations on objects at a global level without regard to internal details (ASTM E2595). Examples include authorization to participate in a session, connect authorization to a database, authorization to participate in an order workflow, or connection to a protected uniform resource locator (URL). A structural role applies to the business process task as a group. The use cases below will use structural roles commonly used for information access privileges to health information based on ASTM E1986 as part of the cross-enterprise authorization process.

2.3.1 DEMO ASTM 1986 Structured Role Access Control - Permit

Pre-Condition
Dr. Bob, of healthcare organization 'DOMAIN A' is assigned the ASTM 1986 structured role of "Physician". The "Physician" role allows Dr. Bob full review access to the patient record. Healthcare organization 'DOMAIN B' also allows full access to the role of 'Physician'. Patient 'Bambi Smith' has created a consent directive at 'DOMAIN B'. Patient 'Bambi Smiths's consent directives does not constrain access of a 'Physician' to their medical record. No organization policies exist to limit 'Physician' access to Bambi Smith's medical record. There is an existing trust relationship between DOMAIN A and DOMAIN B.

Scenario
Bambi Smith is on an out-of-town business trip. Bambi Smith develops a slight fever and cough and determines she may have an infection and goes to the local urgent care center. Dr. Bob sees patient 'Bambi Smith'. During the discussion patient 'Bambi Smith' states that she recently had a physical and that some blood work was done at 'DOMAIN B'. Dr. Bob believes these results might contain information valuable to this encounter. Since Dr. Bob has the role of 'Physician', a existing trust relationship exists between DOMAIN A and DOMAIN B, and that 'Bambi Smith' generated a consent directive at DOMAIN B, Dr. Bob with attempt to access Bambi's medical record at DOMAIN B by performing a cross-enterprise lookup of Bambi's medical record.

Result:
Dr. Bob is able to access and view Bambi Smith's medical record.

Attributes Asserted Across Enterprises	
SAMLIssuer	Bob, Doctor
IssuerName	Bob, Doctor
SubjectID	#########
NPI <U.S.A. Only>	#########
ASTM 1986 Structured Role	Physician
Purpose Of Use	TPO

2.3.2 DEMO ASTM 1986 Structured Role Access Control - Deny

Pre-Condition
Dr. Bob, of healthcare organization 'DOMAIN A' is assigned the ASTM 1986 structured role of "Physician". The "Physician" role allows Dr. Bob full review access to the patient record. Healthcare organization 'DOMAIN B' also allows full access to the role of 'Physician' and denies all others. Patient 'Bambi Smith' has created a consent directive at 'DOMAIN B'. Patient 'Bambi Smiths's consent directives does not constrain access of a 'Physician' to their medical record. No organization policies exist to limit a 'Physicians' access, it does however deny access to all other structured rolesThere is an existing trust relationship between DOMAIN A and DOMAIN B. An office administrator 'Joan', with the role of 'Administrator', performs billing functions at DOMAIN A.

Scenario
Bambi Smith is on an out-of-town business trip. Bambi Smith develops a slight fever and cough and determines she may have an infection and goes to the local urgent care center. Dr. Bob sees patient 'Bambi Smith'. During the discussion patient 'Bambi Smith' states that she recently had a physical and that some blood work was done at 'DOMAIN B'. Dr. Bob believes these results might contain information valuable to this encounter. Dr. Bob does not have access to a computer. Dr. Bob asked Joan, the office administrator, to login to system and perform a cross-enterprise look up of patient Bambi Smiths medical record.

Result:
Joan, the office administrator, is denied access to Bambi Smith's medical record at DOMAIN B.

Attributes Asserted Across Enterprises	
SAMLIssuer	Administrator, Joan
IssuerName	Administrator, Joan
SubjectID	#########
NPI <U.S.A. Only>	
ASTM 1986 Structured Role	Administrator
Purpose Of Use	TPO

2.3.3 DEMO ASTM 1986 Structured Role Access Control – Patient Consent Denies

Pre-Condition
Mike, of healthcare organization 'DOMAIN A' is assigned the ASTM 1986 structured role of "Pharmacist". The "Pharmacist" role allows Mike full review access to the patient record. Healthcare organization 'DOMAIN B' also allows full access to the role of 'Pharmacist'. Patient 'Bambi Smith' has created a consent directive at 'DOMAIN B'. Bambi Smith's consent directive denies access to a 'Pharmacist' under normal treatment circumstances. No organization policies exist to limit a 'Pharmacists' access. There is an existing trust relationship between DOMAIN A and DOMAIN B.

Scenario
Bambi Smith is on an out-of-town business trip. Bambi Smith develops a slight fever and cough and determines she may have an infection and goes to the local urgent care center. Dr. Bob sees patient 'Bambi Smith'. During the discussion patient 'Bambi Smith' states that she recently had a physical and that some blood work was done at 'DOMAIN B'. Dr. Bob believes these results might contain information valuable to this encounter. Since Dr. Bob has the role of 'Physician', a existing trust relationship exists between DOMAIN A and DOMAIN B, and that 'Bambi Smith' generated a consent directive at DOMAIN B, Dr. Bob with attempt to access Bambi's medical record at DOMAIN B by performing a cross-enterprise lookup of Bambi's medical record. Dr. Bob notes a change needs to be made on one of her prescriptions, notifies the onsite pharmacy of the change, and sends Bambi to pick it up. Before the Pharmacist, Mike, fills Bambi prescription, he needs to check for any drug-to-drug interaction from her other medications. Mike attempts to access Bambi's record at DOMAIN B.

Result:
Mike access to Bambi's medical record is denied.

Attributes Asserted Across Enterprises	
SAMLIssuer	Pharmacist, Mike
IssuerName	Pharmacist, Mike
SubjectID	#########
NPI <U.S.A. Only>	
ASTM 1986 Structured Role	Pharmacist
Purpose Of Use	TPO

2.4 USE CASE – Purpose of Use

Purpose of use provides context to requests for information resources. Each purpose of use will be unique to a specific assertion, and will establish the context for other security and privacy attributes. For a given claim, all assertions must be bound to the same purpose of use. Purpose of use allows the service to consult its policies to determine if the user's authorizations meet or exceed those needed for access control.

The following list of healthcare related purposes of use is specified by this profile:

- Healthcare Treatment, Payment and Operations (TPO),
- Emergency Treatment,
- System Administration,
- Research, and
- Marketing.

2.4.1 DEMO Purpose of Use – Deny Local Policy

Pre-Condition
A policy at DOMAIN B exists to grant access to cross-enterprise network resource if and only if an emergency exists. All other outside requests are denied.

Scenario
Bambi Smith is on an out-of-town business trip. Bambi Smith develops a slight fever and cough and determines she may have an infection and goes to the local urgent care center. Dr. Bob sees patient 'Bambi Smith'. During the discussion patient 'Bambi Smith' states that she recently had a physical and that some blood work was done at 'DOMAIN B'. Dr. Bob believes these results might contain information valuable to this encounter. Since Dr. Bob has the role of 'Physician', a existing trust relationship exists between DOMAIN A and DOMAIN B, and that 'Bambi Smith' generated a consent directive at DOMAIN B, Dr. Bob with attempt to access Bambi's medical record at DOMAIN B by performing a cross-enterprise lookup of Bambi's medical record.

Result:
Dr. Bob is denied access Bambi Smith's medical record.

Attributes Asserted Across Enterprises	
SAMLIssuer	Bob, Doctor
IssuerName	Bob, Doctor
SubjectID	#########
NPI <U.S.A. Only>	#########
ASTM 1986 Structured Role	Physician
Purpose Of Use	TPO

2.4.2 DEMO Purpose of Use – Deny Patient Consent Directive

Pre-Condition
Bambi Smith has created a patient consent directive to deny access to her medical record to all Radiologists under normal treatment circumstances.

Scenario
During her visit at the urgent care center Bambi also mentions to Dr. Bob that her knee has been sore and swollen. Dr. Bob writes radiology order for a standard series on her knee. Mike, the radiologist performs the procedure and prepares his findings. Mike is concerned over some abnormal findings and feels it necessary to review her clinical history. Mike attempts to access Bambi's medical record at DOMAIN B.

Result:
Mike is denied access to Bambi Smith's medical record.

Attributes Asserted Across Enterprises	
SAMLIssuer	Radiologist, Mike
IssuerName	Radiologist, Mike
SubjectID	#########
NPI <U.S.A. Only>	#########
ASTM 1986 Structured Role	Radiologist
Purpose Of Use	TPO

2.4.3 DEMO Purpose of Use – Permit Patient Consent Directive

Pre-Condition
Bambi Smith has created a patient consent directive to deny access to her medical record to all Radiologists under normal treatment circumstances.

Scenario
The radiologist Mike, feeling his concerns are warranted, asserts the purpose of use as 'Emergency Treatment.'

Result:
Mike is granted access to Bambi Smith's medical record.

Attributes Asserted Across Enterprises	
SAMLIssuer	Radiologist, Mike
IssuerName	Radiologist, Mike
SubjectID	#########
NPI <U.S.A. Only>	#########
ASTM 1986 Structured Role	Radiologist
Purpose Of Use	Emergency Treatment

2.5 USE CASE – Object Access

2.5.1 DEMO Controlling Object Access – Deny Local Policy Based on Permissions

Pre-Condition
A policy at DOMAIN B states that to grant read–only access to a patients medical record requires the ASTM 1986 role of 'Physician' and the specific permissions (from the HL7 Permssion Catalog) PRD-003, PRD-005, PRD-006, PRD-009, PRD-010, PRD-012, PRD-017. In this case Dr. Bob, of DOMAIN A, does not have all the necessary permissions assigned to him, and is unable to assert the necessary requirements in his request.

Scenario
Bambi Smith is on an out-of-town business trip. Bambi Smith develops a slight fever and cough and determines she may have an infection and goes to the local urgent care center. Dr. Bob sees patient 'Bambi Smith'. During the discussion patient 'Bambi Smith' states that she recently had a physical and that some blood work was done at 'DOMAIN B'. Dr. Bob believes these results might contain information valuable to this encounter. Since Dr. Bob has the role of 'Physician', a existing trust relationship exists between DOMAIN A and DOMAIN B, and that 'Bambi Smith' generated a consent directive at DOMAIN B, Dr. Bob with attempt to access Bambi's medical record at DOMAIN B by performing a cross-enterprise lookup of Bambi's medical record.

Result:
Dr. Bob is denied access Bambi Smith's medical record.

Attributes Asserted Across Enterprises	
SAMLIssuer	Bob, Doctor
IssuerName	Bob, Doctor
SubjectID	#########
NPI <U.S.A. Only>	#########
ASTM 1986 Structured Role	Physician
Purpose Of Use	TPO
HL7-Permissions	PRD-003,PRD-005,PRD-006,PRD-009,PRD-010
Requested Resource	Medical-record
Request Action	Read

2.5.2 DEMO Controlling Object Access – Permit Local Policy Based on Permissions

Pre-Condition
A policy at DOMAIN B states that to grant read –only access to a patients medical record requires the ASTM 1986 role of 'Physician' and the specific permissions (from the HL7 Permssion Catalog) PRD-003, PRD-005, PRD-006, PRD-009, PRD-010, PRD-012, PRD-017. In this case, Dr. Bob from DOMAIN A does not have all the necessary permissions assigned to him, and is unable to assert the necessary requirements in his request.

Scenario
Dr. Bob notes the error message he received in the previous denial and asks DOMAIN A security administrator to correct the oversight. Dr. Bob then attempts to access Bambi's medical record at DOMAIN B by performing a cross-enterprise lookup of Bambi's medical record with the newly granted site permissions.

Result:
Dr. Bob is allowed access to Bambi Smith's medical record.

Attributes Asserted Across Enterprises	
SAMLIssuer	Bob, Doctor
IssuerName	Bob, Doctor
SubjectID	#########
NPI <U.S.A. Only>	#########
ASTM 1986 Structured Role	Physician
Purpose Of Use	TPO
HL7-Permissions	PRD-003,PRD-005,PRD-006,PRD-009,PRD-010,PRD-012,PRD-017
Requested Resource	Medical-record
Request Action	Read

2.5.3 DEMO Controlling Object Access – Patient Consent Directive Denies

Pre-Condition
Bambi Smith the patient has created a consent directive that denies access of her medication record to all radiologists. Normal healthcare treatment between DOMAIN A and DOMAIN B allows access to all participating patients' medical record.

Scenario
During her visit at the urgent care center Bambi also mentions to Dr. Bob that her knee has been sore and swollen. Dr. Bob writes radiology order for a standard series on her knee. Mike, the radiologist performs the procedure and prepares his findings. Mike is concerned over some abnormal findings and feels it necessary to review her clinical history. Mike attempts to access Bambi's medical record at DOMAIN B.

Result:
Mike the radiologist is able to see all of Bambi's medical-record at DOMAIN B with the exception of her medication history.

Attributes Asserted Across Enterprises	
SAMLIssuer	Radiologist, Mike
IssuerName	Radiologist, Mike
SubjectID	#########
NPI <U.S.A. Only>	#########
ASTM 1986 Structured Role	Radiologist
Purpose Of Use	TPO
Requested Resource	Medical-record
Request Action	Read

3 Appendix A - Revision History

Document ID	Date	Committer	Comment
XSPAUseCases.docx	11/13/2008	Duane DeCouteau	Initial Draft
XSPAUseCases_SAML.doc	11/17/2008	David Staggs	Background information and reformatting
XSPAUserCases_SAML20081211.doc	12/11/2008	Duane DeCouteau	Incorporate review comments