Cross-Enterprise Security and Privacy Authorization (XSPA) Profile of Security Assertion Markup Language (SAML) for Healthcare

Working Draft 15 September, 2008

Document identifier:

xspa-saml-profile-02

Location:

Editors:

Duane DeCouteau, Department of Veterans Affairs (Edmond Scientific Company)

Mike Davis, Department of Veterans Affairs

David Staggs, Department of Veterans Affairs (SAIC)

Brett Burley, Department of Veterans Affairs (Near Infinity Corporation)

Contributors:

Abstract:

This profile describes a framework of how SAML and standard candidates encompassed by cross-enterprise security and privacy authorization (XSPA) can be used to satisfy requirements pertaining to information-centric security within the healthcare community.

Table of Contents

Section **Page**

List of Figures

Figure **Page**

List of Appendices

Appendix **Page**

1 Introduction

This document describes a framework that provides access control interoperability useful in the healthcare environment. Interoperability is achieved using SAML assertions that carry common semantics and vocabularies in exchanges specified below.

1.1. Document Roadmap

- Presentation of requirements, non-goals and terminology
- Review of components that are encompassed by this XSPA profile of SAML

1.2. Requirements and Non-goals

Requirements

This XSPA profile of SAML is required to achieve cross-enterprise authorization of entities operating within a healthcare workflow by providing common semantics and vocabulary for interoperable coarse grain access control.

Non-Goals

The following topic is outside the scope of this document:

- The use of eXtensible Access Control Markup Language (XACML) as means for creating rules and policy sets for access control to data or functionality within or across security domains.

2 Terminology

The following definitions establish the terminology and usage in this profile:

Access Control Service (ACS) – The Access Control Service is the enterprise security service that supports and implements user-side and service-side access control capabilities. The service would be utilized by the Service and/or Service User.

Object – An *object* is an entity that contains or receives information. The *objects* can represent information containers (e.g., files or directories in an operating system, and/or columns, rows, tables, and views within a database management system) or *objects* can represent exhaustible system resources, such as printers, disk space, and central processing unit (CPU) cycles. ANSI RBAC (American National Standards Institute Role Based Access Control)

Operation - An *operation* is an executable image of a program, which upon invocation executes some function for the user. Within a file system, *operations* might include read, write, and execute. Within a database management system, *operations* might include insert, delete, append, and update. An *operation* is also known as an action or privilege. ANSI RBAC

Permission - *An* approval to perform an operation on one or more RBAC protected objects. ANSI RBAC

Structural Role - A job function within the context of an organization whose permissions are defined by operations on workflow objects. ASTM (American Society for Testing and Materials) **E2595-2007**

Service Provider (SP) - The service provider represents the system providing a protected resource and relies on the provided security service.

Service User - The entity represents any individual entity [such as on an Electronic Health Record (EHR)/personal health record (PHR) system] that needs to make a service request of a Service Provider. The Entity may also be known as a principal and/or entity, which represents an application, a machine, or any other type of entity that may act as a requester in a transaction.

3 XSPA profile of SAML Implementation

The XSPA profile of SAML provides access control over resources and functionality within and between healthcare information technology (IT) systems. Additional introductory information and examples can be found in Cross-Enterprise Security and Privacy Authorization (XSPA) a Profile of Security Assertion Markup Language (SAML) Implementation Examples [XSPA-SAML-EXAMPLES].

3.1 Interactions between Parties

Figure 1 displays an overview of interactions between parties in the exchange of healthcare information. Elements described in the figure are explained in the subsections below.

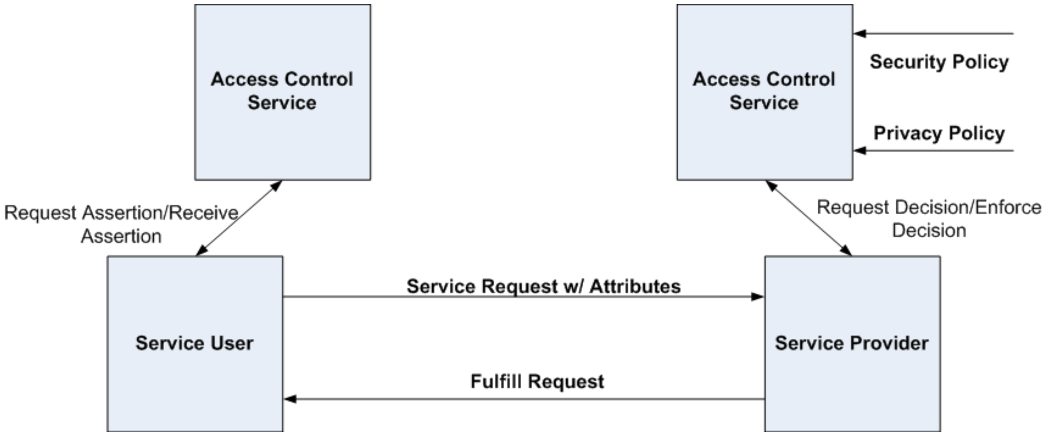

Figure 1: Interaction between Parties

3.1.1 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 requirement and actions. The requesting ACS is responsible of enforcement the access control decision.

3.1.2 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.

3.1.3 Attributes

Attributes are information related to user location, role, purpose of use, and requested resource requirement and actions necessary to make an access control decision.

3.1.4 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.

3.1.5 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.

3.2 Transmission Integrity

The XSPA profile of SAML recommends the use of reliable transmission protocols. Where transmission integrity is required, this profile makes no specific recommendations regarding mechanism or assurance level.

3.3 Transmission Confidentiality

The XSPA profile of SAML recommends the use of secure transmission protocols. Where transmission confidentiality is required, this profile makes no specific recommendations regarding mechanisms.

3.4 Error States

This profile adheres to error states describe in SAML 2.0.

3.5 Security Considerations

The following security considerations are established for the XSPA profile of SAML:

- Entities must be members of defined information domains under the authorization control of a defined set of policies,
- Entities must have been identified and provisioned (credentials issued, privileges granted, etc.) in accordance with policy,
- Privacy policies must have been identified and provisioned (consents, user preferences, etc.) in accordance with policy,
- Pre-existing security and privacy policies must have been provisioned to access control services,
- The capabilities and location of requested information/document repository services must be known,
- Secure channels must be established as required by policy,
- Audit services must be operational and initialized, and

- Entities have pre-asserted membership in an information domain by successful and unique authentication.

3.6 Confirmation Identifiers

The manner used by the relying party to confirm that the requester message came from a system entity that is associated with the subject of the assertion will depend upon the context and sensitivity of the data. For confirmations requiring a specific level of assurance, this profile specifies the use of National Institute of Standards and Technology (NIST) Special Publication 800-63 Electronic Authentication Guideline. In addition, this profile specifies the Liberty Identity Access Framework (LIAF) criteria for evaluating and approving credential service providers.

3.7 Metadata Definitions

This profile will utilize the SAML <Attribute> element for all assertions.

3.8 Naming Syntax, Restrictions and Acceptable Values

This profile conforms to SAML 2.0 specification.

3.9 Namespace Requirements

The NameFormat Extensible Markup Language (XML) attribute in <Attribute> elements MUST be urn:oasis:names:tc:SAML:2.0:attrname-format:uri.

3.10 Attribute Rules of Equality

All asserted attributes will be typed as strings. Two <Attribute> elements refer to the same SAML attribute if and only if their Name XML attribute values are equal in a binary comparison.

3.11 Attribute Naming Syntax, Restrictions and Acceptable Values

The Name XML attribute MUST adhere to the rules specified for that format, as defined by **[SAMLCore]**. For purposes of human readability, there may also be a requirement for some applications to carry an optional string name together with the Object Identifier (OID) Uniform Resource Name (URN). The optional XML attribute FriendlyName (defined in **[SAMLCore]**) MAY be used for this purpose, but is not translatable into an XACML attribute equivalent.

This profile will utilize the namespace of
urn:oasis:names:tc:SAML:2.0:profiles:attribute:XPSA

Example of use:

```
<saml:Attribute NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
Name="urn:oasis:names:tc:SAML:2.0:profiles:attribute:XPSA:organization">
    <saml:AttributeValue xsi:type="http://www.w3.org/2001/XMLSchema#string">
                    County Hospital
    </saml:AttributeValue>
</saml:Attribute>
```

Name

This is the name of the user as required by Health Insurance Portability and Accountability Act (HIPAA) Privacy Disclosure Accounting. The name will be typed as a string and in plain text with an identifying tag of

<urn:oasis:names:tc:SAML:2.0:profiles:attribute:XPSA:subject>.

National Provider Identifier - NPI(optional)

This is a US Government provided unique provider identifier required for all Health Insurance Portability and Accountability Act (HIPAA) Privacy Disclosure Accounting transactions. NPI will be typed as a string in plain text with an identifying element of <urn:oasis:names:tc:SAML:2.0:profiles:attribute:XPSA:US:npi>.

Organization

This is the organization that the user belongs to as required by HIPAA Privacy Disclosure Accounting. Organization will be typed as a string in plain text with an identifying element of <urn:oasis:names:tc:SAML:2.0:profiles:attribute:XPSA:organization>.

Structural Role

This is the value of the principal's structural role Structural roles are described in ASTM E2595-07, Standard Guide for Privilege Management Infrastructure.

Structural roles provide authorizations on objects at a global level without regard to internal details. 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). The structural role is the role name referenced by the patient's consent directive.

This profile specifies ASTM 1986-98 (2005) Standard Guide for Information Access Privileges to Health Information persons for whom role based access control is warranted as the defined default structural roles to be used in this profile. ASTM E1986

NOTE: At the time of this writing, ASTM E31 is still in the process of completing the formal enumeration ASTM 1986 roles.

Structural roles are specified by reference to an OID. Roles will be typed as strings and an OID will be assigned to each unique structural role authority. The enumerated ASTM E1986 role will be passed with the assertion. Enumerated roles under the OID will be identified through the use of the element <urn:oasis:names:tc:SAML:2.0:profiles:attribute:XPSA: structural_role> within the assertion.

Permission (optional)

There is no explicit assertion of permission required by this profile. The permission in use is determined by the Action on the Target. See Action below. The Permission is the ANSI INCITS (InterNational Committee for Information Technology Standards) RBAC compliant action-object pair representing the authorization required for access by the protected resource.

ACTIONS

The HL7 (Health Level Seven) RBAC Permission catalog is an ANSI INCITS 359-2004 RBAC compliant vocabulary that provides a minimal permission subset for interoperability. This profile specifies the use of the following HL7 RBAC Permission Catalog Actions: (include HL7 OID TBD)

Append
Create
Delete
Read
Update

Execute

Execute refer to complex functions and stored procedures that provide for extended actions within the healthcare environment. Examples include "print", "suspend", and "sign". This profile specifies the use of SNOMED CT (Systematized Nomenclature of Medicine--Clinical Terms) action vocabularies to define execute operations.

OBJECTS

This profile specifies the use of SNOMED CT as the object vocabulary in an action-object permission pair. SNOMED CT provides the core general terminology for the electronic health record (EHR). As used in this profile, SNOMED CT is used to designate clinically relevant protected information objects.

SNOMED CT is one of a suite of designated standards for use in U.S. Federal Government systems for the electronic exchange of clinical health information and is also a required standard in interoperability specifications of the U.S. Healthcare Information Technology Standards Panel. SNOMED CT is also being implemented internationally as a standard within other International Health Terminology Standards Development Organisation (IHTSDO) Member countries.

This profile also permits the use of the HL7 RBAC Permission Catalog objects. The HL7 RBAC Permission Catalog objects are functionally equivalent to terms in SNOMED CT and may be used in lieu of the complete SNOMED CT set.

Purpose of Use (POU)

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. Purpose of Use will be typed as string with an identifying element of

<urn:oasis:names:tc:SAML:2.0:profiles:attribute:XPSA:purposeofuse>

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.

Figure 2 illustrates the general relationship between subject (user) and granted permissions to specific objects as a relationship to their POU. Roles in this relationship are placeholders for permissions. Permission defines the object-action relationship.

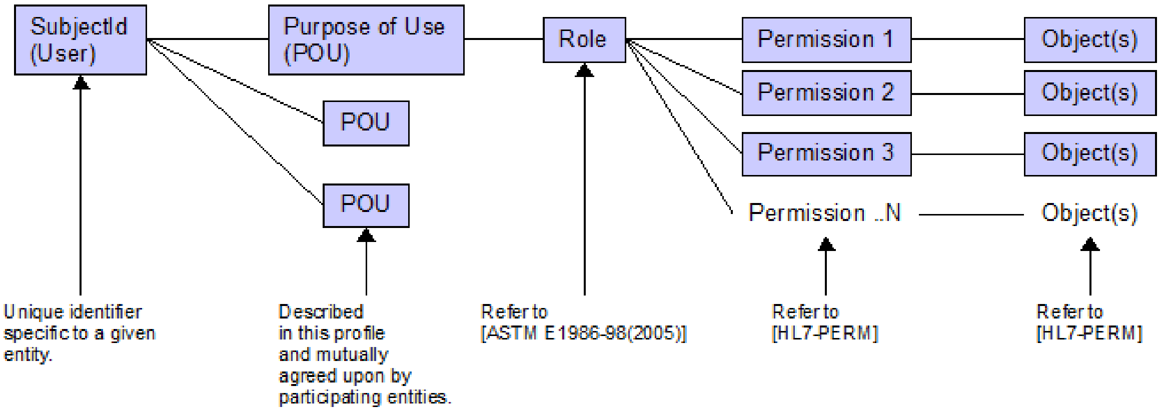

Figure 2: Determining Subject Permissions

Resource

The resource(s) for which access is requested must be identical to the object(s) for which the authorization assertions of this profile apply. The resource vocabulary then must be either SNOMED CT or objects from the HL7 RBAC Permission Catalog minimal SNOMED CT subset.

Evidence

The <urn:oasis:names:tc:SAML:2.0:profiles:attribute:XPSA:evidence> element contains an assertion or assertion reference that the SAML authority relied on in issuing the authorization decision.

The evidence is an assertion and contains complex content. At a minimum the evidence should contain three items which are needed for computational or instruction at the responding ACS:

1. The description of the destination of the disclosure,
2. Expiration date of the authorization, and
3. Reference to the paper authorization document.

4 References

[SAMLPROF] Organization for the Advancement of Structured Information Standards. *Profiles for the OASIS Security Assertion Markup Language, v2.0*, February 2005.

[ASTM E1986-98 (2005)] Standard Guide for Information Access Privileges to Health Information.

[ASTM E2595 (2007)] Standard Guide for Privilege Management Infrastructure

[SAML] Security Assertion Markup Language (SAML) V2.0 Technical Overview

[HL7-PERM] HL7 Security Technical Committee, HL7 Version 3 Standard: Role-based Access Control Healthcare Permission Catalog, (Available through http://www.hl7.org/library/standards.cfm), Release 1, Designation: ANSI/HL7 V3 RBAC, R1-2008, Approval Date 2/20/2008.

[HL7-CONSENT] HL7 Consent Related Vocabulary ConfidentialityCodes Recommendation, http://lists.oasis-open.org/archives/xacml-demo-tech/200712/doc00003.doc, from project submission: http://lists.oasis-open.org/archives/xacml-demo-tech/200712/msg00015.html

[SNOMED CT] SNOMED CT User Guide (July 2008)
http://www.ihtsdo.org/snomed-ct/snomed-ct-publications/

5 References (Non-Normative)

[XSPA-SAML-INTRO] Draft Cross-Enterprise Security and Privacy Authorization (XSPA) Introduction to Profile of Security Assertion Markup Language (SAML) for Healthcare.

[XSPA-SAML-EXAMPLES] DRAFT Cross-Enterprise Security and Privacy Authorization (XSPA) Profile of Security Assertion Markup Language (SAML) Implementation Examples.

Appendix A. Revision History

Document ID	Date	Committer	Comment
xspa-saml-profile-01	12 Sep 2008	Mike Davis & David Staggs	Initial draft v1.0
xspa-saml-profile-02	15 Sep 2008	Craig Winter	QA Review / Revision v1.1