Cross-Enterprise Security and Privacy Authorization (XSPA) Profile of Security Assertion Markup Language (SAML) for Healthcare Version 1.0

OASIS Standard

1 November 2009

Specification URIs:
This Version:

http://docs.oasis-open.org/security/xspa/v1.0/saml-xspa-1.0-os.html
http://docs.oasis-open.org/security/xspa/v1.0/saml-xspa-1.0-os.pdf
http://docs.oasis-open.org/security/xspa/v1.0/saml-xspa-1.0-os.doc (Authoritative)

Previous Version:

http://docs.oasis-open.org/security/xspa/v1.0/saml-xspa-1.0-cs01.html
http://docs.oasis-open.org/security/xspa/v1.0/saml-xspa-1.0-cs01.pdf
http://docs.oasis-open.org/security/xspa/v1.0/saml-xspa-1.0-cs01.doc (Authoritative)

Latest Version:

http://docs.oasis-open.org/security/xspa/v1.0/saml-xspa-1.0.html
http://docs.oasis-open.org/security/xspa/v1.0/saml-xspa-1.0.pdf
http://docs.oasis-open.org/security/xspa/v1.0/saml-xspa-1.0.doc (Authoritative)

Technical Committee:

OASIS Security Services (SAML) TC

Chair(s):

Brian Campbell, Ping Identity Corporation
Hal Lockhart, Oracle Corporation

Editor(s):

Mike Davis, Department of Veterans Affairs
Duane DeCouteau, Department of Veterans Affairs
David Staggs, Department of Veterans Affairs

Related work:

- Security Assertion Markup Language (SAML) v2.0

Declared XML Namespace(s):

urn:oasis:names:tc:xacml:2.0
urn:oasis:names:tc:xspa:1.0
urn:oasis:names:tc:saml:2.0

Abstract:

This profile describes a framework in which SAML is encompassed by cross-enterprise security and privacy authorization (XSPA) to satisfy requirements pertaining to information-centric security within the healthcare community.

Status:

This document was last revised or approved by the OASIS Security Services (SAML) TC on the above date. The level of approval is also listed above. Check the “Latest Version” or “Latest Approved Version” location noted above for possible later revisions of this document.

Technical Committee members should send comments on this specification to the Technical Committee’s email list. Others should send comments to the Technical Committee by using the “Send A Comment” button on the Technical Committee’s web page at http://www.oasis-open.org/committees/security/.

For information on whether any patents have been disclosed that may be essential to implementing this specification, and any offers of patent licensing terms, please refer to the Intellectual Property Rights section of the Technical Committee web page (http://www.oasis-open.org/committees/security/ipr.php.

The non-normative errata page for this specification is located at http://www.oasis-open.org/committees/security/.

Notices

This document and the information contained herein is provided on an "AS IS" basis and OASIS DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY OWNERSHIP RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

OASIS requests that any OASIS Party or any other party that believes it has patent claims that would necessarily be infringed by implementations of this OASIS Committee Specification or OASIS Standard, to notify OASIS TC Administrator and provide an indication of its willingness to grant patent licenses to such patent claims in a manner consistent with the IPR Mode of the OASIS Technical Committee that produced this specification.

OASIS invites any party to contact the OASIS TC Administrator if it is aware of a claim of ownership of any patent claims that would necessarily be infringed by implementations of this specification by a patent holder that is not willing to provide a license to such patent claims in a manner consistent with the IPR Mode of the OASIS Technical Committee that produced this specification. OASIS may include such claims on its website, but disclaims any obligation to do so.

OASIS takes no position regarding the validity or scope of any intellectual property or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; neither does it represent that it has made any effort to identify any such rights. Information on OASIS' procedures with respect to rights in any document or deliverable produced by an OASIS Technical Committee can be found on the OASIS website. Copies of claims of rights made available for publication and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this OASIS Committee Specification or OASIS Standard, can be obtained from the OASIS TC Administrator. OASIS makes no representation that any information or list of intellectual property rights will at any time be complete, or that any claims in such list are, in fact, Essential Claims.

The names "OASIS", “SAML” and “XSPA” are trademarks of OASIS, the owner and developer of this specification, and should be used only to refer to the organization and its official outputs. OASIS welcomes reference to, and implementation and use of, specifications, while reserving the right to enforce its marks against misleading uses. Please see http://www.oasis-open.org/who/trademark.php for above guidance.

Table of Contents

Table of Figures

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 Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in **[RFC2119]**.

The keywords "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" are to be interpreted as described in [RFC2119].

The following definitions establish additional 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.

Entity - An entity may also be known as a principal and/or subject, which represents an application, a machine, or any other type of entity that may act as a requester in a transaction.

Service User - The service user 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.

1.2 Normative References

[RFC2119] S. Bradner, *Key words for use in RFCs to Indicate Requirement Levels*, http://www.ietf.org/rfc/rfc2119.txt, IETF RFC 2119, March 1997.

[SAMLPROF] OASIS Standard, "Profiles for the OASIS Security Assertion Markup Language, v2.0," March 2005. http://docs.oasis-open.org/security/saml/v2.0/saml-profiles-2.0-os.pdf

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

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

[SAML] OASIS Standard, "Security Assertion Markup Language (SAML) v2.0" http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf

[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 Confidentiality Codes 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

1.3 Non-Normative References

[XSPA-SAML-INTRO]

OASIS Committee Working Draft, “Introductory overview of XSPA Profile of SAML for Healthcare,” http://www.oasis-open.org/committees/document.php?document_id=30407

[XSPA-SAML-EXAMPLES]

OASIS Committee Working Draft, “Implementation examples of XSPA Profile of SAML for Healthcare,” http://www.oasis-open.org/committees/document.php?document_id=30408

2 XSPA profile of SAML Implementation

The XSPA profile of SAML describes the minimum vocabulary necessary to provide 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].

2.1 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. The Service Request, Identity Assertion, and Authorization Attributes in Figure 1 are prepared by the Service User Access Control Service and MAY be passed in a single assertion from the Service User to the Service Provider. The Service Provider Access Control Service evaluates the request against policy and indicates to the Service Provider if the request may be fulfilled.

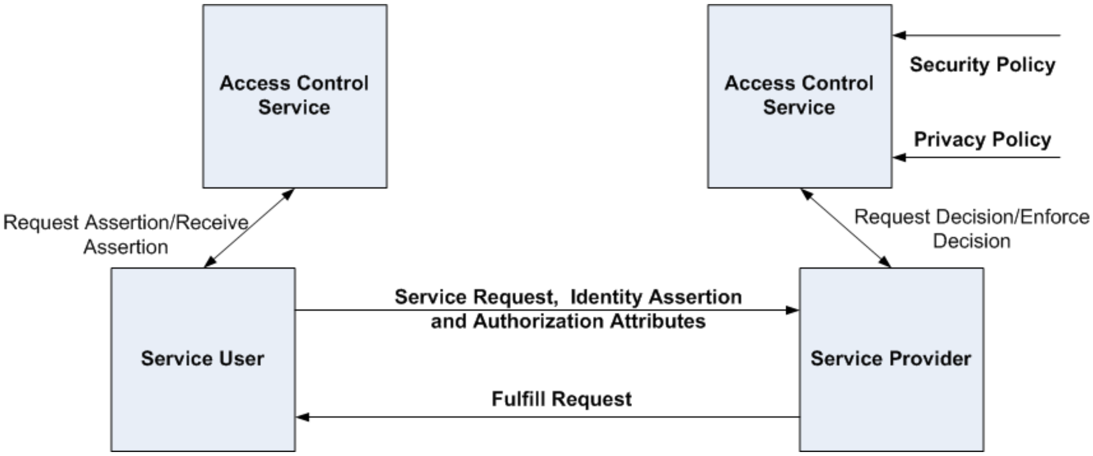
Access Control Service
Access Control Service
Security Policy
Privacy Policy
Request Assertion/Receive Assertion
Request Decision/Enforce Decision
Service Request, Identity Assertion and Authorization Attributes
Service User
Service Provider
Fulfill Request

Figure 1: Interaction between Parties

2.1.1 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 collects all the attributes (e.g. organization-id, structural role, functional role, purpose of use, requested resource, and actions) necessary to create the Service User requested assertion.

In addition to creating the request, the requesting ACS is responsible for enforcing local security and privacy policy.

2.1.2 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.

2.1.3 Attributes

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

2.1.4 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.

2.1.5 Privacy Policy

The privacy policy includes the set of consent directives and other privacy conditions (object masking, object filtering, user, role, purpose, etc.) that constrain enforcement.

2.2 Protocols

This profile utilizes the SAML 2.0 core specification to define the elements exchanged in a cross-enterprise service request that supports security and privacy policies. Requests MAY be exchanged using a SAML assertion containing elements such as saml2:Issuer, saml2:NameID, and saml2:AttributeStatement.

2.3 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.

2.4 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.

2.5 Error States

This profile adheres to error states describe in SAML 2.0.

2.6 Security Considerations

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

- Participating information domains have agreed to use XSPA profile and that a trust relationship exists,
- Entities are members of defined information domains under the authorization control of a defined set of policies,
- Entities have been identified and provisioned (credentials issued, privileges granted, etc.) in accordance with policy,
- Privacy policies have been identified and provisioned (consents, user preferences, etc.) in accordance with policy,
- Pre-existing security and privacy policies have been provisioned to Access Control Services,
- The capabilities and location of requested information/document repository services are known,
- Secure channels are established as required by policy,
- Audit services are operational and initialized, and
- Entities have asserted membership in an information domain by successful and unique authentication.

2.7 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.

2.8 Metadata Definitions

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

2.9 Naming Syntax, Restrictions and Acceptable Values

This profile conforms to SAML 2.0 specification.

2.10 Namespace Requirements

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

2.11 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.

2.12 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:xspa:1.0

Example of use:

```
<saml:Attribute NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
Name="urn:oasis:names:tc:xspa:1.0:organization">
 <saml:AttributeValue xsi:type="http://www.w3.org/2001/XMLSchema#string">
   County Hospital
 </saml:AttributeValue>
</saml:Attribute>
```

2.12.1 Name

Name 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:xspa:1.0:subject:subject-id>.

2.12.2 National Provider Identifier (NPI) – (optional)

NPI is a US Government issued 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:xspa:1.0:subject:npi>.

2.12.3 Organization

Organization 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:xspa:1.0:subject:organization>.

2.12.4 Organization-ID

Organization-ID is the unique identifier of the consuming organization and/or facility.

2.12.5 Structural Role

Structural Role is the value of the principal's structural role. Structural roles that are used in this profile are defined in Table 2 "Healthcare Personnel that Warrant Differing Levels of Access Control" of ASTM 1986-98 (2005) Standard Guide for Information Access Privileges to Health Information. ASTM E1986

Structural roles are described in greater depth 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, authorization to connect 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.

2.12.6 Functional Role

Functional role can include custom attributes related to application functionality agreed upon by the parties in an exchange.

2.12.7 Permission (optional)

Permission is not required by this profile. Permission 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.

2.12.8 Action

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:

- Append
- Create
- Delete
- Read
- Update
- Execute

2.12.9 Execute (optional)

Execute refers to complex functions and stored procedures that provide for extended actions within the healthcare environment. Examples include "print", "suspend", and "sign". Execute can include custom attributes related to functionality agreed upon by the parties in an exchange.

2.12.10 Object

Objects are any system resource subject to access control. This profile specifies the use of HL7 RBAC Permission Catalog as the object vocabulary in an action-object permission pair. HL7 RBAC Permission Catalog provides the minimum set of interoperable objects suitable for the support of security and privacy access control decisions in this profile.

2.12.11 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:xspa:1.0:subject:purposeofuse>

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

Table 1: Values for Purpose of Use

Description	Allowed Value
Healthcare Treatment	TREATMENT
Payment	PAYMENT
Operations	OPERATIONS
Emergency Treatment	EMERGENCY
System Administration	SYSADMIN
Research	RESEARCH
Marketing	MARKETING
Request of the Individual	REQUEST
Public Health	PUBLICHEALTH

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.

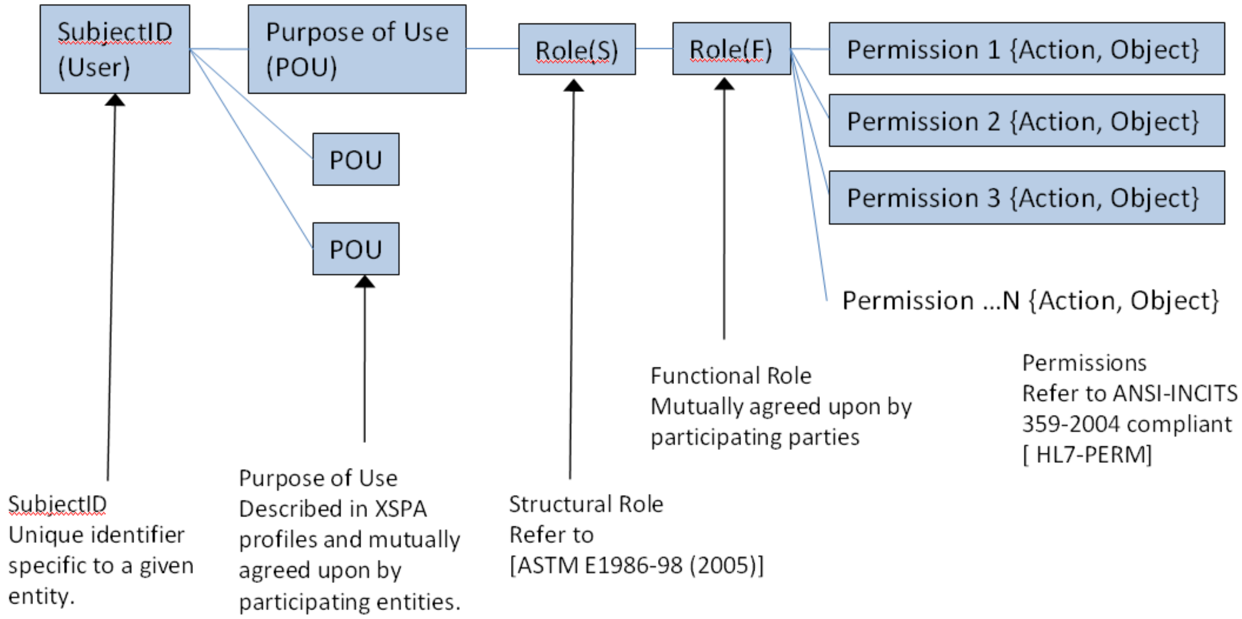
SubjectID (User)
Purpose of Use (POU)
Role(S)
Role(F)
Permission 1 {Action, Object}
Permission 2 {Action, Object}
Permission 3 {Action, Object}
Permission …N {Action, Object}
POU
POU
Functional Role Mutually agreed upon by participating parties
Permissions Refer to ANSI-INCITS 359-2004 compliant [HL7-PERM]
SubjectID Unique identifier specific to a given entity.
Purpose of Use Described in XSPA profiles and mutually agreed upon by participating entities.
Structural Role Refer to [ASTM E1986-98 (2005)]

Figure 2: Determining Subject Permissions

2.12.12 Resource

The object(s) for which access is requested must be identical to the object(s) for which the authorization assertions of this profile apply. A requested resource is not required to be a simple object but may instead be a process or workflow. This profile specifies the use of HL7 RBAC Permission Catalog as the resource vocabulary. .

3 Conformance

3.1 Introduction

The XSPA profile of SAML addresses the following aspects of conformance:

This profile describes a minimum vocabulary set that must be supported in order to claim conformance.

An Implementation must conform at minimum to the SAML v2.0 specification. The following tables describes the Attribute naming syntax, restrictions, and acceptable values,

Table 2: Attribute Naming, Typing, and Acceptable Value Set

Identifier	Type	Valid Values
urn:oasis:names:tc:xacml:1.0:subject:subject-id	String	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.
urn:oasis:names:tc:xpsa:1.0:subject:organization	String	Organization the requestor belongs to as required by Health Insurance Portability and Accountability Act (HIPAA)Privacy Disclosure Accounting.
urn:oasis:names:tc:xspa:1.0:subject:organization-id	anyURI	Unique identifier of the consuming organization and/or facility
urn:oasis:names:tc:xspa:1.0:subject:hl7:permission	String	Refer to [HL7-PERM] and its OID representation.
urn:oasis:names:tc:xacml:2.0:subject:role	String	Structural Role refer to [ASTM E1986-98 (2005)] and its OID representation.
urn:oasis:names:tc:xspa:1,0:subject:purposeofuse	String	TREATMENT, PAYMENT, OPERATIONS, EMERGENCY, SYSADMIN, MARKETING, RESEARCH, REQUEST, PUBLICHEALTH
urn:oasis:names:tc:xacml:1.0:resource:resource-id	String	Unique identifier of the resource defined by and controlled by the servicing organization. In healthcare this is the patient unique identifier.
urn:oasis:names:tc:xspa:1.0:resource:hl7:type	String	For minimum interoperability set of objects and supporting actions refer to [HL7-PERM] and their OID representations.
urn:oasis:names:tc:xspa:1.0:environment:locality urn:oasis:names:tc:xspa:2.0:subject:npi	String String	Unique identifier of the servicing organization. National Provider ID provided by U.S. Government for all active providers.

*Note: The OID for the HL7 Permission Catalog [HL7-PERM] is 2.16.840.1.113883.13.27. The OID for structural roles referenced in [ASTM E1986-98 (2005)] is 1.2.840.10065.1986.7

The mechanism used to identify the patent in a standardized way, e.g. resource:resource-id, is outside the scope of the profile.

HL7 RBAC Permission Catalog [HL7-PERM] represents a conformant minimum interoperability set for object/action pairings.

3.2 Conformance Tables

The following section identifies portions of the profile that MUST be adhered to in order to claim conformance.

Note: “M” is mandatory “O” is optional.

Attributes

The implementation MUST use the attributes associated with the following identifiers in the way this profile has defined.

Table 3: Conformance Attributes

Identifiers	
urn:oasis:names:tc:xacml:1.0:subject:subject-id	M
urn:oasis:names:tc:xspa:1.0:subject:organization-id	M
urn:oasis:names:tc:xspa:1.0:organization	M
urn:oasis:names:tc:xspa:1.0:subject:hl7:permission	O
urn:oasis:names:tc:xacml:2.0:subject:role ASTM E1986-98 (2005) Structured Role Value	M
Urn:oasis:names:tc:xspa:1.0:subject:functional-role	O
urn:oasis:names:tc:xspa:1.0:subject:purposeofuse	M
urn:oasis:names:tc:xacml:1.0:resource:resource-id	M
urn:oasis:names:tc:xacml:1.0:action:action-id HL7 Permission Catalog Resource Action Value	O
urn:oasis:names:tc:xspa:1.0:resource:hl7:type HL7 Permission Catalog Object Value	O
urn:oasis:names:tc:xspa:1.0:environment:locality	M
urn:oasis:names:tc:xspa:2.0:subject:npi	O

A. Acknowledgements

The following individuals have participated in the creation of this specification and are gratefully acknowledged:

Participants in the 2009 HIMSS Interoperability Demonstration of the XSPA profile:

Steve Steffensen, Department of Defense
Daniel Dority, Jericho Systems Corporation
Brian McClung, Jericho Systems Corporation
Brendon Unland, Jericho Systems Corporation
Anil Saldhana, Red Hat
Dilli Doral, Sun Microsystems
Steven Jarosz, Sun Microsystems
Mike Davis, Veterans Health Administration
Duane DeCouteau, Veterans Health Administration
David Staggs, Veterans Health Administration

Security Services (SAML) TC members during the development of this specification:

George Fletcher, AOL
Scott Messick, Booz Allen Hamilton
Keiron Salt, BTplc
Colin Young, BTplc
Kyle Meadors, Drummond Group Inc.
Michael Merrill, EMC Corporation
Rob Philpott, EMC Corporation
Giles Hogben, ENISA
Carolina Canales-Valenzuela, Ericsson
Lakshmi Thiyagarajan, Hewlett-Packard
Guy Denton, IBM
Heather Hinton, IBM
Maryann Hondo, IBM
Anthony Nadalin, IBM
John Bradley, Individual
David Chadwick, Individual
Jeff Hodges, Individual
Conor Cahill, Intel Corporation
Scott Cantor, Internet2
Nathan Klingenstein, Internet2
Bob Morgan, Internet2
Yassir Elley, Juniper Networks
Steve Hanna, Juniper Networks
Thomas Hardjono, M.I.T.
Tom Scavo, National Center for Supercomputing Applications (NCSA)
Peter Davis, NeuStar, Inc.
Marie Henderson, New Zealand State Services Commission
Colin Wallis, New Zealand State Services Commission
William Young, New Zealand State Services Commission
Frederick Hirsch, Nokia Corporation
Abbie Barbir, Nortel
Srinath Godavarthi, Nortel
Paul Madsen, NTT Corporation
Harry Haury, NuParadigm Government Systems, Inc.
Will Hopkins, Oracle Corporation
Ari Kermaier, Oracle Corporation

Hal Lockhart, Oracle Corporation
Prateek Mishra, Oracle Corporation
Vamsi Motukuru, Oracle Corporation
Willem de Pater, Oracle Corporation
Paul Toal, Oracle Corporation
Brian Campbell, Ping Identity Corporation
Anil Saldhana, Red Hat
Michael Engler, SAP AG
Kent Spaulding, Skyworth TTG Holdings Limited
Humphrey Zhang, Skyworth TTG Holdings Limited
Bhavna Bhatnagar, Sun Microsystems
Eve Maler, Sun Microsystems
Ronald Monzillo, Sun Microsystems
Emily Xu, Sun Microsystems
Mike Beach, The Boeing Company
Karsten Huneycutt, University of North Carolina at Chapel Hill
Duane DeCouteau, Veterans Health Administration
David Staggs, Veterans Health Administration

B. Revision History

Document ID	Date	Committer	Comment
xspa-saml-profile-01	12 Sep 2008	Mike Davis & David Staggs	Initial draft v0.0
xspa-saml-profile-02	15 Sep 2008	Craig Winter	QA Review / Revision v0.1
xspa-saml-profile-wd-03	31 Oct 2008	Duane DeCouteau	Incorporate initial SS TC feedback
xspa-saml-profile-cd-01	4 Nov 2008	Duane DeCouteau	Approved Committee Draft v1.0
xspa-saml-profile-cd-01	5 Nov 2008	Craig Winter	QA Review / Revision v1.1
xspa-saml-profile-pr-01	5 Nov 2008	David Staggs	Approved Public Review Draft v1.0
xspa-saml-profile-pr-02	29 May 2009	David Staggs	Changes to Public Review Draft pr02
saml-xspa-1.0-cd04	15 July 2009	Duane DeCouteau	Final TC Review Comments