Cross-Enterprise Security and Privacy Authorization (XSPA) Profile of SAML v2.0 for Healthcare Version 2.0

Committee Specification Draft 01

01 April 2014

Specification URIs

This version:

http://docs.oasis-open.org/xspa/saml-xspa/v2.0/csd01/saml-xspa-v2.0-csd01.doc (Authoritative)
http://docs.oasis-open.org/xspa/saml-xspa/v2.0/csd01/saml-xspa-v2.0-csd01.html
http://docs.oasis-open.org/xspa/saml-xspa/v2.0/csd01/saml-xspa-v2.0-csd01.pdf

Previous version:

N/A

Latest version:

http://docs.oasis-open.org/xspa/saml-xspa/v2.0/saml-xspa-v2.0.doc (Authoritative)
http://docs.oasis-open.org/xspa/saml-xspa/v2.0/saml-xspa-v2.0.html
http://docs.oasis-open.org/xspa/saml-xspa/v2.0/saml-xspa-v2.0.pdf

Technical Committee:

OASIS Cross-Enterprise Security and Privacy Authorization (XSPA) TC

Chair:

Mohammad Jafari (mjafari@edmondsci.com), Veterans Health Administration

Editors:

John M. Davis (mike.davis@va.gov), Veterans Health Administration
Duane DeCouteau (ddecouteau@edmondsci.com), Veterans Health Administration
Mohammad Jafari (mjafari@edmondsci.com), Veterans Health Administration

Related work:

This specification replaces or supersedes:

- *Cross-Enterprise Security and Privacy Authorization (XSPA) Profile of Security Assertion Markup Language (SAML) for Healthcare Version 1.0*. 1 November 2009. OASIS Standard. http://docs.oasis-open.org/security/xspa/v1.0/saml-xspa-1.0-os.html.

This specification is related to the OASIS Security Assertion Markup Language (SAML) V2.0, comprised of the following documents:

- *Authentication Context for the OASIS Security Assertion Markup Language (SAML) V2.0*. 15 March 2005. OASIS Standard. http://docs.oasis-open.org/security/saml/v2.0/saml-authn-context-2.0-os.pdf.
- *Bindings for the OASIS Security Assertion Markup Language (SAML) V2.0*. 15 March 2005. OASIS Standard. http://docs.oasis-open.org/security/saml/v2.0/saml-bindings-2.0-os.pdf.
- *Conformance Requirements for the OASIS Security Assertion Mark Markup Language (SAML) V2.0*. 15 March 2005. OASIS Standard. http://docs.oasis-open.org/security/saml/v2.0/saml-conformance-2.0-os.pdf.

- *Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0*. 15 March 2005. OASIS Standard. http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf.
- *Glossary for the OASIS Security Assertion Markup Language (SAML) V2.0*. 15 March 2005. OASIS Standard. http://docs.oasis-open.org/security/saml/v2.0/saml-glossary-2.0-os.pdf.
- *Metadata for the OASIS Security Assertion Markup Language (SAML) V2.0*. 15 March 2005. OASIS Standard. http://docs.oasis-open.org/security/saml/v2.0/saml-metadata-2.0-os.pdf.
- *Profiles for the OASIS Security Assertion Markup Language (SAML) V2.0*. 15 March 2005. OASIS Standard. http://docs.oasis-open.org/security/saml/v2.0/saml-profiles-2.0-os.pdf.
- *Security Considerations for the OASIS Security Assertion Markup Language (SAML) V2.0*. 15 March 2005. OASIS Standard. http://docs.oasis-open.org/security/saml/v2.0/saml-sec-consider-2.0-os.pdf.
- *SAML Version 2.0 Errata 05*. 01 May 2012. OASIS Approved Errata. http://docs.oasis-open.org/security/saml/v2.0/errata05/os/saml-v2.0-errata05-os.html.

Declared XML namespace:

- urn:oasis:names:tc:xspa: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 Cross-Enterprise Security and Privacy Authorization (XSPA) TC on the above date. The level of approval is also listed above. Check the "Latest 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 https://www.oasis-open.org/committees/xspa/.

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 (https://www.oasis-open.org/committees/xspa/ipr.php).

Citation format:

When referencing this specification the following citation format should be used:

[SAML-XSPA-v2.0]

Cross-Enterprise Security and Privacy Authorization (XSPA) Profile of SAML v2.0 for Healthcare Version 2.0. Edited by John M. Davis, Duane DeCouteau, and Mohammad Jafari. 01 April 2014. OASIS Committee Specification Draft 01. http://docs.oasis-open.org/xspa/saml-xspa/v2.0/csd01/saml-xspa-v2.0-csd01.html. Latest version: http://docs.oasis-open.org/xspa/saml-xspa/v2.0/saml-xspa-v2.0.html.

Notices

All capitalized terms in the following text have the meanings assigned to them in the OASIS Intellectual Property Rights Policy (the "OASIS IPR Policy"). The full Policy may be found at the OASIS website.

This document and translations of it may be copied and furnished to others, and derivative works that comment on or otherwise explain it or assist in its implementation may be prepared, copied, published, and distributed, in whole or in part, without restriction of any kind, provided that the above copyright notice and this section are included on all such copies and derivative works. However, this document itself may not be modified in any way, including by removing the copyright notice or references to OASIS, except as needed for the purpose of developing any document or deliverable produced by an OASIS Technical Committee (in which case the rules applicable to copyrights, as set forth in the OASIS IPR Policy, must be followed) or as required to translate it into languages other than English.

The limited permissions granted above are perpetual and will not be revoked by OASIS or its successors or assigns.

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 name "OASIS" is a trademark 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 https://www.oasis-open.org/policies-guidelines/trademark for above guidance.

Table of Contents

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 following definitions establish additional terminology and usage in this profile:

Access Control Service (ACS)

A service that provides the basic operational aspects of access control such as making access control decision information (ADI) available to access decision components and performing access control functions **[HL7-SLS]**. This service would be utilized by both the Service Provider and/or Service User**.**

Functional Role

Functional roles reflect the essential business functions that need to be performed. Functional roles are defined by a set of standard healthcare tasks such as *Neurologist* **[HL7-ROLE-ENG]**.

Permission

An approval to perform an operation on one or more protected resources **[ANSI-INCITS 359-2004]**.

Structural Role

Structural roles (also known as Organizational Roles) correspond to the organizational positions and represent a job function within the context of an organization. Assigning a user to a structural role **[HL7-ROLE-ENG]**; for example *Attending Physician* **[ASTM E2595]**.

Service Consumer (SC)

An individual entity, such as on an Electronic Health Record (EHR) or personal health record (PHR) system, that makes a service request of a Service Provider.

Service Provider (SP)

A system, such as an electronic health record system at a hospital, which provides protected resources and relies on the provided security service **[HL7-SLS]**.

1.2 Normative References

[RFC2119] Bradner, S., “Key words for use in RFCs to Indicate Requirement Levels”, BCP 14, RFC 2119, March 1997. http://www.ietf.org/rfc/rfc2119.txt.

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

[ANSI-INCITS 359-2004] Role-Based Access Control. 2004.

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

[ASTM E2595] ASTM International, Standard Guide for Privilege Management Infrastructure. 2007.

[SAML] “Security Assertion Markup Language (SAML) v2.0”, OASIS Standard, 15 March 2005, http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf

[HL7-HCS] HL7 Security Technical Committee, HL7 Healthcare Privacy and Security Classification System (HCS) Release 1 September 2013.

[HL7-PERM] HL7 Security Technical Committee, HL7 Version 3 Standard: Role-based Access Control Healthcare Permission Catalog, Release 1, February 2008.

[HL7-RIMv3] HL7 International's Version 3 Normative Edition 2013, May 2013.

[HL7-ROLE-ENG] HL7 Security Technical Committee, HL7 Role-Based Access Control (RBAC) Role Engineering Process Version 1.3, September 2007.

[HL7-SLS] HL7 Version 3 Standard: Privacy, Access and Security Services Conceptual Model; Security Labeling Service, Release 1:2014

[NIST-800-63-1] National Institute of Standards and Technology, Electronic Authentication Guideline, December 2011, http://csrc.nist.gov/publications/nistpubs/800-63-1/SP-800-63-1.pdf

[XACML-V3.0] eXtensible Access Control Markup Language (XACML) Version 3.0. 22 January 2013. OASIS Standard. http://docs.oasis-open.org/xacml/3.0/xacml-3.0-core-spec-os-en.html

1.3 Non-Normative References

[XSPA-EXAMPLES] “Implementers Guide of XSPA for Healthcare – The Nationwide Health Information Network (NwHIN),” OASIS Committee Working Draft, March 2012, https://www.oasis-open.org/committees/download.php/45525/xspa-nwhin-adapter-guide.doc

2 The XSPA Use-Case

Figure 1 depicts an overview of interactions between parties in the exchange of healthcare information. The main scenario is as follows

- A user residing at the Service Consumer (SC) organization initiates a request to access a protected resource which is in custody of the Service Provider (SP).
- This request is captured by the Service Consumer's service interface and authorization is performed by the consumer's Access Control System to make sure the requesting user is authorized to make such a request.
- If the request is deemed authorized, the Service Consumer system, sends a request to its ACS to receive Identity and Authorization Attribute Assertions.
- The SC sends a request to the SP for acquiring a copy of the health record in question. It provides Identity Assertions and Authorization Attributes alongside its request to prove to the SP its identity and that it is authorized to receive the requested resource. These MAY be passed in a single assertion from the SU to the SP. In this request, the attributes of both the requesting user and the Consumer Organization are included.
- The Service Provider's Service Interface captures the request and sends it to the service provider's Access Control Service.
- If the request is deemed authorized, the Service Provider system sends a packaged copy of the requested record to the Consumer System. The copy of the data is not necessarily identical to the original records; it may bear annotations with *handling instructions* and some portions of it may be *redacted* or *masked* per policy requirements.
- The Consumer System receives the protected resource and makes it available to the requesting user while enforcing the corresponding handling instructions and policies.

The above use-case may have some variations.

- The Consumer System may proactively send the request to acquire the record before the user's explicit request. For example, when an appointment is scheduled for a patient at a facility, the Consumer System may request the patient's record in advance, before the physician requests it at the time of appointment. This is especially the case when large data volumes need to be exchanged. Depending on the circumstances, the Consumer System may or may not know the identity of the requesting user at the time of data exchange. For example, if an appointment is scheduled for a patient for next month, the identity of the physician who will be assigned to this appointment may not be known until later.
- Sometimes, a user may initiate the request for exchange on behalf of the actual another user. For example, an admin assistant may initiate a request for the exchange of the record of a patient who will be visited by a physician.

The focus of this profile is the cross-enterprise exchange of the protected resource, which is the exchange between the Service Provider and the Service Consumer.

Entities described in the figure are explained in the subsections below.

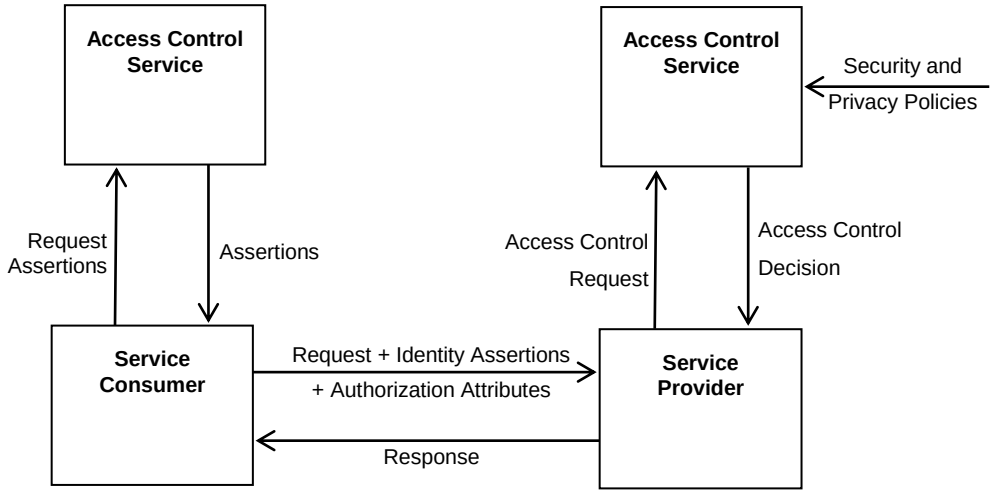

Figure 1: The main event flow in the XSPA use case.

2.1 Service User Access Control Service

The Service Consumer Access Control Service (ACS) provides identity and access control functions for the SC. The Identity Provider (IdP) resides within the ACS although it may actually act as a bridge to a third-part identity attribute provider. Upon request, the ACS produces SAML assertions for the identity and authorization attributes, such as the requesting user's ID, organization ID, structural role, functional role, and purpose of use. These assertions are included in the request sent by the SC to the SP.

2.2 Service Provider Access Control Service

The Service Provider ACS provides identity and access control functions for the SP. It includes components for parsing assertions, evaluating the assertions against the security and privacy policy, and making authorization decisions. The Service Provider enforces the decision made by its ACS.

2.3 Security Policy

The security policy includes the authorization rules applicable to access a protected resource which may be based on various attributes such as the requester's role, purpose of use, time and location of access, etc.

2.4 Privacy Policy

The privacy policy includes the set of privacy rules about packaging (e.g. security labels and handling instructions) and segmenting of resources (e.g. masking and redaction), as well as the preferences of the patient which are encoded as his or her consent directive.

2.5 Attributes

Attributes are information related about the access request (e.g. the user ID, role, location, purpose of use, etc.) which are consequential in making access control decisions.

3 XSPA profile of SAML

The XSPA profile of SAML describes the minimum vocabulary necessary to provide access control over resources and functionality within and between healthcare systems. 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`.

3.1 Data Types

Table 1 the standard data types used for the attributes in this profile. We use the abbreviated form to refer to the data types in the rest of this document.

Table 1: Standard Data Types (Normative)

Type ID	Abbreviated Form
http://www.w3.org/2001/XMLSchema#string	String
http://www.w3.org/2001/XMLSchema#anyURI	anyURI

Table 2 shows the normative data type defined by this profile for representing values belonging to a code system.

Table 2: New Data Types (Normative)

Type ID	Abbreviated Form
urn:hl7-org:v3:cd	HI7CD

This data type, which corresponds to the *Concept Descriptor* (CD) data type in HL7, is a tuple that can model a coded concept. Details of the attributes and the full schema for this data type is presented in Appendix A. The following code depicts an XML encoded example of a value of type CD:

```
<value xmlns="urn:hl7-org:v3" xsi:type="CD"
       code="RECORDMGT"
       displayName="records management"
       codeSystem="2.16.840.1.113883.1.11.20448"
       codeSystemName="Purpose of Use" />
```

3.1 Metadata Definitions

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

3.2 Namespace Requirements

The XML attribute `NameFormat` in `<Attribute>` elements MUST be:

```
urn:oasis:names:tc:SAML:2.0:attrname-format:uri
```

This profile will utilize the following namespaces:

```
urn:oasis:names:tc:xspa:1.0
urn:oasis:names:tc:xspa:2.0
```

3.3 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.

3.4 Attribute Naming Syntax, Restrictions and Acceptable Values

Attribute names MUST adhere to the rules 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) or Uniform Resource Name (URN). The optional XML attribute `FriendlyName` (defined in **[SAMLCore]**) MAY be used for this purpose.

3.5 Example of Use

```
<saml:Attribute
       NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
       Name=" urn:oasis:names:tc:xacml:2.0:action:purpose">
        <saml:AttributeValue>
              <value xmlns="urn:hl7-org:v3" xsi:type="CD"
                     code="RECORDMGT"
                     displayName="records management"
                     codeSystem="2.16.840.1.113883.1.11.20448"
                     codeSystemName="Purpose of Use" />
       </saml:AttributeValue>
</saml:Attribute>
```

Table 3: Attributes

Normative	Identifier[1]	Type	Description and Valid Values
Yes	`urn:oasis:names:tc:xacml:1.0:subject:subject-id`	String	The End User's identifier. Deprecates `urn:oasis:names:tc:xspa:1.0:subject:subject-id`
Yes	`urn:oasis:names:tc:xspa:1.0:organization`	String	The name of the organization to which the requesting End User belongs.
Yes	`urn:oasis:names:tc:xspa:1.0:subject:organization-id`	anyURL	The unique identifier of the organization, sub-organization and facility of the Service Consumer. To represent the organizational hierarchy, using `urn:oasis:names:tc:xspa:2.0:subject:organizational-hierarchy` (below) is preferred.
Yes	`urn:oasis:names:tc:xspa:1.0:subject:child-organization`	anyURI	
Yes	`urn:oasis:names:tc:xspa:1.0:subject:facility`	anyURI	

[1] Line-breaks in this column are for the purpose of readability and type setting; attribute identifiers are strings with no line-breaks.

Normative	Identifier[1]	Type	Description and Valid Values
Yes	urn:oasis:names:tc:xspa:2.0:subject:organizational-hierarchy	anyURI	Unique identifiers of the consuming sub-organizations. This is an alternative to using the separate attributes for each level as defined above. Various levels of sub-organizations hierarchy shall be represented as multiple values of type anyURI in order of the most significant organization to the least.
Yes	urn:oasis:names:tc:xacml:2.0:subject:role	HL7CD	The requesting user's structural role. The values must be taken from a standard vocabulary such as the structural roles referenced in **[ASTM E1986-98]**.
No	urn:oasis:names:tc:xspa:1.0:subject:functional-role	HL7CD	Functional roles provide a placeholder to group permissions required for fine grain access control. The values must come from a standard vocabulary.
No	urn:oasis:names:tc:xspa:1.0:subject:npi	String	National Provider ID provided by U.S. Government for all active providers as required by Health Insurance Portability and Accountability Act (HIPAA) Privacy Disclosure Accounting.
No	urn:oasis:names:tc:xspa:1.0:permissions	HL7CD	The requesting user's permissions which represent the user's capabilities. The values must be taken from a standard vocabulary such as HL7 RBAC Permission Catalog **[HL7-PERM]**.
No	urn:oasis:names:tc:xspa:2.0:confidentiality-clearance	HL7CD	The requesting user's confidentiality clearance. The values must be taken from a standard vocabulary such as HL7 Confidentiality Codeset **[HL7-HCS]**.
No	urn:oasis:names:tc:xspa:2.0:sensitivity-clearance	HL7CD	The requesting user's sensitivity clearance. The values must be taken from a standard vocabulary such as HL7 ActInformationSensitivityCodes **[HL7-HCS]**.
Yes	urn:oasis:names:tc:xacml:1.0:resource:resource-id	String	Unique identifier of the resource defined by and controlled by the Servicing Provider. In the XSPA use-case this is the patient unique identifier. The mechanism for identifying patients in a standardized way is outside the scope of the profile.
Yes	urn:oasis:names:tc:xspa:2.0:resource:type	HL7CD	The type of the resource. The values must be taken from a standard vocabulary such as **[HL7-PERM]**. Deprecates urn:gov:hhs:fha:nhinc:service-type
Yes	urn:oasis:names:tc:xspa:2.0:resource:patient-consent	anyURI	The pointer to the patient consent corresponding to the requested resource.
Yes	urn:oasis:names:tc:xacml:1.0:action:action-id	HL7CD	The identifier of the requested action. The values must be taken from a standard vocabulary such as **[HL7-PERM]**.
Yes	urn:oasis:names:tc:xacml:2.0:action:purpose	HL7CD	The purpose of use for the requested resource. The values must be taken from a standard purpose of use vocabulary such as HL7 Security and Privacy Vocabulary **[HL7-HCS]**.

Normative	Identifier[1]	Type	Description and Valid Values
Yes	urn:oasis:names:tc:xspa:2.0:subject:supported-obligations	HL7CD	List of obligations that the service consumer ACS supports. This is encoded as a multi-valued attribute with values taken from a standard vocabulary such as HL7 Security and Privacy Vocabulary **[HL7-HCS]**.
Yes	urn:oasis:names:tc:xspa:2.0:subject:supported-refrains	HL7CD	List of refrains that the service consumer ACS supports. This is encoded as a multi-valued attribute with values taken from a standard vocabulary such as HL7 Security and Privacy Vocabulary **[HL7-HCS]**.

Table 4 shows the list of deprecated attributes. These attributes SHALL still be supported but the vendors should be warned that the future versions of this profile may no longer support these attributes.

Table 4: Attributes Planned for Deprecation

Normative	Identifier	Type	Description and Valid Values
No	urn:oasis:names:tc:xspa:1.0:subject:subject-id	String	Deprecated by: urn:oasis:names:tc:xacml:1.0:subject:subject-id
No	urn:gov:hhs:fha:nhinc:service-type	String	Deprecated by: urn:oasis:names:tc:xspa:2.0:resource:type
No	urn:oasis:names:tc:xspa:1.0:subject:purposeofuse	String	Deprecated by: urn:oasis:names:tc:xacml:2.0:action:purpose

4 Other Considerations

4.1 Error States

This profile adheres to error states describe in SAML 2.0.

4.2 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.

4.2.1 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.

4.2.2 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.

4.3 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 **[NIST-800-63-1]**. In addition, this profile specifies the Liberty Identity Access Framework (LIAF) criteria for evaluating and approving credential service providers.

5 Conformance

In order to claim conformance, an implementation must conform to SAML 2.0 and support the attributes listed in Table 5.

Table 5: Conformance Attributes

Identifiers	Normative
urn:oasis:names:tc:xacml:1.0:subject:subject-id	Yes
urn:oasis:names:tc:xspa:1.0:organization	Yes
urn:oasis:names:tc:xspa:1.0:subject:organization-id	Yes
urn:oasis:names:tc:xspa:1.0:subject:child-organization	Yes
urn:oasis:names:tc:xspa:1.0:subject:facility	Yes
urn:oasis:names:tc:xspa:2.0:subject:organizational-hierarchy	Yes
urn:oasis:names:tc:xacml:2.0:subject:role	Yes
urn:oasis:names:tc:xspa:1.0:subject:functional-role	No
urn:oasis:names:tc:xspa:1.0:subject:npi	No
urn:oasis:names:tc:xspa:1.0:permissions	No
urn:oasis:names:tc:xspa:2.0:confidentiality-clearance	No
urn:oasis:names:tc:xspa:2.0:sensitivity-clearance	No
urn:oasis:names:tc:xacml:1.0:resource:resource-id	Yes
urn:oasis:names:tc:xspa:2.0:resource:type	Yes
urn:oasis:names:tc:xspa:2.0:resource:patient-consent	Yes
urn:oasis:names:tc:xacml:1.0:action:action-id	Yes
urn:oasis:names:tc:xacml:2.0:action:purpose	Yes
urn:oasis:names:tc:xspa:2.0:subject:supported-obligations	Yes
urn:oasis:names:tc:xspa:2.0:subject:supported-refrains	Yes
urn:oasis:names:tc:xspa:1.0:subject:subject-id	No
urn:gov:hhs:fha:nhinc:service-type	No
urn:oasis:names:tc:xspa:1.0:subject:purposeofuse	No

Appendix A. HL7 Concept Descriptor Data Type

The Concept Descriptor data type is a complex data type including the following fields:

Name	Description
code	The plain code symbol defined by the code system, or an expression in a syntax defined by the code system which describes the concept.
codeSystem	The code system that defines the code.
codeSystemName	The common name of the coding system.
codeSystemVersion	If applicable, a version descriptor defined specifically for the given code system.
valueSet	The value set that applied when this CD was created.
valueSetVersion	The version of the value set that applied when this CD was created.
displayName	A name, title, or representation for the code or expression as it exists in the code system identified by the value of codeSystem.
originalText	The text as seen and/or selected by the user who entered the data which represents the intended meaning of the user.
codingRationale	The reason a particular CD has been provided.
translation	A set of other CDs that each represent a translation of this CD into equivalent codes within the same code system or into corresponding concepts from other code systems.
source	The CD from which this CD was translated, if it was translated from another CD.

The XML schema for this data type is as follows. For the complete schema of all the related HL7 types see **[HL7-RIMv3]**.

```
<xsd:complexType name="CD">
  <xsd:annotation>
    <xsd:appinfo>
      <sch:pattern name="null or code and/or originalText">
        <sch:rule abstract="true" id="CD-0">
          <sch:assert test="@nullFlavor or @code or (originalText and
not(originalText/@nullFlavor) or (originalTextReference and
not(originalTextReference/@nullFlavor))"/>
        </sch:rule>
      </sch:pattern>
      <sch:pattern name="other requires codeSystem or valueSet">
        <sch:rule abstract="true" id="CD-1">
          <sch:assert test="@nullFlavor != "OTH" or @codeSystem or @valueSet"/>
        </sch:rule>
      </sch:pattern>
      <sch:pattern name="code requires codeSystem">
        <sch:rule abstract="true" id="CD-2">
          <sch:assert test="@codeSystem or not(@code)"/>
        </sch:rule>
      </sch:pattern>
      <sch:pattern name="codeSystemName only if codeSystem">
        <sch:rule abstract="true" id="CD-3">
          <sch:assert test="@codeSystem or not(@codeSystemName)"/>
        </sch:rule>
```

```
      </sch:pattern>
      <sch:pattern name="codeSystemVersion only if codeSystem">
        <sch:rule abstract="true" id="CD-4">
          <sch:assert test="@codeSystem or not(@codeSystemVersion)"/>
        </sch:rule>
      </sch:pattern>
      <sch:pattern name="displayName only if code">
        <sch:rule abstract="true" id="CD-5">
          <sch:assert test="@code or not(@displayName)"/>
        </sch:rule>
      </sch:pattern>
      <sch:pattern name="valueSet requires valueSetVersion">
        <sch:rule abstract="true" id="CD-6">
          <sch:assert test="not(@valueSet) or (@valueSet and @valueSetVersion)"/>
        </sch:rule>
      </sch:pattern>
      <sch:pattern name="No original text on translations">
        <sch:rule abstract="true" id="CD-7">
          <sch:assert test="not translation/originalText"/>
        </sch:rule>
      </sch:pattern>
      <sch:pattern name="Translations cannot have translations">
        <sch:rule abstract="true" id="CD-8">
          <sch:assert test="not translation/translation"/>
        </sch:rule>
      </sch:pattern>
      <sch:pattern name="no updateMode or History on CD elements">
        <sch:rule abstract="true" id="CD-9">
          <sch:assert test="count(*[self::displayName or self::originalText or
self::originalTextReference or self::translation][@validTimeLow or @validTimeHigh or
@controlActRoot or @controlActExtension or @updateMode])=0"/>
        </sch:rule>
      </sch:pattern>
    </xsd:appinfo>
  </xsd:annotation>
  <xsd:complexContent>
    <xsd:extension base="ANY">
      <xsd:sequence>
        <xsd:element name="displayName" type="ST" minOccurs="0"/>
        <xsd:element name="originalText" type="ED" minOccurs="0"/>
        <xsd:element name="translation" type="CD" minOccurs="0" maxOccurs="unbounded"/>
        <xsd:element name="source" type="XReference" minOccurs="0"/>
      </xsd:sequence>
      <xsd:attribute name="code" type="xsd:string" use="optional"/>
      <xsd:attribute name="codeSystem" type="Uid" use="optional"/>
      <xsd:attribute name="codeSystemName" type="xsd:string" use="optional"/>
      <xsd:attribute name="codeSystemVersion" type="xsd:string" use="optional"/>
      <xsd:attribute name="valueSet" type="Uid" use="optional"/>
      <xsd:attribute name="valueSetVersion" type="xsd:string" use="optional"/>
      <xsd:attribute name="codingRationale" type="CodingRationale" use="optional"/>
      <xsd:attribute name="id" type="xsd:ID" use="optional"/>
```



```
    </xsd:extension>
  </xsd:complexContent>
</xsd:complexType>
```


Appendix B. Acknowledgments

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

Participants:

Kel Callahan, HIPAAT International, Inc.
John Davis, Veterans Health Administration
DeCouteau, Duane, Veterans Health Administration
Mohammad Jafari, Veterans Health Administration

The TC especially thanks Kathleen Connor from HL7 Security and Privacy workgroup for her contribution to this profile.

Appendix C. Revision History

Revision	Date	Editor	Changes Made
saml-xspa-2.0-wd01	11 Mar 2012	Duane DeCouteau	Working Draft revisions 01
saml-xspa-2.0-wd02	6 April 2012	Duane DeCouteau	Comments and Changes updated from April 6th TC Meetings.
saml-xspa-2.0-wd03	27 April 2012	Duane DeCouteau	Comments and Changes updated from April 27th TC Meetings
saml-xspa-2.0-wd04	23 May 2012	Duane DeCouteau	Update to organizational-heirarchy purpose of use vocabulary, supported-obligation-policies, supported-refrain-policies
saml-xspa-2.0-wd05	19 July 2013	Mohammad Jafari	Updating the template. Minor editorial corrections.
saml-xspa-2.0-wd05	11 March 2014	Mohammad Jafari	Update to the structure and attribute IDs. - Harmonization with XACML standard attributes.
saml-xspa-2.0-wd05	21 March 2014	Mohammad Jafari	Added HL7 CD data type. Updated the conformance table.
saml-xspa-2.0-wd05	28 March 2014	Mohammad Jafari	Comments from March 25 meeting.