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

Committee Specification Draft 02 / Public Review Draft 02

16 March 2017

Specification URIs

This version:

http://docs.oasis-open.org/xspa/saml-xspa/v2.0/csprd02/saml-xspa-v2.0-csprd02.docx (Authoritative)
http://docs.oasis-open.org/xspa/saml-xspa/v2.0/csprd02/saml-xspa-v2.0-csprd02.html
http://docs.oasis-open.org/xspa/saml-xspa/v2.0/csprd02/saml-xspa-v2.0-csprd02.pdf

Previous version:

http://docs.oasis-open.org/xspa/saml-xspa/v2.0/csprd01/saml-xspa-v2.0-csprd01.doc (Authoritative)
http://docs.oasis-open.org/xspa/saml-xspa/v2.0/csprd01/saml-xspa-v2.0-csprd01.html
http://docs.oasis-open.org/xspa/saml-xspa/v2.0/csprd01/saml-xspa-v2.0-csprd01.pdf

Latest version:

http://docs.oasis-open.org/xspa/saml-xspa/v2.0/saml-xspa-v2.0.docx (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*. Edited by Mike Davis, Duane DeCouteau and David Staggs. 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*. Edited by John Kemp, Scott Cantor, Prateek Mishra, Rob Philpott, and Eve Maler. 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*. Edited by Scott Cantor, Frederick Hirsch, John Kemp, Rob Philpott, and Eve Maler. 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*. Edited by Prateek Mishra, Rob Philpott, and Eve Maler. 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*. Edited by Scott Cantor, John Kemp, Rob Philpott, and Eve Maler. 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*. Edited by Jeff Hodges, Rob Philpott, and Eve Maler. 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*. Edited by Scott Cantor, Jahan Moreh, Rob Philpott, and Eve Maler. 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*. Edited by John Hughes, Scott Cantor, Jeff Hodges, Frederick Hirsch, Prateek Mishra, Rob Philpott, and Eve Maler. 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*. Edited by Frederick Hirsch, Rob Philpott, and Eve Maler. 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*. Edited by Scott Cantor. 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 namespaces:

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

Abstract:

This profile defines a set of SAML attributes and corresponding vocabularies for healthcare information exchange applications.

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. Any other numbered Versions and other technical work produced by the Technical Committee (TC) are listed at https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=xspa#technical.

TC members should send comments on this specification to the TC’s email list. Others should send comments to the TC’s public comment list, after subscribing to it by following the instructions at the “Send A Comment” button on the TC’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).

Note that any machine-readable content (Computer Language Definitions) declared Normative for this Work Product is provided in separate plain text files. In the event of a discrepancy between any such plain text file and display content in the Work Product's prose narrative document(s), the content in the separate plain text file prevails.

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. 16 March 2017. OASIS Committee Specification Draft 02 / Public Review Draft 02. http://docs.oasis-open.org/xspa/saml-xspa/v2.0/csprd02/saml-xspa-v2.0-csprd02.html. Latest version: http://docs.oasis-open.org/xspa/saml-xspa/v2.0/saml-xspa-v2.0.html.

Notices

Table of Contents

1 Introduction

This profile defines a set of SAML attributes and corresponding vocabularies for healthcare information exchange applications.

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: Appendix A. Glossary of Terms]**. This service would be utilized by both the Service Provider and/or Service User.

Functional Role

Functional roles are roles that are bound to the realization/performance of actions, such as *Authorizer*. **[ISO/TS 21298:2008: 5.5 Functional Roles]**.

Permission

An approval to perform an operation on one or more protected resources **[ANSI-INCITS 359-2004: 4. Terms and Definitions]**.

Principal

An entity whose identity can be authenticated. Examples include a human user, a process, a system, or an organization **[ITUT-X.811: 3.15. Principal]**.

Structural Role

Structural roles (also referred to as Organizational Roles) correspond to human or organizational categories and describe prerequisites, feasibilities, or competences for actions, for example *Dental Assistant*. Structural roles differ from policy domain to policy domain, within and across organizational boundaries, and especially between different jurisdictions and countries. **[ISO/TS 21298:2008: 5.3 Structural Roles]**.

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: Appendix A. Glossary of Terms]**.

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.

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

[ASTM E1986-09(2013)] ASTM International, Standard Guide for Information Access Privileges to Health Information, DOI: 10.1520/E1986-09R13, 2013.

[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

[SAML-PROF] "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

[HL7-HCS] HL7 Security Technical Committee, HL7 Healthcare Privacy and Security Classification System (HCS) Release 1, August 2014. http://www.hl7.org/implement/standards/product_brief.cfm?product_id=345

[ISO 21090:2011] International Organization for Standardization, ISO 21090, Health Informatics--Harmonized Data Types for Information Interchange, 2011.

[ISO/TS 21298:2008] International Organization for Standardization, ISO/TS 21298, Health Informatics-- Functional and Structural Roles, 2008.

[HL7-PERM] HL7 Security Technical Committee, HL7 Version 3 Standard: Role-based Access Control Healthcare Permission Catalog, Release 2, February 2010. http://www.hl7.org/implement/standards/product_brief.cfm?product_id=72

[HL7-SLS] HL7 Version 3 Standard: Privacy, Access and Security Services Conceptual Model; Security Labeling Service, Release 1:2014. http://www.hl7.org/implement/standards/product_brief.cfm?product_id=360

[ITUT-X.811] ITU-T Recommendation X.811, Information Technology, Open Systems Interconnection, Security Framework for Open Systems, Authentication Framework, April 1995.

[NIST-800-63-1] National Institute of Standards and Technology, Special Publication 800-63-1, 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

[HL7-Core-Schema-v3] HL7 International's Version 3 Normative Edition 2013, Processable Content, Core Schemas, ISO 21090 HL7 R2 Data Types, May 2013.

[JSON] T. Bray, The JavaScript Object Notation (JSON) Data Interchange Format, https://tools.ietf.org/html/rfc7159

2 The XSPA Use-Cases

{non-normative}

The core use-cases for this profile are the cross-enterprise exchange of protected data objects from a Service Provider (SP) to a Service Consumer (SC). Figure 1 depicts an overview of these use-cases. Entities in this figure will be discussed in the upcoming subsections.

There are two main exchange use-cases: Pull and Push. In the Pull scenario, the SC sends a request to the SP asking for a data object (a Read command). In the Push Scenario, the SC sends a request to the SP which includes some data object to be accepted by the SP (a Create or Update command).

In some cases, the request may include only a command and no data (a Delete or Execute command). The event flow for processing such requests is similar to that of Push.

In both scenarios, the request includes SAML attribute assertions that vouch for the identity of the requesting Principal and other attribute that are consequential in making the access control decision at the SP's side such as the SC's organizational attributes and transaction attributes such as the purpose of use.

In the Pull scenario, these attributes are used by the SP's ACS to make the decision whether or not the requesting Principal is authorized to receive a copy of the requested data. In the Push scenario, these attributes are used by the SP's ACS to decide whether or not the requesting Principal is authorized to add new data to the SP, update existing data, or run a command such as Delete. These attributes may also vouch for the identity attributes of the Principal's signature on the submitted data object. In both scenarios, the presented attributes are also used by the SP to record auditing information about the transaction.

In the Pull scenario, the SP's response includes the requested data (if the request is authorized) or otherwise, a signaling message indicating the SP's decision that the request is unauthorized. In the Push scenario, the SP's response includes the signaling message indicating whether or not the request was accepted by the SP.

In addition to the main cases described above the attributes names and values defined in this profile can be used in some other cases as well. For example, the SP may include some SAML Assertions in its response to vouch for some of SP's organizational attributes, or carry the identity attributes of the signer of the data object when a requested data object is included in the response. Some of these attributes may also be used by either of the parties involved in the information exchange to record an audit event.

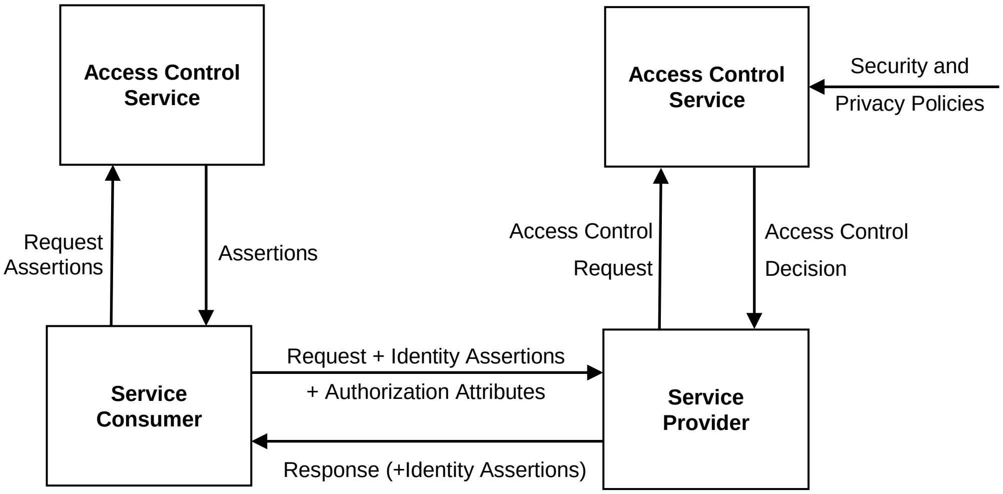

Figure 1: The main event flow in the XSPA use case.

2.1 The Pull Use-Case

The main scenario for Pull is as follows

- A Principal residing at the SC initiates a request to access a protected resource residing at the SP.
- SC's ACS performs authorization to make sure the requesting Principal is authorized to make such a request. The current profile does not cover this transaction.
- If the request is deemed authorized, the SC sends a request to its ACS to receive Identity and Authorization Attribute Assertions corresponding to the Principal, the organization, and the context of the transaction, e.g. purpose of use.
- The SC sends a request to the SP for receiving a copy of the data object in question. The request includes the Identity Assertions and other Authorization Attributes.
- The SP captures the request and calls its own ACS.
- If the ACS deems the request authorized, the SP sends a packaged copy of the requested data object to the SC. This copy is not necessarily identical to the original data; it may be annotated with security labels and handling instructions or some portions of it may be redacted or masked depending on the policies.
- The SC receives the packaged data and makes the data available to the requesting Principal while enforcing the corresponding handling instructions and policies.

2.1.1 Variations

The Pull use-case may have some variations.

- **Proactive Pull:** The SC may proactively send the request to acquire the data before the Principal's request. For example, when an appointment is scheduled for a patient at a facility, the scheduling system at the facility may request the patient's health record in advance, before the physician explicitly asks for it at the time of appointment. In such cases, the Principal making the request is a system entity, e.g. the scheduling system. This is especially the case when large data volumes need to be exchanged or the connection has a high latency/delay. Depending on the circumstances, at the time of data exchange the SC may or may not know the precise identity of the principal which will eventually use the data. For example, if an appointment is scheduled for a patient a week in advance, the identity of the physician assigned to the appointment may not be known in advance and at the time of exchange. In such cases, only a limited set of attributes will be provided by SC.
- **Delegated Pull:** A Principal may initiate a request on behalf of another Principal, for example, an admin assistant may request a patient's record on behalf of a physician. In such cases, depending on the application, the asserted attributes may include the attributes of either or both Principals.
- **Poll-Based Subscription:** The Principal may register with a Subscription Broker at SC's side to set up a poll-based subscription so that the Broker repeats the request on a regular basis to get a fresh copy of the requested data objects. Depending on the frequency of the poll, the Broker may also re-use the assertions issued by its local ACS if they are still valid. This is equivalent to making multiple Pull requests.
- **Notification-Based Subscription:** A Broker at the SP's side can provide a subscription service so that the SC can register to receive a fresh copy of the data object whenever the data object is updated. This is equivalent to sending a Pull request and receiving multiple responses.

2.2 The Push Use-Case

The main scenario for Push is as follows

- The Principal residing at the SC initiates a Push request to submit a data object to SP. This may be for creating a new data object or updating an existing one.

- SC’s ACS performs authorization to make sure the requesting Principal is authorized to make such a request. The current profile does not cover this transaction.
- If the request is deemed authorized, the SC sends a request to its ACS to receive attribute assertions corresponding to the Principal, the organization, and the transaction.
- The SC sends a Push request to the SP which includes a data object to be submitted to SP as well as the attribute assertions corresponding to the requesting principal and the SC.
- The SP captures the request and calls its own ACS.
- If the ACS finds the request authorized, the SP consumes the data object and sends back a signaling message to acknowledge the receipt of data. This may include other information such as the unique identifier assigned to the data object by the server in the case of creating a new data object.

2.3 Service Consumer Access Control Service

The Service Consumer Access Control Service (ACS) provides identity and access control functions to the SC. The Identity Provider (IdP) resides within the ACS although it may also act as a bridge to a third-party identity 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.

2.4 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 policies and making authorization decisions, security labeling services for deciding security labels for a data object, and privacy preserving services for enforcing privacy decisions such as masking and redaction. The Service Provider enforces the decisions made by its ACS.

2.5 Security and Privacy Policies

Security and privacy policies include the rules applicable to accessing protected resources. Such rules are based on various attributes such as the requesting Principal’s, organization, role, purpose of use, security clearance, time and location of access, etc. They may also include rules about packaging the data objects (e.g. annotating with security labels and handling instructions) and segmenting the data (e.g. masking or redacting parts of the data object), as well as patients’ preferences encoded as patient Consent Directives. This profile does not discuss the details of such policies.

2.6 Attributes

Attributes are information pertaining to the access request such as the user ID, role, organization, and purpose of use 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. The XSPA profile of SAML is an Attribute Profile as defined by Section 2.2 of Profiles for the OASIS Security Assertion Markup Language (SAML) **[SAML-PROF]**.

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 shows 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`

Moreover, this profile defines a special data type, based on Concept Descriptor (CD) **[ISO 21090:2011: 7.5.2 CD (Concept Descriptor)]** which is also commonly used by HL7 **[HL7-Core-Schema-v3]**. The Concept Descriptor structure can capture values belonging to a code system by specifying the value code alongside the code for the vocabulary.

Concept descriptors can be encoded in various forms including a number of XML structures. In order to keep the attribute values in this profile within the basic XML data types and guarantee interoperability with existing SAML and XACML products which may not support complex XML data structures, we suggest the following scheme to flatten CDs into a value of type `anyURI`:

[Fully-Qualified Unique identifier of the Code System ID]/[Code]

For example, the purpose of "record management" (`RECORDMGT`) from HL7's purpose of use vocabulary (`2.16.840.1.113883.1.11.20448`) can be encoded as the following:

```
<saml:Attribute
      xmlns:xacmlprof="urn:oasis:names:tc:SAML:2.0:profiles:attribute:XACML"
      NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
      Name="urn:oasis:names:tc:xacml:2.0:action:purpose"
      xacmlprof:DataType="http://www.w3.org/2001/XMLSchema#anyURI">
  <saml:AttributeValue xsi:type="http://www.w3.org/2001/XMLSchema#anyURI">
      2.16.840.1.113883.1.11.20448/RECORDMGT
  </saml:AttributeValue>
</saml:Attribute>
```

Note that the above mechanism for flattening the CD structure into a value of type `anyURI` requires some caution when the codes include URI-reserved characters such as the delimiter character "/". In such cases the implementers must either use URI-encoding or use XML complex datatypes discussed below in order to avoid any ambiguity.

If an ACS implementation supports complex attribute values and can guarantee interoperability with other ACS components, it MAY use XML encodings of the Concept Descriptor. The following two examples demonstrate using two different alternative XML encodings for Concept Descriptor attribute values:

```
<saml:Attribute
      xmlns:xacmlprof="urn:oasis:names:tc:SAML:2.0:profiles:attribute:XACML"
      NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
```

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

```
<saml:Attribute
       xmlns:xacmlprof="urn:oasis:names:tc:SAML:2.0:profiles:attribute:XACML"
       NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
       Name="urn:oasis:names:tc:xacml:2.0:action:purpose"
       xacmlprof:DataType="http://hl7.org/fhir/coding">
       <saml:AttributeValue
              xsi:type=http://hl7.org/fhir/coding
              xmlns:fhir="http://hl7.org/fhir">
            <fhir:code>
              <fhir:system fhir:value="2.16.840.1.113883.1.11.20448" />
              <fhir:code fhir:value="RECORDMGT" />
           </fhir:code>
       </saml:AttributeValue>
</saml:Attribute>
```

3.2 Namespace Requirements

This profile defines the following namespaces:

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

3.3 Assertion Structure

This profile uses the SAML `<Attribute>` element for all assertions. Since SAML Core Specifications require having a `<Subject>` element when attribute assertions are provided, it is RECOMMENDED that the value of `<NameID>` is provided with an appropriate value for `Format` and match the value of the following attribute if present:

```
urn:oasis:names:tc:xacml:1.0:subject:subject-id
```

3.4 Attribute Naming Syntax, Restrictions and Acceptable Values

Attribute names MUST adhere to the rules defined by Section 2.7.3.1 of SAML 2.0 Core Specifications **[SAMLCore]**.

Additionally, to guarantee interoperability with OASIS eXtensible Access Control Markup Language (XACML), attribute names and values MUST also adhere to the XACML Attribute Profile of SAML **[SAML-PROF:8.5 XACML Attribute Profile]**.

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

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

The optional XML attribute `FriendlyName` (defined in Section 2.7.3.1 of SAML Core Specifications **[SAMLCore]**) MAY be used to carry an optional string name for the purposes of human readability.

As prescribed by the XACML Attribute Profile of SAML **[SAML-PROF:8.5 XACML Attribute Profile]**, each attribute element also includes a URI-valued XML attribute called `DataType` in the following XML namespace:

```
urn:oasis:names:tc:SAML:2.0:profiles:attribute:XACML
```

The DataType XML attribute MUST be present unless its value can be assumed to be the default, i.e. http://www.w3.org/2001/XMLSchema#string.

3.5 Attribute Rules of Equality

Two <Attribute> elements refer to the same SAML attribute if and only if their Name XML attribute values are equal in a binary comparison. The optional XML attribute FriendlyName plays no role in the comparison.

3.6 Attributes

Table 2 shows the normative and optional attributes defined by this profile. Table 3 shows the list of deprecated attributes. Future versions of this profile may no longer support these attributes.

Table 2: Attributes

Normative	Identifier[1]	DataType	Description and Valid Values
Yes	urn:oasis:names:tc:xacml:1.0:subject:subject-id	String	The Principal's identifier. Deprecates urn:oasis:names:tc:xspa:1.0:subject:subject-id
Yes	urn:oasis:names:tc:xspa:1.0:subject:organization	String	The name of the organization to which the requesting Principal belongs if applicable.
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	
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 Principal's structural role. The values must be taken from a standard vocabulary such as the ASTM Structural Roles Vocabulary **[ASTM E1986-09(2013)]**.
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.

[1] In this and subsequent tables, line-breaks in attribute names are for the purpose of type setting and readability; attribute identifiers are strings with no line-breaks.

Normative	Identifier[1]	DataType	Description and Valid Values
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:subject:permissions	HL7CD	The requesting Principal'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:subject:confidentiality-clearance	HL7CD	The requesting Principal'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:subject:sensitivity-clearance	HL7CD	The requesting Principal's sensitivity clearance. The values must be taken from a standard vocabulary such as HL7 ActInformationSensitivityCodes **[HL7-HCS]**.
No	urn:oasis:names:tc:xspa:2.0:subject:integrity-clearance	HL7CD	The requesting Principal's integrity clearances. The values must be taken from a standard vocabulary such as HL7 Data Integrity Codeset **[HL7-HCS]**.
No	urn:oasis:names:tc:xspa:2.0:subject:compartment-clearance	HL7CD	The requesting Principal's integrity clearance. The values must be taken from a standard vocabulary.
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: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]**.
Yes	urn:oasis:names:tc:xspa:2.0:subject:supported-obligations	HL7CD	List of caveats 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 caveats 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]**.
No	urn:oasis:names:tc:xspa:2.0:resource:patient-consent-directive	anyURI	The pointer to the patient consent directive corresponding to the requested resource.

Normative	Identifier[1]	DataType	Description and Valid Values
No	urn:oasis:names:tc:xspa:2.0:resource:patient-consent-directive-type	anyURI	In case the pointer to the patient consent attribute (above) is used, optionally, a document type can be specified using this attribute. This attribute SHALL NOT be present without a corresponding urn:oasis:names:tc:xspa:2.0:resource:patient-consent-directive attribute.

Table 3: Attributes Planned for Deprecation

Normative	Identifier	DataType	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

{non-normative}

4.1 Error States

This profile adheres to error states described SAML 2.0 Core Specifications **[SAMLCore].**

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.

4.4 JSON Encoding

Many modern applications use protocols other than SAML which are based on JSON **[JSON]** but need to exchange the same attributes as defined in this profile —sometimes referred to as *claims*. This profile suggests using the same attribute identifiers in JSON format. Attribute values of type `String` and anyURI can be encoded straightforwardly in JSON. For encoding values of type Hl7CD, implementers should either use the flattened notation described in Section 3.1 or use the following JSON structure:

```
{
  "system":[code system id]
  "code":[code]
}
```

The example attribute assertion from Section 3.1 can thus be encoded in JSON as:

```
{
  "urn:oasis:names:tc:xacml:2.0:action:purpose":
  {
    "system":"2.16.840.1.113883.1.11.20448",
    "code":"RECORDMGT",
  }
}
```

Note in both of the above snippets the whitespace is added only for the sake of readability.

5 Conformance

In order to claim conformance, an access control system MUST conform to Section 2 of SAML 2.0 Core Specifications **[SAML]** and support all the requirements mentioned in Sections 3.1 and Section 3.3 through 3.7 including all the attributes marked as normative in Table 2.

5.1 US-Realm Conformance

In addition to the above requirements, an access control system belonging to the United States jurisdiction MUST use specific vocabularies for some of the attributes values as described in Table 4. Note that some of these value-sets are extensible and therefore new extended values can be added to the vocabulary if needed.

Table 4. Vocabulary Requirements for US-Realm Conformance

Attribute Identifier	Vocabulary
`urn:oasis:names:tc:xacml:2.0:subject:role`	ASTM Structural Roles Vocabulary **[ASTM E1986-09(2013)]**.
`urn:oasis:names:tc:xspa:1.0:subject:permissions`	HL7 Healthcare Permissions Vocabulary **[HL7-PERM: Appendix A - Healthcare Permission Tables]**.
`urn:oasis:names:tc:xspa:2.0:subject:confidentiality-clearance`	HL7 Confidentiality Codeset (OID: 2.16.840.1.113883.5.25) **[HL7-HCS: Security Observation Vocabulary]**.
`urn:oasis:names:tc:xspa:2.0:subject:sensitivity-clearance`	HL7 Information Sensitivity Codeset (OID: 2.16.840.1.113883.5.4) **[HL7-HCS: Security Observation Vocabulary]**.
`urn:oasis:names:tc:xspa:2.0:subject:integrity-clearance`	HL7 Integrity Codeset (OID: 2.16.840.1.113883.5.1063) **[HL7-HCS: Security Observation Vocabulary]**.
`urn:oasis:names:tc:xspa:2.0:subject:compartment-clearance`	HL7 Information Compartment Codeset (OID: 2.16.840.1.113883.5.4) **[HL7-HCS: Security Observation Vocabulary]**.
`urn:oasis:names:tc:xspa:2.0:resource:type`	HL7 Healthcare Object Codeset **[HL7-PERM: 6.Object Definitions]**.
`urn:oasis:names:tc:xacml:1.0:action:action-id`	HL7 Healthcare Operations Codeset **[HL7-PERM: 5. Operation Definitions]**.
`urn:oasis:names:tc:xacml:2.0:action:purpose`	HL7 Purpose of Use Codeset (OID: 2.16.840.1.113883.5.8) **[HL7-HCS: Security Observation Vocabulary]**.
`urn:oasis:names:tc:xspa:2.0:subject:supported-obligations`	HL7 Obligation and Refrain Policy Codeset (OID: 2.16.840.1.113883.5.4) **[HL7-HCS: Security Observation Vocabulary]**.
`urn:oasis:names:tc:xspa:2.0:subject:supported-refrains`	HL7 Obligation and Refrain Policy Codeset (OID: 2.16.840.1.113883.5.4) **[HL7-HCS: Security Observation Vocabulary]**.

Appendix A. Acknowledgments

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

Participants:

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

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

Appendix B. 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 Apr. 2012	Duane DeCouteau	Comments and Changes updated from April 6th TC Meetings.
saml-xspa-2.0-wd03	27 Apr. 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 Jul. 2013	Mohammad Jafari	Updating the template. Minor editorial corrections.
saml-xspa-2.0-wd05	11 Mar. 2014	Mohammad Jafari	Update to the structure and attribute IDs. - Harmonization with XACML standard attributes.
saml-xspa-2.0-wd05	21 Mar. 2014	Mohammad Jafari	Added HL7 CD data type. Updated the conformance table.
saml-xspa-2.0-wd05	28 Mar. 2014	Mohammad Jafari	Comments from March 25 meeting.
saml-xspa-2.0-csd01	1 Apr. 2014	Mohammad Jafari	Approved by the TC as CSD.
saml-xspa-2.0-wd06	25 Jun. 2014	Mohammad Jafari	Public Review Comments Adding push scenario
saml-xspa-2.0-wd06	10 Sep. 2014	Mohammad Jafari	Resolved OASIS Technical Advisory Board Comments
saml-xspa-2.0-wd06	15 Oct. 2014	Mohammad Jafari	Added US-realm conformance clauses.
saml-xspa-2.0-wd06	25 Nov 2014	Mohammad Jafari	Added: - Requirement for compliance with XACML Attribute Profile - Requirement for providing DataType XML attributed to guarantee interoperability with XACML. - Correcting CD data type to include URN-based modeling. Allowing alternative XML formats if the ACS implementation can ensure complex data types are supported. - Note on how to fill the NameID of the saml:Subject element.
saml-xspa-2.0-wd07	10 Dec 2014	Mohammad Jafari	Minor edits
saml-xspa-2.0-wd08	27 July 2015	Mohammad Jafari	Adding new attributes for clearance: Integrity, Compartment, Purpose. Adding a note in the introduction about the consequences of this profile for recording the principal's attributes in audit.
saml-xspa-2.0-wd09	25 August 2015	Mohammad Jafari	Including OIDs for valuesets. Updating clearance attributes. Merging obligations and refrains into caveats. Adding Consent Directive pointer.
saml-xspa-2.0-wd10	16 March 2016	Mohammad Jafari	Editorial corrections.
saml-xspa-2.0-wd11	10 March 2017	Mohammad Jafari	Preparing for the next committee draft.