



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

**Committee Draft 04**

**28 July 2009**

**Specification URIs:**

**This Version:**

<http://docs.oasis-open.org/security/xspa/v1.0/saml-xspa-1.0-cd04.html>  
<http://docs.oasis-open.org/security/xspa/v1.0/saml-xspa-1.0-cd04.pdf>  
<http://docs.oasis-open.org/security/xspa/v1.0/saml-xspa-1.0-cd04.doc> (Authoritative)

**Previous Version:**

<http://docs.oasis-open.org/security/xspa/v1.0/saml-xspa-1.0-cd02.html>  
<http://docs.oasis-open.org/security/xspa/v1.0/saml-xspa-1.0-cd02.pdf>  
<http://docs.oasis-open.org/security/xspa/v1.0/saml-xspa-1.0-cd02.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

Copyright © OASIS® 2009. All Rights Reserved.

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 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

1	Introduction.....	5
1.1	Terminology.....	5
1.2	Normative References.....	5
1.3	Non-Normative References.....	6
2	XSPA profile of SAML Implementation.....	7
2.1	Interactions between Parties.....	7
2.1.1	Access Control Service (Service User).....	7
2.1.2	Access Control Service (Service Provider).....	7
2.1.3	Attributes.....	7
2.1.4	Security Policy.....	8
2.1.5	Privacy Policy.....	8
2.2	Protocols.....	8
2.3	Transmission Integrity.....	8
2.4	Transmission Confidentiality.....	8
2.5	Error States.....	8
2.6	Security Considerations.....	8
2.7	Confirmation Identifiers.....	9
2.8	Metadata Definitions.....	9
2.9	Naming Syntax, Restrictions and Acceptable Values.....	9
2.10	Namespace Requirements.....	9
2.11	Attribute Rules of Equality.....	9
2.12	Attribute Naming Syntax, Restrictions and Acceptable Values.....	9
2.12.1	Name.....	9
2.12.2	National Provider Identifier (NPI) – (optional).....	9
2.12.3	Organization.....	10
2.12.4	Organization-ID.....	10
2.12.5	Structural Role.....	10
2.12.6	Functional Role.....	10
2.12.7	Permission (optional).....	10
2.12.8	Action.....	10
2.12.9	Execute (optional).....	10
2.12.10	Object.....	11
2.12.11	Purpose of Use (POU).....	11
2.12.12	Resource.....	12
3	Conformance.....	13
3.1	Introduction.....	13
3.2	Conformance Tables.....	14
A.	Acknowledgements.....	15
B.	Revision History.....	17

---

## Table of Figures

Figure 1: Interaction between Parties 7

Figure 2: Determining Subject Permissions 12

---

# 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>

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

48 **[HL7-CONSENT]** HL7 Consent Related Vocabulary Confidentiality Codes Recommendation,  
49 <http://lists.oasis-open.org/archives/xacml-demo-tech/200712/doc00003.doc>, from  
50 project submission: [http://lists.oasis-open.org/archives/xacml-demo-](http://lists.oasis-open.org/archives/xacml-demo-tech/200712/msg00015.html)  
51 [tech/200712/msg00015.html](http://lists.oasis-open.org/archives/xacml-demo-tech/200712/msg00015.html)

## 52 **1.3 Non-Normative References**

### 53 **[XSPA-SAML-INTRO]**

54 OASIS Committee Working Draft, "Introductory overview of XSPA Profile of  
55 SAML for Healthcare," [http://www.oasis-](http://www.oasis-open.org/committees/document.php?document_id=30407)  
56 [open.org/committees/document.php?document\\_id=30407](http://www.oasis-open.org/committees/document.php?document_id=30407)

### 57 **[XSPA-SAML-EXAMPLES]**

58 OASIS Committee Working Draft, "Implementation examples of XSPA Profile of  
59 SAML for Healthcare," [http://www.oasis-](http://www.oasis-open.org/committees/document.php?document_id=30408)  
60 [open.org/committees/document.php?document\\_id=30408](http://www.oasis-open.org/committees/document.php?document_id=30408)

61

## 2 XSPA profile of SAML Implementation

62

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.

63

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].

66

### 2.1 Interactions between Parties

67

Figure 1 displays an overview of interactions between parties in the exchange of healthcare information.

68

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

69

Service and MAY be passed in a single assertion from the Service User to the Service Provider. The

70

Service Provider Access Control Service evaluates the request against policy and indicates to the Service

71

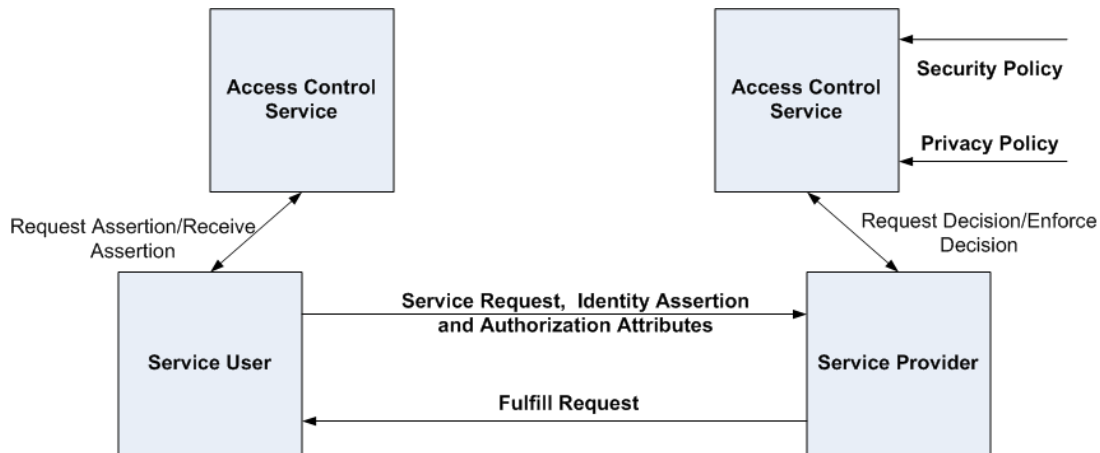
Provider if the request may be fulfilled.

72

The Service Provider Access Control Service evaluates the request against policy and indicates to the Service

73

Provider if the request may be fulfilled.



74

75

Figure 1: Interaction between Parties

#### 2.1.1 Access Control Service (Service User)

76

The XSPA profile of SAML supports sending all requests through an Access Control Service (ACS). The

77

Access Control Service receives the Service User request and responds with a SAML assertion

78

containing user authorizations and attributes. To perform its function, the ACS collects all the attributes

79

(e.g. organization-id, structural role, functional role, purpose of use, requested resource, and actions)

80

necessary to create the Service User requested assertion.

81

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

82

privacy policy.

83

#### 2.1.2 Access Control Service (Service Provider)

84

The Service Provider ACS is responsible for the parsing of assertions, evaluating the assertions against

85

the security and privacy policy, and making and enforcing a decision on behalf of the Service Provider.

86

#### 2.1.3 Attributes

87

Attributes are information related to user location, role, purpose of use, and requested resource

88

requirements and actions necessary to make an access control decision.

89

## 90 **2.1.4 Security Policy**

91 The security policy includes the rules regarding authorizations required to access a protected resource  
92 and additional security conditions (location, time of day, cardinality, separation of duty, purpose, etc.) that  
93 constrain enforcement.

## 94 **2.1.5 Privacy Policy**

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

## 97 **2.2 Protocols**

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

## 102 **2.3 Transmission Integrity**

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

## 106 **2.4 Transmission Confidentiality**

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

## 109 **2.5 Error States**

110 This profile adheres to error states describe in SAML 2.0.

## 111 **2.6 Security Considerations**

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

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



## 127 **2.7 Confirmation Identifiers**

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

## 134 **2.8 Metadata Definitions**

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

## 136 **2.9 Naming Syntax, Restrictions and Acceptable Values**

137 This profile conforms to SAML 2.0 specification.

## 138 **2.10 Namespace Requirements**

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

## 141 **2.11 Attribute Rules of Equality**

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

## 144 **2.12 Attribute Naming Syntax, Restrictions and Acceptable Values**

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

150 This profile will utilize the namespace of urn:oasis:names:tc:xspa:1.0

### 151 **Example of use:**

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

### 158 **2.12.1 Name**

159 Name is the name of the user as required by Health Insurance Portability and Accountability Act (HIPAA)  
160 Privacy Disclosure Accounting. The name will be typed as a string and in plain text with an identifying tag  
161 of <urn:oasis:names:tc:xspa:1.0:subject:subject-id>.

### 162 **2.12.2 National Provider Identifier (NPI) – (optional)**

163 NPI is a US Government issued unique provider identifier required for all Health Insurance Portability and  
164 Accountability Act (HIPAA) Privacy Disclosure Accounting transactions. NPI will be typed as a string in  
165 plain text with an identifying element of <urn:oasis:names:tc:xspa:1.0:subject:npi>.

### 166 **2.12.3 Organization**

167 Organization is the organization that the user belongs to as required by HIPAA Privacy Disclosure  
168 Accounting. Organization will be typed as a string in plain text with an identifying element of  
169 <urn:oasis:names:tc:xspa:1.0:subject:organization>.

### 170 **2.12.4 Organization-ID**

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

### 172 **2.12.5 Structural Role**

173 Structural Role is the value of the principal's structural role. Structural roles that are used in this profile  
174 are defined in Table 2 "Healthcare Personnel that Warrant Differing Levels of Access Control" of ASTM  
175 1986-98 (2005) Standard Guide for Information Access Privileges to Health Information. ASTM E1986

176 Structural roles are described in greater depth in ASTM E2595-07, Standard Guide for Privilege  
177 Management Infrastructure.

178 Structural roles provide authorizations on objects at a global level without regard to internal details.  
179 Examples include authorization to participate in a session, authorization to connect to a database,  
180 authorization to participate in an order workflow, or connection to a protected uniform resource locator  
181 (URL). The structural role is the role name referenced by the patient's consent directive.

### 182 **2.12.6 Functional Role**

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

### 185 **2.12.7 Permission (optional)**

186 Permission is not required by this profile. Permission is determined by the action on the target. See  
187 "Action" below. The permission is the ANSI INCITS (International Committee for Information Technology  
188 Standards) RBAC compliant action-object pair representing the authorization required for access by the  
189 protected resource.

### 190 **2.12.8 Action**

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

- 194 • Append
- 195 • Create
- 196 • Delete
- 197 • Read
- 198 • Update
- 199 • Execute

### 200 **2.12.9 Execute (optional)**

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

204 **2.12.10 Object**

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

209 **2.12.11 Purpose of Use (POU)**

210 Purpose of use provides context to requests for information resources. Each purpose of use will be  
211 unique to a specific assertion, and will establish the context for other security and privacy attributes. For  
212 a given claim, all assertions must be bound to the same purpose of use. Purpose of use allows the  
213 service to consult its policies to determine if the user's authorizations meet or exceed those needed for  
214 access control. Purpose of Use will be typed as string with an identifying element of  
215 <urn:oasis:names:tc:xspa:1.0:subject:purposeofuse>

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

217

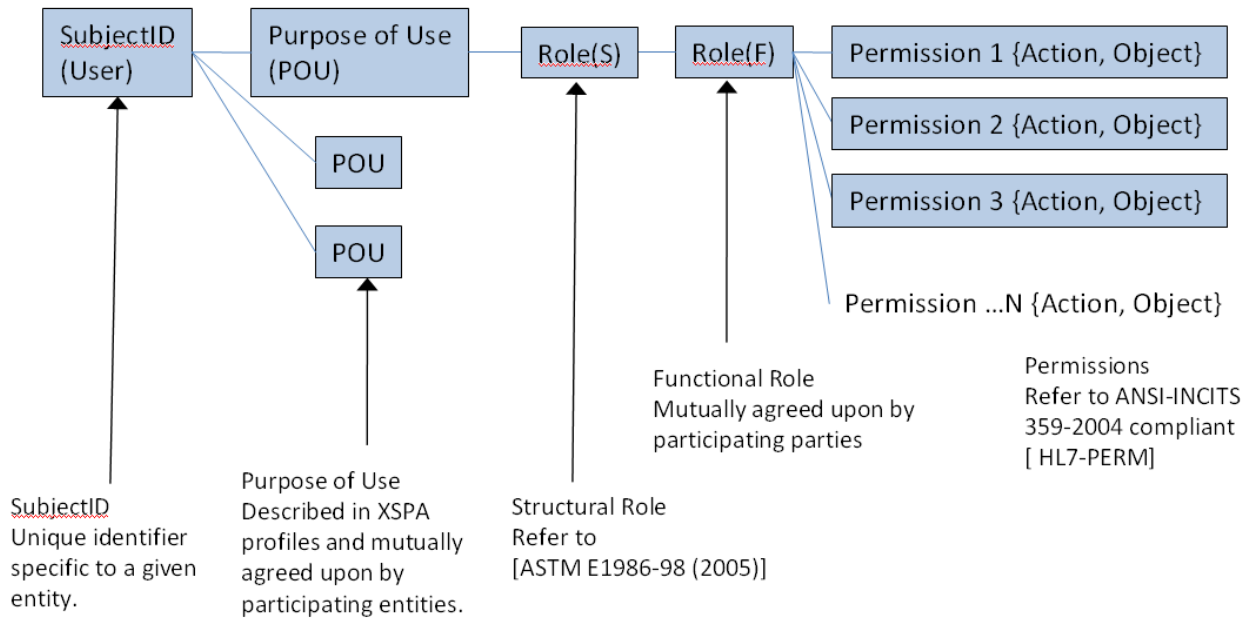
218

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

219

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



223  
224

Figure 2: Determining Subject Permissions

225 **2.12.12 Resource**

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

## 230 3 Conformance

### 231 3.1 Introduction

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

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

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

236

237

*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:xspa: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	String	Unique identifier of the servicing organization.
urn:oasis:names:tc:xspa:2.0:subject:npi	String	National Provider ID provided by U.S. Government for all active providers.

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

240

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

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

245

## 246 3.2 Conformance Tables

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

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

### 250 Attributes

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

253

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

254

---

## 255 A. Acknowledgements

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

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

259 Steve Steffensen, Department of Defense  
260 Daniel Dority, Jericho Systems Corporation  
261 Brian McClung, Jericho Systems Corporation  
262 Brendon Unland, Jericho Systems Corporation  
263 Anil Saldhana, Red Hat  
264 Dilli Doral, Sun Microsystems  
265 Steven Jarosz, Sun Microsystems  
266 Mike Davis, Veterans Health Administration  
267 Duane DeCouteau, Veterans Health Administration  
268 David Staggs, Veterans Health Administration  
269

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

271 George Fletcher, AOL  
272 Scott Messick, Booz Allen Hamilton  
273 Keiron Salt, BTplc  
274 Colin Young, BTplc  
275 Kyle Meadors, Drummond Group Inc.  
276 Michael Merrill, EMC Corporation  
277 Rob Philpott, EMC Corporation  
278 Giles Hogben, ENISA  
279 Carolina Canales-Valenzuela, Ericsson  
280 Lakshmi Thiyagarajan, Hewlett-Packard  
281 Guy Denton, IBM  
282 Heather Hinton, IBM  
283 Maryann Hondo, IBM  
284 Anthony Nadalin, IBM  
285 John Bradley, Individual  
286 David Chadwick, Individual  
287 Jeff Hodges, Individual  
288 Conor Cahill, Intel Corporation  
289 Scott Cantor, Internet2  
290 Nathan Klingenstein, Internet2  
291 Bob Morgan, Internet2  
292 Yassir Elley, Juniper Networks  
293 Steve Hanna, Juniper Networks  
294 Thomas Hardjono, M.I.T.  
295 Tom Scavo, National Center for Supercomputing Applications (NCSA)  
296 Peter Davis, NeuStar, Inc.  
297 Marie Henderson, New Zealand State Services Commission  
298 Colin Wallis, New Zealand State Services Commission  
299 William Young, New Zealand State Services Commission  
300 Frederick Hirsch, Nokia Corporation  
301 Abbie Barbir, Nortel  
302 Srinath Godavarthi, Nortel  
303 Paul Madsen, NTT Corporation  
304 Harry Haury, NuParadigm Government Systems, Inc.  
305 Will Hopkins, Oracle Corporation  
306 Ari Kermaier, Oracle Corporation

307 Hal Lockhart, Oracle Corporation  
308 Prateek Mishra, Oracle Corporation  
309 Vamsi Motukuru, Oracle Corporation  
310 Willem de Pater, Oracle Corporation  
311 Paul Toal, Oracle Corporation  
312 Brian Campbell, Ping Identity Corporation  
313 Anil Saldhana, Red Hat  
314 Michael Engler, SAP AG  
315 Kent Spaulding, Skyworth TTG Holdings Limited  
316 Humphrey Zhang, Skyworth TTG Holdings Limited  
317 Bhavna Bhatnagar, Sun Microsystems  
318 Eve Maler, Sun Microsystems  
319 Ronald Monzillo, Sun Microsystems  
320 Emily Xu, Sun Microsystems  
321 Mike Beach, The Boeing Company  
322 Karsten Huneycutt, University of North Carolina at Chapel Hill  
323 Duane DeCouteau, Veterans Health Administration  
324 David Staggs, Veterans Health Administration



325

## B. Revision History

326

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

327