



Cross-Enterprise Security and Privacy Authorization (XSPA) Profile of WS-Trust for Healthcare

Committee Specification 01

03 September 2010

Specification URIs:

This Version:

<http://docs.oasis-open.org/xspa/ws-trust-v1.0/xspa-ws-trust-profile-cs-01.html>
<http://docs.oasis-open.org/xspa/ws-trust-v1.0/xspa-ws-trust-profile-cs-01.doc> (Authoritative)
<http://docs.oasis-open.org/xspa/ws-trust-v1.0/xspa-ws-trust-profile-cs-01.pdf>

Previous Version:

<http://docs.oasis-open.org/xspa/ws-trust-v1.0/xspa-ws-trust-profile-cd-06.html>
<http://docs.oasis-open.org/xspa/ws-trust-v1.0/xspa-ws-trust-profile-cd-06.doc> (Authoritative)
<http://docs.oasis-open.org/xspa/ws-trust-v1.0/xspa-ws-trust-profile-cd-06.pdf>

Latest Version:

<http://docs.oasis-open.org/xspa/ws-trust-v1.0/xspa-ws-trust-profile.html>
<http://docs.oasis-open.org/xspa/ws-trust-v1.0/xspa-ws-trust-profile.doc> (Authoritative)
<http://docs.oasis-open.org/xspa/ws-trust-v1.0/xspa-ws-trust-profile.pdf>

Technical Committee:

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

Chair(s):

David Staggs, Department of Veterans Affairs (SAIC)
Anil Saldhana, Red Hat

Editor(s):

Mike Davis, Department of Veterans Affairs
Duane DeCouteau, Department of Veterans Affairs (Ascenda)
David Staggs, Department of Veterans Affairs (SAIC)
Jiandong Guo, Oracle Corporation

Related work:

- [WS-Trust v1.3](#)

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
urn:oasis:names:tc:wssx:1.3

Abstract:

This profile describes a framework in which WS-Trust is leveraged 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" 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/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 (<http://www.oasis-open.org/committees/xspa/ipr.php>).

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

Notices

Copyright © OASIS® 2010. 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.....	6
1.1	Terminology.....	6
1.2	Normative References.....	7
1.3	Non-Normative References.....	7
2	XSPA profile of WS-Trust Implementation.....	8
2.1	Interactions between Parties.....	8
2.1.1	Access Control Service at Service User.....	9
2.1.2	Access Control Service at Service Provider.....	9
2.1.3	Security Policy.....	9
2.1.4	Privacy Policy.....	10
2.2	Transmission Integrity.....	10
2.3	Transmission Confidentiality.....	10
2.4	Error States.....	10
2.5	Security Considerations.....	10
2.6	Confirmation Identifiers.....	10
2.7	Metadata Definitions.....	10
2.8	Naming Syntax, Restrictions and Acceptable Values.....	11
2.9	Namespace Requirements.....	11
2.10	Attribute Rules of Equality.....	11
2.11	WS-Trust Claims.....	11
2.11.1	XSPA Dialect (normative).....	11
2.11.2	XSPA ClaimType (normative).....	11
2.11.3	XSPA Claims – Static vs. Runtime.....	12
2.12	Attribute Naming Syntax, Restrictions and Acceptable Values.....	12
2.12.1	Name.....	13
2.12.2	National Provider Identifier (NPI) – (optional).....	13
2.12.3	Organization.....	13
2.12.4	Organization-ID.....	13
2.12.5	Structural Role.....	14
2.12.6	Functional Role.....	14
2.12.7	Permission (optional).....	14
2.12.8	Action.....	14
2.12.9	Execute (optional).....	14
2.12.10	Object.....	14
2.12.11	Purpose of Use (POU).....	14
2.12.12	Resource.....	15
3	Examples of Use.....	17
3.1	WS-Trust Event Flow.....	17
4	Conformance.....	18
4.1	Introduction.....	18
4.2	Conformance Tables.....	18
4.3	Attributes.....	18
A.	Acknowledgements.....	20

B. Revision History 21

Table of Figures

Figure 1: Interaction between Parties 8
Figure 2 Interactions as demonstrated RSA 2010 Oasis XSPA Interop..... 9
Figure 3: Determining Subject Permissions 15
Figure 4: Cross-Enterprise Example Interaction 17

1 Introduction

This document describes a framework that provides access control interoperability useful in the healthcare environment. Interoperability is achieved using WS-Trust secure token request/response elements to 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) – 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.

Attributes - Attributes are information related to user location, role, purpose of use, and requested resource requirements and actions necessary to make an access control decision. This terminology is used by the SAML and XACML specifications and is equivalent in concept to claims.

Claim - A claim is a statement made about a client, service or other resource (e.g. name, identity, key, group, privilege, capability, etc.). This terminology is used by the WS-Trust specification and is equivalent in concept to an attribute.

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.

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

Security Token Service STS - A security token service (STS) is a Web service that issues security tokens. That is, it makes assertions based on evidence that it trusts, to whoever trusts it (or to specific recipients). To communicate trust, a service requires proof, such as a signature, to prove knowledge of a security token or set of security token. A service itself can generate tokens or it can rely on a separate STS to issue a security token with its own trust statement (note that for some security token formats this can just be a re-issuance or co-signature). This forms the basis of trust brokering.

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

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

Service User - The 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.

Web Service - A Web Service is a software component that is described via WSDL and is capable of being accessed via standard network protocols such as but not limited to SOAP over HTTP.

47 1.2 Normative References

- 48 [RFC2119] S. Bradner, *Key words for use in RFCs to Indicate Requirement Levels*,
49 <http://www.ietf.org/rfc/rfc2119.txt>, IETF RFC 2119, March 1997.
- 50 [SAMLPROF] OASIS Standard, "Profiles for the OASIS Security Assertion Markup Language,
51 v2.0," March 2005. [http://docs.oasis-open.org/security/saml/v2.0/saml-profiles-
52 2.0-os.pdf](http://docs.oasis-open.org/security/saml/v2.0/saml-profiles-2.0-os.pdf)
- 53 [ASTM E1986-09 (2009)] Standard Guide for Information Access Privileges to Health Information.
- 54 [ASTM E2595 (2007)] Standard Guide for Privilege Management Infrastructure
- 55 [SAML] OASIS Standard, "Security Assertion Markup Language (SAML) v2.0", March
56 2005. <http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf>
- 57 [HL7-PERM] HL7 Security Technical Committee, HL7 Version 3 Standard: Role-based Access
58 Control Healthcare Permission Catalog, (Available through
59 <http://www.hl7.org/library/standards.cfm>), Release 1, Designation: ANSI/HL7 V3
60 RBAC, R1-2008, Approval Date 2/20/2008.
- 61 [HL7-CONSENT] HL7 Consent Related Vocabulary Confidentiality Codes Recommendation,
62 [http://www.oasis-
63 open.org/committees/download.php/30930/hl7confidentialitycodes.doc](http://www.oasis-open.org/committees/download.php/30930/hl7confidentialitycodes.doc) , from
64 project submission: [http://lists.oasis-open.org/archives/xacml-demo-
65 tech/200712/msg00015.html](http://lists.oasis-open.org/archives/xacml-demo-tech/200712/msg00015.html)
- 66 [WS-TRUST] OASIS Standard, "WS-Trust, Version 1.3", March 2007. [http://docs.oasis-
67 open.org/ws-sx/ws-trust/200512/ws-trust-1.3-os.pdf](http://docs.oasis-open.org/ws-sx/ws-trust/200512/ws-trust-1.3-os.pdf).

68 1.3 Non-Normative References

- 69 [XSPA-SAML-INTRO]
70 OASIS Committee Working Draft, "XSPA Introduction to Profile of SAML for
71 Healthcare", December 2008. [http://www.oasis-
72 open.org/committees/download.php/30407/xspa-saml-introduction-01.doc](http://www.oasis-open.org/committees/download.php/30407/xspa-saml-introduction-01.doc)
- 73 [XSPA-SAML-EXAMPLES]
74 OASIS Committee Working Draft, "XSPA Profile of SAML for Health
75 Implementation Examples", December 2008. [http://www.oasis-
76 open.org/committees/download.php/30408/xspa-saml-examples-01.doc](http://www.oasis-open.org/committees/download.php/30408/xspa-saml-examples-01.doc)

77

2 XSPA profile of WS-Trust Implementation

78

The XSPA profile of WS-Trust provides cross-enterprise authorization of entities within and between healthcare information technology (IT) systems by providing common semantics and vocabularies for interoperable coarse and fine-grained access control.

79

80

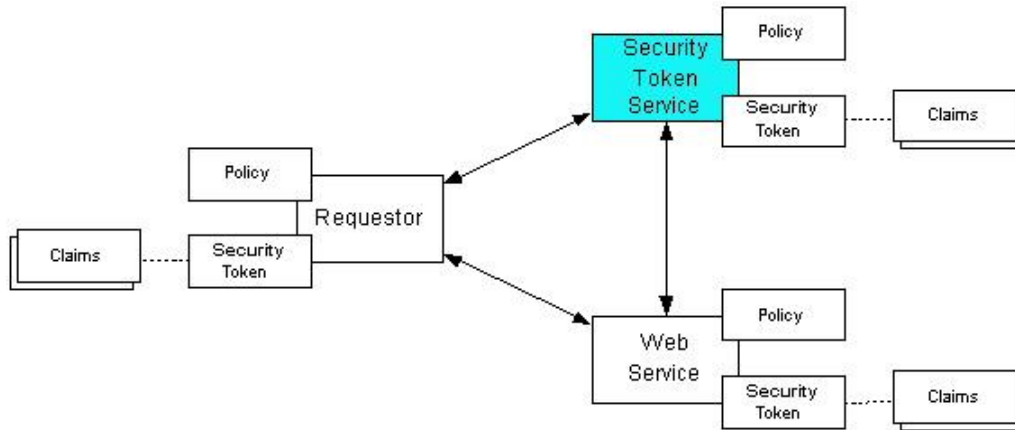
2.1 Interactions between Parties

82

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

83

84



85

86

Figure 1: Interaction between Parties

87

88

In the figure above, extracted from the **[WS-TRUST]** standard, the arrows represent possible communication paths; the requestor MAY obtain a token from the security token service, or it MAY have been obtained indirectly. The requestor then demonstrates authorized use of the token to the Web service. The Web service either trusts the issuing security token service or MAY request a token service to validate the token (or the Web service MAY validate the token itself).

92

93

94

The following figure (2) provides additional detail during a healthcare information exchange between two organizations. This figure is representative of architecture demonstrated at the RSA 2010 Oasis XSPA Interoperability Demonstration (Interop) in March of 2010.

96

97

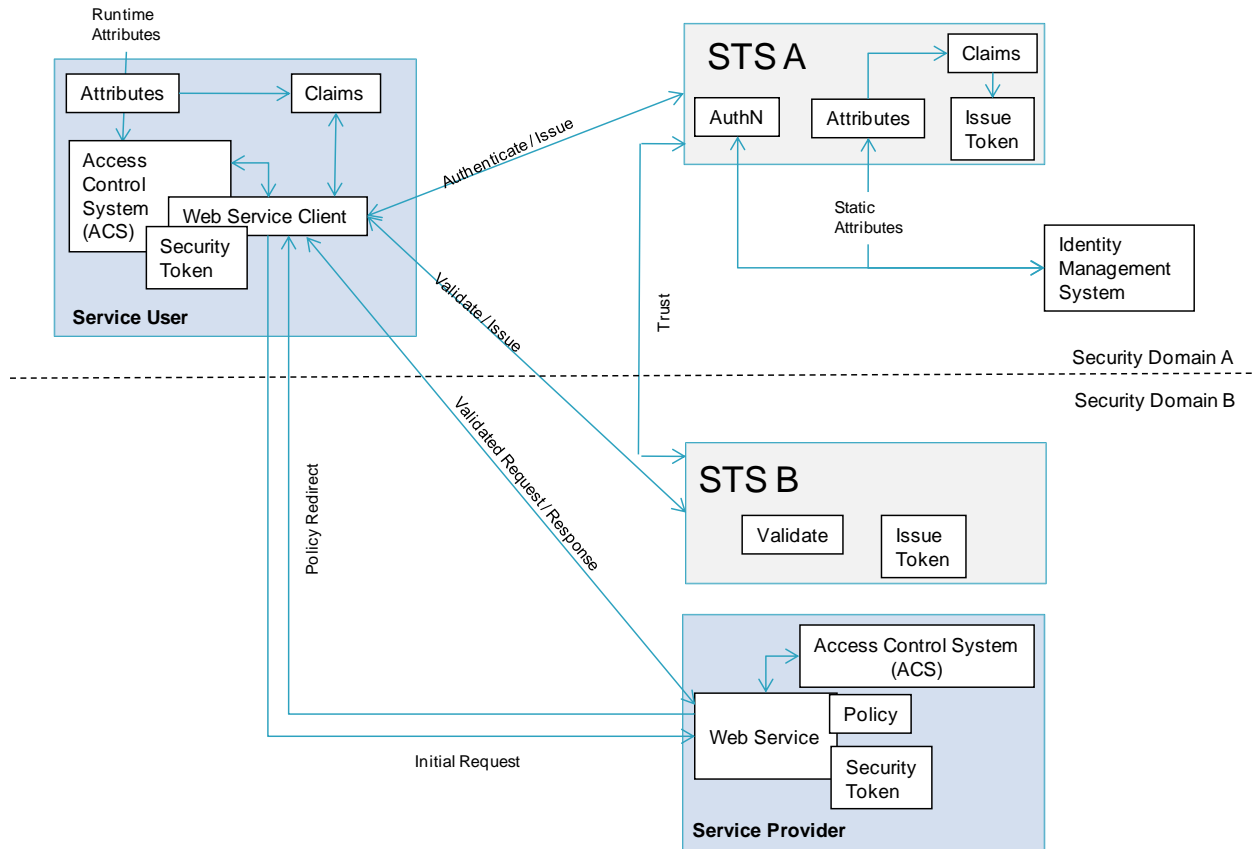


Figure 2 Interactions as demonstrated RSA 2010 Oasis XSPA Interop

98
99

2.1.1 Access Control Service at Service User

101 The XSPA profile of WS-Trust supports sending all requests through an Access Control Service (ACS).
102 The ACS receives the Request Security Token (RST) from the Service User and responds with a Request
103 Security Token Response (RSTR) containing SAML assertions regarding user authorizations and
104 attributes.

105 To perform its function, the ACS may acquire additional attribute information related to user location, role,
106 purpose of use, and requested resource requirement and actions. The requesting ACS is responsible for
107 enforcement of the access control decision.

108 It should be noted that the ACS may make an access control decision to deny access to remote
109 resources based on local internal policies.

2.1.2 Access Control Service at Service Provider

111 The Service Provider ACS is responsible for the parsing of assertions, evaluating the assertions against
112 the security and privacy policy, and making and enforcing a decision on behalf of the Service Provider.

2.1.3 Security Policy

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

117 **2.1.4 Privacy Policy**

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

120 **2.2 Transmission Integrity**

121 The XSPA profile of WS-Trust recommends the use of reliable transmission protocols. Where
122 transmission integrity is required, this profile makes no specific recommendations regarding mechanism
123 or assurance level.

124 **2.3 Transmission Confidentiality**

125 The XSPA profile of WS-Trust recommends the use of secure transmission protocols. Where
126 transmission confidentiality is required, this profile makes no specific recommendations regarding
127 mechanisms.

128 **2.4 Error States**

129 This profile adheres to error states described in WS-Trust v1.3.

130 **2.5 Security Considerations**

131 The following security considerations are established for the XSPA profile of WS-Trust:

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

146 **2.6 Confirmation Identifiers**

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

153 **2.7 Metadata Definitions**

154 This profile will utilize the WS-Trust <AttributeStatement> to inject a SAML assertion into request.

155 **2.8 Naming Syntax, Restrictions and Acceptable Values**

156 This profile conforms to WS-Trust v1.3 specification.

157 **2.9 Namespace Requirements**

158 This profile will support the namespace requirements described in WS-Trust v1.3.

159 **2.10 Attribute Rules of Equality**

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

163 **2.11 WS-Trust Claims**

164 The optional wst:Claims parameter defined in **[WS-Trust]** can be used by the service provider to specify
165 its claims requirements, as well as by the client to pass claims at run time.

166 **2.11.1 XSPA Dialect (normative)**

167 This profile defines a dialect for using wst:Claims with XSPA. The dialect is identified by the following
168 URI:

169 urn:oasis:names:tc:xspa:1.0:claims

170 **2.11.2 XSPA ClaimType (normative)**

171 The XSPA dialect also defines the xspa:ClaimType element. The xspa:ClaimType is a child element of
172 wst:Claims. One or many xspa:ClaimType(s) may be included in a wst:Claims.

173 **Example of use:**

```
174 <xspa:ClaimType uri="xs:anyURI" optional="xs:boolean">  
175 <xspa:ClaimValue>xs:string</xspa:ClaimValue>  
176 </xspa:ClaimType>
```

177

178 *Table 1: XSPA ClaimType (Normative)*

Tag	Description
/xspa:ClaimType	Represents claim
/xspa:ClaimType/@Uri	The unique identifier specifying the claim type.
/xspa:ClaimType/@Optional	Defaults to true.
/xspa:ClaimValue	The specific value specified in the claim, optional.

179

180 **Example of use:**

```
181 <wst:Claims Dialect="urn:oasis:names:tc:xspa:1.0:claims">  
182 <xspa:ClaimType Uri="urn:oasis:names:tc:xacml:1.0:subject:subject-id"/>  
183 <xspa:ClaimType Uri="urn:oasis:names:tc:xacml:2.0:subject:role"/>  
184 <xspa:ClaimType Uri="urn:oasis:names:tc:xacml:2.0:resource:resource-id"/>  
185 <xspa:ClaimType Uri="urn:oasis:names:tc:xspa:1.0:subject:purposeofuse"/>  
186 <xspa:ClaimType Uri="urn:oasis:names:tc:xspa:1.0:subject:npi"  
187 optional="true"/>  
188 </wst:Claims>
```

189

190 **Example of use:**

```

191 <wst:Claims Dialect="urn:oasis:names:tc:xspa:1.0:claims">
192   <xspa:ClaimType Uri="urn:oasis:names:tc:xspa:1.0:subject:purposeofuse">
193     <xspa:ClaimValue>Emergency Treatment</xspa:ClaimValue>
194   </xspa:ClaimType>
195 </wst:Claims>

```

196 **2.11.3 XSPA Claims – Static vs. Runtime**

197 Many of the attributes described in this profile may be delivered to an STS from an Identity Management
 198 Provider. These attributes describe the requesting individual, his or her unique identifier and permissions.
 199 And organization information, all of which are static in nature.

200 Other attributes must be determined at runtime, are usually based on work flow, state, or application
 201 knowledge. It is RECOMMENDED at minimum implementers should support dynamic assertion of
 202 following XSPA claims.

203 *Table 2: XSPA Claims Determined at Runtime*

ClaimType	Description
urn:oasis:names:tc:xspa:1.0:subject:purposeofuse	The standards based healthcare reason why user is requesting resource.
urn:oasis:names:tc:xacml:1.0:resource:resource-id	The resource being requested.
urn:oasis:names:tc:xspa:1.0:resource:hl7:type	The type of resource being requested.
urn:oasis:names:tc:xspa:1.0:subject:functional-role	The role internal to the requesting organization that may be based on current workflow.
urn:oasis:names:tc:xacml:1.0:action:action-id	Create, read, update, delete, execute, etc.

204

205 **2.12 Attribute Naming Syntax, Restrictions and Acceptable Values**

206 This profile leverages the attribute naming syntax, restrictions and acceptable values defined in [XSPA-
 207 SAML] and [XSPA-XACML], both utilize the namespace of urn:oasis:names:tc:xspa:1.0.

208 The following table lists attribute naming syntax, restrictions, and acceptable values that are discussed in
 209 greater detail in the subsections below.

210 Notes on Table 3:

- 211 • The OID for the HL7 Permission Catalog [HL7-PERM] is 2.16.840.1.113883.13.27.
- 212 • The OID for structural roles referenced in [ASTM E1986-09 (2009)] is 1.2.840.10065.1986.7.
- 213 • The mechanism used to identify the patent in a standardized way, e.g. resource:resource-id, is
 214 outside the scope of the profile.
- 215 • HL7 RBAC Permission Catalog [HL7-PERM] represents a conformant minimum interoperability
 216 set for object/action pairings.

217 *Table 3: XSPA Standard Attributes (Normative)*

Identifier	Type	Valid Values
urn:oasis:names:tc:xacml:1.0:subject:subject-id	String	Name of the user as required by Health Insurance Portability and Accountability Act (HIPAA) Privacy Disclosure Accounting. The name will be typed as a string and in plain text.

urn:oasis:names:tc:xpsa:1.0:subject:organization	String	Organization the requestor belongs to as required by Health Insurance Portability and Accountability Act (HIPAA) Privacy Disclosure Accounting.
urn:oasis:names:tc:xpsa:1.0:subject:organization-id	anyURI	Unique identifier of the consuming organization and/or facility
urn:oasis:names:tc:xpsa: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 E1986-09 (2009)] and its OID representation.
urn:oasis:names:tc:xpsa: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:xpsa: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:xpsa:1.0:environment:locality	String	Unique identifier of the servicing organization.
urn:oasis:names:tc:xpsa:2.0:subject:npi	String	National Provider ID provided by U.S. Government for all active providers.

218

219 **2.12.1 Name**

220 Name is the name of the user as required by Health Insurance Portability and Accountability Act (HIPAA)
221 Privacy Disclosure Accounting.

222 **2.12.2 National Provider Identifier (NPI) – (optional)**

223 NPI is a US Government issued unique provider identifier required for all Health Insurance Portability and
224 Accountability Act (HIPAA) Privacy Disclosure Accounting transactions.

225 **2.12.3 Organization**

226 Organization is the organization that the user belongs to as required by HIPAA Privacy Disclosure
227 Accounting.

228 **2.12.4 Organization-ID**

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

230 **2.12.5 Structural Role**

231 Structural Role is the value of the principal's structural role. Structural roles that are used in this profile
232 are defined in Table 2 "Healthcare Personnel that Warrant Differing Levels of Access Control" of ASTM
233 1986-09 (2009) Standard Guide for Information Access Privileges to Health Information.

234 ASTM E1986 Structural roles are described in greater depth in ASTM E2595-07, Standard Guide for
235 Privilege Management Infrastructure.

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

240 **2.12.6 Functional Role**

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

243 **2.12.7 Permission (optional)**

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

248 **2.12.8 Action**

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

- 252 • Append
- 253 • Create
- 254 • Delete
- 255 • Read
- 256 • Update
- 257 • Execute

258 **2.12.9 Execute (optional)**

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

262 **2.12.10 Object**

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

267 **2.12.11 Purpose of Use (POU)**

268 Purpose of use provides context to requests for information resources. Each purpose of use will be
269 unique to a specific assertion, and will establish the context for other security and privacy attributes. For
270 a given claim, all assertions must be bound to the same purpose of use. Purpose of use allows the

271 service to consult its policies to determine if the user's authorizations meet or exceed those needed for
 272 access control.

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

274 *Table 4: 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

275
 276 The figure below illustrates the general relationship between subject (user) and granted permissions to
 277 specific objects as a relationship to their POU. Roles in this relationship are placeholders for permissions.
 278 Permission defines the object-action relationship.

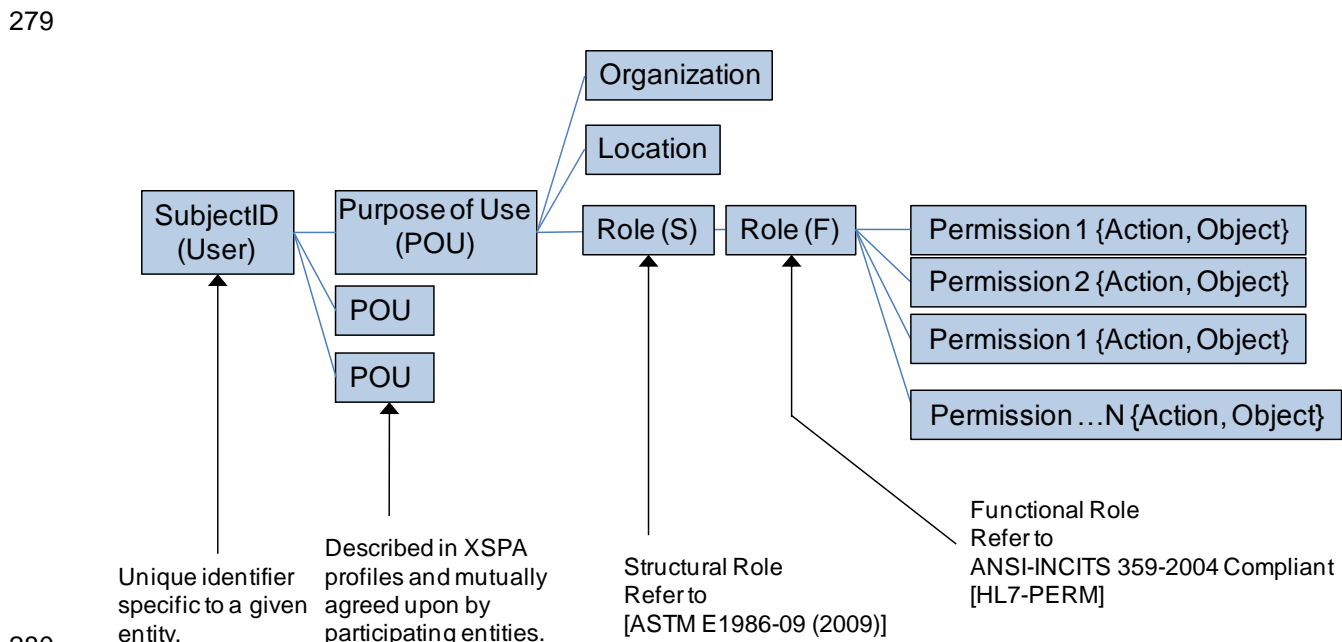


Figure 3: Determining Subject Permissions

282 **2.12.12 Resource**

283 The object(s) for which access is requested must be identical to the object(s) for which the authorization
 284 assertions of this profile apply. A requested resource is not required to be a simple object but may

285 instead be a process or workflow. This profile specifies the use of HL7 RBAC Permission Catalog as the
286 resource vocabulary.

287 **3 Examples of Use**

288 The following examples of WS-Trust request and response messages are intended to provide additional
 289 guidance to implementers of this profile.

290 **3.1 WS-Trust Event Flow**

291 The following figure represents an example flow of messages and attributes and is non-normative.
 292

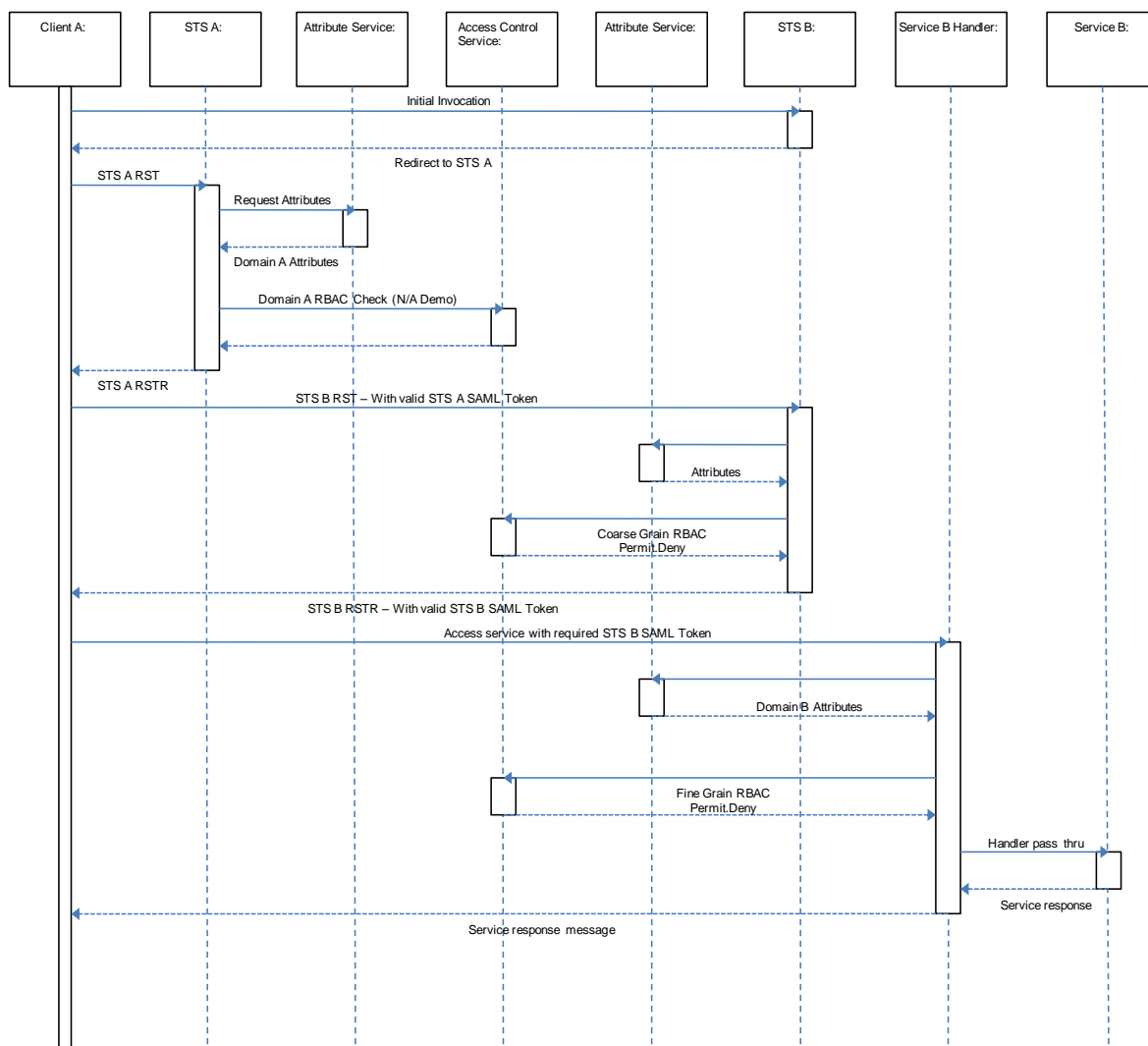


Figure 4: Cross-Enterprise Example Interaction

293
 294

295 4 Conformance

296 4.1 Introduction

297 The XSPA profile of WS-Trust addresses the following aspects of conformance:

- 298 • This profile describes a minimum vocabulary set that must be supported in order to claim
299 conformance.
- 300 • An implementation must conform at minimum to the WS-Trust v1.3 specification and implement
301 support for xspa:Dialect, and xspa:ClaimType described in section 2.11 of this profile.

302 4.2 Conformance Tables

303 The table below identifies portions of the profile that MUST be adhered to in order to claim conformance.

304 Note: “M” is mandatory and MUST be used, “O” is optional, “P” is preferred, and “n/a” is not applicable.

305 4.3 Attributes

306 The implementation MUST use the attributes associated with the identifiers in the table below consistent
307 with descriptions in this profile.

308 *Table 5: Attribute Naming, Typing, and Acceptable Value Set*

Identifier	Required Attribute	Runtime Claim Assertion	Claim Asserted Externally
urn:oasis:names:tc:xacml:1.0:subject:subject-id	M	O	P
urn:oasis:names:tc:xspa:1.0:subject:organization-id	M	O	P
urn:oasis:names:tc:xspa:1.0:organization	M	O	P
urn:oasis:names:tc:xspa:1.0:subject:hl7:permission	O	O	P
urn:oasis:names:tc:xacml:2.0:subject:role (ASTM E1986-09 (2009) Structured Role Value)	M	O	P
urn:oasis:names:tc:xspa:1.0:subject:functional-role	O	P	n/a
urn:oasis:names:tc:xspa:1.0:subject:purposeofuse	M	P	n/a
urn:oasis:names:tc:xacml:1.0:resource:resource-id	M	P	n/a
urn:oasis:names:tc:xacml:1.0:action:action-id (HL7 Permission Catalog Resource Action Value)	O	P	n/a
urn:oasis:names:tc:xspa:1.0:resource:hl7:type (HL7 Permission Catalog Object Value)	O	P	n/a

Identifier	Required Attribute	Runtime Claim Assertion	Claim Asserted Externally
urn:oasis:names:tc:xspa:1.0:environment:locality	M	O	n/a
urn:oasis:names:tc:xspa:2.0:subject:npi	O	O	P

309 A. Acknowledgements

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

312 Participants in the RSAConference 2010 Interoperability Demonstration of the XSPA profile:

313 Daniel Dority, Jericho Systems Corporation
314 Imran Chaudhari, Jericho Systems Corporation
315 Capt. Emory Fry MD, Naval Health Research Center
316 Jiandong Guo, Oracle Corporation
317 Harold Carr, Oracle Corporation
318 Craig Forster, IBM
319 Sridhar Muppidi, IBM
320 Mike Davis, Veterans Health Administration
321 Duane DeCouteau, Veterans Health Administration
322 David Staggs, Veterans Health Administration

323

324 Cross-Enterprise Security and Privacy Authorization (XSPA) TC members during the development of this
325 specification:

326 Srinath Godavarthi, Avaya, Inc.
327 Anil, Tappetia, Cisco Systems, Inc.
328 John Moehrke, GE Healthcare
329 Dr. Steven Meyer, HIPAAT International Inc
330 Richard Franck, IBM
331 Sridhar Muppidi, IBM
332 Vernon Murdoch, IBM
333 Neil Readshaw, IBM
334 Ram Kumar
335 Adam Stone
336 Michael Dufel, Jericho Systems Corporation
337 Derek Anderson, Jericho Systems Corporation
338 Daniel Dority, Jericho Systems Corporation
339 David Weitzel, Mitre Corporation
340 Anil Saldhana, Red Hat
341 Dr. Jiandong Guo, Oracle Corporation
342 Mike Davis, Veterans Health Administration
343 Duane DeCouteau, Veterans Health Administration
344 David Staggs, Veterans Health Administration

345

B. Revision History

346

Document ID	Date	Committer	Comment
xspa-ws-trust-profile-cd-01	01/27/2009	Duane DeCouteau Craig Winter	Initial committee draft v1.0 - QA Review / Revision
xspa-ws-trust-profile-cd-02	03/19/2010	Duane DeCouteau	Changes noted during development and exhibition of profile prior to and during RSA 2010 Oasis XSPA Interop.
xspa-ws-trust-profile-cd-03	03/19/2010	Duane DeCouteau David Staggs	Commit changes discussed and approved during TC Mtg. 3/19/2010.
xspa-ws-trust-profile-cd-04	04/2/2010	Duane DeCouteau David Staggs	Voted to Committee Draft - allowing for formatting changes required for public review.
xspa-ws-trust-profile-cd-05	07/21/2010	Duane DeCouteau	Incorporate public review comments.
xspa-ws-trust-profile-cd-06	08/04/2010	Duane DeCouteau	Correct punctuation errors, insert clearer version of figure 3, and augment terminology definitions.
xspa-ws-trust-profile-cd-06	08/06/2010	Duane DeCouteau	Voted to committee specification at August 6, 2010 TC meeting.

347