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

Committee Draft 06

06 August 2010

Specification URIs:
This 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

Previous Version:
http://docs.oasis-open.org/xspa/ws-trust-v1.0/xspa-ws-trust-profile-cd-04.html
http://docs.oasis-open.org/xspa/ws-trust-v1.0/xspa-ws-trust-profile-cd-04.doc (Authoritative)
http://docs.oasis-open.org/xspa/ws-trust-v1.0/xspa-ws-trust-profile-cd-04.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

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

Table of Figures

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.

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 E1986-09 (2009)] 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", March 2005. http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf

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

[HL7-CONSENT] HL7 Consent Related Vocabulary Confidentiality Codes Recommendation, http://www.oasis-open.org/committees/download.php/30930/hl7confidentialitycodes.doc , from project submission: http://lists.oasis-open.org/archives/xacml-demo-tech/200712/msg00015.html

[WS-TRUST] OASIS Standard, "WS-Trust, Version 1.3", March 2007. http://docs.oasis-open.org/ws-sx/ws-trust/200512/ws-trust-1.3-os.pdf.

1.3 Non-Normative References

[XSPA-SAML-INTRO]

OASIS Committee Working Draft, "XSPA Introduction to Profile of SAML for Healthcare", December 2008. http://www.oasis-open.org/committees/download.php/30407/xspa-saml-introduction-01.doc

[XSPA-SAML-EXAMPLES]

OASIS Committee Working Draft, "XSPA Profile of SAML for Health Implementation Examples", December 2008. http://www.oasis-open.org/committees/download.php/30408/xspa-saml-examples-01.doc

2 XSPA profile of WS-Trust Implementation

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.

2.1 Interactions between Parties

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

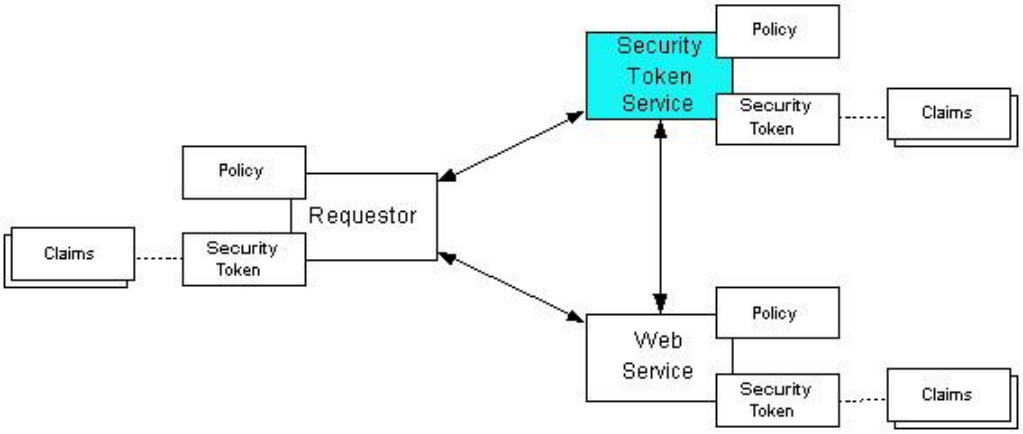

Figure 1: Interaction between Parties

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).

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 Interopability Demonstration (Interop) in March of 2010.

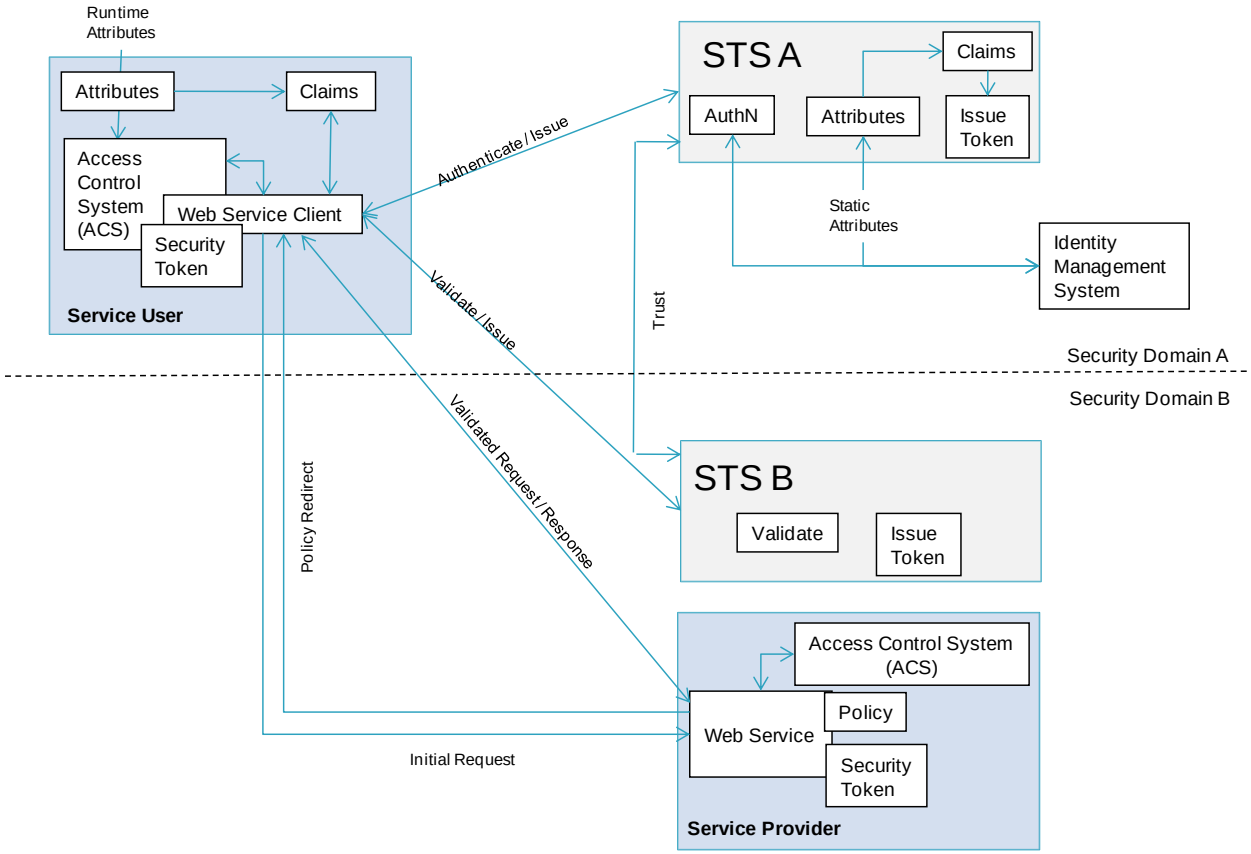

Figure 2 Interactions as demonstrated RSA 2010 Oasis XSPA Interop

2.1.1 Access Control Service at Service User

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

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

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

2.1.2 Access Control Service at Service Provider

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

2.1.3 Security Policy

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

2.1.4 Privacy Policy

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

2.2 Transmission Integrity

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

2.3 Transmission Confidentiality

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

2.4 Error States

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

2.5 Security Considerations

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

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

2.6 Confirmation Identifiers

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

2.7 Metadata Definitions

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

2.8 Naming Syntax, Restrictions and Acceptable Values

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

2.9 Namespace Requirements

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

2.10 Attribute Rules of Equality

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

2.11 WS-Trust Claims

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

2.11.1 XSPA Dialect (normative)

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

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

2.11.2 XSPA ClaimType (normative)

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

Example of use:

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

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.

Example of use:

```
<wst:Claims Dialect="urn:oasis:names:tc:xspa:1.0:claims">
    <xspa:ClaimType Uri="urn:oasis:names:tc:xacml:1.0:subject:subject-id"/>
    <xspa:ClaimType Uri="urn:oasis:names:tc:xacml:2.0:subject:role"/>
    <xspa:ClaimType Uri="urn:oasis:names:tc:xacml:2.0:resource:resource-id"/>
    <xspa:ClaimType Uri="urn:oasis:names:tc:xspa:1.0:subject:purposeofuse"/>
    <xspa:ClaimType Uri="urn:oasis:names:tc:xspa:1.0:subject:npi"
optional="true"/>
</wst:Claims>
```

Example of use:

```
<wst:Claims Dialect="urn:oasis:names:tc:xspa:1.0:claims">
    <xspa:ClaimType Uri="urn:oasis:names:tc:xspa:1.0:subject:purposeofuse">
          <xspa:ClaimValue>Emergency Treatment</xspa:ClaimValue>
      </xspa:ClaimType>
</wst:Claims>
```

2.11.3 XSPA Claims – Static vs. Runtime

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

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

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.

2.12 Attribute Naming Syntax, Restrictions and Acceptable Values

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

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

Notes on Table 3:

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

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: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 E1986-09 (2009)] 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.

2.12.1 Name

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

2.12.2 National Provider Identifier (NPI) – (optional)

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

2.12.3 Organization

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

2.12.4 Organization-ID

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

2.12.5 Structural Role

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

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

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

2.12.6 Functional Role

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

2.12.7 Permission (optional)

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

2.12.8 Action

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

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

2.12.9 Execute (optional)

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

2.12.10 Object

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

2.12.11 Purpose of Use (POU)

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

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

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

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

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

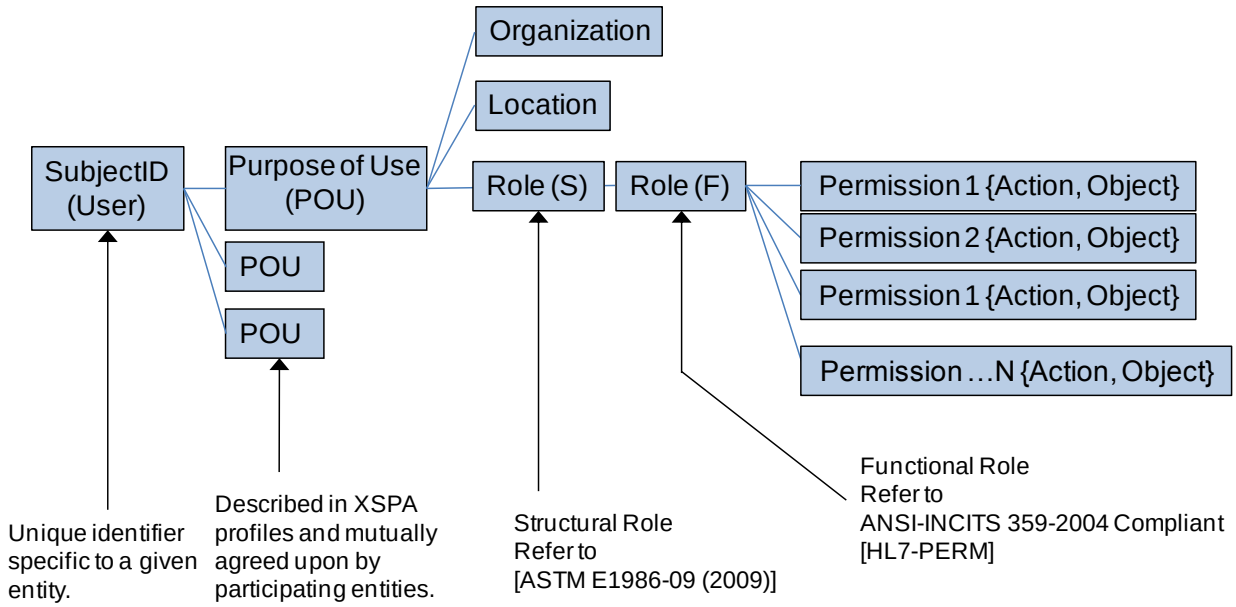

Figure 3: Determining Subject Permissions

2.12.12 Resource

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

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

3 Examples of Use

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

3.1 WS-Trust Event Flow

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

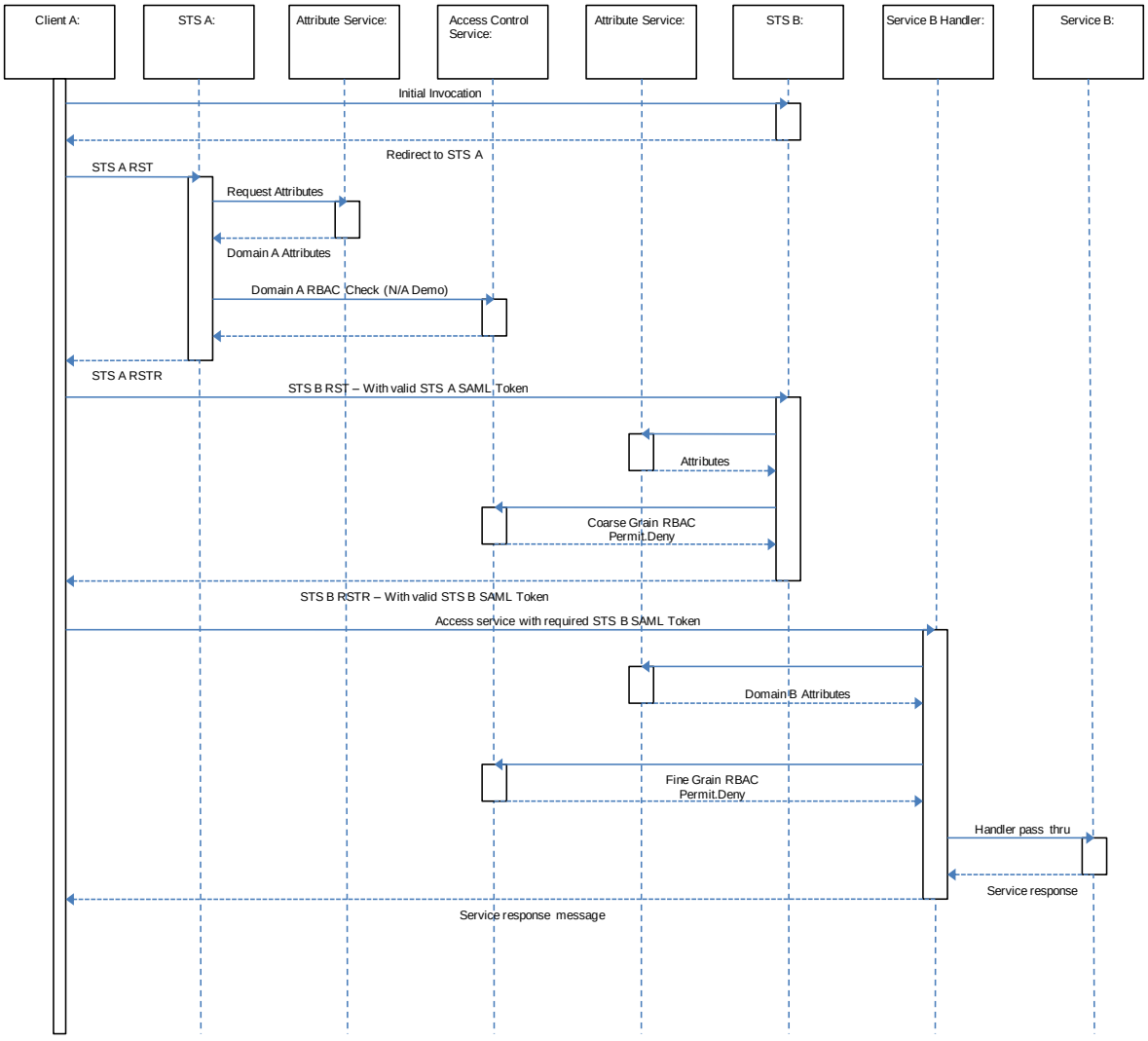

Figure 4: Cross-Enterprise Example Interaction

4 Conformance

4.1 Introduction

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

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

4.2 Conformance Tables

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

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

4.3 Attributes

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

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

A. Acknowledgements

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

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

Daniel Dority, Jericho Systems Corporation
Imran Chaudhari, Jericho Systems Corporation
Capt. Emory Fry MD, Naval Health Research Center
Jiandong Guo, Oracle Corporation
Harold Carr, Oracle Corporation
Craig Forster, IBM
Sridhar Muppidi, IBM
Mike Davis, Veterans Health Administration
Duane DeCouteau, Veterans Health Administration
David Staggs, Veterans Health Administration

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

Srinath Godavarthi, Avaya, Inc.
Anil, Tappetia, Cisco Systems, Inc.
John Moehrke, GE Healthcare
Dr. Steven Meyer, HIPAAT International Inc
Richard Franck, IBM
Sridhar Muppidi, IBM
Vernon Murdoch, IBM
Neil Readshaw, IBM
Ram Kumar
Adam Stone
Michael Dufel, Jericho Systems Corporation
Derek Anderson, Jericho Systems Corporation
Daniel Dority, Jericho Systems Corporation
David Weitzel, Mitre Corporation
Anil Saldhana, Red Hat
Dr. Jiandong Guo, Oracle Corporation
Mike Davis, Veterans Health Administration
Duane DeCouteau, Veterans Health Administration
David Staggs, Veterans Health Administration

B. Revision History

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.