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

Committee Draft 04

2 April 2010

Specification URIs:
This 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

Previous Version:
N/A

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

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, Sun Microsystems/Oracle

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/.
Table of Contents

1 Introduction ................................................................................................................................................. 6
  1.1 Terminology ........................................................................................................................................... 6
  1.2 Normative References ........................................................................................................................... 6
  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 ......................................................................................... 8
    2.1.2 Access Control Service at Service Provider .................................................................................. 8
    2.1.3 Attributes ........................................................................................................................................ 8
    2.1.4 Security Policy ................................................................................................................................. 9
    2.1.5 Privacy Policy .................................................................................................................................. 9
  2.2 Transmission Integrity ............................................................................................................................. 9
  2.3 Transmission Confidentiality .................................................................................................................. 9
  2.4 Error States ............................................................................................................................................ 9
  2.5 Security Considerations ........................................................................................................................ 9
  2.6 Confirmation Identifiers ......................................................................................................................... 9
  2.7 Metadata Definitions .............................................................................................................................. 10
  2.8 Naming Syntax, Restrictions and Acceptable Values ............................................................................. 10
  2.9 Namespace Requirements ..................................................................................................................... 10
  2.10 Attribute Rules of Equality ............................................................................................................... 10
  2.11 WS-Trust Claims .................................................................................................................................. 10
    2.11.1 XSPA Dialect (normative) ............................................................................................................ 10
    2.11.2 XSPA ClaimType (normative) ....................................................................................................... 10
    2.11.3 XSPA Claims – Static vs. Runtime ............................................................................................... 11
  2.12 Attribute Naming Syntax, Restrictions and Acceptable Values ........................................................... 11
    2.12.1 Name ............................................................................................................................................ 12
    2.12.2 National Provider Identifier (NPI) – (optional) ........................................................................... 12
    2.12.3 Organization ................................................................................................................................. 12
    2.12.4 Organization-ID ............................................................................................................................. 13
    2.12.5 Structural Role ............................................................................................................................... 13
    2.12.6 Functional Role ............................................................................................................................... 13
    2.12.7 Permission (optional) .................................................................................................................... 13
    2.12.8 Action ............................................................................................................................................ 13
    2.12.9 Execute (optional) ......................................................................................................................... 13
    2.12.10 Object .......................................................................................................................................... 13
    2.12.11 Purpose of Use (POU) ............................................................................................................... 14
    2.12.12 Resource ...................................................................................................................................... 14

3 Examples of Use ......................................................................................................................................... 16
  3.1 WS-Trust Event Flow .............................................................................................................................. 16

4 Conformance ............................................................................................................................................... 17
  4.1 Introduction ............................................................................................................................................ 17
  4.2 Conformance Tables .............................................................................................................................. 17
  4.3 Attributes .............................................................................................................................................. 17
# Table of Figures

<table>
<thead>
<tr>
<th>Figure</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Figure 1</td>
<td>Interaction between Parties</td>
<td>8</td>
</tr>
<tr>
<td>Figure 2</td>
<td>Determining Subject Permissions</td>
<td>14</td>
</tr>
<tr>
<td>Figure 3</td>
<td>Cross-Enterprise Example Interaction</td>
<td>16</td>
</tr>
</tbody>
</table>
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 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.

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

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.

1.2 Normative References


[ASTM E2595 (2007)] Standard Guide for Privilege Management Infrastructure

1.3 Non-Normative References


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.

Additional introductory information and examples can be found in Cross-Enterprise Security and Privacy Authorization (XSPA) Profile of WS-Trust Implementation Examples [XSPA-WS-TRUST-EXAMPLES].

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.

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 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.
2.1.4 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.

2.1.5 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)

<table>
<thead>
<tr>
<th>Tag</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>/xspa:ClaimType</td>
<td>Represents claim</td>
</tr>
<tr>
<td>/xspa:ClaimType/@Uri</td>
<td>The unique identifier specifying the claim type.</td>
</tr>
<tr>
<td>/xspa:ClaimType/@Optional</td>
<td>Defaults to true.</td>
</tr>
<tr>
<td>/xspa:ClaimValue</td>
<td>The specific value specified in the claim, optional.</td>
</tr>
</tbody>
</table>

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"/>
</wst:Claims>
```
Example of use:

```xml
<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 workflow, state, or application knowledge. It is RECOMMENDED at minimum implementers should support dynamic assertion of following XSPA claims.

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

### 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>
<thead>
<tr>
<th>Identifier</th>
<th>Type</th>
<th>Valid Values</th>
</tr>
</thead>
</table>

---

xspa-ws-trust-profile-cd-04

Copyright © OASIS® 2010. All Rights Reserved.

April 2, 2010

Page 11 of 20
<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>urn:oasis:names:tc:xacml:1.0:subject:subject-id</td>
<td>String</td>
</tr>
<tr>
<td>urn:oasis:names:tc:xpsa:1.0:subject:organization</td>
<td>String</td>
</tr>
<tr>
<td>urn:oasis:names:tc:xpsa:1.0:subject:organization-id</td>
<td>anyURI</td>
</tr>
<tr>
<td>urn:oasis:names:tc:xpsa:1.0:subject:hl7:permission</td>
<td>String</td>
</tr>
<tr>
<td>urn:oasis:names:tc:xspa:1.0:subject:purposeofuse</td>
<td>String</td>
</tr>
<tr>
<td>urn:oasis:names:tc:xacml:1.0:resource:resource-id</td>
<td>String</td>
</tr>
<tr>
<td>urn:oasis:names:tc:xspa:1.0:resource:hl7:type</td>
<td>String</td>
</tr>
<tr>
<td>urn:oasis:names:tc:xspa:1.0:environment:locality</td>
<td>String</td>
</tr>
</tbody>
</table>

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>
<thead>
<tr>
<th>Description</th>
<th>Allowed Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Healthcare Treatment</td>
<td>TREATMENT</td>
</tr>
<tr>
<td>Payment</td>
<td>PAYMENT</td>
</tr>
<tr>
<td>Operations</td>
<td>OPERATIONS</td>
</tr>
<tr>
<td>Emergency Treatment</td>
<td>EMERGENCY</td>
</tr>
<tr>
<td>System Administration</td>
<td>SYSADMIN</td>
</tr>
<tr>
<td>Research</td>
<td>RESEARCH</td>
</tr>
<tr>
<td>Marketing</td>
<td>MARKETING</td>
</tr>
<tr>
<td>Request of the Individual</td>
<td>REQUEST</td>
</tr>
<tr>
<td>Public Health</td>
<td>PUBLICHEALTH</td>
</tr>
</tbody>
</table>

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.

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

![Cross-Enterprise Example Interaction Diagram]

*Figure 3: 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

<table>
<thead>
<tr>
<th>Identifier</th>
<th>Required Attribute</th>
<th>Runtime Claim Assertion</th>
<th>Claim Asserted Externally</th>
</tr>
</thead>
<tbody>
<tr>
<td>urn:oasis:names:tc:xacml:1.0:subject:subject-id</td>
<td>M</td>
<td>O</td>
<td>P</td>
</tr>
<tr>
<td>urn:oasis:names:tc:xspa:1.0:subject:organization-id</td>
<td>M</td>
<td>O</td>
<td>P</td>
</tr>
<tr>
<td>urn:oasis:names:tc:xspa:1.0:organization</td>
<td>M</td>
<td>O</td>
<td>P</td>
</tr>
<tr>
<td>urn:oasis:names:tc:xspa:1.0:subject:hl7:permission</td>
<td>O</td>
<td>O</td>
<td>P</td>
</tr>
<tr>
<td>urn:oasis:names:tc:xspa:1.0:subject:functional-role</td>
<td>O</td>
<td>P</td>
<td>n/a</td>
</tr>
<tr>
<td>urn:oasis:names:tc:xspa:1.0:subject:purposeofuse</td>
<td>M</td>
<td>P</td>
<td>n/a</td>
</tr>
<tr>
<td>urn:oasis:names:tc:xacml:1.0:resource:resource-id</td>
<td>M</td>
<td>P</td>
<td>n/a</td>
</tr>
<tr>
<td>urn:oasis:names:tc:xacml:1.0:action:action-id (HL7 Permission Catalog Resource Action Value)</td>
<td>O</td>
<td>P</td>
<td>n/a</td>
</tr>
<tr>
<td>urn:oasis:names:tc:xspa:1.0:resource:hl7:type (HL7 Permission Catalog Object Value)</td>
<td>O</td>
<td>P</td>
<td>n/a</td>
</tr>
<tr>
<td>Identifier</td>
<td>Required Attribute</td>
<td>Runtime Claim Assertion</td>
<td>Claim Asserted Externally</td>
</tr>
<tr>
<td>------------</td>
<td>--------------------</td>
<td>------------------------</td>
<td>--------------------------</td>
</tr>
<tr>
<td>urn:oasis:names:tc:xspa:1.0:environment:locality</td>
<td>M</td>
<td>O</td>
<td>n/a</td>
</tr>
<tr>
<td>urn:oasis:names:tc:xspa:2.0:subject:npi</td>
<td>O</td>
<td>O</td>
<td>P</td>
</tr>
</tbody>
</table>
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, Sun Microsystems/Oracle
- Harold Carr, Sun Microsystems/Oracle
- 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
- Derek Anderson, Jericho Systems Corporation
- Daniel Dority, Jericho Systems Corporation
- David Weitzel, Mitre Corporation
- Anil Saldhana, Red Hat
- Dr. Jiandong Guo Sun Microsystems
- Mike Davis, Veterans Health Administration
- Duane DeCouteau, Veterans Health Administration
- David Staggs, Veterans Health Administration
# B. Revision History

<table>
<thead>
<tr>
<th>Document ID</th>
<th>Date</th>
<th>Committer</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>xspa-ws-trust-profile-cd-01</td>
<td>01/27/2009</td>
<td>Duane DeCouteau, Craig Winter</td>
<td>Initial committee draft v1.0 - QA Review / Revision</td>
</tr>
<tr>
<td>xspa-ws-trust-profile-cd-02</td>
<td>03/19/2010</td>
<td>Duane DeCouteau</td>
<td>Changes noted during development and exhibition of profile prior to and during RSA 2010 Oasis XSPA Interop.</td>
</tr>
<tr>
<td>xspa-ws-trust-profile-cd-03</td>
<td>03/19/2010</td>
<td>Duane DeCouteau, David Staggs</td>
<td>Commit changes discussed and approved during TC Mtg. 3/19/2010.</td>
</tr>
<tr>
<td>xspa-ws-trust-profile-cd-04</td>
<td>04/2/2010</td>
<td>Duane DeCouteau, David Staggs</td>
<td>Voted to Committee Draft - allowing for formatting changes required for public review.</td>
</tr>
</tbody>
</table>