Cross-Enterprise Security and Privacy Authorization (XSPA) Profile of XACML v2.0 for Healthcare Version 1.0

Committee Draft 02

07 June 2009

Specification URIs:
This Version:
http://docs.oasis-open.org/xacml/xspa/v1.0/xacml-xspa-1.0-cd02.html
http://docs.oasis-open.org/xacml/xspa/v1.0/xacml-xspa-1.0-cd02.doc
http://docs.oasis-open.org/xacml/xspa/v1.0/xacml-xspa-1.0-cd02.pdf

Previous Version:
http://docs.oasis-open.org/xacml/xspa/v1.0/saml-xspa-1.0-pr01.html
http://docs.oasis-open.org/xacml/xspa/v1.0/saml-xspa-1.0-pr01.doc
http://docs.oasis-open.org/xacml/xspa/v1.0/saml-xspa-1.0-pr01.pdf

Latest Version:
http://docs.oasis-open.org/xacml/xspa/v1.0/xacml-xspa-1.0.html
http://docs.oasis-open.org/xacml/xspa/v1.0/xacml-xspa-1.0.doc
http://docs.oasis-open.org/xacml/xspa/v1.0/xacml-xspa-1.0.pdf

Technical Committee:
OASIS eXtensible Access Control Markup Language (XACML) TC

Chair(s):

Hal Lockhart, Oracle Corporation
Bill Parducci, Individual

Editor(s):
Duane DeCouteau, Department of Veterans Affairs
Mike Davis, Department of Veterans Affairs
David Staggs, Department of Veterans Affairs

Related work:
This specification is related to:

- eXtensible Access Control Markup Language(XACML) Version 2.0

Declared XML Namespace(s):
N/A

Abstract:
A profile of XACML used to support cross-enterprise security and privacy authorization.

Status:
This document was last revised or approved by the OASIS eXtensible Access Control Markup Language (XACML) 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.

Copyright © OASIS® 2008. All Rights Reserved.

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/xacml/ .

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/xacml/ipr.php .

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

Copyright © OASIS® 2008. All Rights Reserved.

Notices

Copyright © OASIS® 2008-2009. All Rights Reserved.

All capitalized terms in the following text have the meanings assigned to them in the OASIS Intellectual Property Rights Policy (the "OASIS IPR Policy"). The full Policy may be found at the OASIS website.

This document and translations of it may be copied and furnished to others, and derivative works that comment on or otherwise explain it or assist in its implementation may be prepared, copied, published, and distributed, in whole or in part, without restriction of any kind, provided that the above copyright notice and this section are included on all such copies and derivative works. However, this document itself may not be modified in any way, including by removing the copyright notice or references to OASIS, except as needed for the purpose of developing any document or deliverable produced by an OASIS Technical Committee (in which case the rules applicable to copyrights, as set forth in the OASIS IPR Policy, must be followed) or as required to translate it into languages other than English.

The limited permissions granted above are perpetual and will not be revoked by OASIS or its successors or assigns.

This document and the information contained herein is provided on an "AS IS" basis and OASIS DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY OWNERSHIP RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

OASIS requests that any OASIS Party or any other party that believes it has patent claims that would necessarily be infringed by implementations of this OASIS Committee Specification or OASIS Standard, to notify OASIS TC Administrator and provide an indication of its willingness to grant patent licenses to such patent claims in a manner consistent with the IPR Mode of the OASIS Technical Committee that produced this specification.

OASIS invites any party to contact the OASIS TC Administrator if it is aware of a claim of ownership of any patent claims that would necessarily be infringed by implementations of this specification by a patent holder that is not willing to provide a license to such patent claims in a manner consistent with the IPR Mode of the OASIS Technical Committee that produced this specification. OASIS may include such claims on its website, but disclaims any obligation to do so.

OASIS takes no position regarding the validity or scope of any intellectual property or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; neither does it represent that it has made any effort to identify any such rights. Information on OASIS' procedures with respect to rights in any document or deliverable produced by an OASIS Technical Committee can be found on the OASIS website. Copies of claims of rights made available for publication and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this OASIS Committee Specification or OASIS Standard, can be obtained from the OASIS TC Administrator. OASIS makes no representation that any information or list of intellectual property rights will at any time be complete, or that any claims in such list are, in fact, Essential Claims.

The names "OASIS", “XSPA”, and “XACML” are trademarks of OASIS, the owner and developer of this specification, and should be used only to refer to the organization and its official outputs. OASIS welcomes reference to, and implementation and use of, specifications, while reserving the right to enforce its marks against misleading uses. Please see http://www.oasis-open.org/who/trademark.php for above guidance.

Table of Contents

1 Introduction 5
1.1 Terminology 5
1.2 Normative References 6
1.3 Non-Normative References 6
2 2 XSPA profile of XACML 7
2.1 Interactions between Parties 7
2.1.1 Service Interface 7
2.1.2 Access Control Service (Service Consumer) 7
2.1.3 Attribute Service 7
2.1.4 Policy Authority 7
2.1.5 Access Control Service (Service Provider) 8
2.2 Transmission Integrity 8
2.3 Transmission Confidentiality 8
2.4 Error States 8
2.5 Security Considerations 8
2.6 Confirmation Identifiers 8
2.7 Metadata Definitions 8
2.8 Naming Syntax, Restrictions and Acceptable Values 8
2.9 Namespace Requirements 9
2.10 Attribute Rules of Equality 9
2.11 Attribute Naming Syntax, Restrictions and Acceptable Values 9
2.12 Standard Rules (Normative) 13
2.13 Standard Rules (Non-normative) 13
2.14 Obligations (Normative) 14
2.15 Obligations (Non-normative) 14
2.16 Examples of Use 14
3 Conformance 16
3.1 Introduction 16
3.2 Conformance Tables 16
3.2.1 Attributes 16
A. Acknowledgements 19
B. Revision History 20

Table of Figures

Figure 1: Interaction between Parties 7

Copyright © OASIS® 2008. All Rights Reserved.

1 Introduction

Enterprises, including the healthcare enterprise, need a mechanism to exchange security and privacy policies, evaluate consent directives and determine authorizations in an interoperable manner. This document provides a cross-enterprise security and privacy profile that describes how to use eXtensible Access Control Markup Language (XACML) to provide these functions in an interoperable manner.

The Cross-Enterprise Security and Privacy Authorization (XSPA) profile of XACML describes several mechanisms to authenticate, administer, and enforce authorization policies controlling access to protected information residing within or across enterprise boundaries. The policies being administered and enforced relate to security, privacy, and consent directives. This profile MAY be used in coordination with additional standards including Web Services Trust Language (WS-Trust) and Security Assertion Markup Language (SAML).

This profile specifies the use of XACML 2.0 to promote interoperability within the healthcare community by providing common semantics and vocabularies for interoperable policy request/response, policy lifecycle, and policy enforcement.

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 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 – 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 entity that contains or receives information. 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 represent exhaustible system resources, such as printers, disk space, and central processing unit (CPU) cycles.

Operation - 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.

Permission - An approval to perform an operation on one or more protected objects.

Policy Administration Point (PAP) – Manages and makes available policies that may be stored in and retrieved from the Policy Repository.

Policy Decision Point (PDP) – Accepts information from an Authorization Decision Request and returns an access control decision based on evaluation of XACML policy. PDPs MAY be hierarchical.

Policy Enforcement Point (PEP) – Performs access control by making decision requests and enforcing authorization decisions. It facilitates passing XACML authorization request attributes and enforcing XACML response decisions and obligations. This module MAY be used for obtaining attributes required for authorization from a Policy Information Point (PIP) by an application. Typical attributes collected at this level include ANSI RBAC (American National Standards Institute Role Based Access Control) attributes, Health Level Seven (HL7) provider permissions, HL7 resource permission, and HL7 patient privacy constraints.

Policy Information Point (PIP) – Repository of attribute data that is made available to support authorization decisions.

Copyright © OASIS® 2008. All Rights Reserved.

Structural Role - A job function within the context of an organization whose permissions are defined by operations on workflow objects consistent with the definition of structural role found in 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

[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.

[XACML CORE] OASIS Standard, "XACML 2.0 Core: eXtensible Access Control Markup Language (XACML) Version 2.0", March 2005 http://docs.oasis-open.org/xacml/2.0/access_control-xacml-2.0-core-spec-os.pdf

[SAML-XACML20] OASIS Working Draft, "SAML 2.0 profile of XACML 2.0 Errata", November 2005, http://www.oasis-open.org/committees/download.php/15447/xacml-2.0-saml-errata-wd.zip

[SX20-ASSN-SCH] OASIS Standard, schema (assertion), http://www.oasis-open.org/committees/download.php/11474/access_control-xacml-2.0-saml-assertion-schema-os.xsd

[SX20-PROT-SCH] OASIS Standard, schema (protocol), http://www.oasis-open.org/committees/download.php/11475/access_control-xacml-2.0-saml-protocol-schema-os.xsd

[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.

[HL7-CONSENT] HL7 Consent Related Vocabulary Confidentiality Codes Recommendation, http://lists.oasis-open.org/archives/xacml-demo-tech/200712/doc00003.doc, from project submission: http://lists.oasis-open.org/archives/xacml-demo-tech/200712/msg00015.html

[ASTM E1986-98 (2005)] Standard Guide for Information Access Privileges to Health Information.

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

1.3 Non-Normative References

[SAML-XACML20V2] OASIS Working Draft, "SAML 2.0 profile of XACML Version 2", July 2007 (current working draft covers all versions of XACML). http://www.oasis-open.org/committees/download.php/24681/xacml-profile-saml2.0-v2-spec-wd-5-en.pdf

[XACML-RBAC] OASIS Standard, "Core and hierarchical role based access control (RBAC) profile of XACML v2.0", February 2005 http://docs.oasis-open.org/xacml/2.0/access_control-xacml-2.0-rbac-profile1-spec-os.pdf

[HITSP] Healthcare Information Technology Standards Panel (HITSP) at www.hitsp.org

[XSPA-XACML-EXAMPLES] Cross-Enterprise Security and Privacy Authorization (XSPA) Profile of XACML v2.0 for Healthcare, Implementation Examples. http://www.oasis-open.org/committees/document.php?document_id=30430

Copyright © OASIS® 2008. All Rights Reserved.

2 2 XSPA profile of XACML

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.

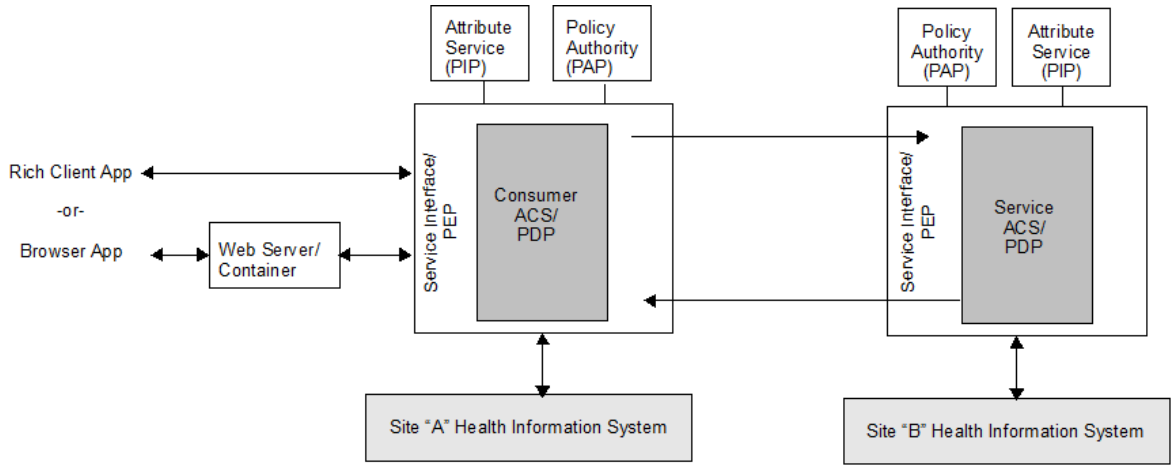

Figure 1: Interaction between Parties

2.1.1 Service Interface

XACML functions of the Policy Enforcement Point (PEP) are carried out by the Service Interface.

The PEP interacts with the Policy Information Point (PIP) of the Attribute Service and the Policy Decision Point (PDP) functionality of the Access Control Service (ACS), in enforcing authorization decisions.

2.1.2 Access Control Service (Service Consumer)

The XSPA profile of XACML supports sending all Service User requests through an ACS. XACML functions of the PDP are carried out by the ACS. The Service Consumer ACS MAY serve as an enterprise gateway.

Attributes necessary to make a local access control decision are determined and HL7 Permission **[HL7-PERM]** are granted to the Service User based on their role, purpose of use (POU), the service endpoint of the external resource, and any site specific operational attributes.

2.1.3 Attribute Service

XACML functions of the Policy Information Point (PIP) are carried out by the Attribute Service.

The Attribute Service has access to attribute information (e.g., location, purpose of use), object preferences, consent directives and other privacy conditions (object masking, object filtering, user, role, purpose, etc.) that constrain enforcement.

2.1.4 Policy Authority

XACML functions of the Policy Administration Point (PAP) are carried out by the Policy Authority.

The Policy Authority has access to security policies that include 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.

Copyright © OASIS® 2008. All Rights Reserved.

2.1.5 Access Control Service (Service Provider)

The Service 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. The Service ACS MAY serve as an enterprise gateway.

2.2 Transmission Integrity

The XSPA profile of XACML 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 XACML 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 **[XACML-CORE]**.

2.5 Security Considerations

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

- Entities MUST be members of defined information domains under the authorization control of a defined set of policies,
- Entities MUST have been identified and provisioned (credentials issued, privileges granted, etc.) in accordance with policy,
- Privacy policies MUST have been identified and provisioned (consents, user preferences, etc.) in accordance with policy,
- Pre-existing security and privacy policies MUST have been provisioned to Access Control Services,
- The capabilities and location of requested information/document repository services MUST be known,
- Secure channels MUST be established as required by policy,
- Audit services MUST be operational and initialized, and
- Entities MUST have pre-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

A XACML extension is used to enable the SAML protocol layer. This is described in the **[SAML-XACML-20]** specification and in the **[SX20-PROT-SCH]** schema.

2.8 Naming Syntax, Restrictions and Acceptable Values

This profile will support the namespace requirements described in **[XACML-CORE]**.

Copyright © OASIS® 2008. All Rights Reserved.

2.9 Namespace Requirements

This profile will support the namespace requirements described in **[XACML-CORE]**.

2.10 Attribute Rules of Equality

This profile will support the attribute evaluation requirements described in **[XACML-CORE]**.

2.11 Attribute Naming Syntax, Restrictions and Acceptable Values

Table 1: Standard Attributes (Normative)

Attribute ID*	Identifier	Type	Valid Values
subject:subject-id	urn:oasis:names:tc:xacml:2.0:subject:subject-id	String	Unique identifier of subject, if in the US domain, a National Provider Identifier issued by HHS/CMS and mandated by HIPAA.
subject:locality	urn:oasis:names:tc:xacml:2.0:subject:locality	String	Unique identifier of the consuming organization and/or facility.
subject:hl7:permission	urn:oasis:names:tc:xspa:1.0:subject:hl7:permission	String	Refer to [HL7-PERM] and its OID representation.
subject:role	urn:oasis:names:tc:xacml:2.0:subject:role	String	Structural Role refer to [ASTM E1986-98 (2005)] and its OID representation.
subject:purposeofuse	urn:oasis:names:tc:xspa:1,0:subject:purposeofuse	String	Healthcare Treatment, Emergency Treatment, System Administration, Operations, Payment, Research, Marketing, Public Health
resource:resource-id	urn:oasis:names:tc:xacml:2.0: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.
resource:hl7:type	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.
resource:org:permission	urn:oasis:names:tc:xspa:1.0:resource:org:hl7:permissions	String	Refer to [HL7-PERM] and its OID representation. This attribute holds permissions required by the servicing organization to grant access to a specific resource.

Copyright © OASIS® 2008. All Rights Reserved.

Attribute ID*	Identifier	Type	Valid Values
resource:org:role	urn:oasis:names:tc:xspa:1.0:resource:org:role	String	S tructural Role refer to [ASTM E1986-98 (2005)] and its OID representation. This attribute holds roles required by the servicing organization to grant access to a specific resource.
resource:patient:confidentiality-code	urn:oasis:names:tc:xspa:1.0:resource:patient:hl7:confidentiality-code	String	Refer to [HL7-CONSENT] The default value for this attribute is N (normal operations.)
resource:hl7:dissenting-subject-id	urn:oasis:names:tc:xspa:1.0:resource:patient:dissenting-subject-id	String	US domain specific is National Provider issued by HHS/CMS and mandated by HIPAA.
resource:hl7:dissenting-role	urn:oasis:names:tc:xspa:1.0:resource:patient:dissenting-role	String	Structural Role refer to [ASTM E1986-98 (2005)] and its OID representation.
environment:locality	urn:oasis:names:tc:xspa:1.0:environment:locality	String	Unique identifier of the servicing organization.

*Note: Attribute-ID is provided for mapping to pseudo-code in the [XSPA-XACML-EXAMPLES] document.

The confidentiality-code may be used to identify sensitive information, such as records relating to drug abuse, alcoholism, or alcohol abuse, infection with the human immunodeficiency virus (HIV) or sickle cell anemia.

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

The dissenting-subject-id identifies those denied access to a protected resource based on a patient's consent directive. The format of dissenting-subject-id MUST be consistent with the format of the subject-id.

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

Table 2: Standard Attributes (Non-Normative)

Attribute ID*	Identifier	Type	Valid Values
subject:npi	urn:oasis:names:tc:xspa:1.0:subject:npi	String	National Provider ID provided by U.S. Government for all active providers.
subject:functional-role	urn:oasis:names:tc:xspa:1.0:subject:functional-role	String	Functional roles provide a placeholder to group permissions required for fine grain access control. There MUST be mutual agreement of there use and definition between participating organizations.
resource:org:allowed-organizations	urn:oasis:names:tc:xspa:1.0:resource:org:allowed-organizations	String	Holds identification of allowed trading partners.

Copyright © OASIS® 2008. All Rights Reserved.

Attribute ID*	Identifier	Type	Valid Values
resource:org:hoursofoperations:start	urn:oasis:names:tc:xspa:1.0:resource:org:hoursofoperation:start	Time	Time plus locale
resource:org:hoursofoperation:end	urn:oasis:names:tc:xspa:1.0:resource:org:hoursofoperation:end	Time	Time plus locale
resource:patient:opt-in	urn:gov:hhs:fha:nhinc:patient-opt-in	String	Yes or No. US realm specific and required for v2.1 of NHIN connect.
resource:patient:allowed-organizations	urn:oasis:names:tc:xspa:1.0:resource:patient:allowed-organizations	String	Holds identification of organizations allowed to access patients medical record as defined by patient's consent directive.
obligation:patient:mask:advancedirectives:dissenting-role	urn:oasis:names:tc:xspa:1.0:resource:patient:masked:advancedirectives:dissenting-role	String	Structural Role refer to [ASTM E1986-98 (2005)] and its OID representation.
obligation:patient:mask:alerts:dissenting-role	urn:oasis:names:tc:xspa:1.0:resource:patient:masked:alerts:dissenting-role	String	Structural Role refer to [ASTM E1986-98 (2005)] and its OID representation.
obligation:patient:mask:encounters:dissenting-role	urn:oasis:names:tc:xspa:1.0:resource:patient:masked:encounters:dissenting-role	String	Structural Role refer to [ASTM E1986-98 (2005)] and its OID representation.
obligation:patient:mask:familyhistory:dissenting-role	urn:oasis:names:tc:xspa:1.0:resource:patient:masked:familyhistory:dissenting-role	String	Structural Role refer to [ASTM E1986-98 (2005)] and its OID representation.
obligation:patient:mask:functionalstatus:dissenting-role	urn:oasis:names:tc:xspa:1.0:resource:patient:masked:functionalstatus:dissenting-role	String	Structural Role refer to [ASTM E1986-98 (2005)] and its OID representation.
obligation:patient:mask:immunizations:dissenting-role	urn:oasis:names:tc:xspa:1.0:resource:patient:masked:immunizations:dissenting-role	String	Structural Role refer to [ASTM E1986-98 (2005)] and its OID representation.
obligation:patient:mask:medicalequipment:dissenting-role	urn:oasis:names:tc:xspa:1.0:resource:patient:masked:medicalequipment:dissenting-role	String	Structural Role refer to [ASTM E1986-98 (2005)] and its OID representation.
obligation:patient:mask:medications:dissenting-role	urn:oasis:names:tc:xspa:1.0:resource:patient:masked:medications:dissenting-role	String	Structural Role refer to [ASTM E1986-98 (2005)] and its OID representation.
obligation:patient:mask:payers:dissenting-role	urn:oasis:names:tc:xspa:1.0:resource:patient:masked:payers:dissenting-role	String	Structural Role refer to [ASTM E1986-98 (2005)] and its OID representation.
obligation:patient:mask:planofcare:dissenting-role	urn:oasis:names:tc:xspa:1.0:resource:patient:masked:planofcare:dissenting-role	String	Structural Role refer to [ASTM E1986-98 (2005)] and its OID representation.

Copyright © OASIS® 2008. All Rights Reserved.

Attribute ID*	Identifier	Type	Valid Values
obligation:patient:mask:problems:dissenting-role	urn:oasis:names:tc:xspa:1.0:resource:patient:masked:problems:dissenting-role	String	Structural Role refer to [ASTM E1986-98 (2005)] and its OID representation.
obligation:patient:mask:procedures:dissenting-role	urn:oasis:names:tc:xspa:1.0:resource:patient:masked:procedures:dissenting-role	String	Structural Role refer to [ASTM E1986-98 (2005)] and its OID representation.
obligation:patient:mask:purpose:dissenting-role	urn:oasis:names:tc:xspa:1.0:resource:patient:masked:purpose:dissenting-role	String	Structural Role refer to [ASTM E1986-98 (2005)] and it's OID representation.
obligation:patient:mask:results:dissenting-role	urn:oasis:names:tc:xspa:1.0:resource:patient:masked:results:dissenting-role	String	Structural Role refer to [ASTM E1986-98 (2005)] and it's OID representation.
obligation:patient:mask:socialhistory:dissenting-role	urn:oasis:names:tc:xspa:1.0:resource:patient:masked:socialhistory:dissenting-role	String	Structural Role refer to [ASTM E1986-98 (2005)] and it's OID representation.
obligation:patient:mask:vitals:dissenting-role	urn:oasis:names:tc:xspa:1.0:resource:patient:masked:vitals:dissenting-role	String	Structural Role refer to [ASTM E1986-98 (2005)] and it's OID representation.
obligation:patient:mask:advancedirectives:dissenting-subject-id	urn:oasis:names:tc:xspa:1.0:resource:patient:masked:advancedirectives:dissenting-subject-id	String	Provider unique identifier. US Domain this is National Provider Indentifier NPI.
obligation:patient:mask:alerts:dissenting-subject-id	urn:oasis:names:tc:xspa:1.0:resource:patient:masked:alerts:dissenting-subject-id	String	Provider unique identifier. US Domain this is National Provider Indentifier NPI.
obligation:patient:mask:encounters:dissenting-subject-id	urn:oasis:names:tc:xspa:1.0:resource:patient:masked:encounters:dissenting-subject-id	String	Provider unique identifier. US Domain this is National Provider Indentifier NPI.
obligation:patient:mask:familyhistory:dissenting-subject-id	urn:oasis:names:tc:xspa:1.0:resource:patient:masked:familyhistory:dissenting-subject-id	String	Provider unique identifier. US Domain this is National Provider Indentifier NPI.
obligation:patient:mask:functionalstatus:dissenting-subject-id	urn:oasis:names:tc:xspa:1.0:resource:patient:masked:functionalstatus:dissenting-subject-id	String	Provider unique identifier. US Domain this is National Provider Indentifier NPI.
obligation:patient:mask:immunizations:dissenting-subject-id	urn:oasis:names:tc:xspa:1.0:resource:patient:masked:immunizations:dissenting-subject-id	String	Provider unique identifier. US Domain this is National Provider Indentifier NPI.
obligation:patient:mask:medicalequipment:dissenting-subject-id	urn:oasis:names:tc:xspa:1.0:resource:patient:masked:medicalequipment:dissenting-subject-id	String	Provider unique identifier. US Domain this is National Provider Indentifier NPI.

Copyright © OASIS® 2008. All Rights Reserved.

Attribute ID*	Identifier	Type	Valid Values
obligation:patient:mask:medications:dissenting-subject-id	urn:oasis:names:tc:xspa:1.0:resource:patient:masked:medications:dissenting-subject-id	String	Provider unique identifier. US Domain this is National Provider Indentifier NPI.
obligation:patient:mask:payers:dissenting-subject-id	urn:oasis:names:tc:xspa:1.0:resource:patient:masked:payers:dissenting-subject-id	String	Provider unique identifier. US Domain this is National Provider Indentifier NPI.
obligation:patient:mask:planofcare:dissenting-subject-id	urn:oasis:names:tc:xspa:1.0:resource:patient:masked:planofcare:dissenting-subject-id	String	Provider unique identifier. US Domain this is National Provider Indentifier NPI.
obligation:patient:mask:problems:dissenting-subject-id	urn:oasis:names:tc:xspa:1.0:resource:patient:masked:problems:dissenting-subject-id	String	Provider unique identifier. US Domain this is National Provider Indentifier NPI.
obligation:patient:mask:procedures:dissenting-subject-id	urn:oasis:names:tc:xspa:1.0:resource:patient:masked:procedures:dissenting-subject-id	String	Provider unique identifier. US Domain this is National Provider Indentifier NPI.
obligation:patient:mask:purpose:dissenting-subject-id	urn:oasis:names:tc:xspa:1.0:resource:patient:masked:purpose:dissenting-subject-id	String	Provider unique identifier. US Domain this is National Provider Indentifier NPI.
obligation:patient:mask:results:dissenting-subject-id	urn:oasis:names:tc:xspa:1.0:resource:patient:masked:results:dissenting-subject-id	String	Provider unique identifier. US Domain this is National Provider Indentifier NPI.
obligation:patient:mask:socialhistory:dissenting-subject-id	urn:oasis:names:tc:xspa:1.0:resource:patient:masked:socialhistory:dissenting-subject-id	String	Provider unique identifier. US Domain this is National Provider Indentifier NPI.
obligation:patient:mask:vitals:dissenting-subject-id	urn:oasis:names:tc:xspa:1.0:resource:patient:masked:vitals:dissenting-subject-id	String	Provider unique identifier. US Domain this is National Provider Indentifier NPI.
resource:snomedct:type	urn:oasis:names:tc:xspa:2.0:resource:snomedct:type	String	For full implementation information on healthcare objects refer to [SNOMED CT].

178 *Note: Attribute-ID is provided for mapping to pseudo-code in the **[XSPA-XACML Example]** document.

179 2.12 Standard Rules (Normative)

180 At this time no Standard Rule requirements have been defined for this profile.

181 2.13 Standard Rules (Non-normative)

182 At this time no optional Rules have been defined for this profile.

Copyright © OASIS® 2008. All Rights Reserved.

2.14 Obligations (Normative)

This profile describes the use of <Obligation> element as optional.

2.15 Obligations (Non-normative)

The <Obligation> element will be used in the XACML response to notify requestor that additional processing requirements are needed. This profile focuses on the use of obligations to enforce patient privacy election. The XACML response may contains one or more obligations. Processing of an obligation is application specific. An <Obligation> may contain the object(resource) action pairing information. If multiple vocabularies are used for resource definitions the origin of the vocabulary MUST be identified.

The obligation should conform to following structure:

urn:oasis:names:tc:xspa:1.0:patient:<action>:<healthcareobject>:<constraint-identifier>

The following is an example response obligation segment.

```
<xacml:Obligations
xmlns:xacml="urn:oasis:names:tc:xacml:2.0:policy:schema:os" >
   <xacml:Obligation
 ObligationId="urn:oasis:names:tc:xspa:1.0:patient:masked:vitals:dissenting-
subject-id" FulfillOn="Permit">
   </xacml:Obligation>
</xacml:Obligations>
```

2.16 Examples of Use

The following section of this profile provides examples of XACML request and response messages. The examples are intended to provide additional guidance to implementers of this profile.

All XACML request and response attributes are identified by a Uniform Resource Name (URN) from the vocabulary. This enables seamless mapping of data values between the client interface and policy services.

It is recommended that the SAML 2.0 profile of XACML v2.0 **[SAML-XACML20]** be used for PEP-PDP communications. (Note: use **[SX20-ASSN-SCH]** and **[SX20-PROT-SCH]** schema files and specification in 17-Nov-05 Errata version.)

Following are the expected SOAP-wrapped request and response messages. Note that request MUST have a unique ID which is used to map to a unique response as specified in [XACML-CORE]. The request MAY be returned with the response.

Sample SOAP SAML XACML Request wrapper:

```
<?xml version="1.0" encoding="UTF-8"?>
<soapenv:Envelope
    xmlns:soapenv ="http://schemas.xmlsoap.org/soap/envelope/"
    xmlns:xsd="http://www.w3.org/2001/XMLSchema"
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  <soapenv:Body>
    <xacml-samlp:XACMLAuthzDecisionQuery
        xmlns:xacml-samlp="urn:oasis:xacml:2.0:saml:protocol:schema:os"
        ID="_e064bd912f83c1544fea110307000acf"
        IssueInstant="2007-05-21T22:00:36Z"
        Version="2.0">
      <xacml-context:Request
          xmlns:xacml-
context="urn:oasis:names:tc:xacml:2.0:context:schema:os">
        <!-- See [XACML-Request-01] for sample content of this element -->
      </xacml-context:Request>
    </xacml-samlp:XACMLAuthzDecisionQuery>
  </soapenv:Body>
</soapenv:Envelope>
```

The request message above contains three protocol layers:

Copyright © OASIS® 2008. All Rights Reserved.

- **soapenv:** is the SOAP layer. A SOAP Envelope contains a SOAP Body.
- **xacml-samlp:** is the SAML protocol layer, which is enabled by the XACML extension to the SAML protocol, which is described in **[SAML-XACML-20]** specification and in the **[SX20-PROT-SCH]** schema. Note that the usual samlp: is not declared here because xacml-samlp: extends samlp: and will transparently include the samlp: base declarations.
- **xacml-context:** is the XACML request/response layer which is described in **[XACML-CORE]**.

Sample SOAP SAML XACML response wrapper:

```
<soapenv:Envelope
    xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
    xmlns:xsd="http://www.w3.org/2001/XMLSchema"
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  <soapenv:Body>
    <samlp:Response
      xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
      ID="A12345602"
      Version="2.0"
      IssueInstant="2007-05-09T00:00:01Z">
      <samlp:Status>
        <samlp:StatusCode
          Value="urn:oasis:names:tc:SAML:2.0:status:Success"/>
      </samlp:Status>
      <saml:Assertion
          xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
          Version="2.0"
          ID="A12345603"
          IssueInstant="2007-05-09T00:00:01Z">
        <saml:Issuer>xacml.interop.com</saml:Issuer>
        <saml:Statement
            xmlns:xacml-saml="urn:oasis:xacml:2.0:saml:assertion:schema:os"
            xsi:type="xacml-saml:XACMLAuthzDecisionStatementType">
          <xacml-context:Response
              xmlns:xacml-
context="urn:oasis:names:tc:xacml:2.0:context:schema:os">
            <!-- See [XACML-Response-01] for sample content of this element --
>
          </xacml-context:Response>
        </saml:Statement>
      </saml:Assertion>
    </samlp:Response>
  </soapenv:Body>
</soapenv:Envelope>
```

The response message above contains three protocol layers:

- **soapenv:** is the SOAP layer. A SOAP Envelope contains a SOAP Body.
- **samlp:** is the SAML Protocol layer, which is explicitly declared this time because in the response case the xacml extension is lower in the samlp: protocol. In particular, samlp: requires a saml:Assertion, which in turn includes a saml:Statement. It is within the saml:Statement that the xacml extension occurs and is referred to as xacml-saml: because it extends the saml:Assertion/saml:Statement with the XACMLAuthzDecisionStatementType. The details are described in the **[SAML-XACML-20]** specification and the **[SX20-ASSN-SCH]** schema.
- **xacml-context:** is the XACML request/response layer which is described in **[XACML-CORE]**

Copyright © OASIS® 2008. All Rights Reserved.

3 Conformance

3.1 Introduction

The XSPA profile of XACML addresses the following aspects of conformance:

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

An Implementation of a PDP MUST conform to XACML v2.0 specification.

3.2 Conformance Tables

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

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

3.2.1 Attributes

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

Table 3: Conformance Attributes

Identifiers	
urn:oasis:names:tc:xacml:2.0:subject:subject-id	M
urn:oasis:names:tc:xacml:2.0:subject:locality	M
urn:oasis:names:tc:xspa:1.0:subject:hl7:permission	M
urn:oasis:names:tc:xacml:2.0:subject:role	M
urn:oasis:names:tc:xspa:1.0:subject:purposeofuse	M
urn:oasis:names:tc:xacml:2.0:resource:resource-id	M
urn:oasis:names:tc:xspa:1.0:resource:hl7:type	M
urn:oasis:names:tc:xspa:1.0:resource:org:hl7:permissions	M
urn:oasis:names:tc:xspa:1.0:resource:org:role	M
urn:oasis:names:tc:xspa:1.0:resource:patient:hl7:confidentiality-code	M
urn:oasis:names:tc:xspa:1.0:resource:patient:dissenting-subject-id	M
urn:oasis:names:tc:xspa:1.0:resource:patient:dissenting-role	M
urn:oasis:names:tc:xspa:1.0:environment:locality	M
urn:oasis:names:tc:xspa:1.0:subject:npi	O
urn:oasis:names:tc:xspa:1.0:subject:functional-role	O

Copyright © OASIS® 2008. All Rights Reserved.

Identifiers	
urn:oasis:names:tc:xspa:1.0:resource:org:allowed-organizations	O
urn:oasis:names:tc:xspa:1.0:resource:org:hoursofoperation:start	O
urn:oasis:names:tc:xspa:1.0:resource:org:hoursofoperation:end	O
urn:gov:hhs:fha:nhinc:patient-opt-in	O
urn:oasis:names:tc:xspa:1.0:resource:patient:allowed-organizations	O
urn:oasis:names:tc:xspa:1.0:resource:patient:masked:advancedirectives:dissenting-role	O
urn:oasis:names:tc:xspa:1.0:resource:patient:masked:alerts:dissenting-role	O
urn:oasis:names:tc:xspa:1.0:resource:patient:masked:encounters:dissenting-role	O
urn:oasis:names:tc:xspa:1.0:resource:patient:masked:familyhistory:dissenting-role	O
urn:oasis:names:tc:xspa:1.0:resource:patient:masked:functionalstatus:dissenting-role	O
urn:oasis:names:tc:xspa:1.0:resource:patient:masked:immunizations:dissenting-role	O
urn:oasis:names:tc:xspa:1.0:resource:patient:masked:medicalequipment:dissenting-role	O
urn:oasis:names:tc:xspa:1.0:resource:patient:masked:medications:dissenting-role	O
urn:oasis:names:tc:xspa:1.0:resource:patient:masked:payers:dissenting-role	O
urn:oasis:names:tc:xspa:1.0:resource:patient:masked:planofcare:dissenting-role	O
urn:oasis:names:tc:xspa:1.0:resource:patient:masked:problems:dissenting-role	O
urn:oasis:names:tc:xspa:1.0:resource:patient:masked:procedures:dissenting-role	O
urn:oasis:names:tc:xspa:1.0:resource:patient:masked:purpose:dissenting-role	O
urn:oasis:names:tc:xspa:1.0:resource:patient:masked:results:dissenting-role	O
urn:oasis:names:tc:xspa:1.0:resource:patient:masked:socialhistory:dissenting-role	O
urn:oasis:names:tc:xspa:1.0:resource:patient:masked:vitals:dissenting-role	O
urn:oasis:names:tc:xspa:1.0:resource:patient:masked:advancedirectives:dissenting-subject-id	O
urn:oasis:names:tc:xspa:1.0:resource:patient:masked:alerts:dissenting-subject-id	O
urn:oasis:names:tc:xspa:1.0:resource:patient:masked:encounters:dissenting-subject-id	O
urn:oasis:names:tc:xspa:1.0:resource:patient:masked:familyhistory:dissenting-subject-id	O
urn:oasis:names:tc:xspa:1.0:resource:patient:masked:functionalstatus:dissenting-subject-id	O
urn:oasis:names:tc:xspa:1.0:resource:patient:masked:immunizations:dissenting-subject-id	O
urn:oasis:names:tc:xspa:1.0:resource:patient:masked:medicalequipment:dissenting-subject-id	O

Copyright © OASIS® 2008. All Rights Reserved.

Identifiers	
urn:oasis:names:tc:xspa:1.0:resource:patient:masked:medications:dissenting-subject-id	O
urn:oasis:names:tc:xspa:1.0:resource:patient:masked:payers:dissenting-subject-id	O
urn:oasis:names:tc:xspa:1.0:resource:patient:masked:planofcare:dissenting-subject-id	O
urn:oasis:names:tc:xspa:1.0:resource:patient:masked:problems:dissenting-subject-id	O
urn:oasis:names:tc:xspa:1.0:resource:patient:masked:procedures:dissenting-subject-id	O
urn:oasis:names:tc:xspa:1.0:resource:patient:masked:purpose:dissenting-subject-id	O
urn:oasis:names:tc:xspa:1.0:resource:patient:masked:results:dissenting-subject-id	O
urn:oasis:names:tc:xspa:1.0:resource:patient:masked:socialhistory:dissenting-subject-id	O
urn:oasis:names:tc:xspa:1.0:resource:patient:masked:vitals:dissenting-subject-id	O

298
299

Copyright © OASIS® 2008. All Rights Reserved.

A. Acknowledgements

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

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

Steve Steffensen, Department of Defense
Daniel Dority, Jericho Systems Corporation
Brian McClung, Jericho Systems Corporation
Brendon Unland, Jericho Systems Corporation
Emory Fry, Naval Health Research Center
Anil Saldhana, Red Hat
Dilli Doral, Sun Microsystems
Steven Jarosz, Sun Microsystems
Mike Davis, Veterans Health Administration
Duane DeCouteau, Veterans Health Administration
David Staggs, Veterans Health Administration

XACML TC Members during the development of this specification:

Erik Rissanen, Axiomatics AB
Steve Anderson, BMC Software
Ronald Jacobson, CA
Masum Hasan, Cisco Systems, Inc.
Anil Tappetla, Cisco Systems, Inc.
Tim Moses, Entrust
Michiharu Kudo, IBM
Michael McIntosh, IBM
Ron Williams, IBM
Guy Denton, IBM
Craig Forster, IBM
Vernon Murdoch, IBM
Anthony Nadalin, IBM
Bill Parducci, Individual
David Chadwick, Individual
Abbie Barbir, Nortel
Harry Haury, NuParadigm Government Systems, Inc.
Hal Lockhart, Oracle Corporation
Willem de Pater, Oracle Corporation
Prateek Mishra, Oracle Corporation
Kamalendu Biswas, Oracle Corporation
Rich Levinson, Oracle Corporation
Anil Saldhana, Red Hat
Darran Rolls, SailPoint Technologies
Daniel Engovatov, Stream Dynamics, Inc.
Aravindan Ranganathan, Sun Microsystems
Dilli Arumugam, Sun Microsystems
Seth Proctor, Sun Microsystems
John Tolbert, The Boeing Company
Martin Smith, US Department of Homeland Security
Duane DeCouteau, Veterans Health Administration
David Staggs, Veterans Health Administration

Copyright © OASIS® 2008. All Rights Reserved.

348 # B. Revision History

349

Document ID	Date	Committer	Comment
xspa-xacml-profile-01	09/29/2008	Brett Burley	Initial draft v1.0
xspa-xacml-profile-01	09/29/2008	Craig Winter	QA review / revision v1.1
xspa-xacml-profile-01	10/03/2008	Duane DeCouteau	Obligation, rules, and Snomed CT. v,1,2
xspa-xacml-profile-cd01	10/10/2008	Brett Burley	Formatting as Committee Draft
xspa-xacml-profile-cd-02	10/23/2008	Duane DeCouteau	Action Items, structural roles, HL7 OID, conformance section
xspa-xacml-profile-cd-02	11/05/2008	Craig Winter	QA review / revision v1.3
xspa-xacml-profile-pr-01	11/05/2008	David Staggs	Approved Public Review Draft v1.0
xspa-xacml-profile-pr-02	4/20/2008	David Staggs	Post-Public Review Draft
xspa-xacml-profile-cd-02	6/7/2009	David Staggs	CD prior to Public Review Draft v2.0

350

Copyright © OASIS® 2008. All Rights Reserved.