

Integrating the Healthcare Enterprise



5

IHE IT Infrastructure Technical Framework Supplement

10 **Cross-Enterprise User Assertion – Attribute Extension (XUA++)**

Trial Implementation

15

Date: August 19, 2011
Author: ITI Technical Committee
Email: iti@ihe.net

20

Foreword

This is a supplement to the IHE IT Infrastructure Technical Framework 8.0. Each supplement undergoes a process of public comment and trial implementation before being incorporated into the volumes of the Technical Frameworks.

- 25 This supplement is submitted for Trial Implementation as of August 19, 2011 and will be available for testing at subsequent IHE Connectathons. The supplement may be amended based on the results of testing. Following successful testing it will be incorporated into the IT Infrastructure Technical Framework. Comments are invited and can be submitted at <http://www.ihe.net/iti/iticomments.cfm> or by email to iti@ihe.net.
- 30 This supplement describes changes to the existing technical framework documents and where indicated amends text by addition (**bold underline**) or removal (~~**bold strikethrough**~~), as well as addition of large new sections introduced by editor's instructions to "add new text" or similar, which for readability are not bolded or underlined.
- 35 "Boxed" instructions like the sample below indicate to the Volume Editor how to integrate the relevant section(s) into the relevant Technical Framework volume:

<i>Replace Section X.X by the following:</i>
--

General information about IHE can be found at: www.ihe.net

- 40 Information about the IHE IT Infrastructure can be found at:
<http://www.ihe.net/Domains/index.cfm>

Information about the structure of IHE Technical Frameworks and Supplements can be found at:
<http://www.ihe.net/About/process.cfm> and <http://www.ihe.net/profiles/index.cfm>

- 45 The current version of the IHE Technical Framework can be found at:
http://www.ihe.net/Technical_Framework/index.cfm

CONTENTS

50	Introduction.....	4
	1.1 Use-cases	4
	1.1.1 Role-Based-Access Control	4
	1.1.2 Consent/Authorization	5
	1.1.3 Level of Assurance	5
55	1.1.4 Extended Audit Logging.....	6
	1.1.5 Purpose of Use	6
	1.1.6 Relationship-to-Patient	7
	Profile Abstract	7
	Open Issues and Questions	7
60	Closed Issues.....	8
	Volume 1 – Integration Profiles.....	10
	13.5 Options	10
	13.5.1 Subject-Role.....	10
	13.5.2 Authz-Consent.....	11
65	13.5.3 PurposeOfUse.....	11
	Glossary	12
	Volume 2 - Transactions.....	13
	3.40.3 Referenced Standards.....	13
	3.40.3.1 Normative -- required to use this profile.....	13
70	3.40.3.2 Informative -- assist with understanding or implementing this profile.....	13
	3.40.4.1.2.1 Subject-Role Option.....	16
	3.40.4.1.2.2 Authz-Consent Option.....	17
	3.40.4.1.2.3 PurposeOfUse Option	19
	3.40.4.1.3.1 Subject-Role Option.....	19
75	3.40.4.1.3.2 Authz-Consent Option.....	20
	3.40.4.1.3.3 PurposeOfUse Option	20
	3.20.7.8 Audit Encoding of the Purpose of Use value	20

80

Introduction

85 This supplement extends the Cross-Enterprise User Assertion (XUA) profile with Options that will enable access controls on the service side. The current XUA profile allows attributes but does not require any specific attributes beyond the user identity that is used for audit logging. There is now experience on how to extend an XUA Assertion to support some service side access control. These use-cases come from current experience in the USA NHIN, the EU epSOS, and other Health Information Exchanges globally. The solutions will also be informed by these experiences as well as an OASIS Standard on Cross-Enterprise Security and Privacy Authorizations (XSPA). Further guidance is provided by the [IHE Access Control Whitepaper](#).

1.1 Use-cases

95 The Attribute Extension use-cases are explained here in detail; they will be significantly simplified when integrated into the formal text. This year the first two use-cases were found to have mature standards and implementation. The other use-cases are described so that the reader can find the current standards development and projects. The expectation is that these other use-cases will be addressed in the future based on need, standards maturity, and implementation experience.

1.1.1 Role-Based-Access Control

100 Role-Based-Access Control is a common architecture for managing and enforcing authorizations. In this model users are assigned to roles, and permissions are assigned to these roles. In this way the administration of permissions to users is grouped through roles. In an RBAC model these roles are well-known and agreed to between the system that is managing users and the access control system. Given that a Federated Identity environment allows for a loose-coupling of the Identity-Manager and the Access Control point, there is a need to have a well-defined vocabulary for the roles. This set of roles will likely expand over time and will be extended with local codes into a Value-Set within any specific Security-Domain.

110 For this use-case we look to the roles defined in the XSPA standard, ASTM E1986, SNOMED, and ISO 21298. Although there are many organizations that have defined roles, there does not appear to be any specifically mature vocabulary in use at this time.

This use-case was determined to have mature standards and experience, although not mature enough for vocabulary to select, so it has been moved into the supplement section as part of the XUA Volume 1 and Volume 2 specification.

1.1.2 Consent/Authorization

115 There are transactions where the requester of the transaction knows of specific
Consent/Authorization evidence that would enable that transaction. The identification of the
specific Consent/Authorization object could be used by the relying party Access Control engine
as a hint. The Access Control engine could explicitly retrieve that specific object, validate that it
120 is indeed a properly formed Consent/Authorization, and determine if that Consent/Authorization
does indeed affect the Access Control decision.

This can be used where the requester had previously published Consent/Authorization evidence
Document but where this new knowledge had not yet propagated fully to the Access Control
infrastructure. This mechanism is also useful where the requester is under regulatory obligations
to include evidence of Consent/Authorization on each transaction. When this Option is used in
125 conjunction with the BPPC Profile, this would allow for the requester to include in the XUA
Assertion identification of a newly published BPPC Document. This option leverages the BPPC
consent model.

A specific use-case that might be satisfied with these functionalities is the need in epSOS to
include assertions that the ‘user’ as a provider has a legitimate relationship to the ‘patient’. In
130 this use-case, there could be a set of policies that declared these different legitimate relationship
types, and a policy assertion could additionally be included in the SAML assertion that indicates
that an access control decision has been made on the service user side of the transaction that
determined that the user does have the specified relationship to the patient. This would be done
with the AccessConsentPolicy mechanism.

135 There is experience using a system like this with the USA NHIN project, specifically when the
Social Security Administration (SSA) is explicitly authorized by the patient to retrieve Health
Information about a work related injury. The Explicit Authorization by the patient is captured as
a BPPC Acknowledgement document.

140 This use-case was determined to have mature standards and experience so it has been moved into
the supplement section as part of XUA Volume 1 and Volume 2 specification.

1.1.3 Level of Assurance

Level of Assurance is a measure of how sure the identity claimed represents the actual entity
(e.g., Human). It can be a Level of Assurance claim against the authentication event or the
provisioning event. This Level of Assurance can be a critical attribute used in Access Control
145 decisions, especially where actions are being taken such as ordering drugs or signing a
document.

At the time the XUA profile was written, there was no mature standard vocabulary for the Level
of Assurance. There are many guidance documents but they all stop short of defining a
vocabulary. There is USA regulation text in OMB M-04-04. There is guidance in NIST SP 800-
150 63, Liberty Alliance, and OASIS [sstc-saml-assurance-profile-draft-01.pdf].

This use-case is partially satisfied through the existing SAML assertion method of carrying the method used to authenticate the user (e.g., <AuthnContext>). Further specification is not clear at this time as there are many standards developments in play. Thus this use-case does not have mature enough standards and experience to continue at this time.

155 **1.1.4 Extended Audit Logging**

The current audit logging support simply puts the user identity found in the XUA assertion, into the IHE-ATNA audit log message. This is a good solution for most environments as it allows for minimal descriptors to be in the Security-Audit-Log and thus keep the risks associated with the audit log use low. The expectation is that at the time that the audit log is analyzed the Audit
160 Record Repository will have access to the identity directory. There are some environments where this level of access to the identity directory is not available, and the risks of adding user identity descriptions to the audit log are determined to be acceptable. In these environments there is a need for the XUA Assertion to include a descriptive identifier of the entity claimed.

165 There is experience with this in the USA NHIN project. The expansion of the user attributes to include descriptive values that are then placed into the ATNA audit log is an obvious extension of the XUA profile and does not require a specific extension. Further the inclusion of descriptive values in the ATNA audit log is considered counter to the principle IHE has applied to the ATNA audit log message to be minimal criteria resulting in few descriptive values in the audit log.

170 This use-case has not been further developed in this supplement as the inclusion of descriptive values in the ATNA audit log is discouraged by IHE and thus communicating the descriptive values in the SAML assertion is not justified. Local Policy may include these descriptive values and may require them in audit logs.

1.1.5 Purpose of Use

175 As explained in the [IHE Access Control White Paper](#), there are Access Control decisions that are based on the ultimate use of the data. For example a Patient may have provided a BPPC Consent/Authorization for treatment purposes, but explicitly disallowed any use for research regardless of de-identification methods used. The purpose of use is also informative to the ATNA audit log to enable specific reporting of Accounting of Disclosures and Breach
180 Notification. To enable this type of Audit Logging and Access Control decision there is a need to include in the XUA Assertion the intended purpose for which the data will be used. One specific purpose of use would be a Break-Glass / Emergency-Mode-Access.

185 There is emerging experience with purpose of use in some projects and vocabularies are available in XSPA, ASTM, and likely elsewhere. These vocabularies are incomplete and contain conflicting purpose of use values.

This use-case was determined to have mature standards and experience, although not mature enough vocabulary to select, so it has been moved into the supplement section as part of XUA

Volume 1 and Volume 2 specification. This use-case also updates the ATNA Audit Message to include an additional attribute for encoding the purpose of use value.

190 1.1.6 Relationship-to-Patient

There are Access Control rules that would allow specific access based on the users relationship to the patient. For example, care providers that have a direct or indirect treatment relationship with the patient may be given access, but other care providers would not be given access. The XUA Assertion would carry a claim, by the Identity Provider, as to the relationship between the
195 Entity (user) and the Patient. These relationships might include: Direct-Care, Indirect-Care, Care-Team, Billing-Team, Parent, Guardian, Spouse, etc.

No vocabulary has been brought forth at this time.

This use-case will be presented in a Profile Proposal for potential development next year. At this time the epSOS project is developing experience with using a second SAML assertion containing
200 the relationship-to-patient. We alternatively suggest that the Authz-Consent option may be used where the policy identified is a relationship-to-patient policy rather than a classical consent policy. This experience should inform future IHE profiling.

Profile Abstract

This supplement extends the Cross-Enterprise User Assertion (XUA) profile with Options that
205 will enable access controls on the service side.

Open Issues and Questions

XUA++003) Could the Authz-Consent mechanism be used to support the epSOS need for relationship to patient? It is believed that the mechanism provided in this supplement may be a lighter weight solution than the current epSOS mechanism that requires 2 SAML assertions, with
210 the second assertion purely an authorization statement about consent/authorization.

XUA++004) The XSPA profile encodes the user role using a simple string, where as the NHIN specification uses an XML element defined by HL7 as a way to carry a coded element with value, code-set identifier, and description of the value. This has the benefit of allowing multiple code-sets to be active. One example of where this is useful is in a community that might have a
215 more loose security domain that couples (federates) multiple Affinity Domains that have more strict security domains. There is ongoing concern that the HL7 coded entry mechanism may not be supported by identity providers and access control engines. We did not have specific evidence to change our current plan, to use the XML element rather than simple string; therefore the Trial Implementation still indicates this as an open issue. This issue happens with Role,
220 PurposeOfUse, NPI, and could be used in other places too. We invite comment on this topic.

Option A: Use strings only, implied assigning authority

```
<saml:Attribute Name="urn:oasis:names:tc:xspa:2.0:subject:npi">
```

```
<saml:AttributeValue>1234567890</saml:AttributeValue>
</saml:Attribute>
```

225 Option B: Use HL7 v3 CE data type

```
<saml:Attribute Name="urn:oasis:names:tc:xspa:2.0:subject:npi ">
  <saml:AttributeValue>
    <Role xmlns="urn:hl7-org:v3" xsi:type="CE"
      code="1234567890"
      codeSystem="2.16.840.1.113883.6.101"
      codeSystemName="Healthcare Provider Taxonomy"
      displayName="Dr Bob"/>
  </saml:AttributeValue>
</saml:Attribute>
```

230

235 Option C: Use HL7 v2 CX data type

```
<saml:Attribute Name="urn:oasis:names:tc:xspa:2.0:subject:npi">
  <saml:AttributeValue>1234567890^^^&2.16.840.1.113883.6.101&ISO
</saml:AttributeValue>
</saml:Attribute>
```

240

Closed Issues

245 **XUA++001)** Given the current state of the standards maturity necessary to support each of these use-cases, we choose to support use-case #1 (Role) and #2 (Consent). Public comment should provide evidence of use of standards to resolve the other use-cases indicated in the introduction.

We decided to Add ‘well-known’ attribute tags to be used to carry some informative values that are not mandatory, but when supported need to be done in the defined way. We take these attributes come from XSPA as emphasized by NHIN

- Subject ID - Descriptive Name of the user
- 250 • Subject Organization - Descriptive Name of the Organization the user is coming from
- Subject Organization ID - URN identifier of the Organization the user is coming from
- Home Community ID -- when in the context of XCA defined Communities the home community ID the user is coming from
- National Provider ID - When the user is a provider and has a National Provider ID

255 **XUA++002)** It is clear how an X-Service User would encode the attributes. It is not clear what behaviors we must require on the X-Service Provider Actor. In most cases these receiving behaviors would be very policy specific, access control policy.

Public comment was clear that there is no need to further define the behavior of the service provider. This behavior is purely contextual and policy driven.

260 **XUA++005)** This draft points to the use of SNOMED CT as the vocabulary for security role. This vocabulary is not managed with the intention of being used as security roles, they are maintained as occupations. There is ASTM E1986-09 that has an explicit list of security roles and is managed as a vocabulary for this purpose. The standard shows cross-reference to
265 SNOMED CT where there is equivalence. We invite comment on preference to the use of SNOMED CT vs. ASTM E1986-09.

We decided that none of these vocabularies are specifically best suited for profiling at this time. Therefore we will remove the requirement for SNOMED CT; and rather explain that the roles will come from a “Value-Set”, point at the SVS/ESVS Profiles on managing Value-Sets, and indicate that a Value-Set must be chosen by the Operational Implementation (Security
270 Domain Policy). We will point to the three standards vocabularies as a basis for the Security Domain to build their value-set.

Volume 1 – Integration Profiles

Edit the following section 13.5 with the following

275 13.5 Options

Options that may be selected for this Integration Profile are listed in Table 13.5-1 along with the Actors to which they apply. Dependencies between options when applicable are specified in notes.

280 **Table 13.5-1 XUA - Actors and Options**

Actor	Option	Section
X-Service User	<u>NoneSubject-Role</u>	<u>13.5.1</u>
	<u>Authz-Consent</u>	<u>13.5.2</u>
	<u>PurposeOfUse</u>	<u>13.5.3</u>
X-Service Provider	<u>NoneSubject-Role</u>	<u>13.5.1</u>
	<u>Authz-Consent</u>	<u>13.5.2</u>
	<u>PurposeOfUse</u>	<u>13.5.3</u>

Editor, please add the following sections

13.5.1 Subject-Role

285 Role-Based-Access Control is a common architecture for managing and enforcing authorizations. In this model users are assigned to roles, and permissions are assigned to these roles. In this way the administration of permissions to users is grouped through roles. In an RBAC model these roles are well-known and agreed to between the system that is managing users and the access control system. Given that a Federated Identity environment allows for a loose-coupling of the Identity-Manager and the Access Control point, there is a need to have a well-defined vocabulary for the roles. This set of roles will likely expand over time and will be extended with local codes into a Value-Set within any specific Security-Domain.

290 This option recommends that the Value-Set be derived from the role codes found in SNOMED-CT, ISO 21298, or ASTM E1986. The Value-Set used would bridge between different policy domain roles used in a client domain to those used in the service domain. In this way it is possible for local role definitions to be used as long as they can be bridged to the roles found in the selected Value-Set. Implementations should expect that the Value-Set used may be using

locally defined values. The use of the IHE Sharing of Value-Sets (SVS) Profile may assist with this.

See section ITI-TF-2b:3.40.4.1.2.1 and ITI-TF-2b:3.40.4.1.3.1 for transaction requirements.

300 **13.5.2 Authz-Consent**

There are transactions where the requester of the transaction knows of specific Consent/Authorization evidence that would enable that transaction. The identification could be used by the relying party Access Control engine as a hint. The Access Control engine could explicitly retrieve that specific object, validate that it is indeed a properly formed
305 Consent/Authorization, and determine if that Consent/Authorization does indeed affect the Access Control decision.

This can be used where the requester had previously published Consent/Authorization evidence Document but where this new knowledge had not yet propagated fully to the Access Control infrastructure. This mechanism is also useful where the requester is under regulatory obligations
310 to include evidence of Consent/Authorization on each transaction. When this Option is used in conjunction with the Basic Patient Privacy Consents (BPPC) Profile this would allow for the requester to include in the XUA Assertion identification of a newly published BPPC Document. This option leverages the BPPC consent model.

See section ITI-TF-2b:3.40.4.1.2.2 and ITI-TF-2b:3.40.4.1.3.2 for transaction requirements.

315 **13.5.3 PurposeOfUse**

As explained in the [IHE Access Control White Paper](#), there are Access Control decisions that are based on the ultimate use of the data. For example a Patient may have provided a BPPC Consent/Authorization for treatment purposes, but explicitly disallowed any use for research regardless of de-identification methods used. The purpose of use is also informative to the
320 ATNA audit log to enable specific reporting of Accounting of Disclosures and Breach Notification. To enable this type of Audit Logging and Access Control decision there is a need to include in the XUA Assertion the intended purpose for which the data will be used. One specific purpose of use would be a Break-Glass / Emergency-Mode-Access.

This option recommends that the Value-Set be derived from the codes found in ISO 14265, or
325 XSPA. Implementations should expect that the Value-Set used may be using locally defined values. The use of the IHE Sharing of Value-Sets (SVS) Profile may assist with this.

See section ITI-TF-2b:3.40.4.1.2.3 and ITI-TF-2b:3.40.4.1.3.3 for transaction requirements.

Glossary

330 *Add the following terms to the Glossary:*

Volume 2 - Transactions

Update section 3.40.3 as shown below

335 **3.40.3 Referenced Standards**

3.40.3.1 Normative -- required to use this profile

- OASIS <http://www.oasis-open.org/committees/security/>.
 - [SAMLCore](#) SAML V2.0 Core standard
 - [WSS10](#) OASIS Standard, "OASIS Web Services Security: SOAP Message Security 1.0 (WS-Security 2004)", March 2004.
 - [WSS11](#) OASIS Standard, "OASIS Web Services Security: SOAP Message Security 1.1 (WS-Security 2004)", February 2006.
 - [WSS:SAMLTokenProfile1.0](#) OASIS Standard, "Web Services Security: SAML Token Profile", December 2004
 - 345 • [WSS:SAMLTokenProfile1.1](#) OASIS Standard, "Web Services Security: SAML Token Profile 1.1", February 2006
 - [XSPA-SAMLv1.0](#) OASIS Standard, "**Cross-Enterprise Security and Privacy Authorization (XSPA) Profile of the Security Assertion Markup Language (SAML) for Healthcare v1.0**", November 2009

350

3.40.3.2 Informative -- assist with understanding or implementing this profile

- [IHE](#) Profiles
 - [Personnel White Pages](#) Profile
 - [Enterprise User Authentication](#) Profile
 - 355 ○ [Basic Patient Privacy Consents](#) Profile
- [OASIS-OPEN](#)
 - SAML V2.0 Standards <http://www.oasis-open.org/committees/security/>.
 - SAML V2.0 Technical Overview
 - SAML Executive Overview
 - 360 ○ SAML Tutorial presentation by Eve Maler of Sun Microsystems

- SAML Specifications
 - WS-Trust - OASIS Web Services Secure Exchange (WS-SX) TC
 - [XSPA-XACMLv1.0 OASIS Standard, “Cross-Enterprise Security and Privacy Authorization \(XSPA\) Profile of XACML v2.0 for Healthcare v1.0” , November 2009](#)
- 365
- ISO
 - ISO/TS 21298 Health informatics — Functional and structural roles
 - ISO 14265 - Error! Reference source not found.
 - ASTM

370
 - ASTM E1986 - Information Access Privileges to Health Information
 - SNOMED-CT

Edit the following text in section 3.40.4.1.2

- 375
- The Assertion shall contain an AuthnStatement specify the AuthnContextClassRef or AuthnContextDeclRef
 - The Assertion may contain other statements (e.g. Attributes) The <AttributeStatement> element describes a statement by the SAML authority asserting that the requesting user is associated with the specified attributes. When Local Policy requires that the following attributes are carried in the SAML assertion then they should be encoded as follows:
- 380
- Subject ID : The value on the Subject ID attribute shall be a plain text description of the user's name (not user ID).
 - This <Attribute> element shall have the Name attribute set to “urn:oasis:names:tc:xspa:1.0:subject:subject-id”. The name of the user shall be placed in the value of the <AttributeValue> element. (Keep in mind that the term “subject” in SAML and XACML refers to the individual making the request; in this specification, the term “User” is generally used with the same meaning, but when referring to attributes defined in SAML or XACML, the naming convention of the standard is retained.)
- 385
- 390

```
<saml:Attribute Name="urn:oasis:names:tc:xspa:1.0:subject:subject-id">
  <saml:AttributeValue>Walter H.Brattain IV</saml:AttributeValue>
```

```
</saml:Attribute>
```

- 395
- **Subject Organization** : The value on Subject Organization attribute shall be a plain text description of the organization.

- 400
- **This <Attribute> element shall have the Name attribute set to “urn:oasis:names:tc:xspa:1.0:subject:organization”. In plain text, the organization that the user belongs to shall be placed in the value of the <AttributeValue> element.**

```
<saml:Attribute Name="urn:oasis:names:tc:xspa:1.0:subject:organization">  
  <saml:AttributeValue>Family Medical Clinic</saml:AttributeValue>  
</saml:Attribute>
```

- 405
- **Subject Organization ID Attribute**

- 410
- **This <Attribute> element shall have the Name attribute set to “urn:oasis:names:tc:xspa:1.0:subject:organization-id” A unique identifier for the organization that the user is representing in performing this transaction shall be placed in the value of the <AttributeValue> element. This organization ID shall be consistent with the plain-text name of the organization provided in the User Organization Attribute. The organization ID may be an Object Identifier (OID), using the urn format (that is, “urn:oid:” appended with the OID); or it may be a URL assigned to that organization.**

415

```
<saml:Attribute Name="urn:oasis:names:tc:xspa:1.0:subject:organization-id">  
  <saml:AttributeValue>http://familymedicalclinic.org</saml:AttributeValue>  
</saml:Attribute>
```

- **Home Community ID Attribute**

- 420
- **This <Attribute> element shall have the Name attribute set to “urn:ihe:iti:xca:2010:homeCommunityId”. The value shall be the Home Community ID (an Object Identifier) assigned to the Community that is initiating the request, using the urn format (that is, “urn:oid:” appended with the OID).**

```
<saml:Attribute Name="urn:ihe:iti:xca:2010:homeCommunityId">  
  <saml:AttributeValue>urn:oid:2.16.840.1.113883.3.190</saml:AttributeValue>  
</saml:Attribute>
```

- 425
- **National Provider Identifier (NPI) Attribute**

- 430
- **A National Provider Identifier (NPI) is a unique identifier issued to health care providers by their national authority. (e.g. in the United States this is a 10-digit number assigned by the Centers for Medicare and Medicaid Services (CMS)). This attribute provides the ability to specify an NPI value as part of the SAML assertion that accompanies a message. When a simple string is used there needs to be a mutually agreed upon assigning authority. The HL7 CE type can be used to explicitly show the assigning authority (See use in the Subject-Role Option).**

- **This <Attribute> element SHALL have the Name attribute set to “urn:oasis:names:tc:xspa:2.0:subject:npi”. An example of the syntax of this element follows:**

```
<saml:Attribute Name="urn:oasis:names:tc:xspa:2.0:subject:npi">  
  <saml:AttributeValue>1234567890</saml:AttributeValue>  
</saml:Attribute>
```

- The Assertion shall be signed by the X-Assertion Provider as defined in SAML Core.

Editor please add the following URN to the IHE ITI Wiki “urn:ihe:iti:xca:2010:homeCommunityId”

Add the following text to section 3.40.4.1.2 Message Semantics

3.40.4.1.2.1 Subject-Role Option

When the Subject-Role Option is used the X-Service User shall encode the relevant user subject roles from a locally defined Code-Set into a subject role <Attribute> element(s). The Subject-Role values communicated are assertions from the X-Service User perspective.

The subject role <Attribute> element shall have the Name attribute set to “urn:oasis:names:tc:xacml:1.0:subject:role”. The value of the <AttributeValue> element is a child element, “Role”, in the namespace “urn:hl7-org:v3”, whose content is defined by the “CE” (coded element) data type from the HL7 version 3 specification. The codeSystem shall identify the Value-Set. The codeSystemName shall identify the name of the Value-Set. The Code Element shall contain the role value from the identified Value-Set that represents the role that the XUA user is playing when making the request. No other parts of the CE data type shall be used. The following is an example of the syntax of this element:

```
<saml:Attribute Name="urn:oasis:names:tc:xacml:2.0:subject:role">  
  <saml:AttributeValue>  
    <Role xmlns="urn:hl7-org:v3" xsi:type="CE" code="46255001"  
      codeSystem="2.16.840.1.113883.6.96" codeSystemName="SNOMED_CT"  
      displayName="Pharmacist"/>  
  </saml:AttributeValue>  
</saml:Attribute>
```

3.40.4.1.2.2 Authz-Consent Option

When the Authz-Consent Option is used the X-Service User shall encode the Authz-Consent in the Authorization Decision Statement section of the SAML Assertion in an <Action> element as follows:

- 470 1. The Action shall be specified using a Namespace of 'urn:oasis:names:tc:SAML:1.0:action:rwdc' and a value of Execute.
2. The Decision attribute of the Authorization Decision Statement shall be "Permit".
3. The Resource attribute of the Authorization Decision Statement shall be the URI of the endpoint to which the request is addressed or an empty URI reference ("").
- 475 4. The Authorization Decision Statement shall contain an <Evidence> element, containing a single <Assertion> child element.
5. This <Assertion> element shall contain an ID attribute, an IssueInstant attribute, a Version attribute, an Issuer element, and an Attribute Statement element.
6. There shall be at least one of the following Attributes in the Attribute Statement.
 - 480 a. An <Attribute> element with the name "AccessConsentPolicy" and NameFormat "urn:ihe:iti:xua:acp". The value(s) for this attribute will be the OIDs of the access policies that the asserting entity has previously agreed to with other entities. The OIDs MUST be expressed using the xs:anyURI format of type URN:OID (e.g., - urn:oid:1.2.3.4). This OID may be a BPPC "Patient Privacy Policy Identifier", or may
 - 485 b. An <Attribute> element with the name "InstanceAccessConsentPolicy" and NameFormat "urn:ihe:iti:bppc:2007". The value(s) of this attribute will be the OIDs of the patient specific access policy instances. The OIDs MUST be expressed using the xs:anyURI format of type URN:OID (e.g., - urn:oid:1.2.3.4.123456789). This
 - 490 referenced OID is the unique ID of a BPPC "Patient Privacy Policy Acknowledgement Document". Access to the content would be through local means or with a common XDS/XCA/XDR/XDM mechanism. The following is anAuthz-Consent Decision Statement example.

Figure 3.40-1 Authz-Consent Decision Statement Example

```
495 <saml2:AuthzDecisionStatement xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion"  
Decision="Permit"  
Resource="">  
  <saml2:Action  
    Namespace="urn:oasis:names:tc:SAML:1.0:action:rwdc">Execute</saml2:Action>  
500 <saml2:Evidence>  
  <saml2:Assertion ID="da20c267-0f95-4cf4-8bc1-6daa5d84201e"  
    IssueInstant="2008-10-20T19:59:10.843Z" Version="2.0">  
    <saml2:Issuer Format="urn:oasis:names:tc:SAML:1.1:nameid-format:X509SubjectName"
```

505

```
>CN=SAML User,OU=SU,O=SAML User,L=Los Angeles,ST=CA,C=US</saml2:Issuer>
<saml2:Conditions NotBefore="2008-10-20T19:59:10.843Z
    NotOnOrAfter="2008-12-25T00:00:00.000Z"/>
<saml2:AttributeStatement>
  <saml2:Attribute Name="AccessConsentPolicy"
    NameFormat="urn:ihe:iti:xua:acp">
    <saml2:AttributeValue>urn:oid:1.2.3.4</saml2:AttributeValue>
  </saml2:Attribute>
  <saml2:Attribute Name="InstanceAccessConsentPolicy"
    NameFormat="urn:ihe:iti:bppc:2007">
    <saml2:AttributeValue>urn:oid:1.2.3.4.123456789
  </saml2:AttributeValue>
  </saml2:Attribute>
</saml2:AttributeStatement>
</saml2:Assertion>
</saml2:Evidence>
</saml2:AuthzDecisionStatement>
```

510

515

520

3.40.4.1.2.2.1 Patient Identifier Attribute

This attribute is *optional*, as it may not be needed for cases in which the data being exchanged does not pertain to a specific patient (e.g., population health data). The value of the Patient Identifier attribute is recommended when the InstanceAccessConsentPolicy attribute is specified in an Authorization Decision Statement.

525

This <Attribute> element shall have the Name attribute set to:

“urn:oasis:names:tc:xacml:2.0:resource:resource-id”.

530

The patient identifier of the requesting organization shall be placed in the value of the <AttributeValue> element. The patient identifier shall consist of two parts; the OID for the assigning authority and the identifier of the patient within that assigning authority. The value shall be formatted using the CX syntax. As an example, a patient identifier of 543797436 for an assigning authority with an OID of 1.2.840.113619.6.197, has been encoded into the follow SAML assertion snippet. Please note that the '&' character has been properly encoded in the XML content in the following example.

535

```
<saml:Attribute Name="urn:oasis:names:tc:xacml:2.0:resource:resource-id">
  <saml:AttributeValue>543797436^^^&amp;1.2.840.113619.6.197&amp;ISO</saml:AttributeValue>
</saml:Attribute>
```

540

3.40.4.1.2.3 PurposeOfUse Option

The PurposeOfUse <Attribute> element shall have the Name attribute set to “urn:oasis:names:tc:xspa:1.0:subject:purposeofuse”. The value of the <AttributeValue> element is a child element, “PurposeOfUse”, in the namespace “urn:hl7-org:v3”, whose content is defined by the “CE” (coded element) data type from the HL7 version 3 specification.

The PurposeOfUse element shall contain the coded representation of the Purpose for Use that is in effect for the request.

An example of the syntax of this element is as follows:

```
<saml:Attribute Name="urn:oasis:names:tc:xspa:1.0:subject:purposeofuse">
  <saml:AttributeValue>
    <PurposeOfUse xmlns="urn:hl7-org:v3" xsi:type="CE" code="12"
      codeSystem="1.0.14265.1"
      codeSystemName="ISO 14265 Classification of Purposes for processing personal health
information"
      displayName="Law Enforcement"/>
  </saml:AttributeValue>
</saml:Attribute>
```

Codes are assigned by the local Security Domain and a Code-Set needs to be managed. A good source Vocabulary for PurposeOfUse is ISO 14265 – Health Informatics – Classification of purposes for processing personal health information. The Value-Set used may include local codes or codes drawn from formal vocabulary.

The value of the Purpose of Use attribute shall be a urn:hl7-org:v3:CE element, specifying the coded value representing the user's purpose in issuing the request, choosing from the value set given by local Policy. The codeSystem attribute of this element must be present, and must specify the OID of the "Purpose of Use" code system.

3.40.4.1.2.3.1 ATNA encoding of PurposeOfUse

When the PurposeOfUse Option is used the X-Service User and X-Service Provider SHALL place the PurposeOfUse value into the ATNA Audit Message associated with the transaction according to the ATNA Audit Message Transaction ITI-20, See section ITI-TF-2a:3.20.7.3

Add the following text to section 3.40.4.1.3 Expected Actions

3.40.4.1.3.1 Subject-Role Option

When the Subject-Role Option is used, the X-Service Provider may utilize the Subject-Role values in local policy for access control decision making.

The X-Service Provider may need to bridge the Subject-Role values into local role vocabulary.

The Subject-Role may be used to populate the ATNA Audit Message.

3.40.4.1.3.2 Authz-Consent Option

580 When the Authz-Consent Option is used, the X-Service Provider may utilize the Authz-Consent values in local policy for access control decision making. The Authz-Consent values are offered by the X-Service User as an indicator of the specific consent or authorization that the X-Service User has determined authorizes the transaction. The values are informative to the X-Service Provider which may choose to ignore the values.

585 This may require the X-Service Provider to lookup the metadata by reference to the values given, and may require the X-Service Provider to retrieve the consent documents.

The Authz-Consent value may be used to populate the ATNA Audit Message.

3.40.4.1.3.3 PurposeOfUse Option

590 When the PurposeOfUse Option is used the X-Service Provider SHALL place the PurposeOfUse into the ATNA Audit Message associated with the transaction (see 3.40.4.1.2.3.1). This PurposeOfUse in the audit log can be used at the Audit Record Repository to inform reporting such as Accounting of Disclosures or Breach Notifications. The X-Service Provider MAY use the PurposeOfUse value in Access Control decisions.

Add the following section to the ATNA Audit Message transaction

595 *section 3.20.7.8 Purpose Of Use*

3.20.7.8 Audit Encoding of the Purpose of Use value

600 As explained in the [IHE Access Control White Paper](#), there are Access Control decisions that are based on the ultimate use of the data. For example a Patient may have provided a BPPC Consent/Authorization for treatment purposes, but explicitly disallowed any use for research regardless of de-identification methods used. The purpose of use is also informative to the ATNA audit log to enable specific reporting of Accounting of Disclosures and Breach Notification. To enable this type of Audit Logging and Access Control decision there is a need to include in the XUA Assertion the intended purpose for which the data will be used. One specific PurposeOfUse would be a Break-Glass / Emergency-Mode-Access.

605 The PurposeOfUse value will come from a Value-Set. This Value-Set should be derived from the codes found in ISO 14265, or XSPA. Implementations should expect that the Value-Set used may be using locally defined values. The use of the IHE Sharing of Value-Sets (SVS) Profile may assist with this.

610 When a PurposeOfUse value is available it shall be encoded in the EventIdentification section as “PurposeOfUse” element encoded as a CodedValueType.

For example, the following is how an explicit Disclosure can be recorded when an application knows that the act meets the measure of a Disclosure in the legal domain.

	Field Name	Opt	Value Constraints
Event AuditMessage/ EventIdentification	EventID	M	EV(110106, DCM, "Export")
	EventActionCode	M	"R" (Read)
	<i>EventDateTime</i>	<i>M</i>	<i>not specialized</i>
	<i>EventOutcomeIndicator</i>	<i>M</i>	<i>not specialized</i>
	<i>PurposeOfUse</i>	<i>O</i>	<i>EV(12, 1.0.14265.1, "Law Enforcement")</i>
	EventTypeCode	M	EV("IHE0006", "IHE", "Disclosure")
Source (Document Repository) (1)			
Destination (Document Consumer) (1)			
Audit Source (Document Repository) (1)			
Document (1..n)			