

ACC, HIMSS and RSNA
Integrating the Healthcare Enterprise

5

IHE IT Infrastructure Technical Framework
Supplement 2005-2006

10

Cross-Enterprise User Authentication (XUA)
Integration Profile
June 15, 2005

15

Rev 1.0

Public Comment Version
Comments due: July 15, 2005

20

Contents

	Foreword.....	2
25	Profile Abstract.....	4
	GLOSSARY.....	4
	Volume I – Integration Profiles.....	6
	2.2.13 Cross-Enterprise User Authentication (XUA).....	6
	13 Cross-Enterprise User Authentication (XUA) Integration Profile.....	7
30	13.1 Cross-Enterprise User Authentication Use Cases.....	7
	13.1.1 Overview of Use Cases.....	7
	13.1.2 Assumptions.....	7
	13.1.3 Use Cases.....	8
	0a/b User Authentication.....	9
35	1a Any HL7.....	9
	1b Any HL7.....	9
	2a Any DICOM.....	9
	2b Any DICOM.....	9
	3 XDS – Provide and Register.....	9
40	4 XDS – Register.....	10
	5 XDS – Query.....	10
	6 XDS – Retrieve (HTTP Get – Middleware).....	10
	7 RID – Display (HTTP Get – Browser).....	10
	13.2 Actors / Transactions.....	10
45	13.3 XUA Integration Profile Options.....	12
	13.4 XUA Integration Profile Process Flow.....	12
	13.4.1 Post-Generated Assertion.....	13
	13.4.2 Pre-Generated Assertion.....	14
	13.4.3 XDS Provide and Register Delegation Model.....	15
50	13.4.4 Access Controls.....	16
	Volume 2 - Transactions.....	18
	3.29 Assert X-User Identity.....	18
	3.29.1 Scope.....	18
	3.29.2 Use Case Roles.....	18
55	3.29.3 Referenced Standard.....	19
	3.29.4 Relationship of IHE Transactions to SAML Profiles.....	20
	3.29.5 Trust Relationship.....	20
	3.29.6 Assert X-User Identity.....	20
	3.29.6.1 Assertion Content.....	21
60	3.29.6.2 Enhanced Client or Proxy Profile.....	21
	3.29.6.2 Web Browser SSO Profile.....	21
	3.29.6.4 HL7 Profile.....	21
	3.29.6.5 DICOM Profile.....	22

Foreword

65 Integrating the Healthcare Enterprise (IHE) is an initiative designed to stimulate the integration
of the information systems that support modern healthcare institutions. Its fundamental objective
is to ensure that in the care of patients all required information for medical decisions is both
correct and available to healthcare professionals. The IHE initiative is both a process and a
70 forum for encouraging integration efforts. It defines a technical framework for the
implementation of established messaging standards to achieve specific clinical goals. It includes
a rigorous testing process for the implementation of this framework. And it organizes
educational sessions and exhibits at major meetings of medical professionals to demonstrate the
benefits of this framework and encourage its adoption by industry and users.

75 The approach employed in the IHE initiative is not to define new integration standards, but rather
to support the use of existing standards, HL7, DICOM, IETF, and others, as appropriate in their
respective domains in an integrated manner, defining configuration choices when necessary.
When clarifications or extensions to existing standards are necessary, IHE refers
recommendations to the relevant standards bodies.

80 This initiative has numerous sponsors and supporting organizations in different medical specialty
domains and geographical regions. In North America the primary sponsors are the American
College of Cardiology (ACC), the Healthcare Information and Management Systems Society
(HIMSS) and the Radiological Society of North America (RSNA). IHE Canada has also been
formed. IHE Europe (IHE-EUR) is supported by a large coalition of organizations including the
European Association of Radiology (EAR) and European Congress of Radiologists (ECR), the
85 Coordination Committee of the Radiological and Electromedical Industries (COCIR), Deutsche
Röntgengesellschaft (DRG), the EuroPACS Association, Groupement pour la Modernisation du
Système d'Information Hospitalier (GMSIH), Société Française de Radiologie (SFR), and
Società Italiana di Radiologia Medica (SIRM). In Japan IHE-J is sponsored by the Ministry of
Economy, Trade, and Industry (METI); the Ministry of Health, Labor, and Welfare; and MEDIS-
90 DC; cooperating organizations include the Japan Industries Association of Radiological Systems
(JIRA), the Japan Association of Healthcare Information Systems Industry (JAHIS), Japan
Radiological Society (JRS), Japan Society of Radiological Technology (JSRT), and the Japan
Association of Medical Informatics (JAMI). Other organizations representing healthcare
professionals are invited to join in the expansion of the IHE process across disciplinary and
95 geographic boundaries.

The IHE Technical Frameworks for the various domains (IT Infrastructure, Cardiology,
Laboratory, Radiology, etc.) defines specific implementations of established standards to achieve
integration goals that promote appropriate sharing of medical information to support optimal
patient care. It is expanded annually, after a period of public review, and maintained regularly
100 through the identification and correction of errata. The current version for these Technical
Frameworks may be found at www.ihe.net

The IHE Technical Framework identifies a subset of the functional components of the healthcare
enterprise, called IHE Actors, and specifies their interactions in terms of a set of coordinated,

standards-based transactions. It describes this body of transactions in progressively greater
105 depth. The volume I provides a high-level view of IHE functionality, showing the transactions
organized into functional units called Integration Profiles that highlight their capacity to address
specific clinical needs. The subsequent volumes provide detailed technical descriptions of each
IHE transaction.

**This supplement to the IHE IT Infrastructure Technical Framework is submitted for
110 Public Comment between June 15, 2005 and July 15, 2005, per the scheduled announced in
February 2005.**

Comments shall be submitted before July 15, 2005 to:

<http://forums.rsna.org> under the “IHE” forum

115 Select the “IT Infrastructure Supplements for Public Review” sub-forum.

**The IHE IT Infrastructure Technical Committee will address these comments and publish
the Trial Implementation version in August 2005.**

120 **OPEN ISSUES:**

1. We know of the following resources that would help a vendor implement this profile, and a
provider implement the infrastructure. We would like to request comment on this content
and if it should be involved beyond the “Trial Implementation” version of this profile.
 - 125 a. <http://www.oasisopen.org/committees/security/>
 - b. <http://www.sourceid.org/index.html>
2. We are not constraining the SAML Assertion content at this time. We know that ISO and
ASTM are updating relevant standards that would guide future Assertion constraints: The
following are some potential content that we could require or recommend.
 - 130 a. X.509 certificate compliant from ISO/TS 17090 – Health Informatics PKI, for identify
management
 - b. Assertion LDAP Metadata compliant from ISO/TS 21091 – Healthcare Informatics –
Directory services for security, communications, and identification of professionals and
patients (submitted for publication)
 - 135 c. Functional and Structural Roles from ISO/DTS 21298 (work item in committee)
 - d. List of Professions from ASTM E1633 – Standard Specification for Coded Values Used
in Electronic Health Record.
 - e. Information access privileges from ASTM E1986 – Standard Guide for Information
Access Privileges to Health Information
 - 140 f. Role vocabulary from ASTM – Privilege Management Infrastructure (work item
document number not assigned)

Profile Abstract

145 IHE has defined a profile for Enterprise User Authentication (EUA) and Personnel White Pages (PWP) for use within an enterprise. The IHE is now defining transactions that cross enterprise boundaries, specifically the XDS profile that creates an Affinity Domain. When transactions cross enterprise boundaries the mechanisms found in the EUA and PWP profile are insufficient and often nonfunctional. To provide accountability in these cross enterprise transactions there is a need to identify the requesting user in a way that the receiver can make access decisions and proper audit entries.

GLOSSARY

150

The following items shall be added to the Glossary

- 155 • **Assertion** -- A piece of data produced by a SAML authority regarding either an act of authentication performed on a subject, attribute information about the subject, or authorization data applying to the subject with respect to a specified resource. This Assertion is used in access control and audit trails.
- **Federated Identity** -- A user's identity is said to be federated between a set of Providers when there is an agreement between the providers on a set of identifiers and/or attributes to use to refer to the user.
- **Federation** -- This term is used in two senses in SAML:
 - 160 ○ The act of establishing a relationship between two entities.
 - An association comprising any number of service providers and identity providers.
- **Identity Provider** -- A type of service provider that creates, maintains, and manages identity information for users and provides user authentication to other service providers within a federation, such as with web browser profiles.
- 165 • **Security Assertion Markup Language(SAML)** -- The set of specifications describing security assertions that are encoded in XML, profiles for attaching the assertions to various protocols and frameworks, the request/response protocol used to obtain the assertions, and bindings of this protocol to various transfer protocols (for example, SOAP and HTTP).
- 170 • **Security Domain** -- An environment defined by a single set of security policies, including a set of people, equipment, facilities, procedures. A Security Domain may be a single enterprise or a collection of enterprises (e.g. IHE-XDS Affinity Domain).

- 175
- **User** -- A natural person who makes use of a system and its resources for any purpose. A more generalized term 'principal' is used in SAML. For the purpose of XUA the SAML use of principal should be considered equal to XUA use of user.

Volume I – Integration Profiles

Add the following bullet to the end of the bullet list in section 1.7

180 Added the **Cross-Enterprise User Authentication (XUA)** Profile, which provides user identity to cross-enterprise transactions. This mechanism is not limited to **Cross-Enterprise Document Sharing (XDS)** transactions.

Add the following section to Table 2-1 Integration Profiles Dependencies in section 2.1

Cross-Enterprise User Authentication	<i>Consistent Time</i>		Required to ensure consistent time.
--------------------------------------	------------------------	--	-------------------------------------

185 *Add the following section to section 2.2*

2.2.13 Cross-Enterprise User Authentication (XUA)

190 *Cross-Enterprise User Authentication (XUA)* provides user identity in transactions that cross enterprise boundaries, specifically the XDS profile that creates an Affinity Domain. When transactions cross enterprise boundaries the mechanisms found in the EUA and PWP profile are insufficient and often nonfunctional. Enterprises may choose to have their own user directory and their own unique method of authenticating. To provide accountability in these cross enterprise transactions there is a need to identify the requesting user in a way that the receiver can make access decisions and proper audit entries.

195

The section shall be added to Vol 1

13 Cross-Enterprise User Authentication (XUA) Integration Profile

IHE has defined a profile for Enterprise User Authentication (EUA) and Personnel White Pages (PWP) for use within an enterprise. The IHE is now defining transactions that cross enterprise boundaries, specifically the XDS profile that creates an Affinity Domain. When transactions cross enterprise boundaries the mechanisms found in the EUA and PWP profile are insufficient and often nonfunctional. To provide accountability in these cross enterprise transactions there is a need to identify the requesting user in a way that the receiver can make access decisions and proper audit entries.

13.1 Cross-Enterprise User Authentication Use Cases

13.1.1 Overview of Use Cases

All use cases are shown on Figure 13-1. These use cases are tied together into a treatment of a single patient. The use case starts with a patient getting a CT scan done at St Johns Hospital. There Bob, a radiologist, creates a report that is submitted to an XDS repository and registered with the Affinity Domain's Registry. Then back at North Clinic the patient's family doctor, Alice, queries the XDS Registry for the completed report, and once found pulls the document from the repository. Seeing the results the family doctor pulls the latest results using the Retrieve Information for Display from a lab system at St Johns Hospital. All of these transactions exist today (shown with dashed lines) and today are covered through Audit Trail and Node Authentication Profile (ATNA) Secure Node grouping.

The XUA profile when grouped with these actors will provide the user identity across these enterprise boundaries (shown with the solid lines). In order to provide this functionality the user will need to authenticate (0a & 0b) to an enterprise class user authentication (e.g. EUA) system that is grouped with a cross-enterprise identity provider. The user authentication transaction is not specified in the XUA profile but IHE recommends that it be satisfied through EUA.

13.1.2 Assumptions

- A. The users (Alice and Bob) are authenticated by some authentication authority that is related to an XUA Identity Provider.
- B. The authentication authority may be implemented with one set for a whole Affinity Domain or with enterprise specific sets. The solution must support both types of configurations.
- C. Automated processes need not authenticate them-selves any further than is provided by ATNA. An automated process is sufficiently authenticated through the certificate used in the communications channel (e.g. TLS mutual-authentication, S/MIME).

- 230 D. Export of data is a source sensitive process that requires a specific permission decision to export, the receiving actor of an Export event need not further verify the rights that the user has to export. Thus the transactions on the left side of Figure 13-1 do not require grouping with XUA.
- 235 E. Query of Exported Data and Import of data is sensitive to who is asking and thus requires the identity of the individual asking for the data.
- 240 F. All products implementing XUA, such as XUA Identity Provider Actors, Service Provider Actors, and Service User Actors, must have a trusted method of learning about and verifying the characteristics of any other such entity in accordance with their level of participation in the XUA security context and the transactions at hand.

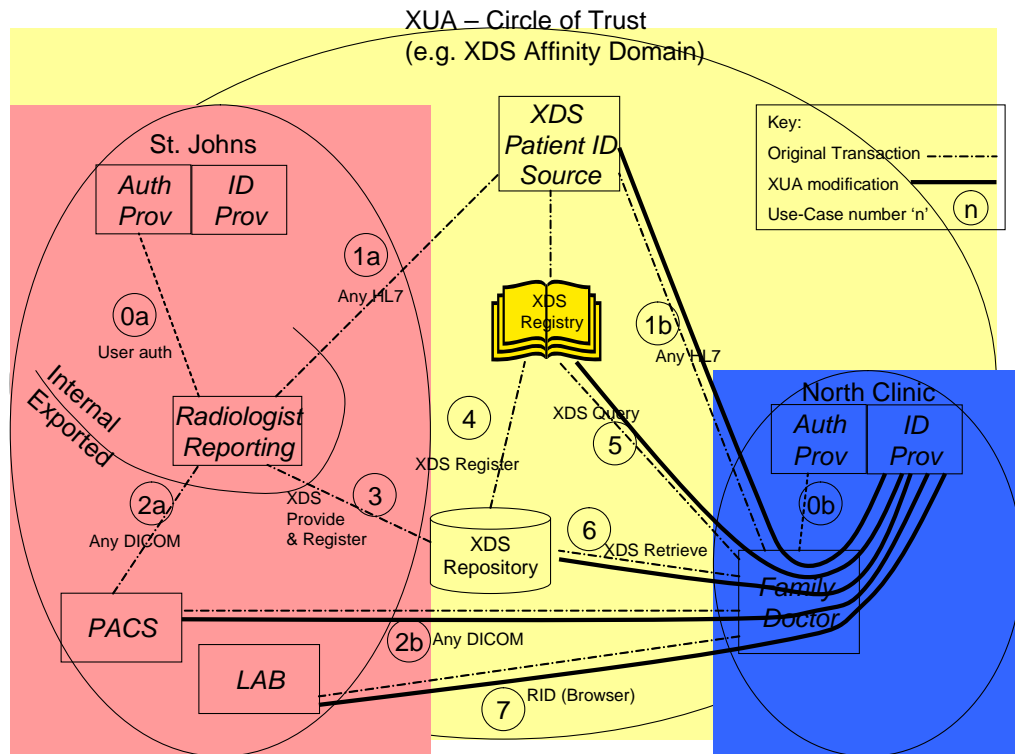


Figure 13-1 – XUA High level use cases

13.1.3 Use Cases

245 The use cases are discussed in further detail below. The number in Figure 13-1 corresponds to the sub-section number listed below. All of the use cases are based on the Assumptions listed in 13.1.2. The user has been authenticated to his/her local authentication provider.

0a/b User Authentication

250 The zero transaction is not part of this profile but is essential to XUA. This transaction is the authentication of the user using some means (e.g. IHE-ITI EUA Profile). This transaction is done with some Authentication Provider that is in a relationship with the Identity Provider. This relationship is also not a part of this profile.

1a Any HL7

255 The Radiologist Reporting system uses HL7 transactions to update information maintained in the Affinity Domain. This transaction is doing an export of data and thus does need to be closely controlled prior to the act. This would include an authentication of the user, access control decisions to determine if the user has permissions and an audit trail of the export event. Because this is an Export event there is little advantage to applying XUA user identity to the transaction that is already protected by ATNA. Using ATNA the “XDS Patient ID Source” Actor can determine that the transaction is coming from a node that should be allowed to update the Patient ID.

1b Any HL7

265 The Family Doctor (Alice) will query the Patient Identity Source for the XDS Affinity specific identifier for a patient domain (See XDS Profile for details). When grouped with XUA this transaction will carry an assertion about Alice embedded in the HL7 stream. This user assertion comes from the XUA Identity Provider that is grouped with the authentication provider used to authenticate the user.

2a Any DICOM

270 The Radiologist Reporting station is used by Radiologist (Bob) to create a DICOM Structured Report that is put on the PACS. This is an export request because it is known that the PACS is available to certain workstations outside the enterprise. It is very important that the Radiologist Reporting station ensures that the user is authenticated, authorized to export and that an appropriate audit log is made. No grouping with XUA is required.

2b Any DICOM

275 The Family Doctor (Alice) will query the PACS for the DICOM Structured Report using common DICOM transactions as defined by IHE Radiology and Cardiology. When grouped with XUA this transaction will carry an assertion about Alice embedded in the DICOM communication channel.

3 XDS – Provide and Register

280 The Radiologist Reporting station will then create a report that is submitted using XDS Provide & Register transaction to a Repository. This Repository may be within the St.

Johns enterprise or it may be outside the enterprise. Either way the document is registered and thus exported. No grouping with XUA is required.

4 XDS – Register

285 The Repository will forward the registration request on to the Affinity Domain’s Registry. This is registration of an export event. No grouping with XUA is required.

5 XDS – Query

290 The family doctor, Alice, at North Clinic will query the Affinity Domain’s Registry to find the new report. When grouped with XUA this transaction will carry an assertion about Alice embedded in the transaction.

6 XDS – Retrieve (HTTP Get – Middleware)

295 Once Alice has found the report, she will retrieve it from the repository. When grouped with XUA this transaction will carry an assertion about Alice embedded in the HTTP GET transaction. This transaction is carried out by an intelligent application that has authenticated the user, knows the user’s identity provider, and is willing to be an active member in the XUA transaction.

7 RID – Display (HTTP Get – Browser)

300 Alice will then use her browser to pull the latest lab results from a laboratory server at St Johns (See RID Profile for details). When grouped with XUA this transaction will carry an assertion about Alice embedded in the HTTP GET transaction. This use case is different than use case 6 in that the application that Alice is using is a simple browser that is unaware of the XUA profile. Note that there are very few SAML requirements on the browser and existing browsers support these requirements.

13.2 Actors / Transactions

305 The XUA Profile is a higher level profile than the SAML v2.0 Profiles it leverages. An understanding of SAML v2.0 is essential to understand the XUA Profile (See [SAMLTechOvw]). The XUA profile has three actors participating in one transaction. This transaction looks very different at the detail level depending on the specific use case. Figure 13.2-1 shows the actors directly involved in the XUA Profile and the single transaction between them. Other actors and transactions that may be indirectly involved due to their participation in other grouped profiles are shown in italics. The “*Authenticate User*” transaction is outside the scope of this profile and may be filled through the use of EUA or some other enterprise class authentication. The “*Request any service*” transaction is outside the scope of this profile and represents an existing transaction that is not passing an XUA assertion.

315

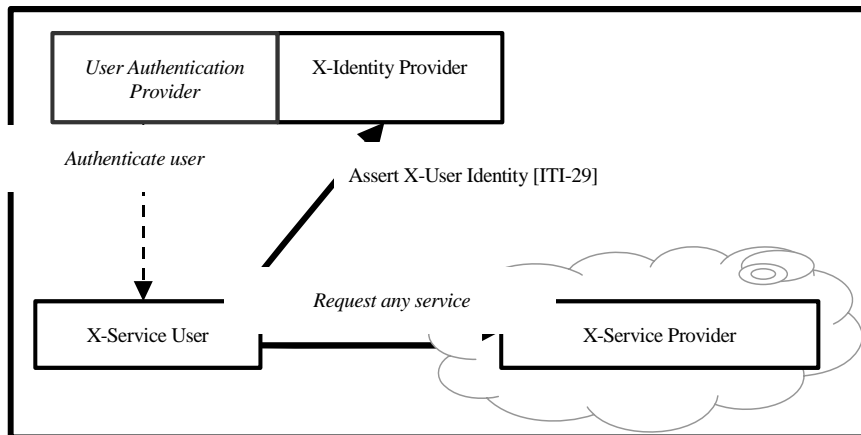


Figure 13.2-1: XUA Profile Actor Diagram

320 Table 13.2-1 lists the transaction for each actor directly involved in the XUA Profile. In order to claim support of this Integration Profile, an implementation must perform the required transactions (labeled “R”). Transactions labeled “O” are optional. A complete list of options defined by this Integration Profile and that implementations may choose to support is listed in Section 13.3.

Table 13.2-1: XUA Integration Profile - Actors and Transactions

Actors	Transactions	Optionality	Section in Vol. 2
X-Identity Provider	Assert X-User Identity	R	ITI TF-2: 3.29
X-Service Provider	Assert X-User Identity	R	ITI TF-2: 3.29
X-Service User	Assert X-User Identity	R	ITI TF-2: 3.29

325 The X-Identity Provider must be related to the user authentication provider. For example an EMR application that does user authentication within the application would group the X-Service User and X-Identity Provider effectively producing self Assertions. The EMR still must meet all external requirements of the combined X-Identity Provider and X-Service Provider. The EMR must also be trusted as an X-Identity Provider by the X-Service Providers. Figure 13.2.2 shows this example EMR application acting as the user authentication provider, X-Identity Provider,
 330 and X-Service User.

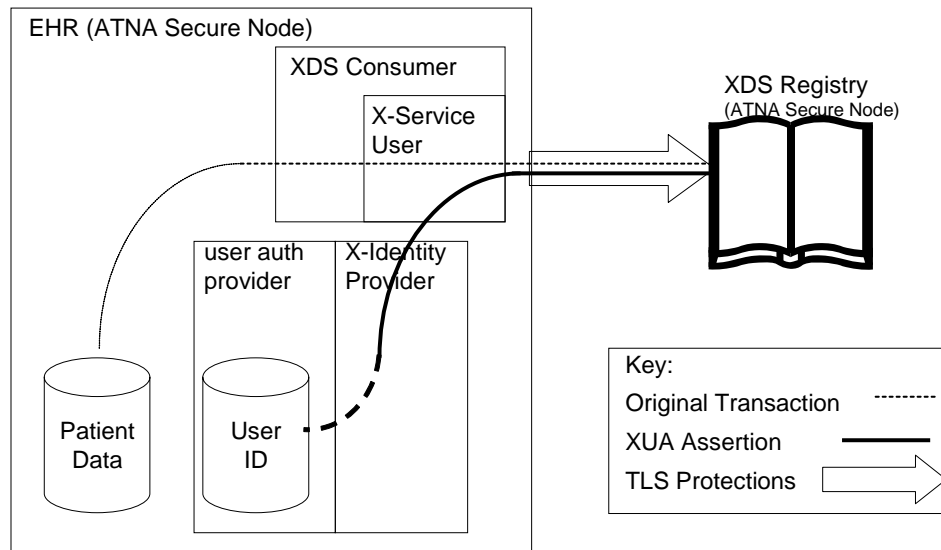


Figure 13.2-2: XUA Profile Actor Diagram

335 The XUA profile encourages the use of a scalable enterprise class user authentication such as
 EUA – Kerberos Authentication Server. This X-Identity Provider relationship to the
 authentication provider is not profiled by IHE or SAML.

13.3 XUA Integration Profile Options

Options that may be selected for this Integration Profile are listed in the table 13.3-1 along with
 the Actors to which they apply. Dependencies between options when applicable are specified in
 notes.

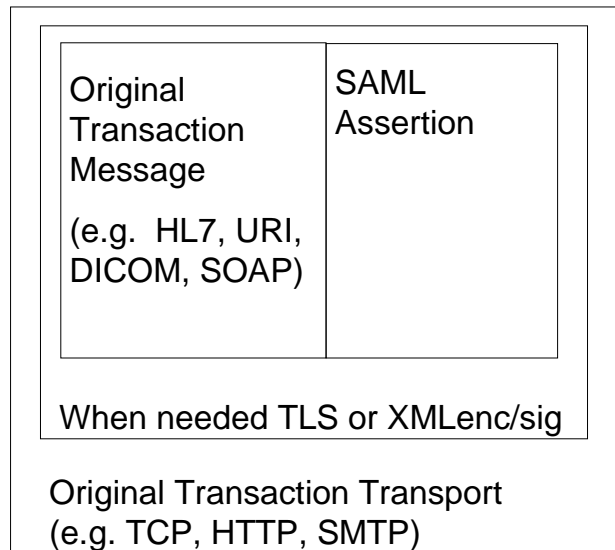
340

Table 13.3-1 XUA Integration Profile - Actors and Options

Actor	Options	Vol & Section
X-Identity Provider	<i>no options</i>	
X-Service Provider	<i>no option</i>	
X-Service User	<i>no option</i>	

13.4 XUA Integration Profile Process Flow

The Cross-Enterprise User Authentication (XUA) Profile addresses the use cases given above
 through two major configurations described below. In all cases there is a pre-existing transaction
 that is modified through proper grouping with XDS actors.



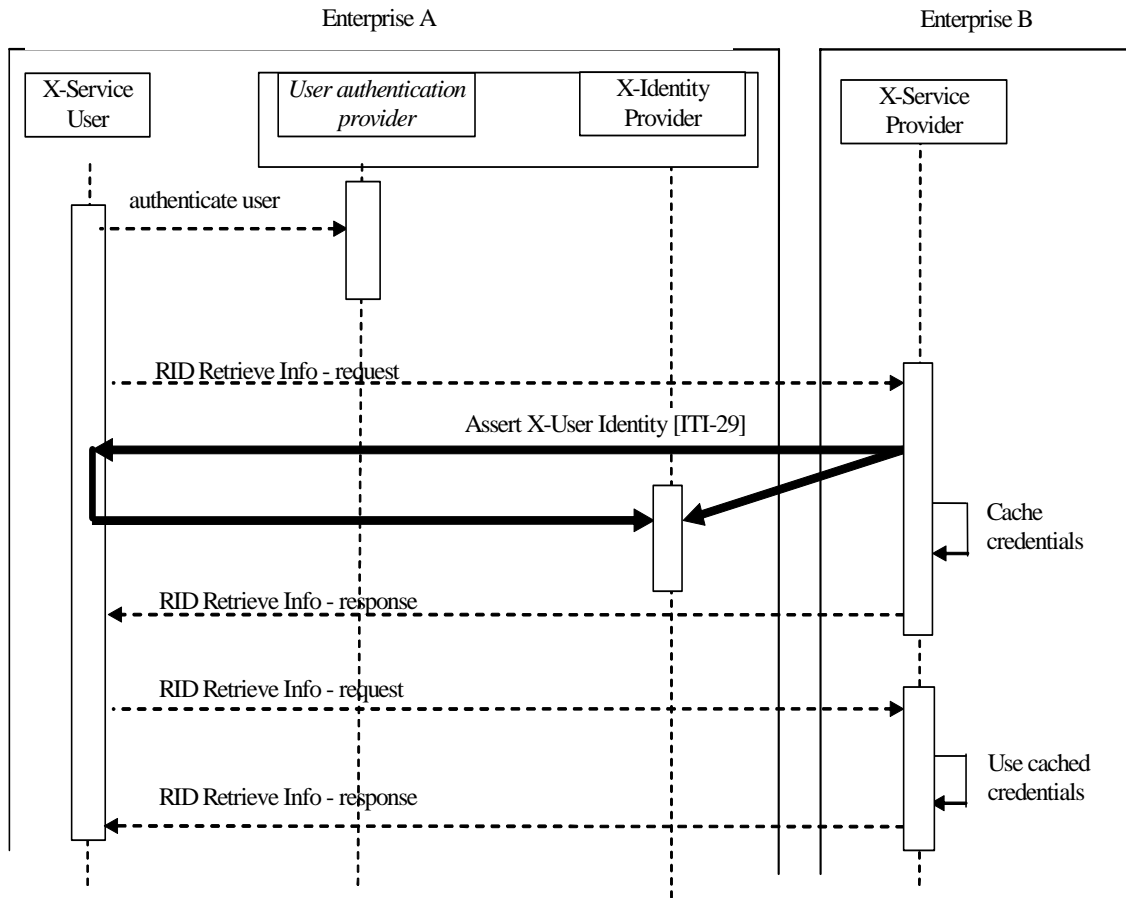
345

Figure 13.4-1 General adaptation of Original Message / Transport

13.4.1 Post-Generated Assertion

350 The first configuration is represented here by an IHE Retrieve Information for Display (RID) transaction. There are other cases where this configuration is used. A healthcare provider, Alice, is seeing a patient and wants to examine the patient's medical history. The patient's clinical data has been made available in accordance with the IHE RID profile. The healthcare provider, Alice, has authenticated to her enterprise authentication system (e.g. EUA). Alice uses her browser to retrieve displayable summaries of lab results. The healthcare provider must supply an assured identity for herself to the RID Information Source Actor. The RID Information Source Actor may use this identity to determine the user's permissions to access the data, and to record the retrieve (export) event. See Figure 13.4-2 for the transaction details. This configuration leverages the SAML v2.0 [SAMLprof] Browser and Enhanced Client/Proxy Profiles.

355



360 **Figure 13.4-2: Post-Generated Assertion Profile Process Flow in XUA Profile**

13.4.2 Pre-Generated Assertion

The second case is represented here by a XDS PIX/PDQ Query that is using HL7. This second case is one where the X-Service User Actor knows that it must provide an Assertion in the transaction.

365 The General Practitioner, Charley, is using an HL7 Query to find the Affinity Domain Patient Identity (See XDS for details on this transaction). Charley has authenticated to his enterprise authentication system (e.g. EUA). Charley is using an intelligent Actor that can generate the user assertion and embed it into the transaction. The XDS Patient Identity Source Actor may use this identity to determine the user's permissions to access the data, and to record the retrieve (export)

370 event. See Figure 13.4-3 for the transaction details. This configuration leverages the SAML v2.0 [SAMLprof] Assertion Query/Request Profile.

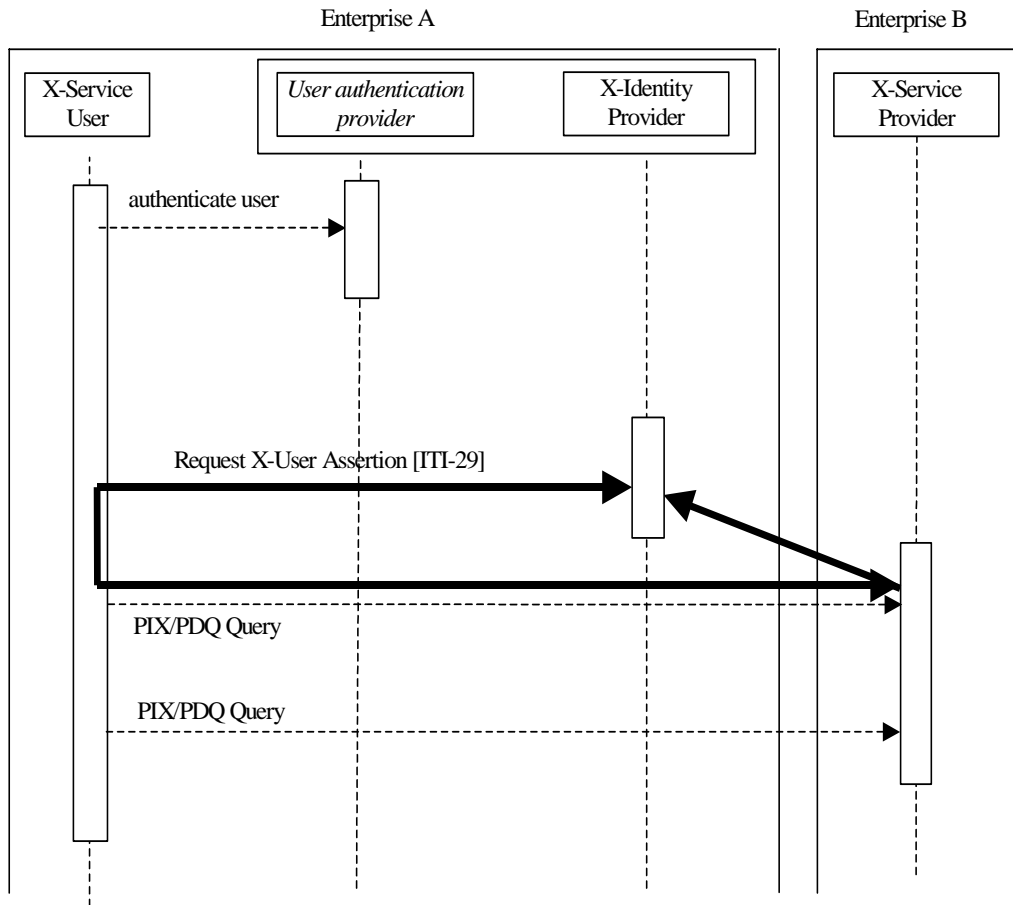


Figure 13.4-3: Pre-Generated Assertion Profile Process Flow in XUA Profile

375 **13.4.3 XDS Provide and Register Delegation Model**

When XUA is grouped with transactions that carry a document author's identity there may be a conflict between the XUA identity and the document author identity. This should not necessarily be considered an error as the author may have delegated the role. For example the XDS Provide and Register transaction contains XDS meta-data that identifies the author of the document being submitted. Yet the task of submitting the documents to the Affinity Domain may fall to a clerk, or records management staff member. Audit Trail analysis is used to determine if proper delegation was authorized. It is possible in the future that we may have strong enough access control policies to support delegation.

380

The XDS query/retrieve side does not have conflicting information, thus access control is clearer and simpler.

385

13.4.4 Access Controls

XDS relies on an Affinity Domain defining access controls at the policy and procedural level. The grouping with XUA does not change this fact.

390 XUA provides the user identity to the service provider; it does not in any way indicate how any access control decisions will be made. These access control decisions should be made in what ever means appropriate to the service provider implementation. In some cases the service request will be allowed simply because the user is authentic within the Circle of Trust. Other cases will require local access control rules to be provisioned.

395 Audit trails should continue to use the ATNA audit mechanism as defined in the XDS profile. There are no specific audit events that XUA adds.

Add the following Actor Summary Definitions in Appendix A

X-Service User: This actor has a use for some Cross-Enterprise service.

X-Service Provider: This actor has a service that it offers using Cross-Enterprise methods.

400 **X-Identity Provider:** This actor has authoritative identity information on the human user that is
operating the X-Service User actor.

Add the following to the Transaction Summary Definitions in Appendix B

405 **Assert X-User Identity:** This transaction will generate a Cross-Enterprise Authentication
Assertion and pass it to a relying service.

Volume 2 - Transactions

Add sections 3.29

410 3.29 Assert X-User Identity

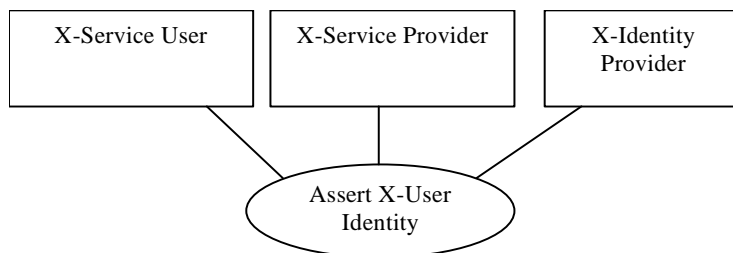
This section corresponds to Transaction ITI-29 of the IHE Technical Framework. Transaction ITI-29 is used by the X-Service Provider, X-Service User, and X-Identity Provider.

415 Assert X-User Identity is a high level transaction that does not always represent the actual transactions between the specified actors. This IHE transaction is defined to convey the concept that is very well worked out within the standards used. In some cases the underlying transactions look very much like the Assert X-User Identity transaction, and other times the actual transactions are only representative in spirit.

3.29.1 Scope

420 This Transaction is used to convey a user authentication assertion for use in a Cross-Enterprise transaction.

3.29.2 Use Case Roles



Actor: X-Service User

425 **Role:** Has authenticated the user with an enterprise authentication system and is now requesting a Cross-Enterprise service.

Actor: X-Service Provider

Role: Providing a Cross-Enterprise service that requires a User Assertion.

Actor: X-Identity Provider

430 **Role:** Provides the User Assertion associated with an X-Service User requesting a Cross-Enterprise service from an X-Service Provider.

Not shown: enterprise user authentication system that is grouped with the X-Identity Provider.

3.29.3 Referenced Standard

- 435 **[ASTM-E1985]** E1985-98 -- Standard guide for user authentication and authorization
http://www.astm.org/cgi-bin/SoftCart.exe/DATABASE.CART/REDLINE_PAGES/E1985.htm?E+mystore
- [ASTM-E1986-98]** E1986-98 -- Standard guide for information access privileges to health information
http://www.astm.org/cgi-bin/SoftCart.exe/DATABASE.CART/REDLINE_PAGES/E1986.htm?E+mystore
- [ASTM-E1987-98]** E1987-98 -- Standard guide for individual rights regarding health information
http://www.astm.org/cgi-bin/SoftCart.exe/DATABASE.CART/REDLINE_PAGES/E1987.htm?E+mystore
- 440 **[DICOM-ENUI]** DICOM Supplement 99: Extended Negotiation of User Identity
ftp://medical.nema.org/medical/dicom/final/sup99_ft.pdf
- [HL7-2.5]** HL7 V2.5 <http://www.hl7.org/library/standards.cfm>
- [HL7-2.6]** HL7 V2.6 <http://www.hl7.org/library/standards.cfm>
- [ISO17090]** ISO/TS 17090 – Health Informatics Digital Signatures for Healthcare
<http://www.iso.org/iso/en/CatalogueDetailPage.CatalogueDetail?CSNUMBER=35489&ICS1=35&ICS2=240&ICS3=80>
- 445 **[XMLDSIG]** XML-Signature Syntax and Processing <http://www.w3.org/TR/2001/PR-xmlsig-core-20010820/>
- [WSI-BSP]** WS-I: Basic Security Profile 1.0 <http://www.ws-i.org/Profiles/BasicSecurityProfile-1.0-2004-05-12.html> Note: when this document is finalized, this URL will be updated.
- 450 **[WSS-SMS]** Web Services Security: SOAP Message Security 1.0 <http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-messagesecurity-1.0.pdf>
- [WSS-SWA]** Web Services Security: SOAP Message with Attachments (SwA) Profile 1.0
<http://www.oasis-open.org/apps/org/workgroup/wss/download.php/10902/wssswa-profile-1.0-cd-01.pdf>
Note: when this document is finalized, this URL will be updated.
- 455 **[SAMLAuthnCxt]** J. Kemp et al. *Authentication Context for the OASIS Security Assertion Markup Language (SAML) V2.0*. OASIS SSTC, March 2005. Document ID saml-authncontext-2.0-os. See <http://www.oasis-open.org/committees/security/>.
- [SAMLBind]** S. Cantor et al. *Bindings for the OASIS Security Assertion Markup Language (SAML) V2.0*. OASIS SSTC, March 2005. Document ID saml-bindings-2.0-os. See <http://www.oasis-open.org/committees/security/>.
- 460 **[SAMLConform]** P. Mishra et al. *Conformance Requirements for the OASIS Security Assertion Markup Language (SAML) V2.0*. OASIS SSTC, March 2005. Document ID samlconformance-2.0-os. <http://www.oasis-open.org/committees/security/>.
- [SAMLGloss]** J. Hodges et al. *Glossary for the OASIS Security Assertion Markup Language (SAML) V2.0*. OASIS SSTC, March 2005. Document ID saml-glossary-2.0-os. See <http://www.oasis-open.org/committees/security/>.
- 465 **[SAMLMeta]** S. Cantor et al. *Metadata for the OASIS Security Assertion Markup Language (SAML) V2.0*. OASIS SSTC, March 2005. Document ID saml-metadata-2.0-os. See <http://www.oasis-open.org/committees/security/>.
- 470 **[SAMPLP-XSD]** S. Cantor et al. SAML protocols schema. OASIS SSTC, March 2005. Document ID saml-schema-protocol-2.0. See <http://www.oasisopen.org/committees/security/>.
- [SAMLProf]** S. Cantor et al. *Profiles for the OASIS Security Assertion Markup Language (SAML) V2.0*. OASIS SSTC, March 2005. Document ID saml-profiles-2.0-os. See <http://www.oasis-open.org/committees/security/>.
- 475 **[SAMLSecure]** F. Hirsch et al. *Security and Privacy Considerations for the OASIS Security Assertion Markup Language (SAML) V2.0*. OASIS SSTC, March 2005. Document ID saml-sec-consider-2.0-os. See <http://www.oasisopen.org/committees/security/>.
- [SAMLTechOvw]** J. Hughes et al. SAML Technical Overview. OASIS, February 2005. Document ID sstc-saml-tech-overview-2.0-draft-03. See <http://www.oasisopen.org/committees/security/>.
- 480 **[SAML-XSD]** S. Cantor et al., SAML assertions schema. OASIS SSTC, March 2005. Document ID saml-schema-assertion-2.0. See <http://www.oasisopen.org/committees/security/>.

3.29.4 Relationship of IHE Transactions to SAML Profiles

The IHE transactions are based on a variety of standards. Depending on the standard they may be protected by one or more of the SAML profiles. The following table shows this relationship.

485

SAML Profile \ Transaction	Web Browser SSO	Enhanced Client/Proxy	Assertion Query/Request
Any HL7 (1b)	N/A	N/A	MUST
Any DICOM (2b)	N/A	N/A	MUST
RID (7)	MUST	MUST	OPTIONAL
XDS Query (5)	MUST	MUST	OPTIONAL
XDS Retrieve (6)	MUST	MUST	OPTIONAL

The table indicates if the SAML Profile is required to be supported by the IHE Transaction when grouped with XUA. Further details found below. The relationship between the IHE Actors for the above IHE Transactions and the SAML Service User and Service Provider is found in the Security Considerations section of the corresponding IHE Profile (e.g. XDS-Registry is a SAML Service Provider, XDS-Consumer is a SAML Service User).

490

3.29.5 Trust Relationship

The XUA X-Service Providers shall be configured to trust the federated X-Identity Providers using the [SAMLMeta] method. The SAMLMeta defines an XML schema for communicating the identity and other characteristics about Service Providers and Identity Providers. This may be done by manual configuration of service and identity provider description tables.

495

3.29.6 Assert X-User Identity

The Assert X-User Identity transaction can be used with many different Cross-Enterprise transactions.

At this time we cannot profile all of uses of the Assert X-User Identity. Future profiling is expected based on the availability of standards (e.g. DICOM) and the maturity of the SAML V2.0 support for other transactions. The IHE will follow the lead of OASIS Security Committees.

500

Note: The user authentication method used between the X-Service User and the authentication provider is not specified and may be done through various methods. The system used must be selected carefully to ensure proper user authentications.

505

The XUA requires ATNA to ensure a secure node: node-to-node authentication, user authentication (to the authentication provider), and proper security audit trails. The XUA requires the TLS encryption Option from ATNA.

3.29.6.1 Assertion Content

510 The Assertion content is the same for all of the IHE use cases. The resulting SAML Assertion should include, when available, the following healthcare information about the user. This information shall be encoded in the SAML Assertion using the SAML v2.0 [SAMLprof] Attribute Profile. This information may be restricted by the X-Identity Provider.

515 The X-Service Provider may use the Assertion content in access control and audit control (user provisioning, credentialing, role assignment, permissions, identity, etc). Access control and audit control are not described in this profile.

SAML Assertions may contain multiple tokens that describe the user. The receiver of a SAML Assertion shall be prepared to support any token type (e.g. Simple, Kerberos, X.509) supported by SAML V2.0.

520 3.29.6.2 Enhanced Client or Proxy Profile

525 This section shall be in compliance with the SAML V2.0 Profile [SAMLprof]: Section 4.2 Enhanced Client or Proxy Profile. This is the recommended SAML mechanism to be supported for the XDS Retrieve transaction. This method works well when the X-Service User (e.g. XDS Consumer) is an intelligent application that has been involved in the user authentication transactions. The Enhanced Client or Proxy Profile ensures the most flexibility in the configurations of the X-Identity Providers. There are no IHE specific requirements.

This transaction is used by the X-Service User and X-Service Provider when a Cross-Enterprise User Authentication assertion is necessary to authenticate the user, determine access rights, and produce security audit trail.

530 X-Service Providers need to carefully use the SAML RequestAssertion method as the X-Service User is not likely to be a simple browser and may not be capable of re-authenticating the user.

3.29.6.2 Web Browser SSO Profile

535 This section shall be in compliance with the SAML V2.0 Profile [SAMLprof]: Section 4.1 Web Browser SSO Profile. Support for this method ensures that the X-Service User may be a simple medical device. Other SAML mechanisms may be used but are not required. There are no IHE specific requirements.

X-Service Providers need to carefully use the SAML RequestAssertion method as the X-Service User may not be a simple browser and may not be capable of re-authenticating the user.

3.29.6.4 HL7 Profile

540 Some HL7 transactions are done across enterprise boundaries. In particular a PIX or PDQ transaction to resolve patient identifiers and demographics are expected to commonly go to a system that is outside the local enterprise. These transactions would typically be attributable to a specific user, and thus a grouping with XUA is needed. Note that some nodes sending HL7 messages may not be able to attribute the HL7 message to a user, so care should be taken to

545 configure HL7 receivers to discern nodes and transaction types that would require XUA
grouping. When grouped with XUA further refined access control decisions could be made and
more accurate security audit trails recorded.

3.29.6.4.1 Trigger Events

550 When configured to use XUA, any event initiated by an interactive user that result in an HL7
transaction that is going to go across the enterprise boundary.

3.29.6.4.2 Message Semantics

555 The X-Service User, X-Service Provider, and X-Identity Provider shall follow the SAML v2.0
Profile [**SAMLprof**]: Section 6 Assertion Query/Request Profile to get an Assertion. This
Assertion is then encoded into the HL7 2.6 [**HL7-2.6**] UAC segment. Note that the inclusion of
the UAC segment does not mandate and HL7 version upgrade for the entire message. In
accordance with the rules in Section 2.6.2(a) of Chapter 2 of HL7 Version 2.5 [**HL7-2.5**], it is
acceptable to include the UAC segment, which is first defined in HL7 Version 2.6, in an HL7
V2.5 (or earlier) message. Recipients not wishing to use this segment may ignore it.

The X-Service User shall use a SAML Artifact.

560 The HL7 transaction shall be protected for integrity, authenticity, and confidentiality using TLS.
Note that ATNA requires only integrity and authentication and leaves confidentiality as optional.
The XUA grouping requires confidentiality to mitigate the risk of a third party replay of a SAML
assertion.

3.29.6.4.3 Expected Actions

565 The X-Service Provider shall validate the Assertion according to the SAML V2.0 Profiles. The
X-Service Provider shall implement the SAML v2.0 Profile [**SAMLprof**]: 5 Artifact Resolution
Profile to allow the X-Service User to send a smaller HL7 message.

570 The X-Service Provider may choose to cache successful Assertions from a known X-Service
User so that future HL7 transactions can be processed quicker. This cache shall expire prior to
the original Assertion timeout.

3.29.6.5 DICOM Profile

575 Not available as DICOM does not have normative reference for the inclusion of SAML
assertions. This work is underway, and will likely look similar to the HL7 Profile. The use of
DICOM in Cross-Enterprise transactions should continue to be protected using ATNA
mechanisms.

Note that DICOM WADO should use the Web Browser SSO or Enhanced Client/Proxy profile.