ACC, HIMSS and RSNA

Integrating the Healthcare Enterprise

IHE IT Infrastructure Technical Framework Supplement 2005-2006

Cross-Enterprise User Authentication (XUA) Integration Profile

July 28, 2005

Rev 1.1

Public Comment II Version

Contents

Foreword 2
Profile Abstract 5
GLOSSARY 5
Volume I – Integration Profiles 6
2.2.13 Cross-Enterprise User Authentication (XUA) 6
13 Cross-Enterprise User Authentication (XUA) Integration Profile 7
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
1a HL7 Export/Import 9
1b HL7 Query 9
2a DICOM Export/Import 9
2b DICOM Query 9
3 XDS – Provide and Register 9
4 XDS – Register 10
5 XDS – Query 10
6 XDS – Retrieve (HTTP Get – Application) 10
7 RID – Display (HTTP Get – Browser) 10
13.2 Actors / Transactions 10
13.2.1 Example EHR with XDS and XUA grouping 11
13.3 XUA Integration Profile Options 12
13.4 XUA Integration Profile Process Flow 13
13.4.1 Post-Generated Assertion 13
13.4.2 Pre-Generated Assertion 14
13.4.3 XDS Provide and Register Delegation Model 15
13.4.4 Access Controls 15
Volume 2 - Transactions 18
3.29 Assert X-User Identity 18
3.29.1 Scope 18
3.29.2 Use Case Roles 18
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
3.29.6.2 Enhanced Client or Proxy Profile 21
3.29.6.3 Web SSO Profile 21
3.29.6.4 HL7 Profile 21
3.29.6.5 DICOM Profile 23

Foreword

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 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.

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.

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 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 Francaise 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-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 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 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 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 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

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.

PROLOGUE

A second comment period has been added for the XUA profile. Although the use of SAML 2.0 profiles is viewed as appropriate, there is another SAML profile needed to complete support for the pre-authorized SAML assertion for XDS transactions. It is critical for supporting the small doctor's office and the initial implementations by hospital EHR's. We have collaborated with OASIS and Liberty Alliance and they are working on this missing profile. It is scheduled for completion in December 2005. The second comment period for XUA will close on 15 January 2006 so that there is time to evaluate the incorporation of the SAML profile.

The XUA profile will be used at the HIMSS 2006 Interoperability Showcase as an experimental demonstration of use cases that do not need the missing SAML profile and can use this second public comment version of the XUA profile. This second version incorporates the other comments from the first comment period. The experimental demonstration will be open for participants that wish to demonstrate and gain experience. Full connectathon validation will be performed after completion of the second XUA public comment period.

OPEN ISSUES:

1. We need OASIS to produce a standard that addresses our SOAP use cases in a more efficient way than SAML Web SSO or ECP Profiles do. This work is the work we expect to complete in December 2005.
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.
    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)
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
f. Role vocabulary from ASTM – Privilege Management Infrastructure (work item document number not assigned)

Profile Abstract

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

The following items shall be added to the Glossary

- **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:
    - 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.
- **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).
- **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).
- **Principal** -- A natural person who makes use of a system and its resources for any purpose. A more restricted term 'user' is sometimes used.

Volume I – Integration Profiles

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

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	*Consistent Time*		Required to ensure consistent time.

Add the following section to section 2.2

2.2.13 Cross-Enterprise User Authentication (XUA)

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.

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 (Principal) 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 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 are protected 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 the Enterprise User Authentication (EUA) Profile.

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 can sufficiently authenticate themselves using ATNA – Node Authentication methods. An automated process is sufficiently authenticated through the certificate used in the communications channel (e.g. TLS mutual-authentication, S/MIME). XUA may be used to authenticate an automated process as a process can be identified as a principal.

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.

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.

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.

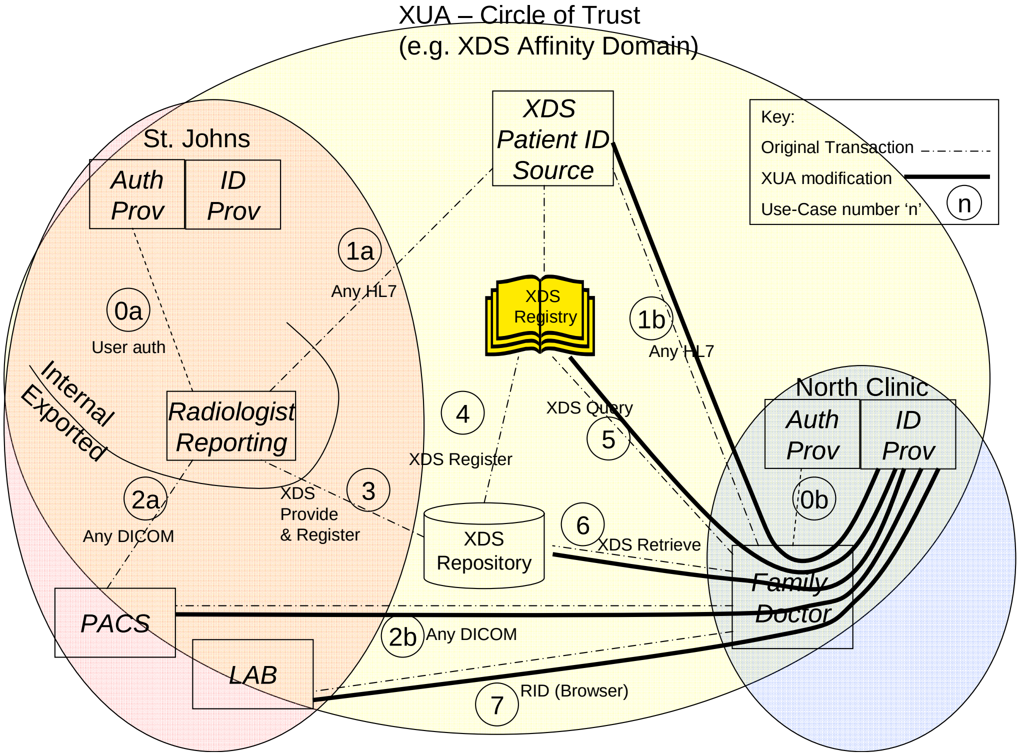


Figure 13-1 – XUA High level use cases

13.1.3 Use Cases

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

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 HL7 Export/Import

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 HL7 Query

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 DICOM Export/Import

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 DICOM Query

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

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

The Repository will forward the registration request on to the Affinity Domain's Registry. The Repository is an automated process, with no interactive user present. The registration is an export event. No grouping with XUA is required.

5 XDS – Query

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 – Application)

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 in the HTTP GET conversation. This conversation is initiated 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)

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 in the HTTP GET conversation. 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.

13.2 Actors / Transactions

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. The following reading list is provided to help get the reader familiar with SAML.

1. **[SAMLTechOvw]** SAML V2.0 Technical Overview (still in active development) http://www.oasis-open.org/committees/download.php/12938/sstc-saml-tech-overview-2.0-draft-06.pdf
2. SAML Tutorial presentation by Eve Maler of Sun Microsystems http://www.oasis-open.org/committees/download.php/12958/SAMLV2.0-basics.pdf
3. SAML V2.0 Standards http://www.oasis-open.org/committees/security/.
4. Open Source Federated Identity Management http://www.sourceid.org/index.html

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 needs to convey user authentication information (i.e. XUA Assertion).

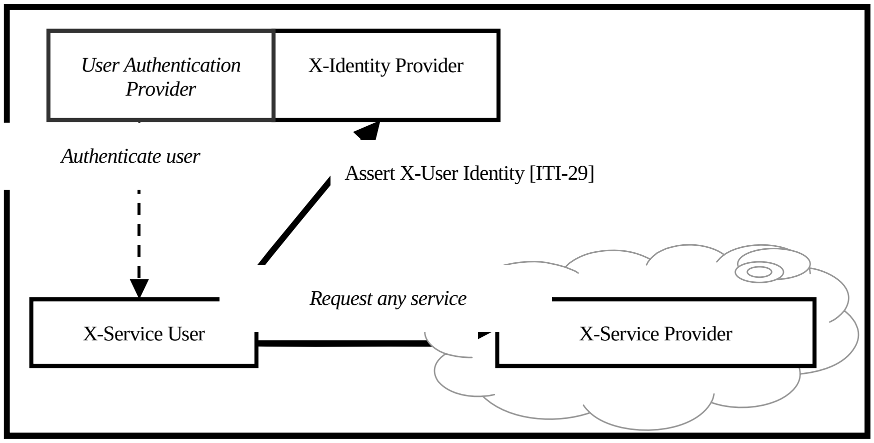


Figure 13.2-1: XUA Profile Actor Diagram

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

13.2.1 Example EHR with XDS and XUA grouping

The X-Identity Provider must be related to the user authentication provider. For example an EHR application that does user authentication within the application could group the X-Service User and X-Identity Provider effectively producing self Assertions. The EHR still must meet all external requirements of the combined X-Identity Provider and X-Service User. These external services must be available to all X-Service Providers that it trusts. Figure 13.2-2 shows this example EMR application acting as the user authentication provider, X-Identity Provider, and X-Service User.

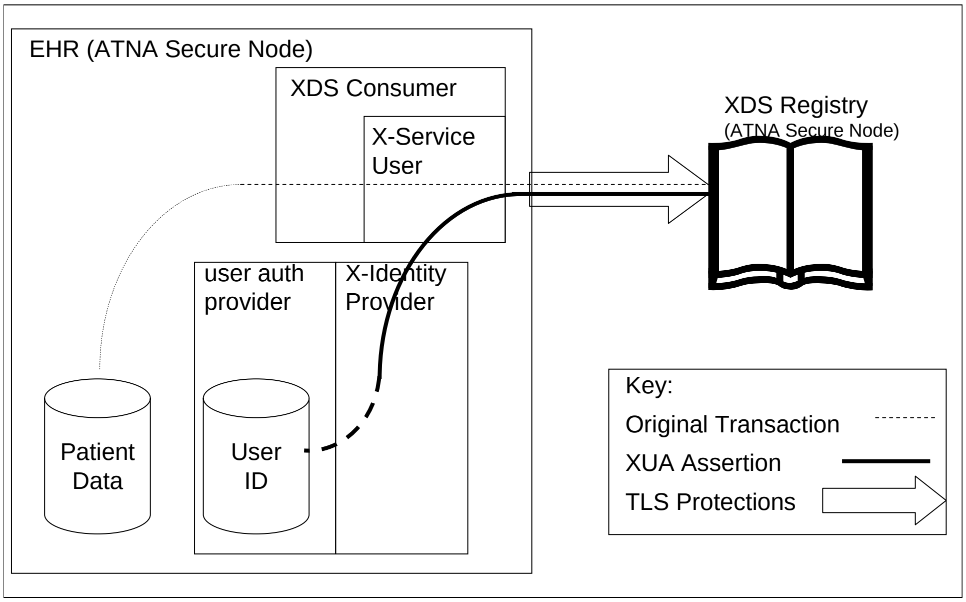


Figure 13.2-2: Example: EHR & XUA Profile Actor Diagram

355 This type of a self-asserting system is a simple example of an XUA implementation that is illustrative purposes. There are many other architectures that are supported by XUA that are not described in this profile. The XUA profile encourages the use of a scalable enterprise class user authentication such as EUA – Kerberos Authentication Server. The X-Identity Provider relationship to the authentication provider is not profiled by IHE or SAML.

360 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.

Table 13.3-1 XUA Integration Profile - Actors and Options

Actor	Options	Vol & Section
X-Identity Provider	*no options*	
X-Service Provider	*no option*	
X-Service User	*no option*	

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.

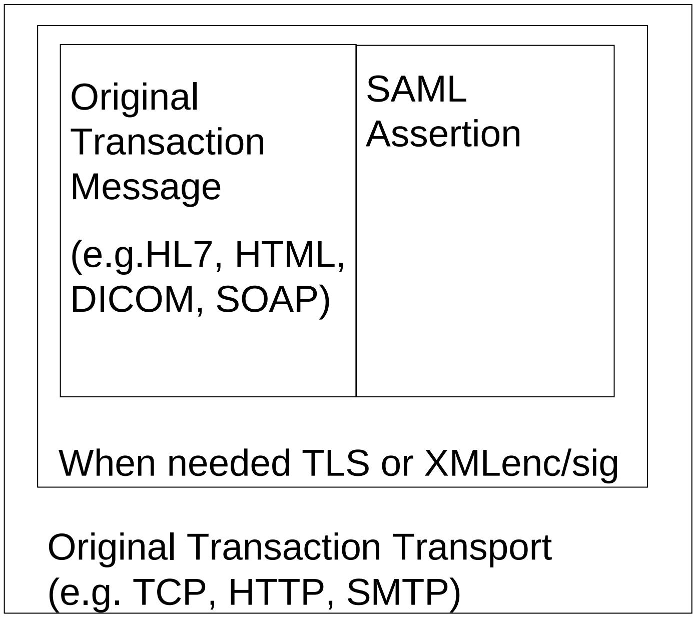

Original Transaction Message
(e.g.HL7, HTML, DICOM, SOAP)
SAML Assertion
When needed TLS or XMLenc/sig
Original Transaction Transport (e.g. TCP, HTTP, SMTP)

Figure 13.4-1 General adaptation of Original Message / Transport

13.4.1 Post-Generated Assertion

The first case that is described might be considered a “post-generated assertion” as the client application attempts the original transaction first and this initiates the creation/communications of the assertion. This 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]** Web SSO and Enhanced Client/Proxy Profiles.

Note at the present time the XDS Query and XDS Retrieve transactions are best implemented using the SAML 2.0 **[SAMLprof]** Enhanced Client/Proxy Profile. The benefit of this profile is that the XDS Consumer Actor takes an active part in the transaction and thus controls the process better.

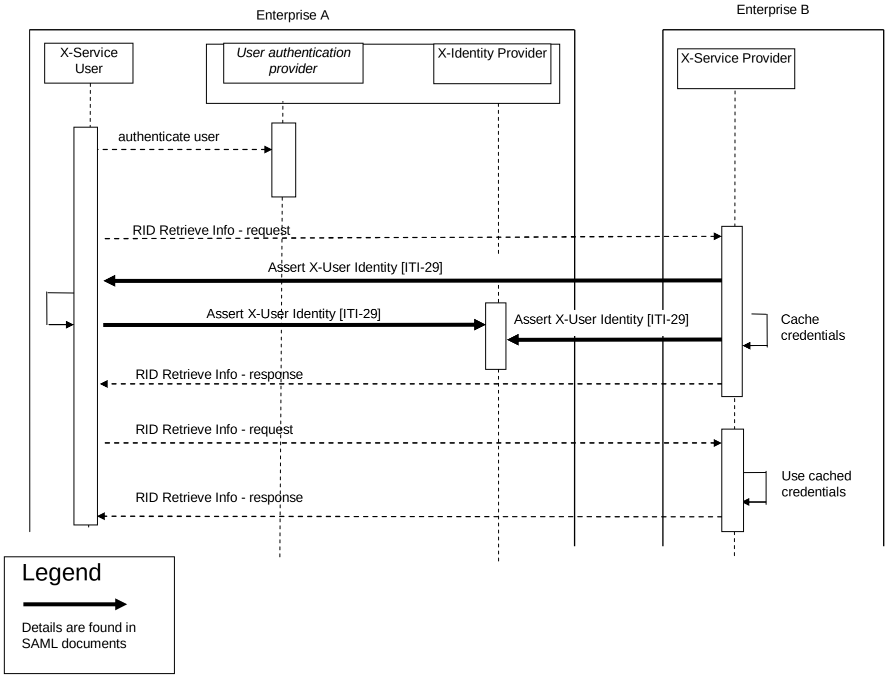

Enterprise A
Enterprise B
X-Service User
User authentication provider
X-Identity Provider
X-Service Provider
authenticate user
RID Retrieve Info - request
Assert X-User Identity [ITI-29]
Assert X-User Identity [ITI-29]
Assert X-User Identity [ITI-29]
Cache credentials
RID Retrieve Info - response
RID Retrieve Info - request
Use cached credentials
RID Retrieve Info - response
Legend
Details are found in SAML documents

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

13.4.2 Pre-Generated Assertion

The second case that is described might be considered a “pre-generated assertion” as the client application gets the user assertion before starting the original transaction. 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.

The General Practitioner, Charley, is using an HL7 Query to find the Affinity Domain Patient Identity (See PIX 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 Patient Identifier Cross-Reference Manager Actor may use this identity to determine the user’s permissions to access the data, and to record the retrieve (export) event. See Figure 13.4-3 for the transaction details. This configuration leverages the SAML v2.0 **[SAMLprof]** Assertion Query/Request Profile.

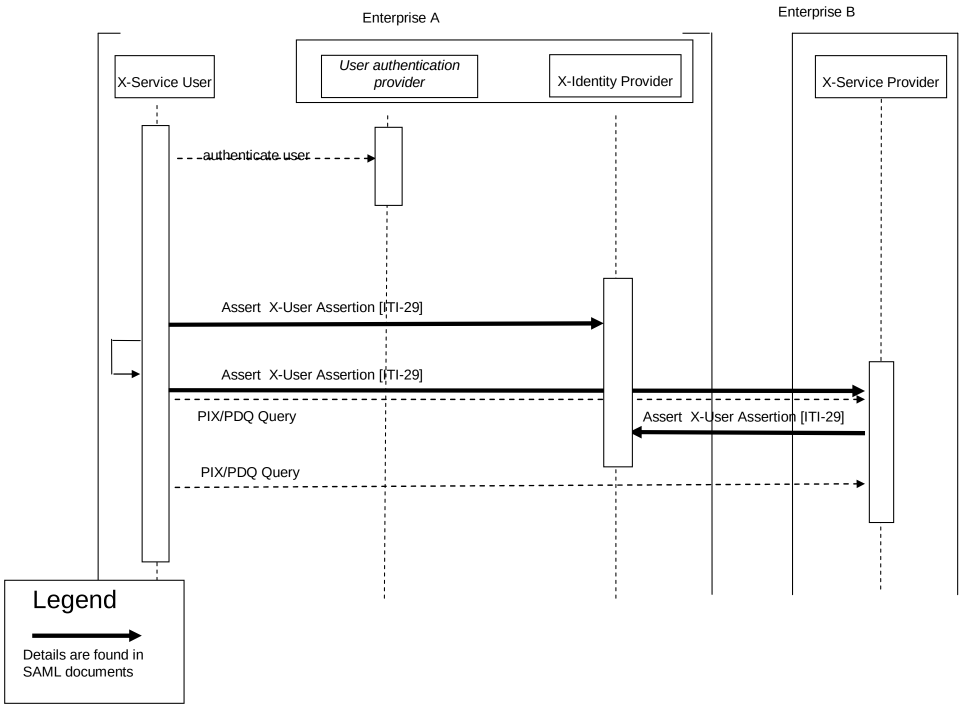

Enterprise A
Enterprise B
X-Service User
User authentication provider
X-Identity Provider
X-Service Provider
authenticate user
Assert X-User Assertion [ITI-29]
Assert X-User Assertion [ITI-29]
PIX/PDQ Query
Assert X-User Assertion [ITI-29]
PIX/PDQ Query
Legend
Details are found in SAML documents

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

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.

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.

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.

Audit trails should continue to use the ATNA audit mechanism. 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.

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

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

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.

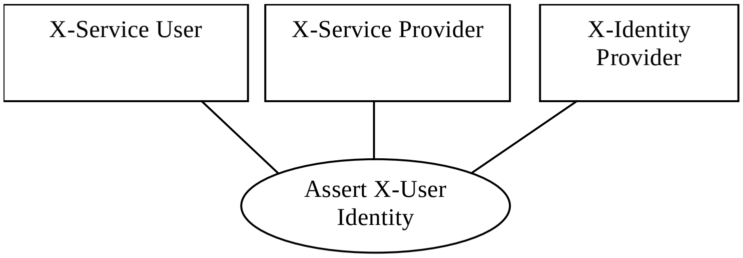
Assert X-User Identity is a high level transaction that does not always represent the actual transactions between the specified actors. This IHE transaction is defined to convey the concept that is very well worked out within the standards used. In some cases the underlying transactions look very much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

This section leverages the SAML Profiles and Standards. This section does not include the implementation details necessary. A strong understanding of SAML V2.0 is required before this transaction can be understood. The following list of documents from the referenced standards (Section 3.29.3) is necessary: SAMLTechOvw, SAMLTutorial, SAMLProf, SAMLGloss, SAMLConform, SAMLBind, and SAMLcore

3.29.1 Scope

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

Role: Has authenticated the user with an enterprise authentication system and is now requesting a Cross-Enterprise service. Equal to the SAML V2.0 User Agent (UA) or ECP.

Actor: X-Service Provider

Role: Providing a Cross-Enterprise service that requires a User Assertion. Equal to the SAML V2.0 Service Provider (SP) or Service Provider Lite.

Actor: X-Identity Provider

Role: Provides the User Assertion associated with an X-Service User requesting a Cross-Enterprise service from an X-Service Provider. Equal to the SAML V2.0 Identity Provider (IDP) or Identity Provider Lite.

Not shown: enterprise user authentication system that is related to the X-Identity Provider.

3.29.3 Referenced Standard

[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

[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.

[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/.

[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/.

[SAMLCore] P. Mishra et al. Assertions and Protocols for the OASIS Security Assertion *Markup Language (SAML) V2.0.* OASIS SSTC, March 2005. Document ID samlcore-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/.

[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/.

[SAMLP-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/.

[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-06. See http://www.oasisopen.org/committees/security/.

[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/.

[SAMLTutorial] Eve Maler, SAML Tutorial, Sun Microsystems, http://www.oasis-open.org/committees/download.php/12958/SAMLV2.0-basics.pdf

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.

Table 3.29-1 Recommended SAML Profiles for protocols/transactions

SAML Profile	Web SSO	Enhanced Client/Proxy	Assertion Query/Request
Protocol/Profile	Section 3.29.6.3	Section 3.29.6.2	Section 3.29.6.4
Any HL7	N/A	N/A	MUST
Any DICOM	N/A	N/A	MUST
Any RID	MUST	MUST	OPTIONAL
XDS Query	MUST	MUST	OPTIONAL
XDS Retrieve	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).

3.29.5 Trust Relationship

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

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 uses of the Assert X-User Identity Transaction. 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.

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.

SAML requires that the transactions that contain a SAML Assertion are protected for integrity and confidentiality. This can be done by grouping with ATNA Secure Node which provides: node-to-node authentication, user authentication (to the authentication provider), and proper security audit trails. When using ATNA to cover transactions that are carrying a SAML Assertion, the ATNA - TLS Encryption Option shall be used.

3.29.6.1 Assertion Content

The Assertion content conveyed in the Assert X-User Identity Transaction, shall be encoded in the SAML Assertion using the SAML v2.0 **[SAMLprof]** Authentication and Attribute Profiles. This information may be further restricted by the X-Identity Provider Actor.

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 addressed 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.

3.29.6.2 Enhanced Client or Proxy Profile

Actors shall follow 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.

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.

3.29.6.3 Web SSO Profile

Actors shall follow the SAML V2.0 Profile **[SAMLprof]**: Section 4.1 Web 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.

Although the Web SSO Profile is most likely to be used by X-Service User Actors that are simple browsers, 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

Some HL7 transactions are done across enterprise boundaries. 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 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

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

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 an 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.

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

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.

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.

If the X-Service Provider accepts the user credentials in the UAC segment, no specific acknowledgement is required. However, if the X-Service Provider detects an error while processing the UAC segment, its acknowledgment message shall report it to the X-Service User via an MSA + ERR segment pair:

- The ERR-3 (error code) field value is 207 to signify an application error
- The ERR-7 (diagnostic information) field reports the specific error. Examples of possible errors are:
    - User credentials expected but not provided
    - User credentials invalid

- User credentials expired
- User credentials from an unknown or untrusted source
- User unknown
- User not allowed to create or access data on the receiving system.
- User not allowed to initiate a processing function on the receiving system.

When an MSA + ERR segment pair is reported to the sender, an application data response shall not occur. In such cases it is correct to assume that the sending application's user is not authorized to get the data.

The processing rules for the ERR segment are outside of scope.

3.29.6.5 DICOM Profile

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 SSO or Enhanced Client/Proxy profile.