

ACC, HIMSS and RSNA
Integrating the Healthcare Enterprise



5 **IHE IT Infrastructure Technical Framework**
White Paper
2006-2007
For Public Comment

10 **Cross-Enterprise User Authentication (XUA)**

15

IHE ITI Technical Committee

Editor:

John F. Moehrke

20

Version 2.0

2006-08-15

25	Contents	
	1	Introduction..... 4
	2	Background..... 5
	2.1	Identity Enabled Services 5
	2.2	SAML Assertion..... 6
30	3	Healthcare Use cases 7
	3.1	Assumptions 7
	3.2	Use Case Categories..... 8
	3.2.1	User Authentication (0a/b/c)..... 8
	3.2.2	HL7 Export/Import (1a)..... 8
35	3.2.3	HL7 Query (1b)..... 9
	3.2.4	DICOM Export/Import (2a)..... 9
	3.2.5	DICOM Query (2b)..... 9
	3.2.6	XDS – Provide and Register (3)..... 9
	3.2.7	XDS – Register (4)..... 9
40	3.2.8	XDS – Query (5)..... 10
	3.2.9	XDS – Retrieve (HTTP Get – Application) (6)..... 10
	3.2.10	RID – Display (HTTP Get – Browser) (7)..... 10
	3.2.11	Sue views note (XDS) (5, 6, 7)..... 10
	4	Actors / Transactions 11
45	4.1	Example EHR with XDS and XUA grouping..... 11
	4.2	XUA Integration Profile Process Flow..... 12
	4.2.1	Post-Generated Assertion 13
	4.2.2	Pre-Generated Assertion..... 14
	4.2.3	XDS Provide and Register Delegation Model..... 15
50	4.3	Access Controls..... 15
	4.4	Audit Logs 16
	5	Guidance..... 17
	5.1	Trust Relationship..... 17
	5.2	Assertion Content..... 17
55	5.3	Enhanced Client or Proxy Profile 18
	5.4	Web SSO Profile 18
	5.5	Web Services Profile 18
	5.6	HL7 Profile 19
	5.7	DICOM Profile 19
60	6	Conclusion..... 20
	7	GLOSSARY..... 21
	8	Referenced Standard..... 22

OPEN ISSUES:..... **24**

65 1 Introduction

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 and others that create an Affinity Domain. When transactions cross enterprise boundaries the mechanisms found in the EUA and PWP profile are
70 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.

This white paper proposes a *Cross-Enterprise User Authentication (XUA)* profile that will provide the user identity in transactions that cross enterprise boundaries. Enterprises may choose
75 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 IHE has decided to publish this white paper instead of a Profile at this time. Although the use of SAML 2.0 Assertions is viewed as appropriate, there is a lack of experience with SAML
80 to understand the need for a Profile. We may need to specify the SAML Assertion content beyond specifying the use of SAML 2.0. We may also need a more complete support for the pre-authorized SAML assertion for many IHE transactions. There is much work going on in OASIS, WS-I, and Liberty Alliance that should fill some of these gaps. We now must decide if we are going to develop profiles that are unique to Healthcare, or wait and leverage the near future
85 standards work.

2 Background

Security protects assets from risks. Information security protects information assets from risks to confidentiality, integrity and availability. Only through a security risk assessment and mitigation plan, executed at each design level, will information assets be appropriately protected. IHE is
90 now evaluating all Profiles in the context of a risk assessment plan to assure that risks are managed in the proper priority and with proper means. For more information on applying risk assessment strategy see the IHE web site for a white paper on risk assessment.

The IHE profiles available today provided for distributed accountability that is tied together through the use of node-to-node authentication between systems that agree to handle access
95 controls and audit trails. Access control policies are becoming more complex. Systems are often built on architectures that are loosely coupled such as n-tier web-services. The result is that the user is further away from the data.

An enterprise can impose a single authentication technology and a single personnel directory. Multiple enterprises that participate in an affinity domain may not be able to impose a single
100 authentication technology or personnel directory. There are many different forms of authentication available today including Kerberos, PKI, token, or biometrics. Services, especially those in a cross-enterprise environment, must be isolated from this variability, yet aware of it.

The user identity that is communicated in a cross-enterprise transaction needs to include enough information about the user authentication event, core attributes about the user, and the
105 functionality being used. This contextual identity is critical for complex policy enforcement. This white paper further discusses this federated identity management, which supports both distributed user identity management as well as centralized. This flexibility is a key attribute needed in cross-enterprise transactions, and assists in extending an enterprises single sign-on environment in a secure and privacy protecting way.

In many transactions the ultimate user of the data is not the one controlling the system during the data discovery and transfer. The transaction might be an automated service that is pre-fetching the data, or might be a clerk working on behalf of a doctor. The XUA solution needs to be standards based and deterministic. Healthcare doesn't simply use common IT systems. Medical Devices are also expected to participate in cross-enterprise transactions.

The IHE has produced presentations and will produce white papers on XDS-Security which is based on the same distributed security model found in all of the IHE use-cases. This security model recognizes the distributed nature of information in healthcare, the sensitivity of the data, and the critical nature of patient care and safety. At this time there is a presentation on XDS-Security that can be found on the IHE web site <http://www.ihe.net>.

2.1 Identity Enabled Services

Transactions are protected using point-to-point solutions like TLS or message level solutions like XML Encryption and XML Signature. These solutions ensure that the conversation is not intercepted or modified. These mechanisms can ensure that the systems involved are trustworthy to handle sensitive data. There are needs to provide a trusted security token that contains identity

125 information that allows the service to authenticate the identity of the user related to the request. The valid security token allows the service to make appropriate authorization decisions based on the subject of the token.

The OASIS standards organization has defined a security token that can span cross-enterprise transactions and can carry the other desired attributes. This security token is defined as the
130 SAML v2.0 Assertion. OASIS WS-Trust standard defines a Security Token Service (STS) that can bridge the enterprise authentication system and the security token.

A client will use the WS-Trust protocols to communicate with the STS to receive a SAML Assertion. This SAML Assertion is carried in the transaction to the service (e.g. WSS headers of the SOAP request). The service needs to trust the STS that issued the SAML Assertion. The
135 service can communicate with the STS using WS-Trust protocols to validate the SAML Assertion.

2.2 SAML Assertion

The SAML Assertion has some important qualities:

- open standard
- 140 • supports homogenous and heterogeneous environments
- can carry multiple user authentication assertions,
- identities are marked with the assurance level each provides
- can carry additional attributes about the user such as email, role, address, preferences
- the identity information can be a pseudonym when appropriate
- 145 • the assertion content can be defined by the service that will consume them

These qualities allow a SAML Assertion to carry security tokens from one or more authentication system including Kerberos and X.509. These qualities also allow the SAML Assertion to enable policy enforcement such as RBAC, PMAC, or XACML. The SAML Assertion provides a unique identifier suited for audit trails.

150 The system allows for each enterprise to manage their users independent of the transactions. Thus the information necessary to build a SAML Assertion is only communicated at the time the transaction happens, not when the user is provisioned. This limits the exposure of the user to the other enterprise. This exposure can also use pseudonyms when necessary.

3 Healthcare Use cases

155 All use cases are shown on Figure 1. These use cases are tied together into a treatment of a single patient. The use case starts with a patient (Fred) getting a CT scan done at St Johns Hospital. There Dr. 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, Dr. Alice, queries the XDS Registry for the completed report, and once found pulls the
160 document from the repository. Seeing the results the family doctor pulls the results using the Retrieve Information for Display Profile from a lab system at St Johns Hospital. Dr Alice sees Fred in her office to discuss the results, and then writes a note, a copy of which is submitted to the XDS repository. At home, Fred's wife Sue (to whom Fred has delegated permission to view his records) queries the registry to look at Dr. Alice's note (Dr. Alice has agreed to share her
165 clinical notes with her patients without a specific medical records request), and her recommendations for Fred.

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 use case above includes two important ways in which participants have authorized the sharing of health
170 information: Fred has given permission to his wife to view his medical records, and Dr. Alice has agreed to share her clinical notes with her patients without a specific medical records request.

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
175 that is grouped with a cross-enterprise identity provider.

3.1 Assumptions

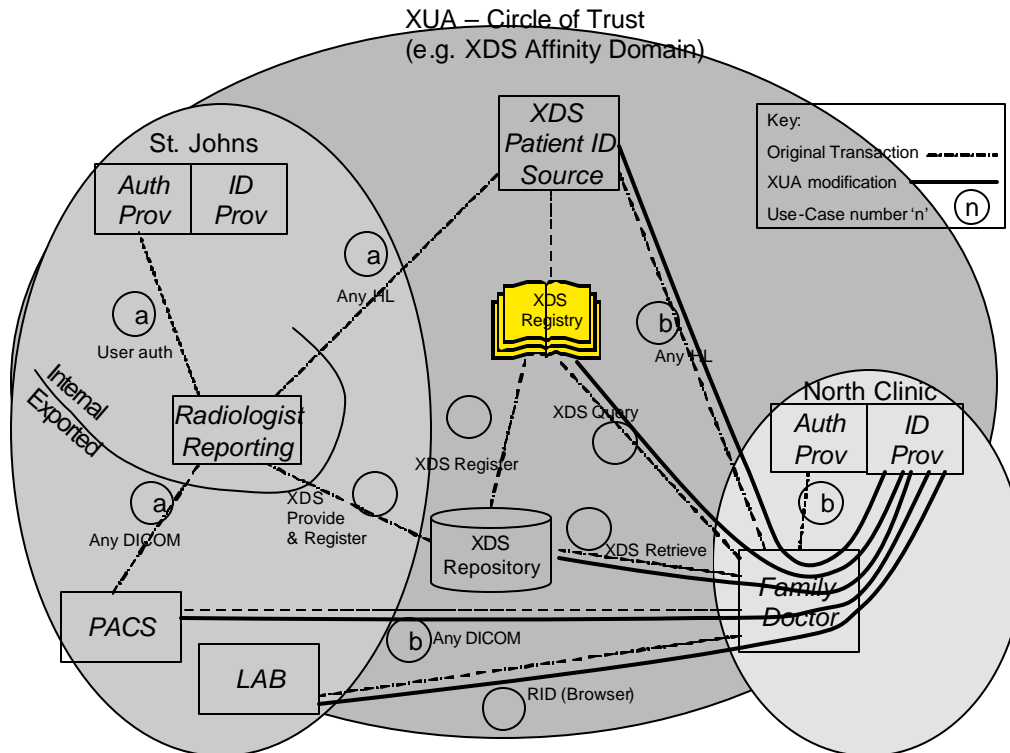
The users (Dr. Alice, Dr. Bob, the patient Fred, and his wife Sue) are each authenticated by an authentication authority that is related to an XUA Identity Provider. The authentication authority may be implemented with one set for a whole Affinity Domain or with enterprise specific sets.
180 The solution must support both types of configurations.

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.

185 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 1 do not require grouping with XUA. 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.

190 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.



195

Figure 1 – XUA High level use cases

3.2 Use Case Categories

The use cases are discussed in further detail below. The number in Figure 1 corresponds to the parenthetical number listed below. The user has been authenticated to his/her local authentication provider. The local authentication provider for the patient and his family can be any XUA Identity Provider.

3.2.1 User Authentication (0a/b/c)

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.

3.2.2 HL7 Export/Import (1a)

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

210 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
215 ID. determine that the transaction is coming from a node that should be allowed to update the Patient

3.2.3 HL7 Query (1b)

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
220 comes from the XUA Identity Provider that is grouped with the authentication provider used to
authenticate the user.

3.2.4 DICOM Export/Import (2a)

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
225 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.

3.2.5 DICOM Query (2b)

The Family Doctor (Alice) will query the PACS for the DICOM Structured Report using
230 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.

3.2.6 XDS – Provide and Register (3)

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

3.2.7 XDS – Register (4)

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

3.2.8 XDS – Query (5)

245 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.

3.2.9 XDS – Retrieve (HTTP Get – Application) (6)

250 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.

3.2.10 RID – Display (HTTP Get – Browser) (7)

255 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.

3.2.11 Sue views note (XDS) (5, 6, 7)

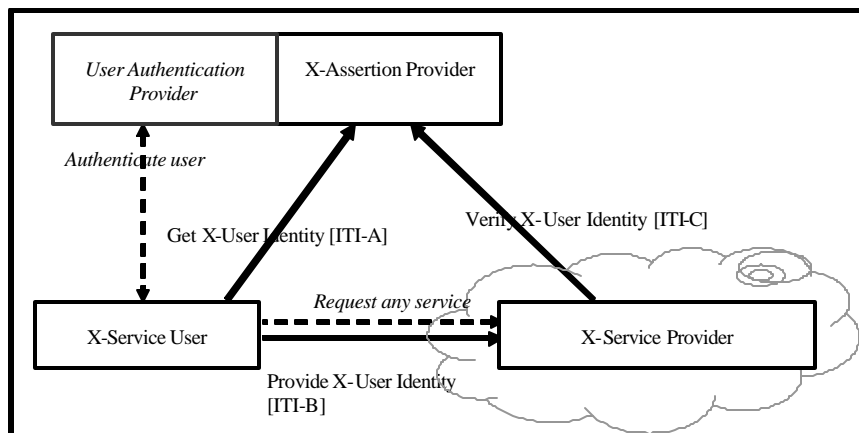
Patient access to the XDS through their PHR is similar to the classic transactions. The difference is that the user is identified as a patient.

4 Actors / Transactions

260 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.

- 265 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>

270 The XUA profile has three actors participating in three transactions. These transactions look very different at the detail level depending on the specific use case. Figure 2 shows the actors directly involved in the XUA Profile and the transactions 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).

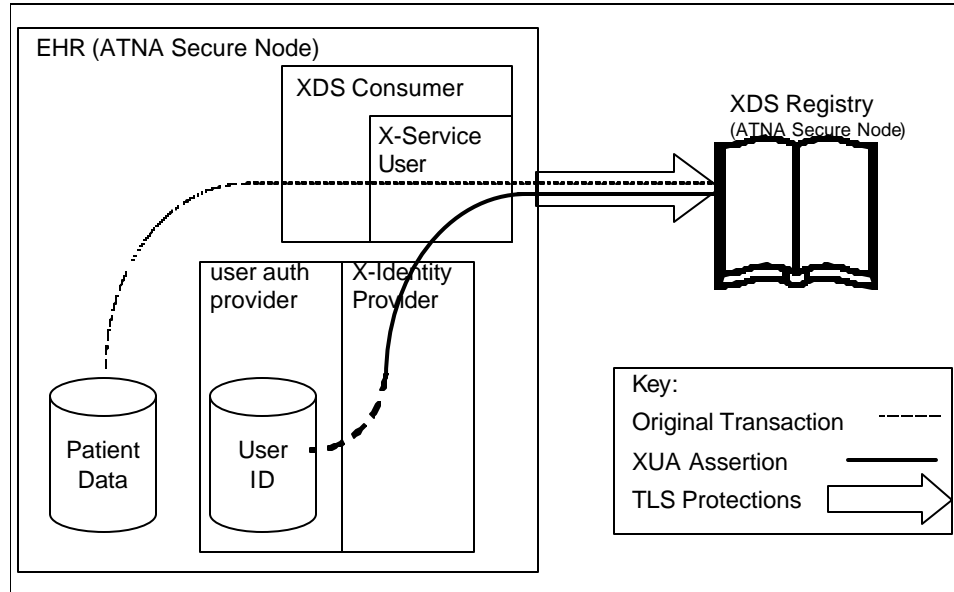


280 **Figure 2: XUA Profile Actor Diagram**

4.1 Example EHR with XDS and XUA grouping

285 The X-Assertion 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-Assertion Provider effectively producing self Assertions. The EHR still must meet all external requirements of the combined X-Assertion Provider and X-Service User. These external services must be available to all X-Service Providers that it trusts. Figure 3 shows this

example EMR application acting as the user authentication provider, X-Assertion Provider, and X-Service User.



290

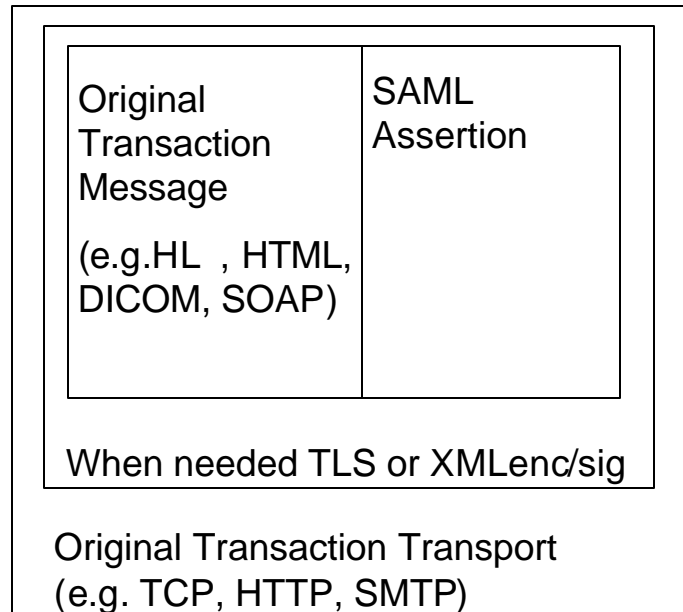
Figure 3: Example: EHR & XUA Profile Actor Diagram

This type of a self-asserting system is a simple example of an XUA implementation that is illustrative purposes. There are 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-Assertion Provider relationship to the authentication provider is not profiled by IHE or SAML.

295

4.2 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.



300

Figure 4 General Adaptations of Original Message / Transport

4.2.1 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 5 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.

320

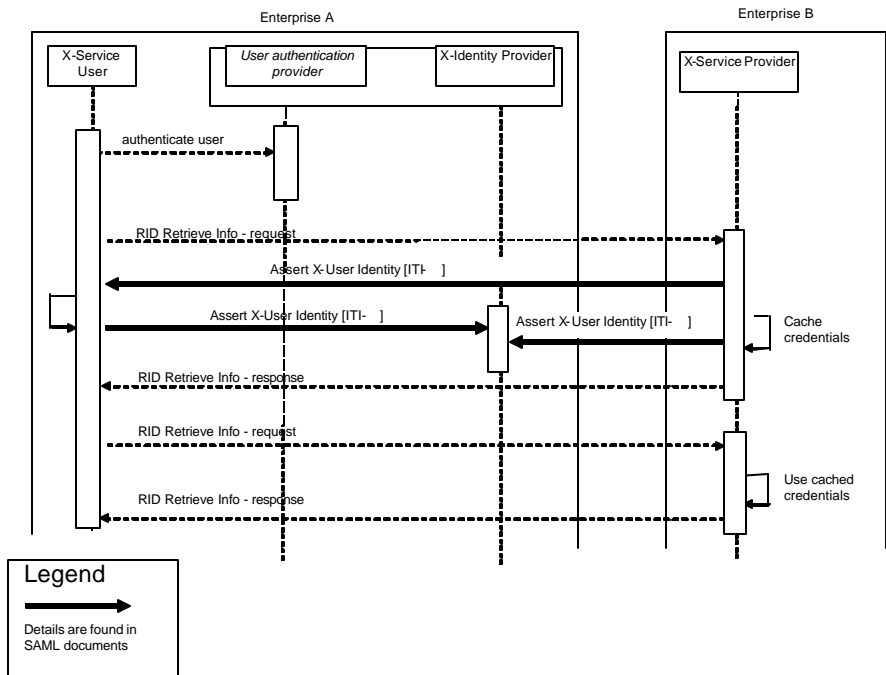


Figure 5: Post-Generated Assertion Profile Process Flow in XUA Profile

4.2.2 Pre-Generated Assertion

325 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.

330 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 6 for the transaction details. This configuration leverages the SAML v2.0 [SAMLprof] Assertion Query/Request Profile.

335

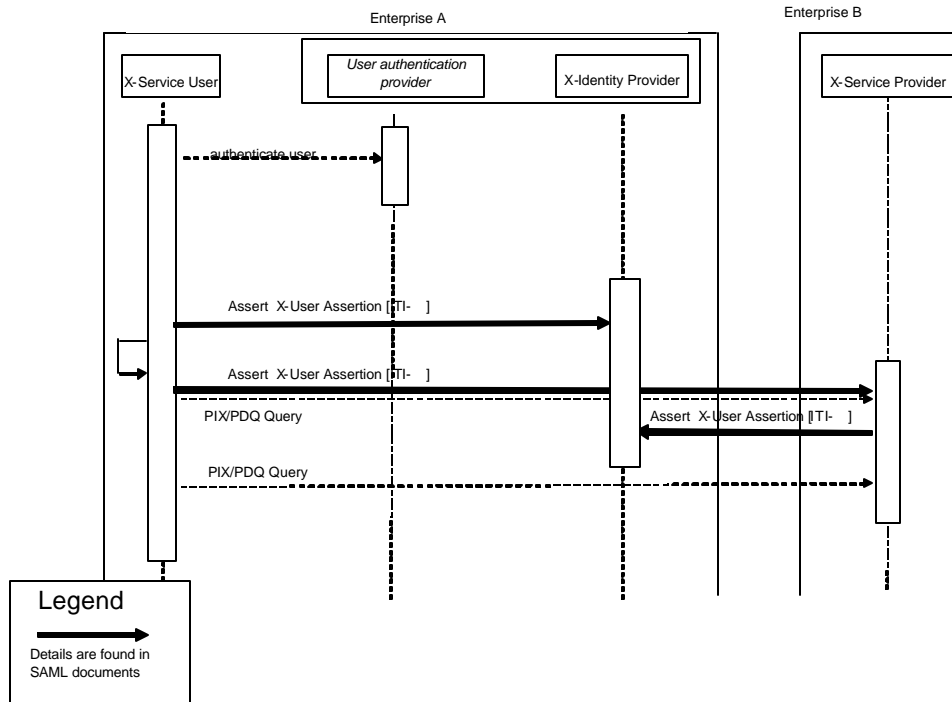


Figure 6: Pre-Generated Assertion Profile Process Flow in XUA Profile

4.2.3 XDS Provide and Register Delegation Model

340 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

345 was authorized. It is possible in the future that we may have strong enough access control policies to support automated delegation.

4.3 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.

350 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 informed by the assertion.

355 4.4 Audit Logs

Audit trails should continue to use the ATNA audit mechanism. There are no specific audit events that XUA adds.

5 Guidance

360 This section proposes some requirements for the X-Service Provider, X-Service User, and X-Assertion 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
365 transactions are only representative in spirit.

This section leverages the SAML Profiles and Standards. This section does not include the implementation details necessary to design a system. 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,
370 SAMLGloss, SAMLConform, SAMLBind, SAMLws-sx, and SAMLcore

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
375 V2.0 support for other transactions. The IHE will follow the lead of OASIS Security Committees and WS-I 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.

380 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.

385 5.1 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-Assertion Providers shall be configured to trust the federated X-Assertion Providers using the [SAMLMeta] method. This may be done by manual configuration of service and identity
390 provider description tables.

5.2 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,

and profiled in WS-I Security Assertion Profile [**WS-I SAML**]. As IHE gets experience there
395 may be further profiling of the Assertion for Healthcare by IHE.

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.

400 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.

5.3 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
405 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-Assertion Providers. There are no IHE specific requirements.

410 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.

5.4 Web SSO Profile

415 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.

420 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.

5.5 Web Services Profile

425 Web Services should follow the WS-I Basic Security Profile [**WS-I Security**] and WS-I SAML Token Profile [**WS-I SAML**]. The WS-I Basic Security profile utilizes WS Security approach for delivery of SAML Assertions. The WS Security header contains both the SAML Assertions together with other transport metadata related to maintaining the integrity and privacy of the message payload.

430 Any required authentication, validation or other processing of the presented SAML assertions may be accomplished using provisions of the SAML V2.0 Profile; related profiles such as WS Trust, WS Policy and WS-SX.

The XUA Web Services Profile can be used in any case where IHE profiles provide for the use of the Web Services Transport binding.

5.6 HL7 Profile

435 HL7 V2 is not recommended to be grouped with XUA and there is no guidance from IHE on how this should be done. There is a USR segment that could be used.

HL7 V3 should use the Web-Services mechanism discussed above.

5.7 DICOM Profile

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

440 DICOM does not have normative reference for the inclusion of SAML assertions. This work is underway. The use of DICOM in Cross-Enterprise transactions should continue to be protected using ATNA mechanisms.

6 Conclusion

445 This white paper is describing the current state of the art in Cross-Enterprise User Authentication and IHE recommendations. This white paper is intended to inform the healthcare industry. This white paper is also requesting input to this architecture to better direct future IHE Profile work. We expect to receive input specifically from the following projects:

- OHF
- IHE PCC – Emergency Room Workflow
- HITSP usecases
- 450 • NHIN Test-beds
- HL7 Web Services Transport Specification
- etc

7 GLOSSARY

455 **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.

460 **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, and an association comprising any number of service providers and identity providers.

465 **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.

470 **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).

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

8 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>

480 [**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.

485 [**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/>.

490 [**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/>.

495 [**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/>.

500 [**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/>.

[**SAMLXSD**] 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/>.

505 [**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/>.

510 [**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/>.

[**SAMLws-sx**] Web Services Secure Exchange.

[**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/>.

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

[**WS-I Security**] Abbie Barbir, Basic Security Profile Version 1.0, <http://www.ws-i.org/Profiles/BasicSecurityProfile-1.0.html>

520 [**WS-I SAML**] Abbie Barbir, SAML Token Profile Version 1.0, <http://www.ws-i.org/Profiles/SAMLTOKENProfile-1.0.html>

OPEN ISSUES:

The following are open issues that the IHE IT Infrastructure Technical Committee has on the XUA profile. We invite comment on these issues as they will assist with the ultimate profiling into the XUA profile.

- 525 1) Should we rename this white paper to “Cross-Enterprise User Assertion (XUA)” to show that we are addressing the user assertion and not the act of authenticating the user?
- 2) 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 expected from the WS-SX, and WS-I efforts.
- 530 3) IHE is changing some of the IHE transactions to use more mainstream web-services transactions thus we would be better able to leverage OASIS WS-* work. For each transaction type:
- a) There are questions around the transactions and how they carry the assertion?
- b) There are questions around how the application calling on a service that needs XUA
535 knows that XUA is needed?
- c) There are questions around how the application calling on a service that needs XUA knows what the XUA Assertion needs to contain?
- d) There are questions around error modes around the assertion, transaction, access rights (e.g. do we tell the user why it fails)?
- 540 e) There are questions around how an application that is calling on a service that needs XUA interacts with the user authentication service (e.g. EUA) and IDP. How do the user authentication service and the IDP communicate?
- 4) We are not constraining the SAML Assertion content at this time. We know that ISO and
545 ASTM are updating relevant standards that would guide future Assertion constraints. As we figure out what needs to be in the SAML Assertion we will need to reflect the same changes in PWP. For example:
- 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 –
550 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.
- 555 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)
 - g) Permissions from HL7 DSTU?
- 560 5) Need to make the assertion from a patient clearly indicating that the assertion is for a patient
- a) Should include the patient ID
 - b) Need to be clear in the profile that there are many issues with patient access that are not handled
- 565 c) Consent, Specific provider restrictions, Specific data restrictions, Workflow of a physician that needs to discuss the data before the patient sees it, Delegates (parent, child, guardian, elder),
- d) Patient accesses XDS through some 'service' like a PHR. The PHR needs to be a member of the Affinity Domain.
- e) Need to be clear on the case where a physician is a patient... which role?
- 570 6) One of the hardest to solve transaction is the XDS Retrieve transaction. This one seems like the browser profile would fit well, but it is often used by middleware and thus the requirements are not nearly clear. We have investigated creating a new XDS Retrieve that uses web-services, but that produces other interoperability problems.
- 575 7) The XDS-Provide and Register transaction has been indicated as being important. This is a very hard transaction to cover. The hardest part of the transaction is that the Repository is an intermediary that also needs the XUA assertion.
- a) The current thinking is that this transaction also doesn't provide much useful users as a clerk or automated machine is likely doing the login.
- 580 8) Need to be clear that self-assertions are a simplified model that doesn't scale well, but gets around client side lack of standards
- 9) Need to profile DICOM because no one else is going to do that.
- a) Do we cryptographically bind the identity to the message?
 - b) Do we need to specify a base64 encoding of the assertion?
- 585 c) How does the SCU know to add the assertion? How does it know what type off assertion to get? Is there a way to limit the assertion types?
- 10) HL7
- a) Now that we will have a Web-Services based PIX and PDQ, do we really need to have anything special for HL7? Can we simply point any use of XUA with HL7 to the HL7 V3 and Web-Services transport?
- 590 b) Do we need to support ebXML Messaging? MMLP? HL7 v2?
- 11) Need to be clear on how EUA and XUA can exist together.

- a) When an application is using EUA to authenticate the user within an enterprise, how does the system respond/act when XUA is needed? There needs to be guidance on how to pass the EUA user authentication to the IDP.

595 12) How is Emergency Mode handled?

- a) This must work for medical devices where the medical device includes all the standards when it is shipped from the manufacture. No 'agent' can be required to make this work.
- b) Do we have a well defined way for one actor to declare that it is in emergency mode? Clearly this mode doesn't have to be accepted. Clearly the use of this mode must be carefully managed with policy.
600
- i) Possibly a 'claimed' functional role.
- c) May need to look at yet a more simple (radical) approach to user identity. This might use something simpler than SAML assertions, or might be SAML assertions in self-assertion mode.

605 13) Do we need to further restrict SAML transactions. (ex. Single Logout)?

- 14) How will this change if we institute a federated XDS Registry where the initial XDS Query transaction may be reflected and spread to multiple other Registries and possibly further?

610