

A stylized world map in light blue and white, centered on the Atlantic Ocean, serving as a background for the text.

Cross-Enterprise User Assertion

IHE Educational Workshop 2007

John F. Moehrke

GE Healthcare

IT Infrastructure Technical Committee





Cross-Enterprise User Assertion *Value Proposition*

- Extend User Identity to Affinity Domain
 - Users include Providers, Patients, Clerical, Processes, etc
 - Must supports cross-enterprise transactions,
 - can be used inside enterprise
 - Distributed or Centralized user management/authentication.
- Provide identity information necessary so that receiving actors could make Access Control decisions
 - Does not include Access Control mechanism
- Provide information necessary so that receiving actors can produce detailed and accurate Security Audit Trail

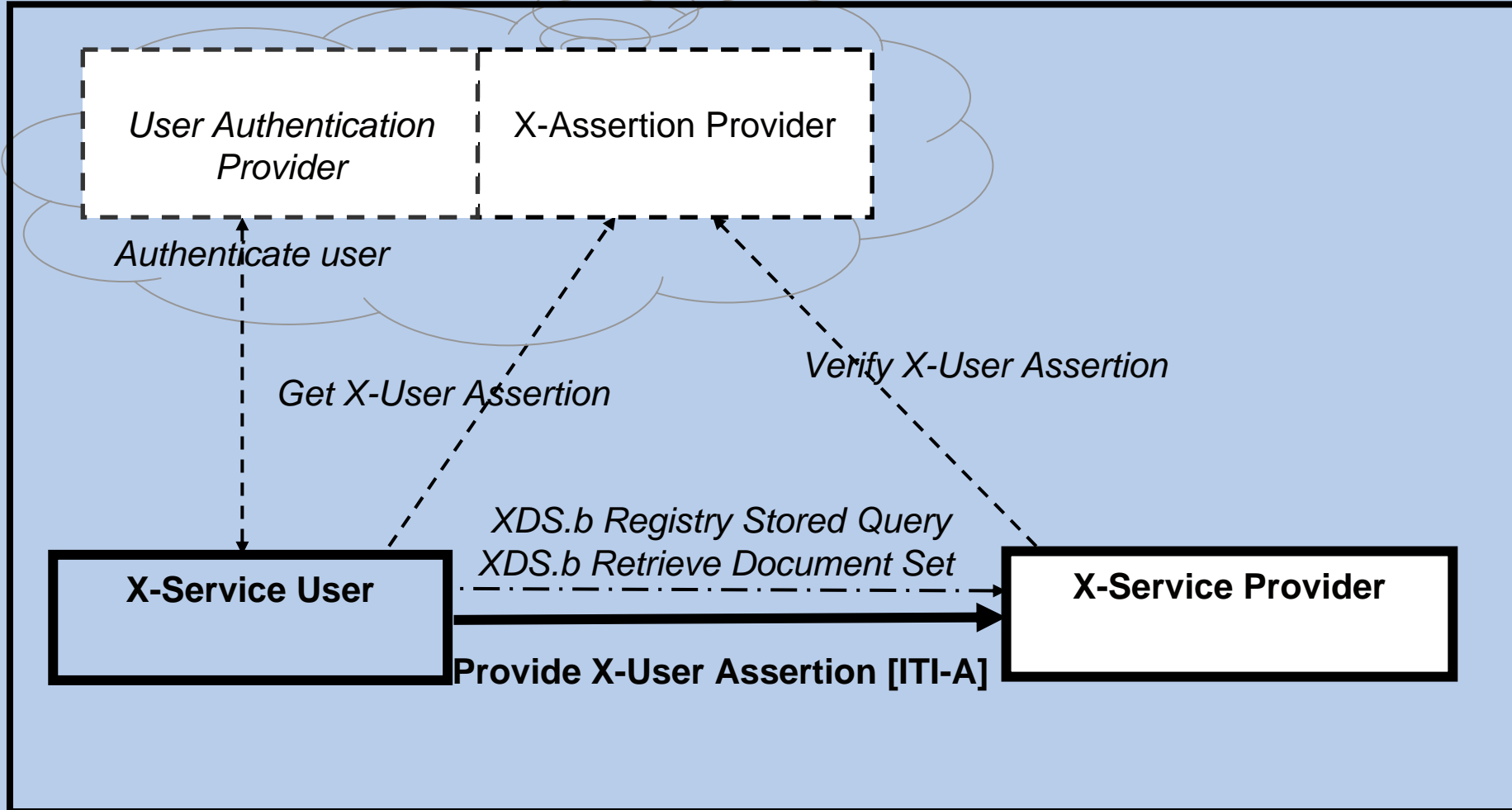


Cross-Enterprise User Assertion *Technical Solution*

- Initial scope to XDS-Registry Stored Query and XDS-Retrieve Document Set
- Relies on Web Services profiling work in progress
- Informed by WS-I Basic Security Profile 1.1
- Use SAML Identity Assertions
- Could leverage PWP Profile
- Define grouping behavior with EUA and ATNA

Cross-Enterprise User Assertion

Actors





Cross-Enterprise User Assertion *Details*

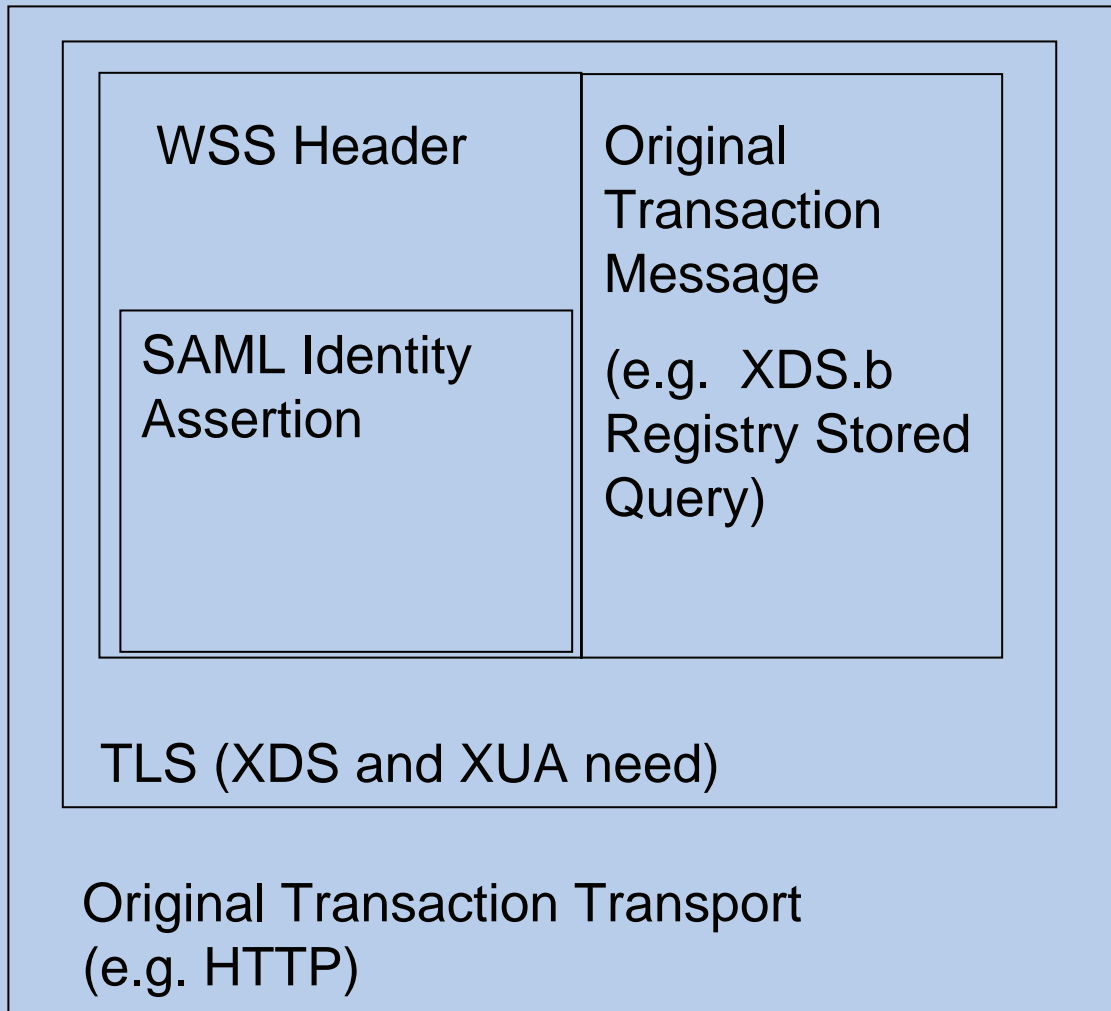
- Scoped to XDS.b Registry Stored Query and XDS.b Retrieve Document Set
- Specifies use Web-Services Security Header
- Employs SAML 2.0 Identity Assertions

Allows other SAML and Web-Services Security mechanisms to be used when both parties have prior agreement



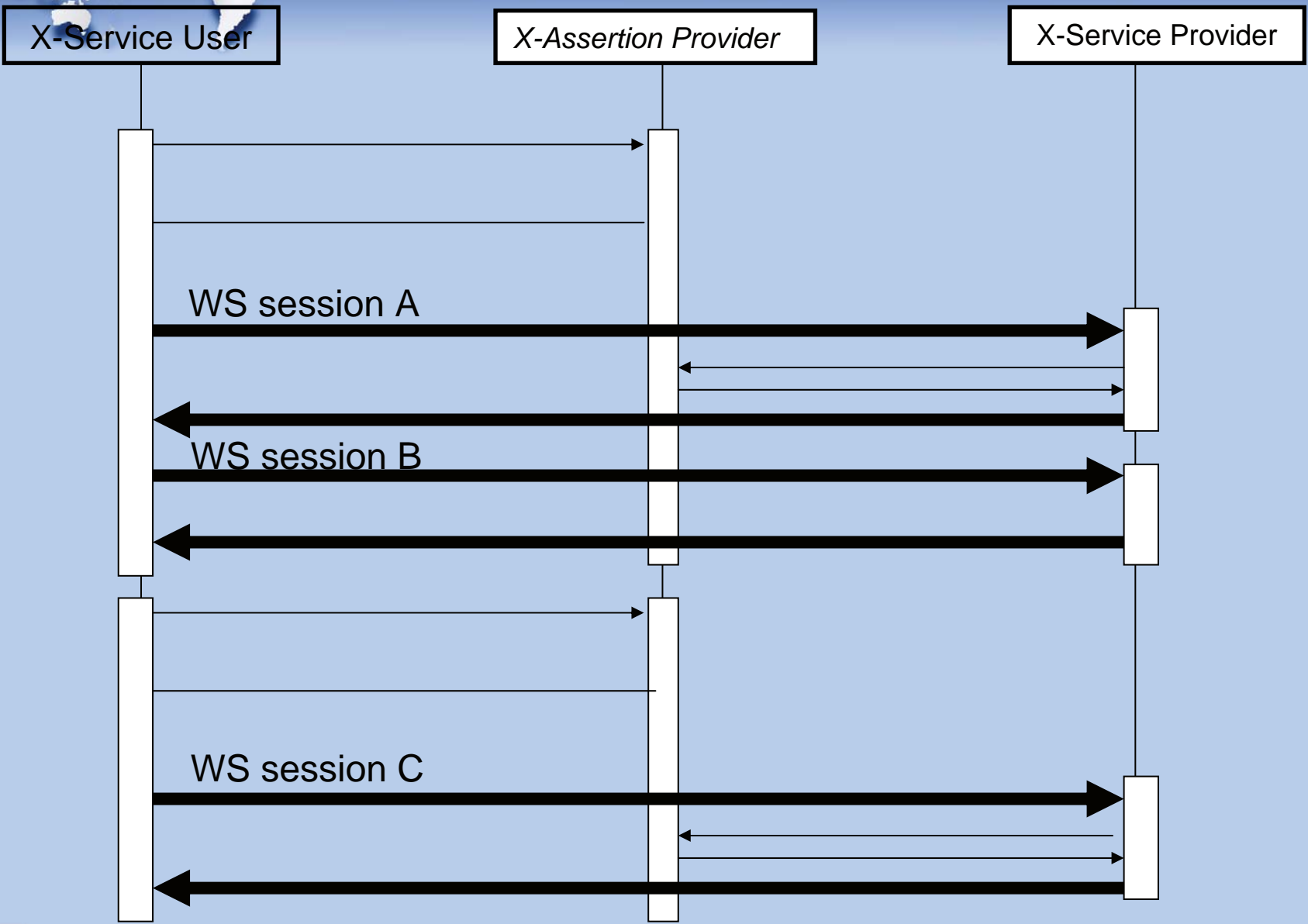
Cross-enterprise User Assertion

SAML encapsulation





XUA: Interaction Diagram





X-Service User

- shall include the OASIS Web Services Security (WSS) Header, and shall include a SAML 2.0 Assertion as the security token.
- The Assertion shall contain a **Subject**. The Subject contains the logical identifier of the principal performing the original service request (person, application, etc.) and remains unchanged through operations acting on the assertion (e.g. proxying the Assertion).
 - The **Subject** shall contain a **SubjectConfirmation** element.
 - The bearer confirmation method shall be supported
- The SAML Assertion **Conditions** are profiled as:
 - **NotBefore** shall be populated with the issue instant of the Assertion
 - **NotOnOrAfter** is not specified by XUA because reasonable time limits are not clear at the IHE Profile level. The Expiration shall be configurable on an Affinity Domain and/or System level.
 - **AudienceRestriction** containing an **Audience** whose value is a URI identifying the relying party (e.g. XDS Registry, XDS Repository). It may contain an Audience whose value is a URI identifying the Affinity Domain.
- The Assertion shall contain a **AuthnStatement** specify the **AuthnContextClassRef** or **AuthnContextDeclRef**
- The Assertion may contain other statements (e.g. Attributes)
- The Assertion shall be signed by the X-Assertion Provider



X-Service Provider

- validate the Identity Assertion by processing the Web-Services Security header in accordance to the Web-Services Security Standard, and SAML 2.0 Standard processing rules.
 - If this validation fails, then the grouped transaction shall be treated as an unauthorized user
- may use standards transactions to communicate with the X-Assertion Provider (e.g., WS-Trust, SAML 2.0 Protocol) to obtain information not included in the assertion provided
- may utilize the identity in access control decisions.
- may ignore any other statements (e.g. Attributes),
- may ignore the one-time-use-condition
- may use the authentication class references to determine the method that was used to authenticate the user.



XUA -- ATNA

- When an ATNA Audit message needs to be generated and the user is authenticated by way of an X-User Assertion, the ATNA Audit message **UserName** element shall record the X-User Assertion using the following encoding:
- **alias<user@issuer>**
 - where:
 - **alias** is the optional string within the SAML Assertion's Subject element SPProvidedID attribute
 - **user** is the required content of the SAML Assertion's Subject element
 - **issuer** is the X-Assertion Provider entity ID contained with the content of SAML Assertion's Issuer element

A stylized world map in shades of blue and white, centered on the Atlantic Ocean, serving as the background for the slide.

Cross-Enterprise User Assertion Questions?

John F. Moehrke

GE Healthcare

IT Infrastructure Technical Committee

