DICOM Correction Item

Correction Number CP-595

Log Summary: Add SAML option to identity negotiation

Type of Modification	Name of Standard
Addition	PS 3.7, 3.15 2006

Rationale for Correction:

The use of SAML is becoming more mature and it is appropriate to add the ability to use it to exchange identity information.

The proposed mechanism will support a wide variety of SAML based identity profiles. OASIS, the Liberty Alliance (and perhaps others) are defining different profiles for different kinds of identity management purposes. All of the profiles that make sense for medical use can be accommodated by the simple exchange of a SAML assertion from the association initiator to the association acceptor, followed by a assertion as part of the association response.

For full interoperability both sides should also agree on the profile that will be used. This CP does not specify any profiles as recommended by DICOM. The selection of recommended protocols may be taken up by DICOM later, or this may be left as outside the scope of DICOM. If communication is attempted between systems that employ different profiles it is unpredictable whether the association will succeed or fail. But the association negotiation will indicate success or failure, and may indicate to the association initiator why it failed, depending upon the rules of the association acceptor's profile.

The encoding of SAML assertions is independent of the profile selection, and there is a single assertion employed for all of the profiles defined to date. Some profiles permit the use of complete self contained assertions (like Kerberos). Some provide data that is confirmed with an identity service, using communications that are separate from the DICOM association. Some include an option to request further information from the user. Those that include the request for further user interactions can be supported only if that additional user interaction is performed separately from the DICOM association. This approach does not provide a means to communicate with the user over the DICOM TCP connection.

This approach does make it difficult to support the profiles that utilize user interactions because the mechanism for this interaction is not specified. This is not expected to be a serious problem because very few (if any) expected DICOM configurations are expected to need a user interaction with the DICOM association acceptor. User identification is expected to be handled using self-contained assertions or artifacts like the Kerberos service ticket, or by means of assertions that are verified using other non-DICOM communications mechanisms.

Sections of documents affected

PS 3.2 7.6

PS 3.7 D.3.3.7

PS 3.15 B.7

Correction Wording:

Amend Section 7 in PS 3.2:

7.6 Security Profiles

DICOM specifies methods for providing security at different levels of the ISO OSI Basic Reference Model through the use of mechanisms specific to a particular layer. The methods for applying these mechanisms are described in the various parts of the DICOM Standard. **Some**~~The~~ mechanisms and algorithms ~~used by those mechanisms~~ are specified in PS 3.15 as Security Profiles. An implementation's Conformance Statement describes which Security Profiles can be used by that application.

Note: For example, the Basic TLS Secure Transport Connection Profile defines a mechanism for authenticating entities participating in the exchange of data, and for protecting the integrity and confidentiality of information during interchange.

An implementation shall list in its Conformance Statement any Security Profiles that it supports, how it selects which Security Profiles it uses, and how it uses features of that Security Profile.

An implementation shall list in its Conformance Statement any additional use of the User Identity association negotiation sub-item that is not specified in a standard Security Profile.

Add to section 2 in Part 7

SAML Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0
OASIS Standard, 15 March 2005

Modify D.3.3.7 in Part 7

The Association-requester conveys in the A-ASSOCIATE request:

- the form of user identity being provided, either a username, username and passcode, ~~or~~ a Kerberos service ticket**, or a SAML assertion**.

Modify Table D.3-14

5	User-Identity-Type	Field value shall be in the range 1 to ~~3~~**4** with the following meanings: 1 – Username as a string in UTF-8 2 – Username as a string in UTF-8 and passcode 3 – Kerberos Service ticket **4 – SAML Assertion** Other values are reserved for future standardization.

Modify Table D.3-15

7-n	Server-response	This field shall contain the Kerberos Server ticket, encoded in accordance with RFC-1510, if the User-Identity-Type value in the A-ASSOCIATE-RQ was 3. **This field shall contain the SAML response if the User-Identity-Type value in the A-ASSOCIATE-RQ was 4** This field shall be zero length if the value of the User-Identity-Type in the A-ASSOCIATE-RQ was 1 or 2.

Add section B.7 to Part 15

B.7 Generic SAML Assertion Identity Negotiation Association Profile

An implementation that supports the Generic SAML Assertion Identity Negotiation Association Profile shall send/accept the User Identity association negotiation sub-item, for User-Identity-Type of 4. If a positive response is requested, the association acceptor implementation shall respond with the association response sub-item containing a SAML response. The SAML Assertion information shall be made available to internal or external authentication systems. The user identity shall be authenticated by means of an authentication system that employs SAML Assertions. If the authentication fails, the association shall be rejected.

The user identity from the Primary-field shall be used within the implementation as the user identification. Such uses include recording user identification in audit messages.

Table B.7-1
Minimum Mechanisms for DICOM Association Negotiation Features

Supported Association Negotiation Feature	Minimum Mechanism
User Identity	SAML Assertion