Status	Final Text
Date of Last Update	2018/03/25
Person Assigned	David Clunie mailto:dclunie@dclunie.com
Submitter Name	David Clunie mailto:dclunie@dclunie.com
Submission Date	2016/08/24

Correction Number CP-1650
Log Summary: Extend User Identity Sub-Item to support web tokens
Name of Standard PS3.7 2018a
Rationale for Correction: Additional methods for communicating access control and authorization are needed, particularly to support bridging between DICOMweb and DICOM message services. The JSON Web Token (JWT) used in HTTP Authorization headers, for example with OAUTH2, is added.
Correction Wording:

Amend DICOM PS3.7 as follows (changes to existing text are bold and ***underlined*** *for additions and* ~~**struckthrough**~~ *for removals):*

2 Normative References

...

RFC-1510 The Kerberos Network Authentication Service (V5)

RFC-2289 A One-Time Password System

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

RFC 6750 The OAuth 2.0 Authorization Framework: Bearer Token Usage https://tools.ietf.org/html/rfc6750

RFC 7519 JSON Web Token (JWT) https://tools.ietf.org/html/rfc7519

...

D.3.3.7 User Identity Negotiation

The User Identity Negotiation is used to notify the association acceptor of the user identity of the association requestor. It may also request that the association acceptor respond with the server identity. This negotiation is optional. If this sub-item is not present in the A-ASSOCIATE request the A-ASSOCIATE response shall not contain a user identity response sub-item.

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

- the form of user identity being provided, either a username, username and passcode, a Kerberos service ticket, ~~**or**~~ a SAML assertion**, or a JSON Web Token (JWT)**.
- an indication whether a positive server response is requested.

The Association-acceptor does not provide an A-ASSOCIATE response unless a positive response is requested and user authentication succeeded. If a positive response was requested, the A-ASSOCIATE response shall contain a User Identity sub-item. If a Kerberos ticket is used the response shall include a Kerberos server ticket.

Since a system may ignore request sub-items, the positive response must be requested if the association requestor requires confirmation. If the association acceptor does not support user identification it will accept the association without making a positive response. The association requestor can then decide whether to proceed.

The association acceptor may utilize the User Identity information provided during the association negotiation to populate the user information fields in DICOM audit trail messages. The association acceptor may utilize the User Identity information provided during the association negotiation to perform authorization controls during the performance of other DIMSE transactions on the same association. The user identity information may also be used to modify the performance of DIMSE transactions for other purposes, such as workflow optimizations.

Note

1. User identity authorization controls may be simple "allow/disallow" rules, or they can be more complex scoping rules. For example, a query could be constrained to apply only to return information about patients that are associated with the identified user. The issues surrounding authorization controls can become very complex. The User Identity SOP conveys user identity to support uses such as authorization controls and audit controls. It does not specify their behavior.
2. The option to include a passcode along with the user identity enables a variety of non-Kerberos secure interfaces. Sending passwords in the clear is insecure, but there are single use password systems such as RFC-2289 and the various smart tokens that do not require protection. The password might also be protected by TLS or other mechanisms.
3. **For JSON Web Tokens (JWTs), RFC 7519 specifies minimal requirements for encryption, MAC and signature algorithms; others may be supported as described in the DICOM Conformance Statement. The encoded format in the Primary-field of the A-ASSOCIATE-RQ is the same as what might be included in an HTTP Authorization: Bearer header field per RFC 6750 when accessing a Protected Resource on a Resource Server, to facilitate bridging between PS3.18 Web Services and PS3.7 Message Exchange implementations.**

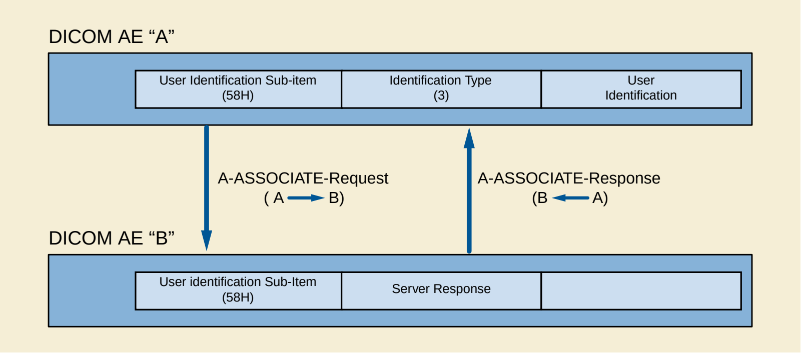
DICOM AE "A"
User Identification Sub-item (58H)
Identification Type (3)
User Identification
A-ASSOCIATE-Request (A → B)
A-ASSOCIATE-Response (B ← A)
DICOM AE "B"
User identification Sub-Item (58H)
Server Response

Figure D.3-8. User Identity Negotiation (With Server Positive Response Requested)

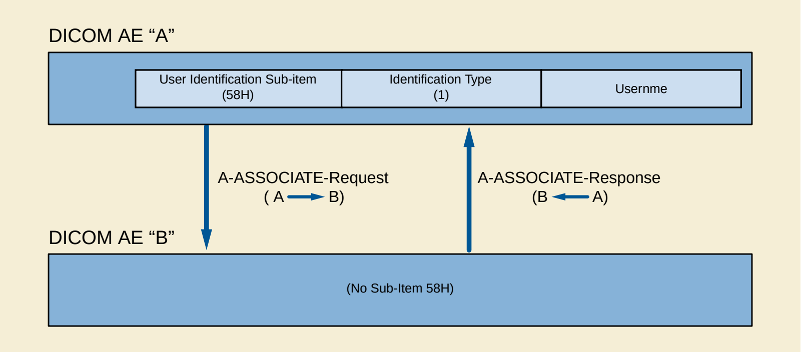
DICOM AE "A"
User Identification Sub-item (58H)
Identification Type (1)
Usernme
A-ASSOCIATE-Request (A → B)
A-ASSOCIATE-Response (B ← A)
DICOM AE "B"
(No Sub-Item 58H)

Figure D.3-9. User Identity Negotiation (Application Entity "A" Provides Username Identity)

D.3.3.7.1 User Identity Sub-Item Structure (A-ASSOCIATE-RQ)

The User Identity Negotiation Sub-Item shall be made of a sequence of mandatory fixed and variable length fields. This Sub-Item is optional and if supported, only one User Identity Negotiation Sub-Item shall be present in the User Data Item of the A-ASSOCIATE-RQ. Table D.3-14 shows the sequence of the mandatory fields.

Table D.3-14. User Identity Negotiation Sub-Item Fields (A-ASSOCIATE-RQ)

Item Bytes	Field Name	Description of Field
1	Item-type	58H
2	Reserved	This reserved field shall be sent with a value 00H but not tested to this value when received.
3 - 4	Item-length	This Item-length shall be the number of bytes from the first byte of the following field to the last byte of the last field sent. It shall be encoded as an unsigned binary number.

Item Bytes	Field Name	Description of Field
5	User-Identity-Type	Field value shall be in the range 1 to 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 **5 - JSON Web Token (JWT)** Other values are reserved for future standardization.
6	Positive-response-requested	Field value: 0 - no response requested 1 - positive response requested
7-8	Primary-field-length	The User-Identity-Length shall contain the length of the User-Identity value.
9-n	Primary-field	This field shall convey the user identity, either the username as a series of characters, or the Kerberos Service ticket encoded in accordance with RFC-1510**, or the JWT encoded in accordance with RFC 7519 using base64url encoded parts**.
n+1-n+2	Secondary-field-length	This field shall be non-zero only if User-Identity-Type has the value 2. It shall contain the length of the secondary-field.
n+3-m	Secondary-field	This field shall be present only if User-Identity-Type has the value 2. It shall contain the Passcode value.

D.3.3.7.2 User Identity Sub-Item Structure (A-ASSOCIATE-AC)

The User Identity Sub-Item shall be made of a sequence of mandatory fixed and variable length fields. This Sub-Item is optional and if supported, only one User Identity Sub-Item shall be present in the User Data Item of the A-ASSOCIATE-AC. Table D.3-15 shows the sequence of the mandatory fields.

Table D.3-15. User Identity Negotiation Sub-Item Fields (A-ASSOCIATE-AC)

Item Bytes	Field Name	Description of Field
1	Item-type	59H
2	Reserved	This reserved field shall be sent with a value 00H but not tested to this value when received.
3 - 4	Item-length	This Item-length shall be the number of bytes from the first byte of the following field to the last byte of the final field. It shall be encoded as an unsigned binary number.
5-6	Server-response-length	This field shall contain the number of bytes in the Server-response. May be zero.
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.

If the Association-Requestor has requested a positive acknowledgment, the Server-response shall be returned with the Kerberos Server ticket when User-Identity-Type is Kerberos Service ticket (3).

D.3.3.7.3 User Identity Rejection

The association acceptor may utilize the username or username and passcode information to determine whether the user is permitted to establish an association. If the Kerberos mechanism is chosen, the association acceptor shall utilize the Kerberos service ticket to determine whether the user is permitted to establish an association.

If the association acceptor rejects the association because of an authorization failure, the rejection shall be indicated to be rejected-permanent (see ????). The source shall be value (2) "DICOM UL service provided (ACSE related function) ". The rejection is indicated to be rejected-permanent because retries with the same user identity fields will continue to be rejected. A different and valid username, username and passcode, or Kerberos ticket must be provided.

This standard does not define how the association acceptor performs authentication or what rules apply to this authentication.