DICOM Correction Proposal

STATUS	Letter Ballot
Date of Last Update	2024/08/24
Person Assigned	
Submitter Name	rjhorniii@gmail.com
Submission Date	2024/03/11

Correction Number CP-2405
Log Summary: Add note clarifying DIMSE JWT and DICOMweb access token can be the same
Name of Standard PS3.2, PS3.7
Rationale for Correction: WG14 discussion has confirmed that the JWT form of User Identity Negotiation can convey the same tokens as are used for HTTP access tokens in a DICOMWeb header. A proxy application may choose to use the same token contents with the same meaning in both. The specific trust model and method, e.g., OAuth, is not specified by DICOM. Both DICOM DIMSE and DICOMWeb implementations are free to choose different trust models and methods. If they both choose the same model and chose to use the DIMSE User Identification as equivalent to DICOMWeb access tokens, the JWT token and the HTTP access token can be the same. Since DICOM does not specify the trust model and methods, this equivalence can only be determined in the context of specific implementation and deployment choices. This CP adds notes to that effect to the DIMSE User Identity negotiation and the DICOMWeb HTTP headers sections. Also, it notes that these tokens must not be revealed as part of logs or any unprotected files or transactions. Where user identity is needed, as in logs, a service such as the OAuth Introspection service might be used to obtain user identity information associated with a token. WG-06 question: Should the notes in part 7 be moved to be after the table D.3-14 rather than in the text in D.3.3.7? They were not found in early review reading because we expected them to be after the table. They apply to specific aspects of fields described in the table.
Correction Wording:

Add notes to PS 3.7, section D.3.3.7 User Identity Negotiation

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 SOPconveys 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 "PS3.18" and PS3.7 "PS3.7" implementations.~~ **If the same trust mechanisms are used by both the DIMSE SCP and the Resource Server, the contents of the Primary-field can be the same as the value of the HTTP Authorization: Bearer field, avoiding the need to perform a conversion of the contents.**

4. **Care should be taken to not include unnecessary protected content from the User Identity Negotiation into audit log messages. For example, the password, SAML Assertion, and JSON Web Token (JWT) could be disclosed if included in a log message. A service such as the OAuth Introspection Service (See RFC7662 OAuth 2.0 Token Introspection) might be needed to obtain unprotected user identity information from a SAML Assertion or JWT.**

Add notes to PS 3.2, section N.8.6 Web Services Security Features

N.8.6 Web Services Security Features

[Describe in this section the security mechanisms utilized by the implementation. In particular (but not limited to), consider:

• Audit control mechanism used

• Access authorizing policy **and method, including details regarding trust methods, e.g,, use of OAuth, use of access tokens, etc.**

• Personal authentication mechanisms