DICOM Correction Proposal

STATUS	Final Text
Date of Last Update	2025/03/30
Person Assigned	Robert Horn <rjhorniii@gmail.com>
Submitter Name	Robert Horn <rjhorniii@gmail.com>
Submission Date	2023/08/28

Correction Number CP-2340
Log Summary: Specify DICOMWeb security for conformance
Name of Standard PS3.2 2025a
Rationale for Correction: Add specific request for information on use of tokens, URI, and other methods of access, authentication, and authorization for DICOMWeb.

Modify PS3.2 section N.8.6

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*
  - ***Use of HTTP headers such as "Authorization: Bearer"***
  - ***Support for specific publicly defined profiles***
- *Personal authentication mechanisms*
  - ***Use of authentication mechanisms such as OpenID***
  - ***Support for specific publicly defined profiles***
- *De-identification management*
- *~~Certification~~ **Certificate** management tools and process*
- *Web server attack handling*
- ***Credentials Storage Protection (for tokens, assertions, etc.)***
- ***Provisioning, Deprovisioning, Load balancing, Failover, etc. support***
- ***Cross site authorization systems such as Cross-Origin Resource Sharing (CORS)***

These descriptions may be just a reference to another section of the Conformance Statement if these mechanisms are common with DICOM networking services described before or may contain references to other relevant documentation.]