

DICOM Correction Proposal

| | |
|---------------------|--|
| STATUS | Final Text |
| Date of Last Update | 2014/01/02 |
| Person Assigned | Andrei Leontiev (andrei.leontiev@ge.com) |
| Submitter Name | Harry Solomon |
| Submission Date | 2013/05/04 |

| | |
|---|---------|
| Correction Number | CP-1309 |
| Log Summary: Correct references to other standards | |
| Name of Standard PS 3.3 2011 | |
| Rationale for Correction Editorial corrections to Section 3 <ul style="list-style-type: none">• delete text in 3.1 duplicative with 3.14• correct reference in 3.9• correct item numbering in 3.14 | |
| Correction Wording: | |

3.1 REFERENCE MODEL DEFINITIONS

This Part of the Standard is based on the concepts developed in ISO 7498-1 and makes use of the following terms defined in it:

- a. Application Entity
- b. Service or Layer Service

~~This Part of the Standard makes use of the following terms defined in ISO 7498-2:~~

~~a. Data Confidentiality~~

~~Note: The definition is “the property that information is not made available or disclosed to unauthorized individuals, entities or processes.”~~

~~b. Data Origin Authentication~~

~~Note: The definition is “the corroboration that the source of data received is as claimed.”~~

~~c. Data Integrity~~

~~Note: The definition is “the property that data has not been altered or destroyed in an unauthorized manner.”~~

~~d. Key Management~~

~~Note: The definition is “the generation, storage, distribution, deletion, archiving and application of keys in accordance with a security policy.”~~

...

3.9 CHARACTER HANDLING DEFINITIONS

This part of the standard makes use of the following terms defined in ISO/IEC ~~2011~~2022:1994:

- a. Coded character set; code.
- b. Code extension;
- c. Escape sequence.

...

3.14 REFERENCE MODEL SECURITY ARCHITECTURE DEFINITIONS

This Part of the Standard makes use of the following terms defined in ISO 7498-2:

- a. Digital Signature

Note: The definition is “Data appended to, or a cryptographic transformation of, a data unit that allows a recipient of the data unit to prove the source and integrity of that unit and protect against forgery e.g. by the recipient.”

- ~~a.~~b. Data Confidentiality

Note: The definition is “the property that information is not made available or disclosed to unauthorized individuals, entities or processes.”

- ~~b.~~c. Data Origin Authentication

Note: The definition is “the corroboration that the source of data received is as claimed.”

- ~~c.~~d. Data Integrity

Note: The definition is “the property that data has not been altered or destroyed in an unauthorized manner.”

- ~~d.~~e. Key Management

Note: The definition is “the generation, storage, distribution, deletion, archiving and application of keys in accordance with a security policy.”