DICOM Change Proposal

STATUS	Assigned
Date of Last Update	2026/05/28
Person Assigned	steven.nichols@gehealthcare.com
Submitter Name	Alexander Zhang, alexander.zhang@philips.com
Submission Date	2026/02/09

Change Number CP-2614
Log Summary: Update SYSLOG-TLS profile to reference RFC 9662
Name of Standard PS3.2, PS3.15
Rationale for Change: RFC 9662 updates the cipher suite requirements for secure syslog over TLS and DTLS by updating RFC 5425 and RFC 6012. It does not define a separate audit message transport. Therefore, this CP retains RFC 5425 as the normative basis for the SYSLOG-TLS Audit Trail Message Transmission Profile and references RFC 9662 as the applicable update to cipher suite requirements. This preserves compatibility with existing DICOM SYSLOG-TLS implementations while enabling implementations to align with current IETF secure syslog guidance. Notes: • An earlier version of this Change Proposal included the addition of a SYSLOG-DTLS Audit Trail Message Transmission Profile based on RFC 6012. Based on WG-14 feedback, this functionality has been removed to limit the scope of this CP to updates required for alignment with RFC 9662. • IHE ITI is developing a corresponding Change Proposal for the ATNA profile: https://docs.google.com/document/d/1kRU1JU5UV3QNRvrPSn2E_nNj16Ip7MFU/
Change Wording:

Update PS3.2, Section N.11.2.3 A.C.2.3 Audit Trail Message Transmission Profile - SYSLOG – TLS as indicated below:

N.11.2.3 A.C.2.3 Audit Trail Message Transmission Profile - SYSLOG - TLS

See Section N.6.6 Audit Trail Syslog Configuration for information about Syslog-TLS parameters.

[Describe whether the implementation supports SYSLOG-TLS using [RFC 5425] or using [RFC 5425] with the updates specified in [RFC 9662].]

Update PS3.15, Section 2 Normative References as indicated below:

2 Normative References

…

[RFC 5425] IETF. Transport Layer Security (TLS) Transport Mapping for Syslog. http://www.rfc-editor.org/info/rfc5425 .

[RFC 9662] IETF. Updates to the Cipher Suites in Secure Syslog. https://www.rfc-editor.org/info/rfc9662 .

Update PS3.15, Section A.6 Audit Trail Message Transmission Profile - SYSLOG-TLS as follows:

A.6 Audit Trail Message Transmission Profile - SYSLOG-TLS

This profile defines the transmission of audit trail messages. [RFC 5425] provides the mechanisms for reliable transport, buffering, acknowledgement, authentication, identification, and encryption **for syslog messages over TLS**. ~~**[RFC 5424] states that the TLS used MUST be TLS version 1.2 [RFC 9662] updates [RFC 5425]. For this DICOM profile TLS MUST be used, and version 1.2 or later is RECOMMENDED.**~~

Note

The words MUST and RECOMMENDED are used in accordance with the IETF specification for normative requirements.

Any implementation that claims conformance to this profile shall also conform to the Audit Trail Message Format Profile. XML audit trail messages created using the format defined in Audit Trail Message Format Profile shall be transmitted to a collection point using the syslog over TLS mechanism, defined in [RFC 5425]**. Implementations may claim conformance to the SYSLOG-TLS profile by implementing [RFC 5425]. Implementations may additionally claim support for the updates specified in [RFC 9662].** Systems that comply with this profile shall support message sizes of at least 32768 octets.

The Basic DICOM Media Security Profile allows encapsulation of a DICOM File into a Secure DICOM File such that the following aspects of security are addressed:

- confidentiality,
- integrity,
- data origin authentication (optional).

Note

1. *Audit messages for other purposes may also be transferred on the same syslog connection. These messages might not conform to the Audit Trail Message Format.*
2. [RFC 5425] specifies mandatory support for 2KB messages, strongly recommends support for at least 8KB, and does not restrict the maximum size.
3. *When a received message is longer than the receiving application supports, the message might be discarded or truncated. The sending application will not be notified.*

The XML audit trail message shall be inserted into the MSG portion of the SYSLOG-MSG element of the syslog message as defined in [RFC 5424]. The XML audit message may contain Unicode characters that are encoded using the UTF-8 encoding rules.

Note

UTF-8 avoids utilizing the control characters that are reserved by the syslog protocol, but a system that is not prepared for UTF-8 may not be able to display these messages correctly.

The PRI field shall be set using the facility value of 10 (security/authorization messages). Most messages should have the severity value of 5 (normal but significant), although applications may choose other values if that is appropriate to the more detailed information in the audit message. This means that for most audit messages the PRI field will contain the value "<85>".

The MSGID field in the HEADER of the SYSLOG-MSG shall be set. The value "DICOM+RFC3881" may be used for messages that comply with this profile.

The MSG field of the SYSLOG-MSG shall be present and shall be an XML structure following the DICOM Audit Message Schema (see Section A.5.1).

The syslog message shall be created and transmitted as described in [RFC 5424].

Any implementation that claims conformance to this Security Profile shall describe in its conformance statement:

a. Any configuration parameters relevant to [RFC 5424]**,** ~~and~~ [RFC 5425]**, and, where applicable, support for the updates specified in [RFC 9662].**

b. Any STRUCTURED-DATA that is generated or processed.

c. Any implementation schema or message element extensions for the audit messages.

d. The maximum size of messages that can be sent or received.