NEMA Standards Publication PS 3 Supplement 31

Digital Imaging and Communications in Medicine (DICOM)
Security Enhancements One

This is a draft document. Do not circulate, quote, or reproduce it except with the approval of NEMA

Please send comments to Dave Snavely, NEMA (dav_snavely@nema.org)

Status: Final Text – 18th February 2000

Prepared by

DICOM Standards Committee
1300 N. 17th Street, Suite 1847
Rosslyn, Virginia 22209 USA

© 1997, 1998, 1999, 2000 by National Electrical Manufacturers Association

Table of Contents

Foreword

While it is possible for a site to enact some security precautions to protect DICOM data, DICOM has not defined any truly interoperable features to allow sites to exchange DICOM messages and objects in a secure fashion. This supplement is the first attempt to endow DICOM with a limited set of features that facilitate the secure exchange of data between sites. This first set of features is not intended to provide comprehensive security in DICOM environments, since comprehensive security requires site guidelines and policies that are beyond the scope of the DICOM Standard. More comprehensive security might also require other considerations within DICOM that are not covered by this supplement. However, this supplement is a first step toward a more comprehensive secure environment within which DICOM could operate. Enhancements to or possibly even replacements for these mechanisms are expected in future versions as clinical needs are identified, as other related standards evolve, and as technology advances.

This supplement only addresses the following aspects of security:

- Authentication – verifying the identity of entities involved in an operation
- Confidentiality – guarding the data from disclosure to an entity which is not a party to the transaction
- Data Integrity – verifying that data within an object has not been altered or removed

Covering other security aspects requires a more comprehensive security policy.

The authentication is done by verification through a secure handshake protocol of the entities involved in the interchange of SOP Instances. This secure handshake would be done during the establishment of a network Association for network interchanges. During the secure handshake protocol, the entities involved in a network Association identify an encryption protocol and exchange session keys to be used during the Association. Entities then use end to end encryption of the data with the session keys to guard the confidentiality of the data while it traverses the communications links. The encryption protocols used for network interchange might also include a MAC or secure hash to further guard the integrity of the data. Guarding the confidentiality of data stored within an entity (e.g. workstation), though needed for more complete security, is implementation dependent and outside the scope of this Standard.

This supplement adds information to PS 3.8 on layering the DIMSE services on top of a secure transport protocol. This supplement adds sections to PS 3.2 and a new Part to this standard that holds Security Profiles that are used to specify mechanisms and algorithms for providing security. Implementations may claim conformance to one or more Security Profiles. This supplement also adds new status flag Attributes to PS 3.3 and PS 3.6.

SCOPE

The Standard initially considers only the interactive interchange of DICOM objects between application entities in a confidential fashion with facilities to ascertain the integrity of the data during transmission and to authenticate the identity of the single parties involved in network exchanges. Conformance to any of the Security Profiles is optional.

This supplement does not address integrity checks (e.g. digital signatures) embedded directly in DICOM SOP Instances. Such integrity checks may be the topic of future security supplements to DICOM.

The standard does not address “store and forward” or media storage interchanges. “Store and forward” interchanges are where data objects are directed toward intended recipients, and only those recipients should be allowed to view the objects. Such interchanges may be considered in future versions.

The standard does not address issues of security policies, though clearly adherence to appropriate security policies is necessary for any level of security. The standard only provides mechanisms that could be used to implement security policies with regard to the interchange of DICOM objects between Application Entities. For example, a security policy may dictate some level of access control. This Standard would not consider access control policies, but would provide means for the Application Entities involved to exchange sufficient information to implement access control policies.

Wherever possible this Standard utilizes commonly available mechanisms rather than attempt to define DICOM specific mechanisms. The primary reason is to allow faster development and implementation of the Standard. By using existing mechanisms and standards this Standard leverages the knowledge and expertise of those working intimately in the security field. This Standard primarily selects available mechanisms and dictates how they may be applied within DICOM.

The initial focus of this Standard is a short-term solution that can be implemented with existing tools. Since security mechanisms are still maturing, these short-term solutions may be replaced by more appropriate solutions in the future.

PROPOSAL

In network transactions, the standard proposes DICOM Upper Layer Services layered on top of a secure Transport Connection as a means for Application Entities to negotiate or create a trusted communication channel between themselves. The proposed secure Transport Connections provides options for Application Entities to authenticate each other, to check the integrity of messages exchanged, and to encrypt messages for confidentiality. The secure Transport Connections may not provide the level of detail about users that DICOM Application Entities might need for access control, though it may be sufficient for a rudimentary first pass attempt. What information to exchange for access control and how to exchange it is yet to be determined. Such control may be needed by a broader range of applications than just DICOM, and some have suggested that we work with other organizations to specify this access control information.

Several options for security in storage media or “store and forward’ (i.e., messages intended for particular recipients) applications have been discussed, but are not included in this proposal. One could extend the file meta header or DICOM services with additional information for authenticating the source of the file, identifying the intended recipient, and exchanging secret keys which would be used to encrypt and decrypt the DICOM object. Essentially, this could be a TLS-like corollary, just as the file meta header itself is a corollary to the DICOM services. Others have suggested that the DICOM file could just be encapsulated in a secure EDI document (e.g. encrypted with S-MIME or PGP). The later option is being considered by HL7 and other standards committees.

Item 0.1 Add the following new part reference to all parts of PS 3

PS 3.15: Security Profiles

Additions to PS 3.2

Item 1.1 Add the following definitions to Section 3

3.11.11 Security Profile: a mechanism for selecting an appropriate set of choices from the Parts of DICOM along with corresponding security mechanisms (e.g. encryption algorithms) for the support of security facilities.

Item 1.2 Add the following to the conformance requirements in Section 7

7.5 SECURITY PROFILES

DICOM specifies methods for providing security at different levels of the ISO OSI Basic Reference Model through the use of mechanisms specific to a particular layer. The methods for applying these mechanisms are described in the various parts of the DICOM Standard. The mechanisms and algorithms used by those mechanisms are specified in PS 3.15 as Security Profiles. An implementation’s Conformance Statement describes which Security Profiles can be used by that application.

Note: For example, the Basic TLS Secure Transport Connection Profile defines a mechanism for authenticating entities participating in the exchange of data, and for protecting the integrity and confidentiality of information during interchange.

An implementation shall list in its Conformance Statement any Security Profiles that it supports, how it selects which Security Profiles it uses, and how it uses features of that Security Profile.

Item 1.3 Add the following to the network conformance statement template in Annex A

A.8 SECURITY PROFILES

Any support for Security profiles shall be described here.

Item 1.4 Add the following the media conformance statement template in Annex C

C.8 SECURITY PROFILES

Any support for Security profiles shall be described here.

Additions To PS 3.3

2 *Item 2.1 Add the following rows to Table C.12-1 sop common module attributes*

Attribute Name	Tag	Type	Attribute Description
SOP Instance Status	(0100,0410)	3	A flag that indicates the storage status of the SOP Instance. Not Specified (NS) implies that this SOP Instance has no special storage status, and hence no special actions need be taken. Original (OR) implies that this is the primary SOP instance for the purpose of storage, but that it has not yet been authorized for diagnostic use. Authorized Original (AO) implies that this is the primary SOP instance for the purpose of storage, which has been authorized for diagnostic use. Any copies of an Authorized Original should be given the status of Authorized Copy. Authorized Copy (AC) implies that this is a copy of an Authorized Original SOP Instance. Enumerated Values: NS, OR, AO, AC Note: Proper use of these flags is specified in Security Profiles. Implementations that do not conform to such Security Profiles may not necessarily handle these flags properly.
SOP Authorization Date and Time	(0100,0420)	3	The date and time when the SOP Instance Status (0100,0410) was set to AO.
SOP Authorization Comment	(0100,0424)	3	Any comments associated with the setting of the SOP Instance Status (0100,0410) to AO.
Authorization Equipment Certification Number	(0100,0426)	3	The certification number issued to the Application Entity that set the SOP Instance Status (0100,0410) to AO.

Additions to PS 3.6

Item 3.1 Add the following rows to the table in section 6

Tag	Name	VR	VM
(0100,0410)	SOP Instance Status	CS	1
(0100,0420)	SOP Authorization Date and Time	DT	1
(0100,0424)	SOP Authorization Comment	LT	1
(0100,0426)	Authorization Equipment Certification Number	LO	1

Additions to PS 3.8

Item 4.1 Add the following to the end of section 9.1.1

Application Entities may also choose to access the TCP Transport Services via a Secure Transport Connection. The nature of this Secure Transport Connection is specified through Security Profiles (see PS 3.15). Security Profiles select minimum mechanisms needed to support that profile. Other mechanisms may also be used if agreed to during establishment of the Secure Transport Connection.

Notes: 1. DICOM does not specify how a secure transport connection is established, or the significance of any certificates exchanged during peer entity authentication. These issues are left up to the application, which is assumed to be following some security policy. Once the application has established a secure Transport Connection, then an Upper Layer Association can use that secure channel.

2. There may be an interaction between PDU size and record size of the secure Transport Connection that impacts efficiency of transport.

3. Registered ports for Secure Transport Connections are defined in PS3.15.

Part 15 -- Security Profiles

Item 5.1 Add a new Part (Part 15) to hold Security Profiles

FOREWORD

The American College of Radiology (ACR) and the National Electrical Manufacturers Association (NEMA) formed a joint committee to develop a standard for Digital Imaging and Communications in Medicine (DICOM). This DICOM Standard was developed according to the NEMA procedures.

This standard is developed in liaison with other standardization organizations including CEN TC251 in Europe, and JIRA and MEDIS-DC in Japan, with review also by other organizations including IEEE, HL7 and ANSI in the USA.

The DICOM Standard is structured as a multi-part document using the guidelines established in the following document:

¾ ISO/IEC Directives, 1989 Part 3 : Drafting and Presentation of International Standards.

This document is one part of the DICOM Standard, which consists of the following parts:

PS 3.1: Introduction and Overview

PS 3.2: Conformance

PS 3.3: Information Object Definitions

PS 3.4: Service Class Specifications

PS 3.5: Data Structures and Encoding

PS 3.6: Data Dictionary

PS 3.7: Message Exchange

PS 3.8: Network Communication Support for Message Exchange

PS 3.9: Point-to-Point Communication Support for Message Exchange

PS 3.10: Media Storage and File Format for Media Interchange

PS 3.11: Media Storage Application Profiles

PS 3.12: Formats and Physical Media

PS 3.13: Print Management Point-to-Point Communication Support

PS 3.14: Grayscale Standard Display Function

PS 3.15: Security Profiles

These parts are related but independent documents. Their development level and approval status may differ. Additional parts may be added to this multi-part standard. PS 3.1 should be used as the base reference for the current parts of this standard.

1 Scope and field of application

This part of the DICOM Standard specifies Security Profiles to which implementations may claim conformance.

The DICOM standard does not address issues of security policies, though clearly adherence to appropriate security policies is necessary for any level of security. The standard only provides mechanisms that could be used to implement security policies with regard to the interchange of DICOM objects between Application Entities. For example, a security policy may dictate some level of access control. This Standard does not consider access control policies, but does provide the technological means for the Application Entities involved to exchange sufficient information to implement access control policies.

This Standard assumes that the Application Entities involved in a DICOM interchange are implementing appropriate security policies, including, but not limited to access control, audit trails, physical protection, maintaining the confidentiality and integrity of data, and mechanisms to identify users and their rights to access data. Essentially, each Application Entity must insure that their own local environment is secure before even attempting secure communications with other Application Entities.

When Application Entities agree to interchange information via DICOM through association negotiation, they are essentially agreeing to some level of trust in the other Application Entities. Primarily Application Entities trust that their communication partners will maintain the confidentiality and integrity of data under their control. Of course that level of trust may be dictated by local security and access control policies.

Application Entities may not trust the communications channel by which they communicate with other Application Entities. Thus, this Standard provides mechanisms for Application Entities to securely authenticate each other, to detect any tampering with or alteration of messages exchanged, and to protect the confidentiality of those messages while traversing the communications channel. Application Entities can optionally utilize any of these mechanisms, depending on the level of trust they place in the communications channel.

This Standard assumes that Application Entities can securely identify local users of the Application Entity, and that user’s roles or licenses. Note that users may be persons, or may be abstract entities, such as organizations or pieces of equipment. When Application Entities agree to an exchange of information via DICOM, they may also exchange information about the users of the Application Entity via the Certificates exchanged in setting up the secure channel. The Application Entity may then consider the information contained in the Certificates about the users, whether local or remote, in implementing an access control policy or in generating audit trails.

This Standard also assumes that Application Entities have means to determine whether or not the “owners” (e.g. patient, institution) of information have authorized particular users, or classes of users to access information. This Standard further assumes that such authorization might be considered in the access control provided by the Application Entity. At this time, this Standard does not consider how such authorization might be communicated between Application Entities, though that may be a topic for consideration at some future date.

This Standard also assumes that an Application Entity using TLS has secure access to or can securely obtain X.509 key Certificates for the users of the application entity. In addition, this standard assumes that an Application Entity has the means to validate an X.509 certificate that it receives. The validation mechanism may use locally administered authorities, publicly available authorities, or some trusted third party.

This Standard assumes that an Application Entity using ISCL has access to an appropriate key management and distribution system (e.g. smartcards). The nature and use of such a key management and distribution system is beyond the scope of DICOM, though it may be part of the security policies used at particular sites.

2 Normative references

The following standards contain provisions that, through reference in this text, constitute provisions of this Standard. At the time of publication, the editions indicated were valid. All standards are subject to revision, and parties to agreements based on this Standard are encouraged to investigate the possibilities of applying the most recent editions of the standards indicated below.

ECMA 2335, The ECMA GSS-API Mechanism

ISO/IEC Directives, 1989 Part 3 - Drafting and Presentation of International Standards

ISO 7498-1, Information Processing Systems - Open Systems Interconnection - Basic Reference Model

ISO 7498-2, Information processing systems – Open Systems Interconnection – Basic reference Model – Part 2: Security Architecture

ISO/TR 8509, Information Processing Systems - Open Systems Interconnection - Service Conventions

ISO 8649:1987, Information Processing Systems - Open Systems Interconnection - Service Definition for the Association Control Service Element

RFC 2246, Transport Layer Security (TLS) 1.0 Internet Engineering Task Force

Note: TLS is derived from SSL 3.0, and is largely compatible with it.

Integrated Secure Communication Layer V1.00 MEDIS-DC

3 Definitions

For the purposes of this Standard the following definitions apply.

3.1 REFERENCE MODEL DEFINITIONS

This part of the Standard makes use of the following terms defined in ISO 7498-1:

a. Application Entity
b. Protocol Data Unit or Layer Protocol Data Unit
c. Transport Connection

3.2 REFERENCE MODEL SECURITY ARCHITECTURE DEFINITIONS

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.”

3.3 ACSE SERVICE DEFINITIONS

This part of the Standard makes use of the following terms defined in ISO 8649:

a. Association or Application Association

3.4 SECURITY DEFINITIONS

This Part of the Standard makes use of the following terms defined in ECMA 235:

a. Security Context

Note: The definition is “security information that represents, or will represent a Security Association to an initiator or acceptor that has formed, or is attempting to form such an association.”

3.5 DICOM INTRODUCTION AND OVERVIEW DEFINITIONS

This Part of the Standard makes use of the following terms defined in PS 3.1:

a. Attribute

3.6 DICOM CONFORMANCE DEFINITIONS

This Part of the Standard makes use of the following terms defined in PS 3.2:

a. Security Profile

3.7 DICOM INFORMATION OBJECT DEFINITIONS

This Part of the Standard makes use of the following terms defined in PS 3.3:

a. Module

3.8 DICOM SERVICE CLASS DEFINITIONS

This Part of the Standard makes use of the following terms defined in PS 3.4:

a. Service Class
b. Service-Object Pair (SOP) Instance

3.9 DICOM COMMUNICATION SUPPORT DEFINITIONS

This Part of the Standard makes use of the following terms defined in PS 3.8:

a. DICOM Upper Layer

3.10 DICOM SECURITY PROFILE DEFINITIONS

The following definitions are commonly used in this Part of the DICOM Standard:

Secure Transport Connection: a Transport Connection that provides some level of protection against tampering, eavesdropping, masquerading.

4 Symbols and abbreviations

The following symbols and abbreviations are used in this Part of the Standard.

ACR	American College of Radiology
AE	Application Entity
ANSI	American National Standards Institute
CEN TC251	Comite European de Normalisation-Technical Committee 251-Medical Informatics
CBC	Cipher Block Chaining
CCIR	Consultative Committee, International Radio
DES	Data Encryption Standard
DICOM	Digital Imaging and Communications in Medicine
ECMA	European Computer Manufacturers Association
EDE	Encrypt-Decrypt-Encrypt
HL7	Health Level 7
IEEE	Institute of Electrical and Electronics Engineers
IEC	International Electrical Commission
IOD	Information Object Definition
ISCL	Integrated Secure Communication Layer
ISO	International Standards Organization

JIRA	Japan Industries association of RAdiological systems
MAC	Message Authentication Code
MD-5	Message Digest - 5
MEDIS-DC	Medical Information System Development Center
NEMA	National Electrical Manufacturers Association
PDU	Protocol Data Unit
RSA	Rivest-Shamir-Adleman
SCP	Service Class Provider
SCU	Service Class User
SHA	Secure Hash Algorithm
SOP	Service-Object Pair
SSL	Secure Sockets Layer
TLS	Transport Layer Security
UID	Unique Identifier

5 Conventions

Terms listed in Section 3 Definitions are capitalized throughout the document.

6 Security Profile Outlines

An implementation may claim conformance to any of the Security Profiles individually. It may also claim conformance to more than one Security Profile. It shall indicate in its Conformance Statement how it chooses which profiles to use for any given transaction.

6.1 SECURE USE PROFILES

An implementation may claim conformance to one or more Secure Use Profiles. Such profiles outline the use of attributes and other Security Profiles in a specific fashion.

Secure Use Profiles are specified in Annex A.

6.2 SECURE TRANSPORT CONNECTION PROFILES

An implementation may claim conformance to one or more Secure Transport Connection Profiles.

A Secure Transport Connection Profile includes the following information:

a. Description of the protocol framework and negotiation mechanisms
b. Description of the entity authentication an implementation shall support
    1. The identity of the entities being authenticated
    2. The mechanism by which entities are authenticated
    3. Any special considerations for audit log support

c. Description of the encryption mechanism an implementation shall support
    1. The method of distributing session keys
    2. The encryption protocol and relevant parameters

d. Description of the integrity check mechanism an implementation shall support

Secure Transport Connection Profiles are specified in Annex B.

Annex A SECURE USE PROFILES (Normative)

A.1 ONLINE ELECTRONIC STORAGE SECURE USE PROFILE

The Online Electronic Storage Secure Use Profile allows Application Entities to track and verify the status of SOP Instances in those cases where local security policies require tracking of the original data set and subsequent copies.

The Conformance Statement shall indicate in what manner the system restricts remote access.

A.1.1 SOP Instance Status

An implementation that conforms to the Online Electronic Storage Secure Use Profile shall conform to the following rules regarding the use of the SOP Instance Status (0100,0410) Attribute with SOP Instances that are transferred using the Storage Service Class:

a. An Application Entity that supports the Online Electronic Storage Secure Use Profile and that creates a SOP Instance intended for diagnostic use in Online Electronic Storage shall:
   1. Set the SOP Instance Status to Original (OR).
   2. Include the following Attributes:
      a) the SOP Class UID (0008,0016) and SOP Instance UID (0008,0018)
      b) the Instance Creation Date (0008,0012) and Instance Creation Time (0008,0013), if known
      c) the SOP Instance Status
      d) the SOP Authorization Date and Time (0100,0420)
      e) the SOP Authorization Comment, if any (0100,0424)
      f) the SOP Equipment Certification Number (0100,0426)
      g) the Study Instance UID (0020,000D) and Series Instance UID (0020,000E)
      h) any Attributes of the General Equipment Module that are known
      i) any overlay data present
      j) any image data present

b. The Application Entity that holds a SOP Instance where the SOP Instance Status is Original (OR) may change the SOP Instance Status to Authorized Original(AO) as long as the following rules are followed:
   1. The Application Entity shall determine that an authorized entity has certified the SOP Instance as useable for diagnostic purposes.
   2. The Application Entity shall change the SOP Instance Status to Authorized Original (AO). The SOP Instance UID shall not change.
   3. The Application Entity shall set the SOP Authorization Date and Time (0100,0420) and Authorization Equipment Certification Number (0100,0426) Attributes to appropriate values. It may also add an appropriate SOP Authorization Comment (0100,0424) Attribute.

c. There shall only be one Application Entity that holds a SOP Instance where the SOP Instance Status is Original (OR) or Authorized Original (AO). The Application Entity that holds such a SOP instance shall not delete it.

d. When communicating with an Application Entity that supports Online Electronic Storage the Application Entity that holds a SOP Instance where the SOP Instance Status is Original(OR) or Authorized Original(AO) may transfer that SOP Instance to another Application Entity that also conforms to the Online Electronic Storage Secure Use Profile as long as the following rules are followed:

    1. The transfer shall occur on a Secure Transport Connection.
    2. The two Application Entities involved in the transfer shall authenticate each other and shall confirm via the authentication that the other supports the Online Electronic Storage Secure Use Profile.
    3. The receiving Application Entity shall reject the storage request and discard the received SOP Instance if the data integrity checks done after the transfer indicate that the SOP Instance was altered during transmission.
    4. The transfer shall be confirmed using the push model of the Storage Commitment Service Class. Until it has completed this confirmation, the receiving Application Entity shall not forward the SOP Instance or Authorized Copies of the SOP instance to any other Application Entity.
    5. Once confirmed that the receiving Application Entity has successfully committed the SOP Instance to storage, the sending Application Entity shall do one of the following to its local copy of the SOP Instance:
        a) delete the SOP Instance,
        b) change the SOP Instance Status to Not Specified (NS),
        c) if the SOP Instance Status was Authorized Original (AO), change the SOP Instance Status to Authorized Copy (AC).

e. When communicating with an Application Entity that supports Online Electronic Storage an Application Entity that holds a SOP Instance whose SOP Instance Status is Authorized Original (AO) or Authorized Copy (AC) may send an Authorized Copy of the SOP Instance to another Application Entity as long as the following rules are followed:

    1. The transfer shall occur on a Secure Transport Connection.
    2. The two Application Entities involved in the transfer shall authenticate each other, and shall confirm via the authentication that the other supports the Online Electronic Storage Secure Use Profile.
    3. The sending Application Entity shall set the SOP Instance Status to either Not Specified (NS) or Authorized Copy (AC) in the copy sent. The SOP Instance UID shall not change.
    4. The receiving Application Entity shall reject the storage request and discard the copy if data integrity checks done after the transfer indicate that the SOP Instance was altered during transmission.

f. If communicating with a system that does not support the Online Electronic Storage Secure Use Profile, or if communication is not done over a Secure Transport Connection, then

    1. A sending Application Entity that conforms to this Security Profile shall either set the SOP Instance Status to Not Specified (NS), or leave out the SOP Instance Status and associated parameters of any SOP Instances that the sending Application Entity sends out over the unsecured Transport Connection or to systems that do not support the Online Electronic Storage Secure Use Profile.
    2. A receiving Application Entity that conforms to this Security Profile shall set the SOP Instance Status to Not Specified (NS) of any SOP Instance received over the unsecured Transport Connection or from systems that do not support the Online Electronic Storage Secure Use Profile.

g. The receiving Application Entity shall store SOP Instances in accordance with Level 2 as defined in the Storage Service Class (i.e., all Attributes, including Private Attributes), as required by the Storage Commitment Storage Service Class, and shall not coerce any Attribute other than SOP Instance Status, SOP Authorization Date and Time, Authorization Equipment Certification Number, and SOP Authorization Comment.

h. Other than changes to the SOP Instance Status, SOP Authorization Date and Time, Authorization Equipment Certification Number, and SOP Authorization Comment Attributes, as outlined above, or changes to group length Attributes to accommodate the aforementioned changes, the Application Entity shall not change any Attribute values.

Annex B SECURE TRANSPORT CONNECTION PROFILES (Normative)

B.1 THE BASIC TLS SECURE TRANSPORT CONNECTION PROFILE

An implementation that supports the Basic TLS Secure Transport Connection Profile shall utilize the framework and negotiation mechanism specified by the Transport Layer Security Version 1.0 protocol. Table B.1-1 specifies mechanisms that shall be supported if the corresponding features within TLS are supported by the Application Entity. The profile does not require the implementation to support all of the features (entity authentication, encryption, integrity checks) of TLS. Other mechanisms may also be used if agreed to by negotiation during establishment of the TLS channel.

Table B.1-1
Minimum Mechanisms for TLS Features

Supported TLS Feature	Minimum Mechanism
Entity Authentication	RSA based certificates
Exchange of Master Secrets	RSA
Data Integrity	SHA
Privacy	Triple DES EDE, CBC

IP ports on which an implementation accepts TLS connections, or the mechanism by which this port number is selected or configured, shall be specified in the Conformance Statement. This port shall be different from ports used for other types of transport connections (secure or unsecure).

Note: It is strongly recommended that systems supporting the Basic TLS Secure Transport Connection Profile use as their port the registered port number “2762 dicom-tls” for the DICOM Upper Layer Protocol on TLS: (decimal).

The Conformance Statement shall also indicate what mechanisms the implementation supports for Key Management.

The profile does not specify how a TLS Secure Transport Connection is established, or the significance of any certificates exchanged during peer entity authentication. These issues are left up to the Application Entity, which presumably is following some site specified security policy. The identities of the certificate owners can by used by the application entity for audit log support, or to restrict access based on some external access rights control framework. Once the Application Entity has established a Secure Transport Connection, then an Upper Layer Association can use that secure channel.

Note: There may be an interaction between PDU size and TLS Record size that impacts efficiency of transport. The maximum allowed TLS record size is smaller than the maximum allowed PDU size.

When an integrity check fails, the connection shall be dropped per the TLS protocol, causing both the sender and the receiver to issue an A-P-ABORT indication to the upper layers with an implementation-specific provider reason. The provider reason used shall be documented in the conformance statement.

Note: An integrity check failure indicates that the security of the channel may have been compromised.

B.2 ISCL SECURE TRANSPORT CONNECTION PROFILE

An implementation that supports the ISCL Transport Connection Profile shall utilize the framework and negotiation mechanism specified by the Integrated Secure Communication Layer, V1.00. An Application Entity shall use ISCL to select the mechanisms specified in Table B.2-1. An Application Entity shall as a minimum use an Entity Authentication mechanism and Data Integrity checks. An Application Entity may optionally use a privacy mechanism.

Table B.2-1
Minimum Mechanisms for ISCL Features

Supported ISCL Feature	Minimum Mechanism
Entity Authentication	Three pass (four-way) authentication (ISO/IEC 9798-2)
Data Integrity	Either MD-5 encrypted with DES, or DES-MAC (ISO 8730)
Privacy	DES (see Note)

Notes: The use of DES for privacy is optional for Online Electronic Storage.

For the Data Integrity check, an implementation may either encrypt the random number before applying MD-5, or encrypt the output of MD-5. The order is specified in the protocol. A receiver shall be able to perform the integrity check on messages regardless of the order.

IP ports on which an implementation accepts ISCL connections, or the mechanism by which this port number is selected or configured, shall be specified in the Conformance Statement. This port shall be different from ports used for other types of transport connections (secure or unsecure).

Note: It is strongly recommended that systems supporting the ISCL Secure Transport Connection Profile use as their port the registered port number “2761 dicom-iscl” for the DICOM Upper Layer Protocol on ISCL.

The Conformance Statement shall also indicate what mechanisms the implementation supports for Key Management.

The profile does not specify how an ISCL Secure Transport Connection is established. This issue is left up to the Application Entity, which presumably is following some site specified security policy. Once the Application Entity has established a Secure Transport Connection, then an Upper Layer Association can use that secure channel.

Note: There may be an interaction between PDU size and ISCL record size that impacts efficiency of transport.

When an integrity check fails, the connection shall be dropped, per the ISCL protocol, causing both the sender and the receiver to issue an A-P-ABORT indication to the upper layers with an implementation-specific provider reason. The provider reason used shall be documented in the conformance statement.

Note: An integrity check failure indicates that the security of the channel may have been compromised.

Index