Digital Imaging and Communications in Medicine (DICOM)

Part 15: Security Profiles

Published by

National Electrical Manufacturers Association
1300 N. 17th Street
Rosslyn, Virginia 22209 USA

Table of Contents

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:

— 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

PS 3.16: Content Mapping Resource

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.

ANSI X9.52 American National Standards Institute. ANSI X9.52-1998, Triple Data Encryption Algorithm Modes of Operation. 1998.

ECMA 235, The ECMA GSS-API Mechanism

FIPS PUB 46 Data Encryption Standard

FIPS PUB 81 DES Modes of Operation

IETF Internet X.509 Public Key Infrastructure; Time Stamp Protocols; March 2000

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

ISO/IEC 10118-:1998 Information technology – Security techniques – Hash-functions – Part 3: Dedicated hash-functions (RIPEMD-160 reference)

Note: The draft RIPEMD-160 specification and sample code are also available at ftp://ftp.esat.kuleuven.ac.be/pub/bosselae/ripemd

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

Integrated Secure Communication Layer V1.00 MEDIS-DC

ITU-T Recommendation X.509 (03/00) “Information technology - Open Systems Interconnection - The directory: Public-key and attribute certificate frameworks”

Note: ITU-T Recommendation X.509 is similar to ISO/IEC 9594-8 1990. However, the ITU-T recommendation is the more familiar form, and was revised in 1993 and 2000, with two sets of corrections in 2001. ITU-T was formerly known as CCITT.

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.

RFC-2313 PKCS #1: RSA Encryption, Version 1.5, March 1998.

RFC 2437 PKCS #1 RSA Cryptography Specifications Version 2.0

Note: The RSA Encryption Standard is also defined in informative annex A of ISO/IEC 9796, and in Normative Annex A of the CEN/TC251 European Prestandard prENV 12388:1996.

RFC-2630 Cryptographic Message Syntax, June 1999

SHA-1 National Institute of Standards and Technology, FIPS Pub 180-1: Secure Hash Standard, 17 April 1995

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.”

e. 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.”

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.

Message Authentication Code: A digest or hash code derived from a subset of Data Elements.

Certificate: An electronic document that identifies a party and that party's public encryption algorithm, parameters, and key. The Certificate also includes, among other things, the identity and a digital signature from the entity that created the certificate. The content and format of a Certificate are defined by ITU-T Recommendation X.509.

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.

6.3 DIGITAL SIGNATURE PROFILE

An implementation may claim conformance to one or more Digital Signature Profiles.

A Digital Signature profile consists of the following information:

a. The role that the Digital Signature plays, including:
    1. Who or what entity the Digital Signature represents.
    2. A description of the purpose of the Digital Signature.
    3. The conditions under which the Digital Signature is included in the Data Set.
b. A list of Attributes that shall be included in the Digital Signature.
c. The mechanisms that shall be used to generate or verify the Digital Signature, including:

1. The algorithm and relevant parameters that shall be used to create the MAC or hash code, including the Value to be used for the MAC Algorithm (0400,0015) Attribute.
2. The encryption algorithm and relevant parameters that shall be used to encrypt the MAC or hash code in forming the Digital Signature.
3. The certificate type or key distribution mechanism that shall be used, including the Value to be used for the Certificate Type (0400,0110) Attribute.
4. Any requirements for the Certified Timestamp Type (0400,305) and Certified Timestamp (0400,310) Attributes.

d. Any special requirements for identifying the signatory.

e. The relationship with other Digital Signatures, if any.

f. Any other factors needed to create, verify, or interpret the Digital Signature

Digital Signature Profiles are specified in Annex C.

6.4 MEDIA STORAGE SECURITY PROFILES

An implementation may claim conformance to one or more Media Storage Application Profiles which in turn require conformance to one or more Media Storage Security Profiles.

Note: An implementation may not claim conformance to a Media Storage Security Profile without claiming conformance to a Media Storage Application Profile.

A Media Storage Security Profile includes the following specifications:

a. What aspects of security are addressed by the profile.
b. The restrictions on the types of DICOM Files that can be secured, if any.
c. How the DICOM Files will be encapsulated and secured.

Media Storage Security Profiles are specified in Annex D.

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.

A.2 BASIC DIGITAL SIGNATURES SECURE USE PROFILE

An implementation that validates and generates Digital Signatures may claim conformance to the Basic Digital Signatures Secure Use Profile. Any implementation that claims conformance to this Security Profile shall obey the following rules in handling Digital Signatures:

a. The implementation shall store any SOP Instances that it receives in such a way that it guards against any unauthorized tampering of the SOP Instance.
b. Wherever possible, the implementation shall validate the Digital Signatures within any SOP Instance that it receives.
c. If the implementation sends the SOP Instance to another Application Entity, it shall do the following:
    1. remove any Digital Signatures that may have become invalid due to any allowed variations to the format of Attribute Values (e.g. trimming of padding, alternate representations of numbers),
    2. generate one or more new Digital Signatures covering the Data Elements that the implementation was able to verify when the SOP Instance was received.

A.3 BIT-PRESERVING DIGITAL SIGNATURES SECURE USE PROFILE

An implementation that stores and forwards SOP Instances may claim conformance to the Bit-Preserving Digital Signatures Secure Use Profile. Any implementation that claims conformance to this Security Profile shall obey the following rules in handling Digital Signatures:

a. The implementation shall store any SOP Instances that it receives in such a way that when the SOP instance is forwarded to another Application Entity, the Value fields of all Attributes are bit-for-bit duplicates of the fields originally received.
b. The implementation shall not change the order of Items in a Sequence.
c. The implementation shall not remove or change any Data Element of any SOP Instance that it receives when sending that SOP Instance on to another Application Entity via DICOM. This includes any Digital Signatures received.

Note: Implementations may add new Data Elements that do not alter any existing Digital Signatures.

d. The implementation shall utilize an explicit VR Transfer Syntax.

Note: Implementations that cannot use an explicit VR Transfer Syntax cannot conform to this Secure Use Profile, since it may not be able to verify Digital Signatures that are received with an implicit VR Transfer Syntax.

e. The implementation shall not change the VR of any Data Element that it receives when it transmits that object to another Application Entity.

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.

Annex C DIGITAL SIGNATURE PROFILES (Normative)

C.1 BASE RSA DIGITAL SIGNATURE PROFILE

The Base RSA Digital Signature Profile outlines the use of RSA encryption of a MAC to generate a Digital Signature. This Profile does not specify any particular set of Data Elements to sign. Other Digital Signature profiles may refer to this profile, adding specifications of which Data Elements to sign or other customizations.

The creator of a digital signature shall use one of the RIPEMD-160, MD5, or SHA-1 hashing functions to generate a MAC, which is then encrypted using a private RSA key. All validators of digital signatures shall be capable of using a MAC generated by any of three hashing functions specified (RIPEMD-160, MD5, or SHA-1).

Note: The use of MD5 is not recommended by its inventors, RSA. See: ftp://ftp.rsasecurity.com/pub/pdfs/bulletn4.pdf

The MAC to be signed shall be padded to a block size matching the RSA key size, as directed in RFC 2437 (PKCS #1). The Value of MAC Algorithm (0400,0015) shall be set to either "RIPEMD160", “MD5”, or “SHA1”. The public key associated with the private key as well as the identity of the Application Entity or equipment manufacturer that owns the RSA key pair shall be transmitted in an X.509 (1993) signature certificate. The Value of the Certificate Type (0400,0110) Attribute shall be set to "X509_1993_SIG". A site-specific policy determines how the X.509 certificates are generated, authenticated, and distributed. A site may issue and distribute X.509 certificates directly, may utilize the services of a Certificate Authority, or use any reasonable method for certificate generation and verification.

If an implementation utilizes timestamps, it shall use a Certified Timestamp Type (0400,0305) of “CMS_TSP”. The Certified Timestamp (0400,0310) shall be generated as described in “Internet X.509 Public Key Infrastructure; Time Stamp Protocols; March 2000”.

C.2 CREATOR RSA DIGITAL SIGNATURE PROFILE

The creator of a DICOM SOP Instance may generate signatures using the Creator RSA Digital Signature Profile. The Digital Signature produced by this Profile serves as a lifetime data integrity check that can be used to verify that the pixel data in the SOP instance has not been altered since its initial creation. An implementation that supports the Creator RSA Digital Signature Profile may include a Creator RSA Digital Signature with every SOP Instance that it creates; however, the implementation is not required to do so.

As a minimum, an implementation shall include the following attributes in generating the Creator RSA Digital Signature:

a. the SOP Class and Instance UIDs
b. the SOP Creation Date and Time, if present
c. the Study and Series Instance UIDs
d. any attributes of the General Equipment module that are present
e. any attributes of the Overlay Plane, Curve or Graphic Annotation modules that are present
f. any attributes of the General Image and Image Pixel modules that are present
g. any attributes of the SR Document General and SR Document Content modules that are present

h. any attributes of the Waveform and Waveform Annotation modules that are present

The Digital Signature shall be created using the methodology described in the Base RSA Digital Signature Profile. Typically the certificate and associated private key used to produce Creator RSA Digital Signatures are configuration parameters of the Application Entity set by service or installation engineers.

Creator RSA Digital Signatures bear no direct relationship to other Digital Signatures. However, other Digital Signatures, such as the Authorization Digital Signature, may be used to collaborate the timestamp of a Creator RSA Digital Signature.

C.3 AUTHORIZATION RSA DIGITAL SIGNATURE PROFILE

The technician or physician who approves a DICOM SOP Instance for use may request the Application Entity to generate a signature using the Authorization RSA Digital Signature Profile. The Digital Signature produced serves as a lifetime data integrity check that can be used to verify that the pixel data in the SOP instance is the same that the technician or physician saw when they made the approval.

As a minimum, an implementation shall include the following attributes in generating the Authorization RSA Digital Signature:

a. the SOP Class and Instance UIDs
b. the Study and Series Instance UIDs
c. any attributes whose Values are verifiable by the technician or physician (e.g., their Values are displayed to the technician or physician)
d. any attributes of the Overlay Plane, Curve or Graphic Annotation modules that are present
e. any attributes of the General Image and Image Pixel modules that are present
f. any attributes of the SR Document General and SR Document Content modules that are present
g. any attributes of the Waveform and Waveform Annotation modules that are present

The Digital Signature shall be created using the methodology described in the Base RSA Digital Signature Profile. The Application Entity shall determine the identity of the technician or physician and obtain their certificate through a site-specific procedure such as a login mechanism or a smart card.

Authorization RSA Digital Signatures bear no direct relationship to other Digital Signatures. However, other Digital Signatures, such as the Creator RSA Digital Signature, may be used to collaborate the timestamp of an Authorization RSA Digital Signature.

ANNEX D– MEDIA STORAGE SECURITY PROFILES
(Normative)

D.1 BASIC DICOM MEDIA SECURITY PROFILE

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).

This profile specifies the use of Triple-DES for content encryption and RSA for the key transport of Triple-DES content-encryption keys. The encrypted content is a DICOM File which can either

- be signed with one or more digital signatures, using SHA-1 as the digest algorithm and RSA as the signature algorithm, or
- be digested with SHA-1 as digest algorithm, without application of digital signatures.

D.1.1 Encapsulation of a DICOM File in a Secure DICOM File

A Secure DICOM File conforming to this security profile shall contain an Enveloped-data content type of the Cryptographic Message Syntax defined in RFC 2630. The enveloped data shall use RSA [RFC 2313] for the key transport of Triple-DES content-encryption keys. The Triple-DES key length is 168 bits as defined by ANSI X9.52. Encoding shall be performed according to the specifications for RSA Key Transport in RFC-2630.

The encrypted content of the Enveloped-data content type shall be of the following choices:

- Signed-data content type;
- Digested-data content type.

In both cases, SHA-1 [SHA-1] shall be used as the digest algorithm. In case of the Signed-data content type, RSA [RFC 2313] shall be used as the signature algorithm.

Notes: 1. RSA key transport of Triple-DES content-encryption keys is specified as a requirement in the European Prestandard ENV 13608-2: Health Informatics - Security for healthcare communication – Part 2: Secure data objects.

2. No requirements on the size of the asymmetric key pairs used for RSA key transport are defined in this profile.

3. No requirements or restrictions on the use of the SignedAttributes element of the Signed-data content type's SignerInfo structure are defined in this profile. SignedAttributes might for example be used to specify the signing time or SMIME capabilities, as required by ENV 13608-2.

Index