PS3.15

DICOM PS3.15 ~~2015c~~2016a - Security and System Management Profiles

PS3.15: DICOM PS3.15 ~~2015c~~2016a - Security and System Management Profiles

Copyright © ~~2015~~2016 NEMA

Table of Contents

Notice and Disclaimer 11
Foreword 13
1. Scope and Field of Application 15
1.1. Security Policies and Mechanisms 15
1.2. System Management Profiles 15
2. Normative References 17
3. Definitions 19
3.1. Reference Model Definitions 19
3.2. Reference Model Security Architecture Definitions 19
3.3. ACSE Service Definitions 19
3.4. Security Definitions 19
3.5. DICOM Introduction and Overview Definitions 20
3.6. DICOM Conformance Definitions 20
3.7. DICOM Information Object Definitions 20
3.8. DICOM Service Class Definitions 20
3.9. DICOM Communication Support Definitions 20
3.10. DICOM Security Profile Definitions 20
4. Symbols and Abbreviations 21
5. Conventions 23
6. Security and System Management Profile Outlines 25
6.1. Secure Use Profiles 25
6.2. Secure Transport Connection Profiles 25
6.3. Digital Signature Profile 25
6.4. Media Storage Security Profiles 26
6.5. Network Address Management Profiles 26
6.6. Time Synchronization Profiles 26
6.7. Application Configuration Management Profiles 26
6.8. Audit Trail Profiles 27
7. Configuration Profiles 29
7.1. Actors 29
7.2. Transactions 30
A. Secure Use Profiles (Normative) 33
A.1. Online Electronic Storage Secure Use Profile 33
A.1.1. SOP Instance Status 33
A.2. Basic Digital Signatures Secure Use Profile 34
A.3. Bit-preserving Digital Signatures Secure Use Profile 35
A.4. Basic SR Digital Signatures Secure Use Profile 35
A.5. Audit Trail Message Format Profile 35
A.5.1. DICOM Audit Message Schema 36
A.5.1-1. Audit Message Schema 36
A.5.2. General Message Format Conventions 40
A.5.2.1. UserID 43
A.5.2.2. AlternativeUserID 43
A.5.2.3. Username 43
A.5.2.4. Multi-homed Nodes 44
A.5.2.5. EventDateTime 44
A.5.3. DICOM Specific Audit Messages 44
A.5.3.1. Application Activity 44
A.5.3.2. Audit Log Used 45
A.5.3.3. Begin Transferring DICOM Instances 46
A.5.3.4. Data Export 48
A.5.3.4.1. UserIsRequestor 50
A.5.3.5. Data Import 50
A.5.3.6. DICOM Instances Accessed 51
A.5.3.7. DICOM Instances Transferred 53
A.5.3.8. DICOM Study Deleted 54
A.5.3.9. Network Entry 56

A.5.3.10. Query 56
A.5.3.11. Security Alert 58
A.5.3.12. User Authentication 60
A.6. Audit Trail Message Transmission Profile - SYSLOG-TLS 60
A.7. Audit Trail Message Transmission Profile - SYSLOG-UDP 61
B. Secure Transport Connection Profiles (Normative) 63
B.1. The Basic TLS Secure Transport Connection Profile 63
B.2. ISCL Secure Transport Connection Profile 63
B.3. The AES TLS Secure Transport Connection Profile 64
B.4. Basic User Identity Association Profile 65
B.5. User Identity Plus Passcode Association Profile 65
B.6. Kerberos Identity Negotiation Association Profile 66
B.7. Generic SAML Assertion Identity Negotiation Association Profile 66
B.8. Secure Use of Email Transport 66
C. Digital Signature Profiles (Normative) 69
C.1. Base RSA Digital Signature Profile 69
C.2. Creator RSA Digital Signature Profile 69
C.3. Authorization RSA Digital Signature Profile 70
C.4. Structured Report RSA Digital Signature Profile 71
D. Media Storage Security Profiles (Normative) 73
D.1. Basic DICOM Media Security Profile 73
D.1.1. Encapsulation of A DICOM File in a Secure DICOM File 73
E. Attribute Confidentiality Profiles 75
E.1. Application Level Confidentiality Profiles 75
E.1.1. De-identifier 75
E.1.2. Re-identifier 93
E.1.3. Conformance Requirements 94
E.2. Basic Application Level Confidentiality Profile 94
E.3. Basic Application Level Confidentiality Options 94
E.3.1. Clean Pixel Data Option 95
E.3.2. Clean Recognizable Visual Features Option 95
E.3.3. Clean Graphics Option 96
E.3.4. Clean Structured Content Option 96
E.3.5. Clean Descriptors Option 97
E.3.6. Retain Longitudinal Temporal Information Options 97
E.3.7. Retain Patient Characteristics Option 98
E.3.8. Retain Device Identity Option 98
E.3.9. Retain UIDs Option 99
E.3.10. Retain Safe Private Option 99
F. Network Address Management Profiles 103
F.1. Basic Network Address Management Profile 103
F.1.1. Resolve Hostname 103
F.1.1.1. Scope 103
F.1.1.2. Use Case Roles 103
F.1.1.3. Referenced Standards 104
F.1.1.4. DNS Security Considerations (Informative) 104
F.1.1.5. DNS Implementation Considerations (Informative) 105
F.1.1.6. Support For Service Discovery 105
F.1.2. Configure DHCPserver 105
F.1.2.1. Scope 105
F.1.2.2. Use Case Roles 105
F.1.2.3. Referenced Standards 106
F.1.3. Find and Use DHCP Server 106
F.1.3.1. Scope 106
F.1.3.2. Use Case Roles 106
F.1.3.3. Referenced Standards 106
F.1.3.4. Interaction Diagram 107
F.1.4. Maintain Lease 108
F.1.4.1. Scope 108
F.1.4.2. Use Case Roles 108

F.1.4.3. Referenced Standards 108
F.1.4.4. Normal Interaction 108
F.1.5. DDNS Coordination 108
F.1.5.1. Scope 108
F.1.5.2. Use Case Roles 109
F.1.5.3. Referenced Standards 109
F.1.5.4. Basic Course of Events 109
F.1.6. DHCP Security Considerations (Informative) 109
F.1.7. DHCP Implementation Considerations (Informative) 110
F.1.8. Conformance 110
G. Time Synchronization Profiles 111
G.1. Basic Time Synchronization Profile 111
G.1.1. Find NTP Servers 111
G.1.1.1. Scope 111
G.1.1.2. Use Case Roles 112
G.1.1.3. Referenced Standards 112
G.1.1.4. Basic Course of Events. 112
G.1.1.5. Alternative Paths 112
G.1.1.6. Assumptions 112
G.1.1.7. Postconditions 113
G.1.2. Maintain Time 113
G.1.2.1. Scope 113
G.1.2.2. Use Case Roles 113
G.1.2.3. Referenced Standards 113
G.1.2.4. Basic Course of Events. 113
G.1.3. NTP Security Considerations (Informative) 113
G.1.4. NTP Implementation Considerations (Informative) 114
G.1.5. Conformance 114
H. Application Configuration Management Profiles 115
H.1. Application Configuration Management Profile 115
H.1.1. Data ~~Modelcomponent~~Model Component Objects 115
H.1.1.1. Device 116
H.1.1.2. Network Application Entity 117
H.1.1.3. Network Connection 118
H.1.1.4. Transfer Capabilities 119
H.1.1.5. DICOM Configuration Root 119
H.1.1.6. Devices Root 120
H.1.1.7. Unique AE Titles Registry Root 120
H.1.1.8. Unique AE Title 120
H.1.2. Application Configuration Data Model Hierarchy 121
H.1.3. LDAP Schema For Objects and Attributes 122
H.1.4. Transactions 134
H.1.4.1. Find LDAP Server 134
H.1.4.1.1. Scope 134
H.1.4.1.2. Use Case Roles 134
H.1.4.1.3. Referenced Standards 134
H.1.4.1.4. Interaction Diagram 134
H.1.4.1.5. Alternative Paths 135
H.1.4.2. Query LDAP Server 135
H.1.4.2.1. Scope 135
H.1.4.2.2. Use Case Roles 135
H.1.4.2.3. Referenced Standards 135
H.1.4.2.4. Interaction Description 135
H.1.4.3. Update LDAP Server 136
H.1.4.3.1. Scope 136
H.1.4.3.2. Use Case Roles 136
H.1.4.3.3. Referenced Standards 136
H.1.4.3.4. Interaction Description 136
H.1.4.3.5. Special Update For Network AE Creation 136
H.1.4.4. Maintain LDAP Server 137

H.1.5. LDAP Security Considerations (Informative) 137
H.1.5.1. Threat Assessment 137
H.1.5.2. Available LDAP Security Mechanisms 138
H.1.5.3. Recommendations (Informative) 138
H.1.6. Implementation Considerations (Informative) 139
H.1.7. Conformance 139
H.2. DNS Service Discovery 139
H.2.1. Scope 139
H.2.2. Use Case Roles 140
H.2.3. Referenced Standards 140
H.2.4. Examples 141

List of Figures

7-1. Transactions and Actors 32
F.1-1. Resolve Hostname 103
F.1-2. DNS Referenced Standards 104
F.1-3. Configure DHCP Server 105
F.1-4. Find and Use DHCP Server 106
F.1-5. DHCP Interactions 107
F.1-6. Maintain Lease 108
F.1-7. DDNS Coordination 109
G.1-1. Find NTP Servers 112
G.2-1. Maintain Time 113
H.1-1. Application Configuration Data Model 115
H.1-2. DICOM Configuration Hierarchy 121
H.1-3. Find LDAP Server 134
H.1-4. Select LDAP Server 134
H.1-5. Query LDAP Server 135
H.1-6. Update LDAP Server 136
H.2-1. Find DICOM Service 140

List of Tables

A.5.2-1. General Message Format 40
A.5.3.1-1. Application Activity Message 44
A.5.3.2-1. Audit Log Used Message 45
A.5.3.3-1. Audit Message for Begin Transferring DICOM Instances 46
A.5.3.4-1. Audit Message for Data Export 48
A.5.3.5-1. Audit Message for Data Import 50
A.5.3.6-1. Audit Message for DICOM Instances Accessed 51
A.5.3.7-1. Audit Message for DICOM Instances Transferred 53
A.5.3.8-1. Audit Message for DICOM Study Deleted 55
A.5.3.9-1. Audit Message for Network Entry 56
A.5.3.10-1. Audit Message for Query 57
A.5.3.11-1. Audit Message for Security Alert 58
A.5.3.12-1. Audit Message for User Authentication 60
B.1-1. Minimum Mechanisms for TLS Features 63
B.2-1. Minimum Mechanisms for ISCL Features 64
B.3-1. Minimum Mechanisms for TLS Features 64
B.4-1. Minimum Mechanisms for DICOM Association Negotiation Features - Basic User Identity Association Profile 65
B.5-1. User Identity Plus Passcode Association Profile - Minimum Mechanisms for DICOM Association Negotiation Features 66
B.6-1. Kerberos Identity Negotiation Association Profile - Minimum Mechanisms for DICOM Association Negotiation Features 66
B.7-1. Generic SAML Assertion Identity Negotiation Association Profile - Minimum Mechanisms for DICOM Association Negotiation Features 66
E.1-1. Application Level Confidentiality Profile Attributes 79
E.3.10-1. Safe Private Attributes 100
F.1-1. Basic Network Address Management Profile 103
F.1-2. DHCP Parameters 107
G.1-1. Basic Time Synchronization Profile 111
H.1-1. Application Configuration Management Profiles 115
H.1-2. Attributes of Device Object 116
H.1-3. Child Objects of Device Object 117
H.1-4. Attributes of Network AE Object 117
H.1-5. Child Objects of Network AE Object 118
H.1-6. Attributes of Network Connection Object 118
H.1-7. Attributes of Transfer Capability Object 119
H.1-8. Attributes of the DICOM Configuration Root Object 119
H.1-9. Child Objects of DICOM Configuration Root Object 120
H.1-10. Attributes of the Devices Root Object 120
H.1-11. Child Objects of Devices Root Object 120
H.1-12. Attributes of the Unique AE Titles Registry Root Object 120
H.1-13. Child Objects of Unique AE Titles Registry Root Object 120
H.1-14. Attributes of the Unique AE Title Object 120
H.1-15. LDAP Security Patterns 138

Notice and Disclaimer

The information in this publication was considered technically sound by the consensus of persons engaged in the development and approval of the document at the time it was developed. Consensus does not necessarily mean that there is unanimous agreement among every person participating in the development of this document.

NEMA standards and guideline publications, of which the document contained herein is one, are developed through a voluntary consensus standards development process. This process brings together volunteers and/or seeks out the views of persons who have an interest in the topic covered by this publication. While NEMA administers the process and establishes rules to promote fairness in the development of consensus, it does not write the document and it does not independently test, evaluate, or verify the accuracy or completeness of any information or the soundness of any judgments contained in its standards and guideline publications.

NEMA disclaims liability for any personal injury, property, or other damages of any nature whatsoever, whether special, indirect, consequential, or compensatory, directly or indirectly resulting from the publication, use of, application, or reliance on this document. NEMA disclaims and makes no guaranty or warranty, expressed or implied, as to the accuracy or completeness of any information published herein, and disclaims and makes no warranty that the information in this document will fulfill any of your particular purposes or needs. NEMA does not undertake to guarantee the performance of any individual manufacturer or seller's products or services by virtue of this standard or guide.

In publishing and making this document available, NEMA is not undertaking to render professional or other services for or on behalf of any person or entity, nor is NEMA undertaking to perform any duty owed by any person or entity to someone else. Anyone using this document should rely on his or her own independent judgment or, as appropriate, seek the advice of a competent professional in determining the exercise of reasonable care in any given circumstances. Information and other standards on the topic covered by this publication may be available from other sources, which the user may wish to consult for additional views or information not covered by this publication.

NEMA has no power, nor does it undertake to police or enforce compliance with the contents of this document. NEMA does not certify, test, or inspect products, designs, or installations for safety or health purposes. Any certification or other statement of compliance with any health or safety-related information in this document shall not be attributable to NEMA and is solely the responsibility of the certifier or maker of the statement.

Foreword

This DICOM Standard was developed according to the procedures of the DICOM Standards Committee.

The DICOM Standard is structured as a multi-part document using the guidelines established in [ISO/IEC Directives, Part 3].

DICOM® is the registered trademark of the National Electrical Manufacturers Association for its standards publications relating to digital communications of medical information, all rights reserved.

HL7® and CDA® are the registered trademarks of Health Level Seven International, all rights reserved.

SNOMED®, SNOMED Clinical Terms®, SNOMED CT® are the registered trademarks of the International Health Terminology Standards Development Organisation (IHTSDO), all rights reserved.

LOINC® is the registered trademark of Regenstrief Institute, Inc, all rights reserved.

1 Scope and Field of Application

This part of the DICOM Standard specifies Security and System Management Profiles to which implementations may claim conformance. Security and System Management Profiles are defined by referencing externally developed standard protocols, such as TLS, ISCL, DHCP, and LDAP, with attention to their use in a system that uses DICOM Standard protocols for information interchange.

1.1 Security Policies and Mechanisms

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.

1.2 System Management Profiles

The System Management Profiles specified in this Part are designed to support automation of the configuration management processes necessary to operate a system that uses DICOM Standard protocols for information interchange.

This Part assumes that the Application Entities may operate in a variety of network environments of differing complexity. These environments may range from a few units operating on an isolated network, to a department-level network with some limited centralized network support services, to an enterprise-level network with significant network management services. Note that the System Man-

agement Profiles are generally addressed to the implementation, not to Application Entities. The same Profiles need to be supported by the different applications on the network.

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.

[ISO/IEC Directives, Part 3] ISO/IEC. 1989. *Drafting and presentation of International Standards*.

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 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 1035 Domain Name System (DNS)

RFC 1305 Network Time Protocol (Version 3) Specification, Implementation

RFC 2030 Simple Network Time Protocol (SNTP) Version 4

RFC 2131 Dynamic Host Configuration Protocol

RFC 2132 Dynamic Host Configuration Protocol Options

RFC 2136 Dynamic Updates in the Domain Name System (DNS UPDATE)

RFC 2181 Clarifications to the DNS Specification

RFC 2219 Use of DNS Aliases for Network Services

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 2251 Lightweight Directory Access Protocol (v3)

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

RFC 2563 DHCP Option to Disable Stateless Auto-Configuration in IPv4 Clients

RFC 2782 A DNS RR for specifying the location of services (DNS SRV)

RFC 2849 The LDAP Data Interchange Format (LDIF)

RFC 2898 PKCS #5: Password-Based Cryptography Specification Version 2.0, September 2000

RFC 3211 Password-based Encryption for CMS, December 2001

RFC 3268 Advanced Encryption Standard (AES) Ciphersuites for Transport Layer Security (TLS), June 2002.

RFC 3447 PKCS #1 RSA Cryptography Specifications Version 2.1, February 2003

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 3852 Cryptographic Message Syntax,July 2004

RFC 3370 Cryptographic Message Syntax (CMS) Algorithms, August 2002

RFC 3565 Use of the Advanced Encryption Standard (AES) Encryption Algorithm in Cryptographic Message Syntax (CMS), July 2003

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

SHA-2 National Institute of Standards and Technology, FIPS Pub 180-2: Secure Hash Standard, 1 August 2002

RFC 3851 Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.1 Message Specification

RFC 3853 S/MIME Advanced Encryption Standard (AES) Requirement for the Session Initiation Protocol (SIP)

RFC 5424 The Syslog Protocol

RFC 5425 Transport Layer Security (TLS) Transport Mapping for Syslog

RFC 5426 Transmission of Syslog Messages over UDP

Note

Normative RFC's are frequently updated by issuance of subsequent RFC's. The original older RFC is not modified to include references to the newer RFC.

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 PS3.1:

a. Attribute

3.6 DICOM Conformance Definitions

This Part of the Standard makes use of the following terms defined in PS3.2:

a. Security Profile

3.7 DICOM Information Object Definitions

This Part of the Standard makes use of the following terms defined in PS3.3:

a. Module

3.8 DICOM Service Class Definitions

This Part of the Standard makes use of the following terms defined in PS3.4:

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 PS3.8:

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

AES Advanced Encryption Standard

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

CN Common Name

DES Data Encryption Standard

DHCP Dynamic Host Configuration Protocol

DICOM Digital Imaging and Communications in Medicine

DN Distinguished Name

DNS Domain Name System

DDNS Dynamic Domain Name System

ECMA European Computer Manufacturers Association

EDE Encrypt-Decrypt-Encrypt

HL7 Health Level 7

IEC International Electrical Commission

IEEE Institute of Electrical and Electronics Engineers

IETF Internet Engineering Task Force

IOD Information Object Definition

ISCL Integrated Secure Communication Layer

ISO International Standards Organization

JIRA Japan Medical Imaging and Radiological Systems Industries Association

LDAP Lightweight Directory Access Protocol

LDIF LDAP Interchange Format

MAC Message Authentication Code

MD-5 Message Digest - 5

MEDIS-DC Medical Information System Development Center

MTU Maximum Transmission Unit

NEMA	National Electrical Manufacturers Association
NTP	Network Time Protocol
OID	Object Identifier (analogous to UID)
PDU	Protocol Data Unit
RDN	Relative Distinguished Name
RFC	Request For Comment (used for standards issued by the IETF)
RR	Resource Record (when used in the context of DNS)
RSA	Rivest-Shamir-Adleman
SCP	Service Class Provider
SCU	Service Class User
SHA	Secure Hash Algorithm
SNTP	Simple Network Time Protocol
SOP	Service-Object Pair
SSH	Secure Shell
SSL	Secure Sockets Layer
TLS	Transport Layer Security
UID	Unique Identifier
UTC	Universal Coordinated Time

5 Conventions

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

6 Security and System Management Profile Outlines

An implementation may claim conformance to any of the Security and System Management Profiles individually. It may also claim conformance to more than one Security or System Management 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 (0400,0305) and Certified Timestamp (0400,0310) 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.

6.5 Network Address Management Profiles

An implementation may claim conformance to one or more Network Address Management Profiles. Such profiles outline the use of non-DICOM network protocols to obtain the network addresses for the implementation.

Network Address Management Profiles are specified in Annex F.

6.6 Time Synchronization Profiles

An implementation may claim conformance to one or more Time Synchronization Profiles. Such profiles outline the use of non-DICOM protocols to set the current time for the implementation.

Time Synchronization Profiles are specified in Annex G.

6.7 Application Configuration Management Profiles

An implementation may claim conformance to one or more Application Configuration Management Profiles. Such profiles outline the use of non-DICOM network protocols to obtain the descriptions, addresses and capabilities of other devices with which the implementation may communicate using the DICOM Protocol. They also specify the use of those non-DICOM protocols for the implementation to publish or announce its description, addresses and capabilities. They also specify how implementation specific configuration information can be obtained by devices.

Application Configuration Management Profiles are specified in Annex H.

6.8 Audit Trail Profiles

An implementation may claim conformance to one or more Audit Trail Profiles. Such profiles outline the generation and transport of audit messages for security and privacy policy enforcement.

Audit Trail Profiles are specified in Annex A.

7 Configuration Profiles

Configuration management support is implemented by means of protocols defined in standards other than the DICOM standard. These protocols are described here in terms of actors, transactions, and profiles.

Actors are analogous to the Application Entities used within the DICOM profile. An actor is a collection of hardware and software processes that perform a particular role. When a device provides or uses a service it will include an actor to handle the relevant network activity. DICOM Configuration actors may co-exist with other Application Entities on a device. Some DICOM Configuration actors exist as parts of general use IT equipment. Like the Application Entity, specification of an Actor does not imply anything about the details of the actual implementation.

The actor interactions are defined in terms of Transactions. Each transaction is given a name. The transaction may in turn comprise a variety of activity. All transactions are defined in terms of actors that are communicating. The relationships between actors in a transaction may be more complex than the simple SCU and SCP roles in DICOM activities. When the transaction includes interactions with a person, the transactions may be implemented by user interfaces, removable media. and other mechanisms. The person is described in terms of being an actor from the perspective of the transaction use case model. More typically the transactions are a series of network activities that perform a specific operation.

A transaction includes both mandatory and optional components. An Actor that is implementing a transaction is required to implement all of the mandatory components.

Some transactions include human actors in the transaction definition. These actors are not defined as actors elsewhere, nor are they included in profile descriptions. They exist to specify that some sort of mechanism must be provided to permit these people to interact with the computer actor. Other details of how that user interface is provided are not specified by this standard. For an example, see the definition of the Configure DHCP transaction.

Conformance is further managed by means of Profiles. A Profile is defined in terms of what transactions are required for an actor and what transactions are optional. An implementation of a specific actor is documented by specifying what optional transactions and transaction components have been implemented. An implementation that omits any required transactions or components cannot claim to be an implementation of that Actor.

For example, in the Network Address Management Profile the DHCP Server is required to perform the three Transactions to configure the DHCP server, find and use DHCP servers, and maintain the DHCP leases. It may also support the transaction to update the DNS server by means of DDNS coordination.

A Profile includes definitions for more than one Actor. It specifies the transactions for all of the actors that cooperate to perform a function. For example, the Network Address Management Profile covers the DHCP Server actor, the DHCP client Actor, and the DNS Server actor. There must be at least one DHCP Server and one DHCP Client for the system to be useful. The DNS Server itself is optional because the DHCP Server need not implement the DDNS Coordination transaction. If the DNS Server is part of the system, the DDNS coordination is required and the DHCP Server will be expected to participate in the DDNS Coordination transaction.

Note

There may be a DNS server present on the same network as a DHCP Server, but if it is not providing the DNS Server actor from this profile it is not part of the DICOM Configuration activities.

The profiles, actors, and transactions are summarized in the following sections. The detailed description of actor and transactions for each specific profile are described in annexes for each profile. The transactions are documented in terms of parameters and terms from their original standards document, e.g., an RFC for Internet protocols. The full details of the transaction are not described in the annex, only particular details that are relevant to the DICOM application of that transaction. The complete details for these external protocols are documented in the relevant standards documents for the external protocols. Compliance with the requirements of a particular profile shall include compliance with these external protocol documents.

7.1 Actors

DHCP Server

The DHCP Server is a computer/software feature that is provided with a network configuration description, and that provides startup configuration services in accordance with the DHCP protocol.

DHCP Client

The DHCP Client is a software feature that is used to obtain TCP/IP parameters during the startup of a computer. It continues operation to maintain validity of these parameters.

DNS Server

The DNS server is a computer/software feature that provides IP related information in response to queries from clients utilizing the DNS protocol. It is a part of a federated database facility that maintains the current database relating machine names to IP address information. The DNS server may also be isolated from the worldwide federated database and provide only local DNS services.

DNS Client

The DNS client as a computer/software feature that utilizes the DNS protocols to obtain IP information when given hostnames. The hostnames may be in configuration files or other files instead of explicit IP addresses. The hostnames are converted into IP addresses dynamically when necessary. The DNS client uses a DNS server to provide the necessary information.

NTP Server

The NTP server is a computer/software feature that provides time services in accordance with the NTP or SNTP protocol.

NTP Client

The NTP client is software that obtains time information from an NTP server and maintains the client time in synchronization with the time signals from the NTP server.

SNTP Client

The SNTP client is software that obtains time information from an NTP server and maintains the client time in approximate synchronization with time signals from the NTP server. The SNTP client synchronization is not maintained with the accuracy or precision that NTP provides.

LDAP Server

The LDAP server is a computer/ software feature that maintains an internal database of various directory information. Some of this directory information corresponds to DICOM Configuration schema. The LDAP server provides network access to read and update the directory information. The LDAP server provides a mechanism for external loading, unloading, and backup of directory information. The LDAP server may be part of a federated network of servers that provides a coordinated view of a federated directory database in accordance with the rules of the LDAP protocols.

LDAP Client

The LDAP client utilizes the LDAP protocol to make queries to an LDAP server. The LDAP server maintains a database and responds to these queries based on the contents of this database.

7.2 Transactions

The following transactions are used to provide communications between actors in accordance with one or more of the DICOM Configuration protocols.

Configure DHCP Server

This transaction changes the configuration on a DHCP server to reflect additions, deletions, and changes to the IP parameters that have been established for this network.

Find and Use DHCP Server

This transaction is a sequence of network messages that comply with the rules of the DHCP protocol. It allows a DHCP client to find available DHCP servers and select the server appropriate for that client. This transaction obtains the mandatory IP parameter information from the DHCP server and obtains additional optional parameters from the DHCP server.

Configure Client

The service staff uses this transaction to set the initial configuration for a client.

Maintain Lease

This transaction deals with how the DHCP client should behave when its IP lease is not renewed.

DDNS Coordination

This transaction documents whether the DHCP server is coordinating with a DNS server so that access to the DHCP client can be maintained using the hostname assigned to the DHCP client.

Resolve Hostname

This transaction obtains the IP address for a computer when given a hostname.

Maintain Time

These transactions are the activities needed for an NTP or SNTP client to maintain time synchronization with a master time service.

Find NTP Server

This transaction is the autodiscovery procedure defined for NTP. This may use either a broadcast method or a DHCP supported method.

Find LDAP Server

In this transaction the DNS server is queried to obtain the IP address, port, and name of the LDAP server.

Query LDAP Server

In this transaction the LDAP server is queried regarding contents of the LDAP database.

Client Update LDAP Server

This transaction updates the configuration database using LDAP update instructions from the client being configured.

Maintain LDAP Server

This transaction updates the configuration database using local services of the LDAP server.

Figure 7-1 shows the actors and their transactions. The usual device will have an NTP Client, DHCP Client, and LDAP client in addition to the other applications actors. The transactions "Configure DHCP Server", "Configure Client", and "Maintain LDAP Server" are not shown because these transactions are between a software actor and a human actor. DICOM does not specify the means or user interface. It only requires that certain capabilities be supported.

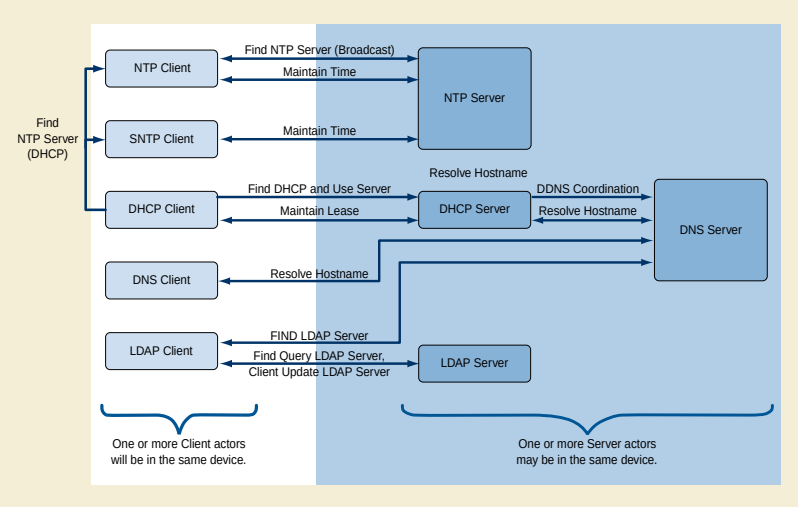

Figure 7-1. Transactions and Actors

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:

        i. the SOP Class UID (0008,0016) and SOP Instance UID (0008,0018)

        ii. the Instance Creation Date (0008,0012) and Instance Creation Time (0008,0013), if known

        iii. the SOP Instance Status

        iv. the SOP Authorization Date and Time (0100,0420)

        v. the SOP Authorization Comment, if any (0100,0424)

        vi. the SOP Equipment Certification Number (0100,0426)

        vii. the Study Instance UID (0020,000D) and Series Instance UID (0020,000E)

        viii. any Attributes of the General Equipment Module that are known

        ix. any overlay data present

        x. 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:

   i. delete the SOP Instance,

   ii. change the SOP Instance Status to Not Specified (NS),

   iii. 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.

A.4 Basic SR Digital Signatures Secure Use Profile

Any implementation that claims conformance to this Security Profile shall obey the following rules when creating a Structured Report or Key Object Selection Document that includes Digital Signatures:

a. When the implementation signs a Structured Report or Key Object Selection Document SOP Instance the Digital Signatures shall be created in accordance with the Structured Report RSA Digital Signature Profile.

b. In every signed Structured Report or Key Object Selection Document SOP Instance created, all referenced SOP Instances listed in the Referenced SOP Sequence Items of the Current Requested Procedure Evidence Sequence (0040,A375) and Pertinent Other Evidence Sequence (0040,A385)shall include either a Referenced Digital Signature Sequence or a Referenced SOP Instance MAC Sequence. The references may include both.

The implementation claiming conformance shall outline in its conformance statement the conditions under which it will either sign or not sign a Structured Report or Key Object Selection Document.

A.5 Audit Trail Message Format Profile

To help assure healthcare privacy and security in automated systems, usage data need to be collected. These data will be reviewed by administrative staff to verify that healthcare data is being used in accordance with the healthcare provider's data security requirements and to establish accountability for data use. This data collection and review process is called security auditing and the data itself

comprises the audit trail. Audit trails can be used for surveillance purposes to detect when interesting events might be happening that warrant further investigation.

This profile defines the format of the data to be collected and the minimum set of attributes to be captured by healthcare application systems for subsequent use by a review application. The data includes records of who accessed healthcare data, when, for what action, from where, and which patients' records were involved. No behavioral requirements are specified for when audit messages are generated, or for what action should be taken on their receipt. These are subject to local policy decisions and legal requirements.

Any implementation that claims conformance to this Security Profile shall:

a. format audit trail messages in accordance with the XML schema specified in A.5.1 in a fashion that allows those messages to be validated against that XML schema, following the general conventions specified in Section A.5.2.

b. for the events described in this Profile comply with the restrictions specified by this Profile in Section A.5.3, and describe in its conformance statement any extensions.

    Note

    An implementation may include implementation-specific extensions as long as the above conditions are met.

c. describe in its conformance statement the events that it can detect and report,

d. describe in its conformance statement the processing it can perform upon receipt of a message

e. describe in its conformance statement how event reporting and processing can be configured

    Note

    Other profiles specify the transmission of audit messages.

A.5.1 DICOM Audit Message Schema

Implementations claiming conformance to this profile shall use the following XML schema to format audit trail messages. This schema is derived from the schema specified in RFC 3881 IETF draft internet standard "Security Audit and Access Accountability XML Message Data Definitions for Healthcare Applications", according to W3C Recommendation "XML Schema Part 1: Structures," version 1.0, May 2001, and incorporates the DICOM extensions and restrictions outlined in Section A.5.2.

This schema is provided in Relax NG Compact format.

    Note

    This schema can be converted into an equivalent XML schema or other electronic format. It includes some modifications to the RFC 3881 schema that reflect field experience with audit message requirements. It extends the RFC 3881 schema.

A.5.1-1 Audit Message Schema

```
datatypes xsd = "http://www.w3.org/2001/XMLSchema-datatypes"

# This defines the coded value type. The comment shows a pattern that can be used to further
# constrain the token to limit it to the format of an OID.  Not all schema software
# implementations support the pattern option for tokens.
other-csd-attributes =
  (attribute codeSystemName { token } |     # OID pattern="[0-2]((\.0)|(\.[1-9][0-9]*))*"
    attribute codeSystemName { token }),   # This makes clear that codeSystemName is
                                  # either an OID or String
  attribute displayName { token }?,
  attribute originalText { token }         # Note: this also corresponds to DICOM "Code Meaning"
CodedValueType =
  attribute csd-code { token },
  other-csd-attributes

# Define the event identification, used later
```

```
EventIdentificationContents =
  element EventID { CodedValueType },
  element EventTypeCode { CodedValueType }*, # Note: DICOM/IHE defines and uses this
                                  # differently than RFC-3881
  attribute EventActionCode {              # Optional action code
    "C" |             ## Create
    "R" |             ## Read
    "U" |             ## Update
    "D" |             ## Delete
    "E"               ## Execute
  }?,

  attribute EventDateTime { xsd:dateTime },
  attribute EventOutcomeIndicator {
    "0" |           ## Nominal Success (use if status otherwise unknown or ambiguous)
    "4" |           ## Minor failure (per reporting application definition)
    "8" |           ## Serious failure (per reporting application definition)
    "12"             ## Major failure, (reporting application now unavailable)
  },

  element EventOutcomeDescription { text }?

# Define AuditSourceIdentification, used later
#  Note: This includes one constraint that cannot be represented yet in RNC.  The use
#        of a token other than the specified codes is permitted only if the codeSystemName
#        is present.
#  Note: This has no elements, only attributes.

AuditSourceIdentificationContents =
  attribute code {
    "1" |               ## End-user display device, diagnostic device
    "2" |               ## Data acquisition device or instrument
    "3" |               ## Web Server process or thread
    "4" |               ## Application Server process or thread
    "5" |               ## Database Server process or thread
    "6" |               ## Security server, e.g., a domain controller
    "7" |               ## ISO level 1-3 network component
    "8" |               ## ISO level 4-6 operating software
    "9" |               ## other
    token },              ## other values are allowed if a codeSystemName is present
  other-csd-attributes?,  ## If these are present, they define the meaning of code

  attribute AuditEnterpriseSiteID { token }?,
  attribute AuditSourceID { token },
  element AuditSourceTypeCode { token }*

# Define ActiveParticipantType, used later

ActiveParticipantContents =
  element RoleIDCode { CodedValueType }*,
  element MediaIdentifier {
    element MediaType { CodedValueType }
  }?,
  attribute UserID { text },
  attribute AlternativeUserID { text }?,
  attribute UserName { text }?,
  attribute UserIsRequestor { xsd:boolean },
  attribute NetworkAccessPointID { token }?,
  attribute NetworkAccessPointTypeCode {
```

```
    "1" |            ## Machine Name, including DNS name
    "2" |            ## IP Address
    "3" |            ## Telephone Number
    "4" |            ## Email address
    "5" }?           ## URI (user directory, HTTP-PUT, ftp, etc.)

# The BinaryValuePair is used in ParticipantObject descriptions to capture parameters.
# All values (even those that are normally plain text) are encoded as xsd:base64Binary.
# This is to preserve details of encoding (e.g., nulls) and to protect against text
# contents that contain XML fragments.  These are known attack points against applications,
# so security logs can be expected to need to capture them without modification by the
# audit encoding process.

ValuePair =
  # clarify the name
  attribute type { token },
  attribute value { xsd:base64Binary } # used to encode potentially binary, malformed XML text, etc.

# Define ParticipantObjectIdentification, used later

# Participant Object Description, used later

DICOMObjectDescriptionContents =
  element MPPS {
    attribute UID { token }       # OID pattern="[0-2]((\.0)|(\.[1-9][0-9]*))*"
  }*,
  element Accession {
    attribute Number { token }
  }*,
  element SOPClass {              # SOP class for one study
    element Instance {
      attribute UID { token }     # OID pattern="[0-2]((\.0)|(\.[1-9][0-9]*))*"
    }*,
    attribute UID { token }?,     # OID pattern="[0-2]((\.0)|(\.[1-9][0-9]*))*"
    attribute NumberOfInstances { xsd:integer }
  }*,
  element ParticipantObjectContainsStudy {
    element StudyIDs {
      attribute UID { token }
    }*
  },
  element Encrypted { xsd:boolean }?,
  element Anonymized { xsd:boolean }?

ParticipantObjectIdentificationContents =
  element ParticipantObjectIDTypeCode { CodedValueType },
  (element ParticipantObjectName { token } |            # either a name or
  element ParticipantObjectQuery { xsd:base64Binary }),  # a query ID field,
  element ParticipantObjectDetail { ValuePair }*,   # optional details, these can be extensive
                                    # and large
  element ParticipantObjectDescription { token }*,  # optional descriptive text
  DICOMObjectDescriptionContents,                # These are extensions made by DICOM to RFC-
                                    # 3881 schema for use describing DICOM objects
  attribute ParticipantObjectID { token },         # mandatory ID
  attribute ParticipantObjectTypeCode {           # optional type
    "1" | #3 Person
    "2" | #3 System object
    "3" | #3 Organization
    "4"   ## Other
  }?,
```

```
 attribute ParticipantObjectTypeCodeRole {         ## optional role
  "1" |        ## Patient
  "2" |        ## Location
  "3" |        ## Report
  "4" |        ## Resource
  "5" |        ## Master File
  "6" |        ## User
  "7" |        ## List
  "8" |        ## Doctor
  "9" |        ## Subscriber
  "10" |       ## guarantor
  "11" |       ## Security User Entity
  "12" |       ## Security User Group
  "13" |       ## Security Resource
  "14" |       ## Security Granulatiry Definition
  "15" |       ## Provider
  "16" |       ## Report Destination
  "17" |       ## Report Library
  "18" |       ## Schedule
  "19" |       ## Customer
  "20" |       ## Job
  "21" |       ## Job Stream
  "22" |       ## Table
  "23" |       ## Routing Criteria
  "24" }?,     ## Query?,

 attribute ParticipantObjectDataLifeCycle {         # optional life cycle stage
  "1" |        ## Origination, Creation
  "2" |        ## Import/ Copy
  "3" |        ## Amendment
  "4" |        ## Verification
  "5" |        ## Translation
  "6" |        ## Access/Use
  "7" |        ## De-identification
  "8" |        ## Aggregation, summarization, derivation
  "9" |        ## Report
  "10" |       ## Export
  "11" |       ## Disclosure
  "12" |       ## Receipt of Disclosure
  "13" |       ## Archiving
  "14" |       ## Logical deletion
  "15" }?,     ## Permanent erasure, physical destruction

 attribute ParticipantObjectSensistityParticipantObjectSensitivity { token }?

# The basic message
message =
 element AuditMessage {
  (element EventIdentification { EventIdentificationContents }, # The event must be identified
   element ActiveParticipant { ActiveParticipantContents }+, # It has one or more active
                                                             # participants
   element AuditSourceIdentification {                       # It is reported by one source
    AuditSourceIdentificationContents
   },
   element ParticipantObjectIdentification {                 # It may have other objects involved
    ParticipantObjectIdentificationContents
   }*)
 }
```

```
# And finally the magic statement that message is the root of everything.
start = message
```

A.5.2 General Message Format Conventions

The following table lists the primary fields from the message schema specified in A.5.1, with additional instructions, conventions, and restrictions on how DICOM applications shall fill in the field values. Please refer to RFC 3881 for the complete definition and specification of fields taken from the schema specified therein. In addition, the following table lists the additional fields that are part of DICOM-specific extensions in the DICOM Audit Message Schema (see Section A.5.1). The fields names are only those leaf elements and attributes that are specialized or extended for this profile. Note that these fields may be enclosed in other XML elements, as specified by the schema.

Table A.5.2-1. General Message Format

	Field Name	Opt.	Description from RFC 3881	Additional Conditions on Field Format/Value
Event	EventID	M	"Identifier for a specific audited event …"	The identifier for the family of event. E.g., "User Authentication". Extended by DICOM using DCID (400)
	EventActionCode	U	"Indicator for type of action performed during the event that generated the audit."	See Schema
	EventDateTime	M	"Universal coordinated time (UTC), i.e., a date/time specification that is unambiguous as to local time zones."	The time at which the audited event occurred.See Section A.5.2.5
	EventOutcomeIndicator	M	"Indicates whether the event succeeded or failed."	When a particular event has some aspects that succeeded and some that failed, then one message shall be generated for successful actions and one message for the failed actions (i.e., not a single message with mixed results).
	EventTypeCode	U	"Identifier for the category of event."	The specific type(s) within the family applicable to the event, e.g., "User Login". Extended by DICOM using DCID (401)
Active Participant (multi-valued)	UserID	M	"Unique identifier for the user actively participating in the event."	See Section A.5.2.1
	AlternativeUserID	U	"Alternative unique identifier for the user."	See Section A.5.2.2
	UserName	U	"The human-meaningful name for the user."	See Section A.5.2.3
	UserIsRequestor	M	"Indicator that the user is or is not the requestor, or initiator, for the event being audited."	Used to identify which of the participants initiated the transaction being audited. If the audit source cannot determine which of the participants is the requestor, then the field shall be present with the value FALSE in all participants. The system shall not identify multiple participants as UserIsRequestor. If there are several known requestors, the reporting system shall pick only one as UserIsRequestor.

	Field Name	Opt.	Description from RFC 3881	Additional Conditions on Field Format/Value
	RoleIDCode	U	"Specification of the role(s) the user plays when performing the event, as assigned in role-based access control security."	Extended by DICOM using DCID (402) Usage of this field is refined in the individual message descriptions below. Other additional roles may also be present, since this is a multi-valued field.
	NetworkAccessPointTypeCode	U	"An identifier for the type of network access point …"	See Section A.5.2.4
	NetworkAccessPointID	U	"An identifier for the network access point of the user device This could be a device id, IP address, or some other identifier associated with a device."	
Audit Source	AuditEnterpriseSiteID	U	"Logical source location within the healthcare enterprise network, e.g., a hospital or other provider location within a multi-entity provider group."	Serves to further qualify the Audit Source ID, since Audit Source ID is not required to be globally unique.
	AuditSourceID	M	"Identifier of the source …"	The identification of the system that detected the auditable event and created this audit message. Although often the audit source is one of the participants, it could also be an external system that is monitoring the activities of the participants (e.g., an add-on audit-generating device).
	AuditSourceTypeCode	U	"Code specifying the type of source …"	Used as defined in RFC 3881. E.g., an acquisition device might use "2" (data acquisition device), a PACS/RIS system might use "4 "(application server process).
Participant Object (multi-valued)	ParticipantObjectTypeCode	U	"Code for the participant object type being audited. This value is distinct from the user's role or any user relationship to the participant object."	Used as defined in RFC 3881
	ParticipantObjectTypeCodeRole	U	"Code representing the functional application role of Participant Object being audited."	Used as defined in RFC 3881
	ParticipantObjectDataLifeCycle	U	"Identifier for the data life-cycle stage for the participant object. This can be used to provide an audit trail for data, over time, as it passes through the system."	Used as defined in RFC 3881.
	ParticipantObjectIDTypeCode	M	"Describes the identifier that is contained in Participant Object ID."	Values may be drawn from those listed in RFC 3881 and DCID (404), as specified in the individual message descriptions.

	Field Name	Opt.	Description from RFC 3881	Additional Conditions on Field Format/Value
	ParticipantObjectSensitivity	U	"Denotes policy-defined sensitivity for the Participant Object ID such as VIP, HIV status, mental health status, or similar topics."	Used as defined in RFC 3881.
	ParticipantObjectID	M	"Identifies a specific instance of the participant object."	Usage refined by individual message descriptions
	ParticipantObjectName	U	"An instance-specific descriptor of the Participant Object ID audited, such as a person's name."	Usage refined by individual message descriptions
	ParticipantObjectQuery	U	"The actual query for a query-type participant object."	Usage refined by individual message descriptions
	ParticipantObjectDetail	U	"Implementation-defined data about specific details of the object accessed or used."	Used as defined in RFC 3881. Note The value field is xs:base64Binary encoded, making this attribute suitable for conveying binary data.
	SOPClass	MC	(DICOM extension)	The UIDs of SOP classes referred to in this participant object. Required if ParticipantObjectIDTypeCode is (110180, DCM, "Study Instance UID") and any of the optional fields (AccessionNumber, ContainsMPPS, NumberOfInstances, ContainsSOPInstances,Encrypted,Anonymized) are present in this Participant Object. May be present if ParticipantObjectIDTypeCode is (110180, DCM, "Study Instance UID") even though none of the optional fields are present.
	Accession	U	(DICOM extension)	An Accession Number(s) associated with this participant object.
	MPPS	U	(DICOM extension)	An MPPS Instance UID(s) associated with this participant object.
	NumberOfInstances	U	(DICOM extension)	The number of SOP Instances referred to by this participant object.
	Instance	U	(DICOM extension)	SOP Instance UID value(s) Note Including the list of SOP Instances can create a fairly large audit message. Under most circumstances, the list of SOP Instance UIDs is not needed for audit purposes.

	Field Name	Opt.	Description from RFC 3881	Additional Conditions on Field Format/Value
	Encrypted	U	(DICOM extension)	A single value of True or False indicating whether or not the data was encrypted. Note If there was a mix of encrypted and non-encrypted data, then create two event reports.
	Anonymized	U	(DICOM extension)	A single value of True or False indicating whether or not all patient identifying information was removed from the data
	ParticipantObjectContainsStudy	U	(DICOM extension)	A Study Instance UID, which may be used when the ParticipantObjectIDTypeCode is not (110180, DCM, "Study Instance UID").

A.5.2.1 UserID

If the participant is a person, then the User ID shall be the identifier used for that person on this particular system, in the form of login-Name@domain-name.

If the participant is an identifiable process, the UserID selected shall be one of the identifiers used in the internal system logs. For example, the User ID may be the process ID as used within the local operating system in the local system logs. If the participant is a node, then User ID may be the node name assigned by the system administrator. Other participants such as threads, relocatable processes, web service end-points, web server dispatchable threads, etc. will have an appropriate identifier. The implementation shall document in the conformance statement the identifiers used, see Section A.6. The purpose of this requirement is to allow matching of the audit log identifiers with internal system logs on the reporting systems. .

When importing or exporting data, e.g., by means of media, the UserID field is used both to identify people and to identify the media itself. When the Role ID Code is EV(110154, DCM, "Destination Media") or EV(110155, DCM, "Source Media"), the UserID may be:

a. a URI (the preferred form) identifying the source or destination,

b. an email address of the form "mailto:user@address"

c. a description of the media type (e.g., DVD) together with a description of its identifying label, as a free text field,

d. a description of the media type (e.g., paper, film) together with a description of the location of the media creator (i.e., the printer).

The UserID field for Media needs to be highly flexible given the large variety of media and transports that might be used.

A.5.2.2 AlternativeUserID

If the participant is a person, then Alternative User ID shall be the identifier used for that person within an enterprise for authentication purposes, for example, a Kerberos Username (user@realm). If the participant is a DICOM application, then Alternative User ID shall be one or more of the AE Titles that participated in the event. Multiple AE titles shall be encoded as:

AETITLES= *aetitle1;aetitle2;…*

When importing or exporting data, e.g., by means of media, the Alternative UserID field is used either to identify people or to identify the media itself. When the Role ID Code is (110154, DCM, "Destination Media") or (110155, DCM, "Source Media"), the Alternative UserID may be any machine readable identifications on the media, such as media serial number, volume label, or DICOMDIR SOP Instance UID.

A.5.2.3 Username

A human readable identification of the participant. If the participant is a person, the person's name shall be used. If the participant is a process, then the process name shall be used.

A.5.2.4 Multi-homed Nodes

The NetworkAccessPointTypeCode and NetworkAccessPointID can be ambiguous for systems that have multiple physical network connections. For these multi-homed nodes a single DNS name or IP address shall be selected and used when reporting audit events. DICOM does not require the use of a specific method for selecting the network connection to be used for identification, but it must be the same for all of the audit messages generated for events on that node.

A.5.2.5 EventDateTime

The EventDateTime is the date and time that the event being reported took place. Some events have a significant duration. In these cases, a date and time shall be chosen by a method that is consistent and appropriate for the event being reported.

The EventDateTime shall include the time zone information.

Creators of audit messages may support leap-seconds, but are not required to. Recipients of audit messages shall be able to process messages with leap-second information.

A.5.3 DICOM Specific Audit Messages

The following subsections define message specializations for use by implementations that claim conformance to the DICOM Audit Trail Profile. Any field (i.e., XML element and associated attributes) not specifically mentioned in the following tables shall follow the conventions specified in A.5.1 and A.5.2.

An implementation claiming conformance to this Profile that reports an activity covered by one of the audit messages defined by this Profile shall use the message format defined in this Profile. However, a system claiming conformance to this Profile is not required to send a message each time the activity reported by that audit message occurs. It is expected that the triggering of audit messages would be configurable on an individual basis, to be able to balance network load versus the severity of threats, in accordance with local security policies.

Note

1. It is a system design issue outside the scope of DICOM as to what entity actually sends an audit event and when. For example, a Query message could be generated by the entity where the query originated, by the entity that eventually would respond to the query, or by a monitoring entity not directly involved with the query, but that generates audit messages based on monitored network traffic.

2. To report events that are similar to the events described here, these definitions can be used as the basis for extending the schema.

In the subsequent tables, the information entity column indicates the relationship between real world entities and the information elements encoded into the message.

A.5.3.1 Application Activity

This audit message describes the event of an Application Entity starting or stopping. This is closely related to the more general case of any kind of application startup or shutdown, and may be suitable for those purposes also.

Table A.5.3.1-1. Application Activity Message

Real World Entities	Field Name	Opt.	Value Constraints
Event	EventID	M	EV (110100, DCM,"Application Activity")
	EventActionCode	M	Enumerated Value E = Execute
	EventDateTime	M	not specialized
	EventOutcomeIndicator	M	not specialized

Real World Entities	Field Name	Opt.	Value Constraints
	EventTypeCode	M	DT (110120, DCM, "Application Start") DT (110121, DCM, "Application Stop")
Active Participant: Application started (1)	UserID	M	The identity of the process started or stopped formatted as specified in A.5.2.1.
	AlternativeUserID	MC	If the process supports DICOM, then the AE Titles as specified in A.5.2.2.
	UserName	U	not specialized
	UserIsRequestor	M	not specialized
	RoleIDCode	M	EV (110150, DCM, "Application")
	NetworkAccessPointTypeCode	U	not specialized
	NetworkAccessPointID	U	not specialized
Active Participant: Persons and or processes that started the Application (0..N)	UserID	M	The person or process starting or stopping the Application
	AlternativeUserID	U	not specialized
	UserName	U	not specialized
	UserIsRequestor	M	not specialized
	RoleIDCode	M	EV (110151, DCM, "Application Launcher")
	NetworkAccessPointTypeCode	U	not specialized
	NetworkAccessPointID	U	not specialized

No Participant Objects are needed for this message.

A.5.3.2 Audit Log Used

This message describes the event of a person or process reading a log of audit trail information.

Note

For example, an implementation that maintains a local cache of audit information that has not been transferred to a central collection point might generate this message if its local cache were accessed by a user.

Table A.5.3.2-1. Audit Log Used Message

Real World Entities	Field Name	Opt.	Value Constraints
Event	EventID	M	EV (110101, DCM, "Audit Log Used")
	EventActionCode	M	Shall be enumerated value: R = read
	EventDateTime	M	not specialized
	EventOutcomeIndicator	M	not specialized
	EventTypeCode	U	not specialized

Real World Entities	Field Name	Opt.	Value Constraints
Active Participant: Persons and or processes that started the Application (1..2)	UserID	M	The person or process accessing the audit trail. If both are known, then two active participants shall be included (both the person and the process).
	AlternativeUserID	U	not specialized
	UserName	U	not specialized
	UserIsRequestor	M	not specialized
	RoleIDCode	U	not specialized
	NetworkAccessPointTypeCode	U	not specialized
	NetworkAccessPointID	U	not specialized
Participating Object: Identity of the audit log (1)	ParticipantObjectTypeCode	M	Shall be: 2 = system
	ParticipantObjectTypeCodeRole	M	Shall be: 13 = security resource
	ParticipantObjectDataLifeCycle	U	not specialized
	ParticipantObjectIDTypeCode	M	Shall be: 12 = URI
	ParticipantObjectSensitivity	U	not specialized
	ParticipantObjectID	M	The URI of the audit log
	ParticipantObjectName	U	Shall be: "Security Audit Log"
	ParticipantObjectQuery	U	not specialized
	ParticipantObjectDetail	U	not specialized
	ParticipantObjectDescription	U	not specialized
	SOPClass	U	See Section A.5.2
	Accession	U	See Section A.5.2
	NumberOfInstances	U	See Section A.5.2
	Instances	U	See Section A.5.2
	Encrypted	U	See Section A.5.2
	Anonymized	U	See Section A.5.2
	ParticipantObjectContainsStudy	U	See Section A.5.2

A.5.3.3 Begin Transferring DICOM Instances

This message describes the event of a system beginning to transfer a set of DICOM instances from one node to another node within control of the system's security domain. This message may only include information about a single patient.

Note

A separate Instances Transferred message is defined for transfer completion, allowing comparison of what was intended to be sent and what was actually sent.

Table A.5.3.3-1. Audit Message for Begin Transferring DICOM Instances

Real World Entities	Field Name	Opt.	Value Constraints
Event	EventID	M	EV (110102, DCM, "Begin Transferring DICOM Instances")
	EventActionCode	M	Shall be: E = Execute
	EventDateTime	M	not specialized
	EventOutcomeIndicator	M	not specialized

Real World Entities	Field Name	Opt.	Value Constraints
	EventTypeCode	U	not specialized
Active Participant: Process Sending the Data (1)	UserID	M	The identity of the process sending the data.
	AlternativeUserID	U	not specialized
	UserName	U	not specialized
	UserIsRequestor	M	not specialized
	RoleIDCode	M	EV (110153, DCM, "Source Role ID")
	NetworkAccessPointTypeCode	U	not specialized
	NetworkAccessPointID	U	not specialized
Active Participant: Process receiving the data (1)	UserID	M	The identity of the process receiving the data.
	AlternativeUserID	U	not specialized
	UserName	U	not specialized
	UserIsRequestor	M	not specialized
	RoleIDCode	M	EV (110152, DCM, "Destination Role ID")
	NetworkAccessPointTypeCode	U	not specialized
	NetworkAccessPointID	U	not specialized
Active Participant: Other Participants (0..N)	UserID	M	The identity of any other participants that might be involved and known, especially third parties that are the requestor
	AlternativeUserID	U	not specialized
	UserName	U	not specialized
	UserIsRequestor	M	not specialized
	RoleIDCode	U	not specialized
	NetworkAccessPointTypeCode	U	not specialized
	NetworkAccessPointID	U	not specialized
Participating Object: Studies being transferred (1..N)	ParticipantObjectTypeCode	M	Shall be: 2 = system
	ParticipantObjectTypeCodeRole	M	Shall be: 3 = report
	ParticipantObjectDataLifeCycle	U	not specialized
	ParticipantObjectIDTypeCode	M	EV (110180, DCM, "Study Instance UID")
	ParticipantObjectSensitivity	U	not specialized
	ParticipantObjectID	M	The Study Instance UID
	ParticipantObjectName	U	not specialized
	ParticipantObjectQuery	U	not specialized
	ParticipantObjectDetail	U	Element "ContainsSOPClass" with one or more SOP Class UID values
	ParticipantObjectDescription	U	not specialized
	SOPClass	MC	not specialized
	Accession	U	not specialized
	NumberOfInstances	U	not specialized
	Instances	U	not specialized
	Encrypted	U	not specialized
	Anonymized	U	not specialized

Real World Entities	Field Name	Opt.	Value Constraints
Participating Object: Patient (1)	ParticipantObjectTypeCode	M	Shall be: 1 = person
	ParticipantObjectTypeCodeRole	M	Shall be: 1 = patient
	ParticipantObjectDataLifeCycle	U	not specialized
	ParticipantObjectIDTypeCode	M	Shall be: 2 = patient ID
	ParticipantObjectSensitivity	U	not specialized
	ParticipantObjectID	M	The patient ID
	ParticipantObjectName	U	The patient name
	ParticipantObjectQuery	U	not specialized
	ParticipantObjectDetail	U	not specialized
	ParticipantObjectDescription	U	not specialized

A.5.3.4 Data Export

This message describes the event of exporting data from a system, meaning that the data is leaving control of the system's security domain. Examples of exporting include printing to paper, recording on film, conversion to another format for storage in an EHR, writing to removable media, or sending via e-mail. Multiple patients may be described in one event message.

Table A.5.3.4-1. Audit Message for Data Export

Real World Entities	Field Name	Opt.	Value Constraints
Event	EventID	M	EV (110106, DCM, "Export")
	EventActionCode	M	Shall be: R = Read
	EventDateTime	M	not specialized
	EventOutcomeIndicator	M	not specialized
	EventTypeCode	U	not specialized
Participating Object: Remote Users and Processes (0..n)	UserID	M	The identity of the remote user or process receiving the data
	AlternativeUserID	U	not specialized
	UserName	U	not specialized
	UserIsRequestor	M	See Section A.5.3.4.1
	RoleIDCode	M	EV (110152, DCM, "Destination Role ID")
	NetworkAccessPointTypeCode	U	not specialized
	NetworkAccessPointID	U	not specialized
Participating Object: User or Process Exporting the data(1..2)	UserID	M	The identity of the local user or process exporting the data. If both are known, then two active participants shall be included (both the person and the process).
	AlternativeUserID	U	not specialized
	UserName	U	not specialized
	UserIsRequestor	M	See Section A.5.3.4.1
	RoleIDCode	M	EV (110153, DCM, "Source Role ID")
	NetworkAccessPointTypeCode	U	not specialized
	NetworkAccessPointID	U	not specialized

Real World Entities	Field Name	Opt.	Value Constraints
Active Participant: Media (1)	UserID	M	See Section A.5.2.3
	AlternativeUserID	U	See Section A.5.2.4
	UserName	U	not specialized
	UserIsRequestor	M	Shall be FALSE
	RoleIDCode	M	EV (110154, DCM, "Destination Media")
	NetworkAccessPointTypeCode	MC	Required if being exported to other than physical media, e.g., to a network destination rather than to film, paper or CD. May be present otherwise.
	NetworkAccessPointID	MC	Required if Net Access Point Type Code is present. May be present otherwise.
	MediaIdentifier	MC	Volume ID, URI, or other identifier for media. Required if digital media. May be present otherwise.
	MediaType	M	Values selected from DCID (405)
Participating Object: Studies (0..N)	ParticipantObjectTypeCode	M	Shall be: 2 = system
	ParticipantObjectTypeCodeRole	M	Shall be: 3 = report
	ParticipantObjectDataLifeCycle	U	not specialized
	ParticipantObjectIDTypeCode	M	EV (110180, DCM, "Study Instance UID")
	ParticipantObjectSensitivity	U	not specialized
	ParticipantObjectID	M	The Study Instance UID
	ParticipantObjectName	U	not specialized
	ParticipantObjectQuery	U	not specialized
	ParticipantObjectDetail	U	not specialized
	ParticipantObjectDescription	U	not specialized
	SOPClass	MC	See Table A.5.2-1
	Accession	U	not specialized
	NumberOfInstances	U	not specialized
	Instances	U	not specialized
	Encrypted	U	not specialized
	Anonymized	U	not specialized
Participating Object: Patients (1..N)	ParticipantObjectTypeCode	M	Shall be: 1 = person
	ParticipantObjectTypeCodeRole	M	Shall be: 1 = patient
	ParticipantObjectDataLifeCycle	U	not specialized
	ParticipantObjectIDTypeCode	M	Shall be: 2 = patient ID
	ParticipantObjectSensitivity	U	not specialized
	ParticipantObjectID	M	The patient ID
	ParticipantObjectName	U	The patient name
	ParticipantObjectQuery	U	not specialized
	ParticipantObjectQuery	U	not specialized
	ParticipantObjectDetail	U	not specialized
	ParticipantObjectDescription	U	not specialized

A.5.3.4.1 UserIsRequestor

A single user (either local or remote) shall be identified as the requestor, i.e., UserIsRequestor with a value of TRUE. This accommodates both push and pull transfer models for media.

A.5.3.5 Data Import

This message describes the event of importing data into an organization, implying that the data now entering the system was not under the control of the security domain of this organization. Transfer by media within an organization is often considered a data transfer rather than a data import event. An example of importing is creating new local instances from data on removable media. Multiple patients may be described in one event message.

A single user (either local or remote) shall be identified as the requestor, i.e., UserIsRequestor with a value of TRUE. This accommodates both push and pull transfer models for media.

Table A.5.3.5-1. Audit Message for Data Import

Real World Entities	Field Name	Opt.	Value Constraints
Event	EventID	M	EV (110107, DCM, "Import")
	EventActionCode	M	Shall be: C = Create
	EventDateTime	M	not specialized
	EventOutcomeIndicator	M	not specialized
	EventTypeCode	U	not specialized
Participating Object: User or Process Importing the data (1..n)	UserID	M	The identity of the local user or process importing the data.
	AlternativeUserID	U	not specialized
	UserName	U	not specialized
	UserIsRequestor	M	See Section A.5.3.5
	RoleIDCode	M	EV (110152, DCM, "Destination Role ID")
	NetworkAccessPointTypeCode	U	not specialized
	NetworkAccessPointID	U	not specialized
Active Participant: Source Media (1)	UserID	M	See Section A.5.2.3
	AlternativeUserID	U	See Section A.5.2.4
	UserName	U	not specialized
	UserIsRequestor	M	Shall be FALSE
	RoleIDCode	M	EV (110155, DCM, "Source Media")
	NetworkAccessPointTypeCode	U	not specialized
	NetworkAccessPointID	MC	Shall be present if Net Access Point Type Code is present. Shall use fields as specified in RFC 3881.
	MediaIdentifier	M	Volume ID, URI, or other identifier for media
	MediaType	M	Values selected from DCID (405)
Active Participant: Source (0..n)	UserID	M	See Section A.5.2.3
	AlternativeUserID	U	See Section A.5.2.4
	UserName	U	not specialized
	UserIsRequestor	M	See Section A.5.3.5
	RoleIDCode	M	EV (110153, DCM, "Source Role ID")
	NetworkAccessPointTypeCode	U	not specialized

Real World Entities	Field Name	Opt.	Value Constraints
	NetworkAccessPointID	MC	Shall be present if Net Access Point Type Code is present.
Participating Object: Studies (0..N)	ParticipantObjectTypeCode	M	Shall be: 2 = system
	ParticipantObjectTypeCodeRole	M	Shall be: 3 = report
	ParticipantObjectDataLifeCycle	U	not specialized
	ParticipantObjectIDTypeCode	M	EV (110180, DCM, "Study Instance UID")
	ParticipantObjectSensitivity	U	not specialized
	ParticipantObjectID	M	The Study Instance UID
	ParticipantObjectName	U	not specialized
	ParticipantObjectQuery	U	not specialized
	ParticipantObjectDetail	U	Not specialized
	ParticipantObjectDescription	U	not specialized
	SOPClass	MC	See Table A.5.2-1
	Accession	U	not specialized
	NumberOfInstances	U	not specialized
	Instances	U	not specialized
	Encrypted	U	not specialized
	Anonymized	U	not specialized
Participating Object: Patients (1..N)	ParticipantObjectTypeCode	M	Shall be: 1 = person
	ParticipantObjectTypeCodeRole	M	Shall be: 1 = patient
	ParticipantObjectDataLifeCycle	U	not specialized
	ParticipantObjectIDTypeCode	M	Shall be: 2 = patient ID
	ParticipantObjectSensitivity	U	not specialized
	ParticipantObjectID	M	The patient ID
	ParticipantObjectName	U	The patient name
	ParticipantObjectQuery	U	not specialized
	ParticipantObjectDetail	U	not specialized
	ParticipantObjectDescription	U	not specialized

A.5.3.6 DICOM Instances Accessed

This message describes the event of DICOM SOP Instances being viewed, utilized, updated, or deleted. This message shall only include information about a single patient and can be used to summarize all activity for several studies for that patient. This message records the studies to which the instances belong, not the individual instances.

If all instances within a study are deleted, then the EV(110105, DCM, "DICOM Study Deleted") event shall be used, see Section A.5.3.8.

Table A.5.3.6-1. Audit Message for DICOM Instances Accessed

Real World Entities	Field Name	Opt.	Value Constraints
Event	EventID	M	EV (110103, DCM, "DICOM Instances Accessed")

Real World Entities	Field Name	Opt.	Value Constraints
	EventActionCode	M	Enumerated value: C = create R = read U = update D = delete
	EventDateTime	M	not specialized
	EventOutcomeIndicator	M	not specialized
	EventTypeCode	U	not specialized
Active Participant: Person and or Process manipulating the data (1..2)	UserID	M	not specialized
	AlternativeUserID	U	not specialized
	UserName	U	not specialized
	UserIsRequestor	M	not specialized
	RoleIDCode	U	not specialized
	NetworkAccessPointTypeCode	U	not specialized
	NetworkAccessPointID	U	not specialized
Participating Object: Studies (1..N)	ParticipantObjectTypeCode	M	Shall be: 2 = system
	ParticipantObjectTypeCodeRole	M	Shall be: 3 = report
	ParticipantObjectDataLifeCycle	U	not specialized
	ParticipantObjectIDTypeCode	M	EV (110180, DCM, "Study Instance UID")
	ParticipantObjectSensitivity	U	not specialized
	ParticipantObjectID	M	The Study Instance UID
	ParticipantObjectName	U	not specialized
	ParticipantObjectQuery	U	not specialized
	ParticipantObjectDetail	U	Not specialized
	ParticipantObjectDescription	U	Not specialized
	SOPClass	MC	See Table A.5.2-1
	Accession	U	not specialized
	NumberOfInstances	U	not specialized
	Instances	U	not specialized
	Encrypted	U	not specialized
	Anonymized	U	not specialized
Participating Object: Patient (1)	ParticipantObjectTypeCode	M	Shall be: 1 = person
	ParticipantObjectTypeCodeRole	M	Shall be: 1 = patient
	ParticipantObjectDataLifeCycle	U	not specialized
	ParticipantObjectIDTypeCode	M	Shall be: 2 = patient ID
	ParticipantObjectSensitivity	U	not specialized
	ParticipantObjectID	M	The patient ID
	ParticipantObjectName	U	The patient name
	ParticipantObjectQuery	U	not specialized
	ParticipantObjectDetail	U	not specialized

Real World Entities	Field Name	Opt.	Value Constraints
	ParticipantObjectDescription	U	not specialized

A.5.3.7 DICOM Instances Transferred

This message describes the event of the completion of transferring DICOM SOP Instances between two Application Entities. This message may only include information about a single patient.

Note

This message may have been preceded by a Begin Transferring Instances message. The Begin Transferring Instances message conveys the intent to store SOP Instances, while the Instances Transferred message records the completion of the transfer. Any disagreement between the two messages might indicate a potential security breach.

Table A.5.3.7-1. Audit Message for DICOM Instances Transferred

Real World Entities	Field Name	Opt.	Value Constraints
Event	EventID	M	EV (110104, DCM, "DICOM Instances Transferred")
	EventActionCode	M	Enumerated Value: C = (create) if the receiver did not hold copies of the instances transferred R = (read) if the receiver already holds copies of the SOP Instances transferred, and has determined that no changes are needed to the copies held. U = (update) if the receiver is altering its held copies to reconcile differences between the held copies and the received copies. If the Audit Source is either not the receiver, or otherwise does not know whether or not the instances previously were held by the receiving node, then use "R" = (Read).
	EventDateTime	M	Shall be the time when the transfer has completed
	EventOutcomeIndicator	M	not specialized
	EventTypeCode	U	not specialized
Active Participant: Process that sent the data (1)	UserID	M	not specialized
	AlternativeUserID	U	not specialized
	UserName	U	not specialized
	UserIsRequestor	M	not specialized
	RoleIDCode	M	EV (110153, DCM, "Source Role ID")
	NetworkAccessPointTypeCode	U	not specialized
	NetworkAccessPointID	U	not specialized
Active Participant: The process that received the data. (1)	UserID	M	not specialized
	AlternativeUserID	U	not specialized
	UserName	U	not specialized
	UserIsRequestor	M	not specialized
	RoleIDCode	M	EV (110152, DCM, "Destination Role ID")

Real World Entities	Field Name	Opt.	Value Constraints
	NetworkAccessPointTypeCode	U	not specialized
	NetworkAccessPointID	U	not specialized
Active Participant: Other participants that are known, especially third parties that are the requestor (0..N)	UserID	M	not specialized
	AlternativeUserID	U	not specialized
	UserName	U	not specialized
	UserIsRequestor	M	not specialized
	RoleIDCode	U	not specialized
	NetworkAccessPointTypeCode	U	not specialized
	NetworkAccessPointID	U	not specialized
Participating Object: Studies being transferred (1..N)	ParticipantObjectTypeCode	M	Shall be: 2 = system
	ParticipantObjectTypeCodeRole	M	Shall be: 3 = report
	ParticipantObjectDataLifeCycle	U	not specialized
	ParticipantObjectIDTypeCode	M	EV (110180, DCM, "Study Instance UID")
	ParticipantObjectSensitivity	U	not specialized
	ParticipantObjectID	M	The Study Instance UID
	ParticipantObjectName	U	not specialized
	ParticipantObjectQuery	U	not specialized
	ParticipantObjectDetail	U	Not specialized
	ParticipantObjectDescription	U	Not specialized
	SOPClass	MC	See Table A.5.2-1
	Accession	U	not specialized
	NumberOfInstances	U	not specialized
	Instances	U	not specialized
	Encrypted	U	not specialized
	Anonymized	U	not specialized
Participating Object: Patient (1)	ParticipantObjectTypeCode	M	Shall be: 1 = person
	ParticipantObjectTypeCodeRole	M	Shall be: 1 = patient
	ParticipantObjectDataLifeCycle	U	not specialized
	ParticipantObjectIDTypeCode	M	Shall be: 2 = patient ID
	ParticipantObjectSensitivity	U	not specialized
	ParticipantObjectID	M	The patient ID
	ParticipantObjectName	U	The patient name
	ParticipantObjectQuery	U	not specialized
	ParticipantObjectDetail	U	not specialized
	ParticipantObjectDescription	U	not specialized

A.5.3.8 DICOM Study Deleted

This message describes the event of deletion of one or more studies and all associated SOP Instances in a single action. This message shall only include information about a single patient.

Table A.5.3.8-1. Audit Message for DICOM Study Deleted

Real World Entities	Field Name	Opt.	Value Constraints
Event	EventID	M	EV (110105, DCM, "DICOM Study Deleted")
	EventActionCode	M	Shall be: D = delete
	EventDateTime	M	not specialized
	EventOutcomeIndicator	M	not specialized
	EventTypeCode	U	not specialized
Active Participant: the person or process deleting the study (1..2)	UserID	M	not specialized
	AlternativeUserID	U	not specialized
	UserName	U	not specialized
	UserIsRequestor	M	not specialized
	RoleIDCode	U	not specialized
	NetworkAccessPointTypeCode	U	not specialized
	NetworkAccessPointID	U	not specialized
Participating Object: Studies being transferred (1..N)	ParticipantObjectTypeCode	M	Shall be: 2 = system
	ParticipantObjectTypeCodeRole	M	Shall be: 3 = report
	ParticipantObjectDataLifeCycle	U	not specialized
	ParticipantObjectIDTypeCode	M	EV (110180, DCM, "Study Instance UID")
	ParticipantObjectSensitivity	U	not specialized
	ParticipantObjectID	M	The Study Instance UID
	ParticipantObjectName	U	not specialized
	ParticipantObjectQuery	U	not specialized
	ParticipantObjectDetail	U	Not specialized
	ParticipantObjectDescription	U	Not specialized
	SOPClass	MC	See Table A.5.2-1
	Accession	U	not specialized
	NumberOfInstances	U	not specialized
	Instances	U	not specialized
	Encrypted	U	not specialized
	Anonymized	U	not specialized
Participating Object: Patient (1)	ParticipantObjectTypeCode	M	Shall be: 1 = person
	ParticipantObjectTypeCodeRole	M	Shall be: 1 = patient
	ParticipantObjectDataLifeCycle	U	not specialized
	ParticipantObjectIDTypeCode	M	Shall be: 2 = patient ID
	ParticipantObjectSensitivity	U	not specialized
	ParticipantObjectID	M	The patient ID
	ParticipantObjectName	U	The patient name
	ParticipantObjectQuery	U	not specialized
	ParticipantObjectDetail	U	not specialized
	ParticipantObjectDescription	U	not specialized

A.5.3.9 Network Entry

This message describes the event of a system, such as a mobile device, intentionally entering or leaving the network.

Note

The machine should attempt to send this message prior to detaching. If this is not possible, it should retain the message in a local buffer so that it can be sent later. The mobile machine can then capture audit messages in a local buffer while it is outside the secure domain. When it is reconnected to the secure domain, it can send the detach message (if buffered), followed by the buffered messages, followed by a mobile machine message for rejoining the secure domain. The timestamps on these messages is the time that the event was noticed to have occurred, not the time that the message is sent.

Table A.5.3.9-1. Audit Message for Network Entry

Real World Entities	Field Name	Opt.	Value
Event	EventID	M	EV (110108, DCM, "Network Entry")
	EventActionCode	M	Shall be: E = Execute
	EventDateTime	M	not specialized
	EventOutcomeIndicator	M	not specialized
	EventTypeCode	M	EV (110124, DCM, "Attach")EV (110125, DCM, "Detach")
Active Participant: Node or System entering or leaving the network (1)	UserID	M	not specialized
	AlternativeUserID	U	not specialized
	UserName	U	not specialized
	UserIsRequestor	M	Shall be FALSE
	RoleIDCode	U	not specialized
	NetworkAccessPointTypeCode	U	not specialized
	NetworkAccessPointID	U	not specialized

No Participant Objects are needed for this message.

A.5.3.10 Query

This message describes the event of a Query being issued or received. The message does not record the response to the query, but merely records the fact that a query was issued. For example, this would report queries using the DICOM SOP Classes:

a. Modality Worklist

b. UPS Pull

c. UPS Watch

d. Composite Instance Query

Note

1. The response to a query may result in one or more Instances Transferred or Instances Accessed messages, depending on what events transpire after the query. If there were security-related failures, such as access violations, when processing a query, those failures should show up in other audit messages, such as a Security Alert message.

2. Non-DICOM queries may also be captured by this message. The Participant Object ID Type Code, the Participant Object ID, and the Query fields may have values related to such non-DICOM queries.

Table A.5.3.10-1. Audit Message for Query

Real World Entities	Field Name	Opt.	Value Constraints
Event	EventID	M	EV (110112, DCM, "Query")
	EventActionCode	M	Shall be: E = Execute
	EventDateTime	M	not specialized
	EventOutcomeIndicator	M	not specialized
	EventTypeCode	U	not specialized
Active Participant: Process Issuing the Query (1)	UserID	M	not specialized
	AlternativeUserID	U	not specialized
	UserName	U	not specialized
	UserIsRequestor	M	not specialized
	RoleIDCode	M	EV (110153, DCM, "Source Role ID")
	NetworkAccessPointTypeCode	U	not specialized
	NetworkAccessPointID	U	not specialized
Active Participant: The process that will respond to the query (1)	UserID	M	not specialized
	AlternativeUserID	U	not specialized
	UserName	U	not specialized
	UserIsRequestor	M	not specialized
	RoleIDCode	M	EV (110152, DCM, "Destination Role ID")
	NetworkAccessPointTypeCode	U	not specialized
	NetworkAccessPointID	U	not specialized
Active Participant: Other Participants that are known, especially third parties that requested the query (0..N)	UserID	M	not specialized
	AlternativeUserID	U	not specialized
	UserName	U	not specialized
	UserIsRequestor	M	not specialized
	RoleIDCode	U	not specialized
	NetworkAccessPointTypeCode	U	not specialized
	NetworkAccessPointID	U	not specialized
Participating Object: SOP Queried and the Query (1)	ParticipantObjectTypeCode	M	Shall be: 2 = system
	ParticipantObjectTypeCodeRole	M	Shall be: 3 = report
	ParticipantObjectDataLifeCycle	U	not specialized
	ParticipantObjectIDTypeCode	M	DT (110181, DCM, "SOP Class UID")
	ParticipantObjectSensitivity	U	not specialized
	ParticipantObjectID	M	If the ParticipantObjectIDTypeCode is (110181, DCM, "SOP Class UID"), then this field shall hold the UID of the SOP Class being queried
	ParticipantObjectName	U	not specialized

Real World Entities	Field Name	Opt.	Value Constraints
	ParticipantObjectQuery	M	If the ParticipantObjectIDTypeCode is (110181, DCM, "SOP Class UID"), then this field shall hold the Dataset of the DICOM query, xs:base64Binary encoded. Otherwise, it shall be the query in the format of the protocol used.
	ParticipantObjectDetail	MC	Required if the ParticipantObjectIDTypeCode is (110181, DCM, "SOP Class UID") A ParticipantObjectDetail element with the XML attribute "TransferSyntax" shall be present. The value of the Transfer Syntax attribute shall be the UID of the transfer syntax of the query. The element contents shall be xs:base64Binary encoding. The Transfer Syntax shall be a DICOM Transfer Syntax.
	ParticipantObjectDescription	U	not specialized
	SOPClass	U	See Table A.5.2-1
	Accession	U	not specialized
	NumberOfInstances	U	not specialized
	Instances	U	not specialized
	Encrypted	U	not specialized
	Anonymized	U	not specialized

A.5.3.11 Security Alert

This message describes any event for which a node needs to report a security alert, e.g., a node authentication failure when establishing a secure communications channel.

Note

The Node Authentication event can be used to report both successes and failures. If reporting of success is done, this could generate a very large number of audit messages, since every authenticated DICOM association, HL7 transaction, and HTML connection should result in a successful node authentication. It is expected that in most situations only the failures will be reported.

Table A.5.3.11-1. Audit Message for Security Alert

Real World Entities	Field Name	Opt.	Value Constraints
Event	EventID	M	EV (110113, DCM, "Security Alert")
	EventActionCode	M	Shall be: E = Execute
	EventDateTime	M	not specialized
	EventOutcomeIndicator	M	Success implies an informative alert. The other failure values imply warning codes that indicate the severity of the alert. A Minor or Serious failure indicates that mitigation efforts were effective in maintaining system security. A Major failure indicates that mitigation efforts may not have been effective, and that the security system may have been compromised.
	EventTypeCode	M	Values selected from DCID(403)

Real World Entities	Field Name	Opt.	Value Constraints
Active Participant: Reporting Person and/or Process (1..2)	UserID	M	not specialized
	AlternativeUserID	U	not specialized
	UserName	U	not specialized
	UserIsRequestor	M	not specialized
	RoleIDCode	U	not specialized
	NetworkAccessPointTypeCode	U	not specialized
	NetworkAccessPointID	U	not specialized
Active Participant: Performing Persons or Processes (0..N)	UserID	M	not specialized
	AlternativeUserID	U	not specialized
	UserName	U	not specialized
	UserIsRequestor	M	Shall be FALSE
	RoleIDCode	U	not specialized
	NetworkAccessPointTypeCode	U	not specialized
	NetworkAccessPointID	U	not specialized
Participating Object: Alert Subject (0..N)	ParticipantObjectTypeCode	M	Shall be: 2 = system
	ParticipantObjectTypeCodeRole	U	Defined Terms: 5 = master file 13 = security resource
	ParticipantObjectDataLifeCycle	U	not specialized
	ParticipantObjectIDTypeCode	M	Defined Terms: 12 = URI(110182, DCM, "Node ID") = Node Identifier
	ParticipantObjectSensitivity	U	not specialized
	ParticipantObjectID	M	For a ParticipantObjectIDTypeCode of 12 (URI), then this value shall be the URI of the file or other resource that is the subject of the alert. For a ParticipantObjectIDTypeCode of (110182, DCM, "Node ID") then the value shall include the identity of the node that is the subject of the alert either in the form ofnode_name@domain_nameor as an IP address. Otherwise, the value shall be an identifier of the type specified by ParticipantObjectIDTypeCode of the subject of the alert.
	ParticipantObjectName	U	not specialized
	ParticipantObjectQuery	U	not specialized
	ParticipantObjectDetail	M	An element with the Attribute "type" equal to "Alert Description" shall be present with a free text description of the nature of the alert as the value
	ParticipantObjectDescription	U	not specialized
	SOPClass	U	See Table A.5.2-1
	Accession	U	not specialized
	NumberOfInstances	U	not specialized
	Instances	U	not specialized

Real World Entities	Field Name	Opt.	Value Constraints
	Encrypted	U	not specialized
	Anonymized	U	not specialized

A.5.3.12 User Authentication

This message describes the event that a user has attempted to log on or log off. This report can be made regardless of whether the attempt was successful or not. No Participant Objects are needed for this message.

Note

The user usually has UserIsRequestor TRUE, but in the case of a logout timer, the Node might be the UserIsRequestor.

Table A.5.3.12-1. Audit Message for User Authentication

Real World Entities	Field Name	Opt.	Value Constraints
Event	EventID	M	EV (110114, DCM, "User Authentication")
	EventActionCode	M	Shall be: E = Execute
	EventDateTime	M	not specialized
	EventOutcomeIndicator	M	not specialized
	EventTypeCode	M	Defined Terms: EV (110122, DCM, "Login") EV (110123, DCM, "Logout")
Active Participant: Person Authenticated or claimed (1)	UserID	M	not specialized
	AlternativeUserID	U	not specialized
	UserName	U	not specialized
	UserIsRequestor	M	not specialized
	RoleIDCode	U	not specialized
	NetworkAccessPointTypeCode	M	not specialized
	NetworkAccessPointID	M	not specialized
Active Participant: Node or System performing authentication (0..1)	UserID	M	not specialized
	AlternativeUserID	U	not specialized
	UserName	U	not specialized
	UserIsRequestor	M	not specialized
	RoleIDCode	U	not specialized
	NetworkAccessPointTypeCode	U	not specialized
	NetworkAccessPointID	U	not specialized

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

This profile defines the transmission of audit trail messages. Transport Layer Security (TLS) Transport Mapping for Syslog (RFC 5425) provides the mechanisms for reliable transport, buffering, acknowledgement, authentication, identification, and encryption. The RFC5424 states that the TLS used MUST be TLS version 1.2. 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. Systems that comply with this profile shall support message sizes of at least 32768 octets.

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 Syslog Protocol".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 RFC 3881 format, as extended in the audit trail message format profile.

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.

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.

A.7 Audit Trail Message Transmission Profile - SYSLOG-UDP

This profile defines the transmission of audit trail messages. Transmission of Syslog Messages over UDP (RFC5426) provides the mechanisms for rapid transport of audit messages. It is the standardized successor to the informative standard "The BSD syslog protocol (RFC3164) ", which is widely used in a variety of settings.

The syslog port number shall be configurable, with the port number (514) as the default.

The underlying UDP transport might not accept messages longer than the MTU size minus the UDP header length. This may result in longer syslog messages being truncated. When these messages are truncated the resulting XML may be incorrect. Because of this potential for truncated messages and other security concerns, the transmission of syslog messages over TLS may be preferred (see Section A.6).

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 values of 4 (warning condition) 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>". Audit repositories shall be prepared to deal appropriately with any incoming PRI value.

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 RFC 3881 format, as extended in this profile.

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 5426.

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.

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)

Note

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.

B.3 The AES TLS Secure Transport Connection Profile

An implementation that supports the AES TLS Secure Transport Connection Profile shall utilize the framework and negotiation mechanism specified by the Transport Layer Security Version 1.0 protocol. Table B.3-1 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.3-1. Minimum Mechanisms for TLS Features

Supported TLS Feature	Minimum Mechanism
Entity Authentication	RSA based Certificates

Two cyphersuite options shall be offered during TLS negotiation by applications that comply with this profile:

TLS_RSA_WITH_AES_128_CBC_SHA

TLS_RSA_WITH_3DES_EDE_CBC_SHA

The application shall offer both options. The AES version shall be preferred. The fallback to 3DES is offered so that this profile can interoperate easily with applications that only support the 3DES cyphersuite.

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 AES 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.4 Basic User Identity Association Profile

An implementation that supports the Basic User Identity Association profile shall accept the User Identity association negotiation sub-item, for User-Identity-Type of 1 or 2. It need not verify the passcode. If a positive response is requested, the implementation shall respond with the association response sub-item.

The user identity from the Primary-field shall be used within the implementation as the user identification. Such uses include recording user identification in audit messages.

Table B.4-1. Minimum Mechanisms for DICOM Association Negotiation Features - Basic User Identity Association Profile

Supported Association Negotiation Feature	Minimum Mechanism
User Identity	Username

B.5 User Identity Plus Passcode Association Profile

An implementation that supports the User Identity plus Passcode Association Profile shall send/accept the User Identity association negotiation sub-item, for User-Identity-Type of 2. If a positive response is requested, the association acceptor implementation shall respond with the association response sub-item. The passcode information shall be made available to internal or external authentication systems. The user identity shall be authenticated by means of the passcode and the authentication system. If the authentication fails, the association shall be rejected.

The user identity from the Primary-field shall be used within the implementation as the user identification. Such uses include recording user identification in audit messages.

Table B.5-1. User Identity Plus Passcode Association Profile - Minimum Mechanisms for DICOM Association Negotiation Features

Supported Association Negotiation Feature	Minimum Mechanism
User Identity	Username and Passcode

B.6 Kerberos Identity Negotiation Association Profile

An implementation that supports the Kerberos Identity Negotiation Association Profile shall send/accept the User Identity association negotiation sub-item, for User-Identity-Type of 3. If a positive response is requested, the association acceptor implementation shall respond with the association response sub-item containing a Kerberos server ticket. The Kerberos server ticket information shall be made available to internal or external Kerberos authentication systems. The user identity shall be authenticated by means of the Kerberos authentication system. If the authentication fails, the association shall be rejected.

The user identity from the Primary-field shall be used within the implementation as the user identification. Such uses include recording user identification in audit messages.

Table B.6-1. Kerberos Identity Negotiation Association Profile - Minimum Mechanisms for DICOM Association Negotiation Features

Supported Association Negotiation Feature	Minimum Mechanism
User Identity	Kerberos

B.7 Generic SAML Assertion Identity Negotiation Association Profile

An implementation that supports the Generic SAML Assertion Identity Negotiation Association Profile shall send/accept the User Identity association negotiation sub-item, for User-Identity-Type of 4. If a positive response is requested, the association acceptor implementation shall respond with the association response sub-item containing a SAML response. The SAML Assertion information shall be made available to internal or external authentication systems. The user identity shall be authenticated by means of an authentication system that employs SAML Assertions. If the authentication fails, the association shall be rejected.

The user identity from the Primary-field shall be used within the implementation as the user identification. Such uses include recording user identification in audit messages.

Table B.7-1. Generic SAML Assertion Identity Negotiation Association Profile - Minimum Mechanisms for DICOM Association Negotiation Features

Supported Association Negotiation Feature	Minimum Mechanism
User Identity	SAML Assertion

B.8 Secure Use of Email Transport

When a DICOM File Set is sent over Email transport in compliance with this profile the following rules shall be followed:

a. The File Set shall be an attachment to the email body.

b. The entire email (body, File Set attachment, and any other attachments) shall be encrypted using AES, in accordance with RFC 3851 and RFC 3853.

c. The email body and attachments may be compressed in accordance with RFC 3851.

d. The email shall be digitally signed by the sender. The signing may be applied before or after encryption. This digital signature shall be interpreted to mean that the sender is attesting to his authorization to disclose the information in this email to the recipient.

The email signature is present to provide minimum sender information and to confirm the integrity of the email transmission (body contents, attachment, etc.). The email signature is separate from other signatures that may be present in DICOM reports and objects contained in the File set attached to the email. Those signatures are defined in terms of clinical uses. Any clinical content attestations shall be encoded as digital signatures in the DICOM SOP instances, not as the email signature. The email may be composed by

someone who cannot make clinical attestations. Through the use of the email signature, the composer attests that he or she is authorized to transmit the data to the recipient.

Note

1. This profile is separate from the underlying use of ZIP File or other File Set packaging over email.

2. Where private information is being conveyed, most country regulations require the use of encryption or equivalent protections. This Profile meets the most common requirements of regulations, but there may be additional local requirements. Additional requirements may include mandatory statements in the email body and prohibitions on contents of the email body to protect patient privacy.

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, SHA-1 or SHA-2 family (SHA256, SHA384, SHA512) of 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 the hashing functions specified (RIPEMD-160, MD5, SHA-1 or SHA256, SHA384, SHA512).

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", "SHA1", "SHA256", "SHA384" or "SHA512". 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~~Module that are present

e. any attributes of the Overlay Plane Module, Curve Module or Graphic Annotation ~~modules~~Module that are present

f. any attributes of the General Image Module and Image Pixel ~~modules~~Module that are present

g. any attributes of the SR Document General Module and SR Document Content ~~modules~~Module that are present

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

i. any attributes of the Multi-frame Functional Groups ~~module~~Module that are present

j. any attributes of the Enhanced MR Image ~~module~~Module that are present

k. any attributes of the MR Spectroscopy ~~modules~~Module that are present

l. any attributes of the Raw Data ~~module~~Module that are present

m. any attributes of the Enhanced CT Image ~~module~~Module that are present

n. any attributes of the Enhanced XA/XRF Image ~~module~~Module that are present

o. any attributes of the Segmentation Image ~~module~~Module that are present

p. any attributes of the Encapsulated Document ~~module~~Module that are present

q. any attributes of the X-Ray 3D Image ~~module~~Module that are present

r. any attributes of the Enhanced PET Image ~~module~~Module that are present

s. any attributes of the Enhanced US Image ~~module~~Module that are present

t. any attributes of the Surface Segmentation ~~module~~Module that are present

u. any attributes of the Surface Mesh Module that are present

v. any attributes of the Structured Display Module, Structured Display Annotation Module, and Structured Display Image Box ~~modules~~Module that are present

w. any Attributes of the Implant Template ~~module~~Module that are present

x. any Attributes of the Implant Assembly Template ~~module~~Module that are present

y. any Attributes of the Implant Template Group ~~module~~Module that are present

z. any attributes of the Point Cloud Module that are present

aa. any attributes of the Enhanced Mammography Image ~~module~~Module that are present

ab. any attributes of the Tractography Results Module that are present

ac. any attributes of the Volumetric Graphic Annotation Module 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

h. any attributes of the Multi-frame Functional Groups module that are present

i. any attributes of the Enhanced MR Image module that are present

j. any attributes of the MR Spectroscopy modules that are present

k. any attributes of the Raw Data module that are present

l. any attributes of the Enhanced CT Image module that are present

m. any attributes of the Enhanced XA/XRF Image module that are present

n. any attributes of the Segmentation Image module that are present

o. any attributes of the Encapsulated Document module that are present

p. any attributes of the X-Ray 3D Image module that are present

q. any attributes of the Enhanced PET Image module that are present

r. any attributes of the Enhanced US Image module that are present

s. any attributes of the Surface Segmentation module that are present

t. any attributes of the Surface Mesh Module that are present

u. any attributes of the Structured Display, Structured Display Annotation, and Structured Display Image Box modules that are present

v. any Attributes of the Implant Template module that are present

w. any Attributes of the Implant Assembly Template module that are present

x. any Attributes of the Implant Template Group module that are present

y. any attributes of the Point Cloud Module that are present

z. any attributes of the Enhanced Mammography Image module that are present

aa. any attributes of the Volumetric Graphic Annotation Module 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.

C.4 Structured Report RSA Digital Signature Profile

This profile defines a mechanism for adding Digital Signatures to Structured Reports or Key Object Selection Documents where there is no more than one Verifying Observer. Instances that follow this Digital Signature Profile shall include at least one Digital Signature at the top level of the Data Set.

All Digital Signatures that follow this profile shall include a Digital Signature Purpose Code Sequence Attribute (0400,0401).

As a minimum, an implementation shall include the following attributes in generating the Digital Signature required by this profile:

a. the SOP Class UID

b. the Study and Series Instance UIDs

c. all attributes of the General Equipment Module that are present

d. the Current Requested Procedure Evidence Sequence

e. the Pertinent Other Evidence Sequence

f. the Predecessor Documents Sequence

g. the Observation DateTime

h. all attributes of the SR Document Content Module that are present

If the Verification Flag is set to "VERIFIED" (and the SOP Instance UID can no longer change) at least one of the Digital Signatures profile shall have the purpose of (5,ASTM-sigpurpose,"Verification Signature") and shall also include the following Attributes in addition to the above attributes:

a. the SOP Instance UID

b. the Verification Flag

c. the Verifying Observer Sequence

d. the Verification DateTime

Note

The system may also add a Creator RSA Digital Signature, which could cover other attributes that the machine can verify.

All occurrences of Referenced SOP Instance MAC Sequence (0400,0403) shall have the Value of MAC Algorithm (0400,0015) set to either "RIPEMD160", "MD5", "SHA1", "SHA256", "SHA384" or "SHA512"..

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 signatories and obtain their certificate through an application-specific procedure such as a login mechanism or a smart card. The conformance statement shall specify how the application identifies signatories and obtains certificates.

Note

Structured Report 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 corroborate the timestamp of a Structured Report RSA Digital Signature.

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 either AES or Triple-DES for content encryption and RSA, or password-based encryption and AES or Triple-DES, for the key transport of the content-encryption keys. The encrypted content is a DICOM File that can either

- be signed with one or more digital signatures, using SHA-1, SHA256, SHA384, or SHA512 as the digest algorithm and RSA as the signature algorithm, or
- be digested with SHA-1, SHA256, SHA384, or SHA512 as digest algorithm, without application of digital signatures.

Note

The digest algorithm requirements will evolve as the threats evolve. As the digest requirements have changed, this profile has changed to include additional requirements.

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 3852, 3370 and 3565. The enveloped data shall use RSA [RFC 3447], or password-based encryption using PBKDF2 [RFC 2898] for the key derivation algorithm and either AES or Triple-DES [RFC 3211], for the key transport of the content-encryption keys. Creators of a Secure DICOM File conforming to this security profile may use either AES or Triple-DES for content-encryption. Readers claiming conformance to this profile shall be capable of decrypting Secure DICOM Files using either AES or Triple-DES. The AES key length may be any length allowed by the RFCs. 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 and Triple DES Content Encryption in RFC-3370, and for AES Content Encryption in RFC-3565.

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], SHA256, SHA384, or SHA512 [SHA-2] 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.

In the case of password-based encryption using PBKDF2, the octet string that contains the password used to generate the key shall be limited to the encoding and the graphic character representation defined by the Default Character Repertoire.

Note

1. RSA key transport of the 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.

4. The use of password-based encryption for key transport of content encryption keys is potentially less secure than certificate-based encryption, but may be useful when the list of recipients is not known a priori or when there is no public key infrastructure deployed. The security depends on the entropy of the password, which if user-selected can be quite low. RFC 3211 strongly recommends the use of a pass "phrase" rather than a single word, and RFC 2898 does not impose any practical length limit. Also, the method used to exchange the password or pass phrase also could have a significant impact on the level of security.

5. PBKDF2 as defined in RFC 2898 specifies the password to be "an octet string of arbitrary length whose interpretation as a text string is unspecified". For interoperability between the sender and recipient, both a character encoding scheme and a graphic character representation needs to be defined. ISO IR6 (US-ASCII), being the Default Character Repertoire for DICOM (see PS3.5), is specified in order to avoid any potential ambiguity caused by the use of other character sets (such as UTF-8) that do not necessarily result in the same binary values for particular graphic character representation.

The graphic character representation of certain symbols in ISO IR6 is explicitly defined, even though the same binary representation may have a different graphic character representation in other 7-bit schemes. For example, in the version of ISO 646 used in Japan (ISO-IR 14 Romaji), 05/12 is represented as "¥" rather than backslash "\". It is the responsibility of the application to assure that the input method and display of such symbols to the user is mapped to the correct encoding, regardless of locale. I.e., if the password is "123\$", then it should be encoded as 03/01 03/02 03/03 05/12 02/04, regardless of whether the user types the backslash "\"(U+005C) on a Japanese or US keyboard; they should not be expected to type the "¥" (U+00A5) key on a Japanese keyboard, nor should 05/12 be displayed as "¥" if the password is displayed as text.

The restriction to the ISO IR 6 encoding and graphic character representation (rather than, for example, the minimal encoding of UTF-8) also eliminates the ambiguity introduced by homographs (characters that look the same but encode differently), and alternative encodings with the same meaning, such as the single German character "ß" (U+00DF) as opposed to the two-character "ss" (U+0073 U+0073), and the use of phonetic as opposed to ideographic representation of the same meaning, such as Japanese hiragana "ぞう" (U+305E U+3046) versus kanji "像" (U+50CF).

It is the responsibility of the application to prevent the user from creating passwords using characters that cannot be represented; e.g., on a Western European keyboard, the user should not be permitted to enter an accented character such as "é" (U+00E9) or "ö" (U+00F6), since there is no defined mapping of such characters to IS IR 6 characters (such as "e" or "o").

E Attribute Confidentiality Profiles

This Annex describes Profiles and Options to address the removal and replacement of Attributes within a DICOM Dataset that may potentially result in leakage of Individually Identifiable Information (III) about the patient or other individuals or organizations involved in acquisition.

Profiles are provided to address the balance between the removal of information and the need to retain information so that the Datasets remain useful for their intended purpose.

Options are used in addition to profiles to prevent a combinatorial expansion of different Profiles.

E.1 Application Level Confidentiality Profiles

Application Level Confidentiality Profiles address the following aspects of security:

- Data Confidentiality at the application layer.

Other aspects of security not addressed by these profiles, that may be addressed elsewhere in the standard include:

- Confidentiality in other layers of the DICOM model;
- Data Integrity.

These Profiles are targeted toward creating a special purpose, de-identified version of an already-existing Data Set. It is not intended to replace the original SOP Instance from which the de-identified SOP Instance is created, nor is it intended to act as the primary representation of clinical Data Sets in image archives. The de-identified SOP Instances are useful, for example, in creating teaching or research files, performing clinical trials, or submission to registries where the identity of the patient and other individuals is required to be protected. In some cases, it is also necessary to provide a means of recovering identity by authorized personnel.

E.1.1 De-identifier

An Application may claim conformance to an Application Level Confidentiality Profile and Options as a de-identifier if it protects and retains *all* Attributes as specified in the Profile and Options. Protection in this context is defined as the following process:

1. The application may create one or more instances of the Encrypted Attributes Data Set and copy Attributes to be protected into the (single) item of the Modified Attributes Sequence (0400,0550) of one or more of the Encrypted Attributes Data Set instances.

   Note

   1. A complete reconstruction of the original Data Set may not be possible; however, Attributes (e.g., SOP Instance UID) in the Modified Attributes Sequence of an Encrypted Attributes Data Set may refer back to the original SOP Instance holding the original Data Set.

   2. It is not required that the Encrypted Attributes Data Set be created; indeed, there may be circumstances where the Dataset is expected to be archived long enough that any contemporary encryption technology may be inadequate to provide long term protection against unauthorized recovery of identification.

   3. Other mechanisms to assist in identity recovery or longitudinal consistency of replaced UIDs or dates and times are deprecated in favor of the Encrypted Attributes Data Set mechanism that is intended for this purpose. For example, if it is desired to include an encrypted hash of the Patient's Name, it should not be encoded in a separate private attribute implemented for that purpose, but should be included in the Encrypted Attributes Data Set and encoded using the standard mechanism. This allows for compatibility between different implementations and provides security based on the quality and control of the encryption keys. Note also, that unencrypted hashes are considerably less secure and should be avoided, since they are vulnerable to trivial dictionary based attacks.

2. Each Attribute to be protected shall then either be removed from the dataset, or have its value replaced by a different "replacement value" that does not allow identification of the patient.

Note

1. It is the responsibility of the de-identifier to ensure that this process does not negatively affect the integrity of the Information Object Definition, i. e. Dummy values may be necessary for Type 1 Attributes that are protected but may not be sent with zero length, and are to be stored or exchanged in encrypted form by applications that may not be aware of the security mechanism.

2. The standard does not mandate the use of any particular dummy value, and indeed it may have some meaning, for example in a data set that may be used for teaching purposes, where the real patient identifying information is encrypted for later retrieval, but a meaningful alternative form of identification is provided. For example, a dummy Patient's Name (0010,0010) may convey the type of pathology in a teaching case. It is the responsibility of the de-identifier software or human operator to ensure that the dummy values cannot be used to identify the patient.

3. It is the responsibility of the de-identifier to ensure the consistency of dummy values for Attributes such as Study Instance UID (0020,000D) or Frame of Reference UID (0020,0052) if multiple related SOP Instances are protected. Indeed, all Attributes of every entity about the Instance level should remain consistent for all Instances protected, e.g., Patient ID for the Patient entity, Study ID for the Study entity, Series Number for the Series entity.

4. Some profiles do not allow selective protection of parts of a Sequence of Items. If an Attribute to be protected is contained in a Sequence of Items, the complete Sequence of Items may need to be protected.

5. The de-identifier should ensure that no identifying information that is burned in to the image pixel data either because the modality does not generate such burned in identification in the first place, or by removing it through the use of the Clean Pixel Data Option; see Section E.3. If non-pixel data graphics or overlays contain identification, the de-identifier is required to remove them, or clean them if the Clean Graphics option is supported. See Section E.3.3 The means by which burned in or graphic identifying information is located and removed is outside the scope of this standard.

3. Each Attribute specified to be retained shall be retained. At the discretion of the de-identifier, Attributes may be added to the dataset to be protected.

   Note

   As an example, the Attribute Patient's Age (0010,1010) might be introduced as a replacement for Patient's Birth Date (0010,0030) if the patient's age is of importance, and the profile permits it.

4. If used, all instances of the Encrypted Attributes Data Set shall be encoded with a DICOM Transfer Syntax, encrypted, and stored in the dataset to be protected as an Item of the Encrypted Attributes Sequence (0400,0500). The encryption shall be done using RSA [RFC 2313] for the key transport of the content-encryption keys. A de-identifier conforming to this security profile may use either AES or Triple-DES for content-encryption. The AES key length may be any length allowed by the RFCs. 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 and Triple DES Content Encryption in RFC-3370 and for AES Content Encryption in RFC-3565.

   Note

   1. Each item of the Encrypted Attributes Sequence (0400,0500) consists of two Attributes, Encrypted Content Transfer Syntax UID (0400,0510) containing the UID of the Transfer Syntax that was used to encode the instance of the Encrypted Attributes Data Set, and Encrypted Content (0400,0520) containing the block of data resulting from the encryption of the Encrypted Attributes Data Set instance.

   2. RSA key transport of the 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.

5. No requirements on the size of the asymmetric key pairs used for RSA key transport are defined in this confidentiality scheme. Implementations claiming conformance to the Basic Application Level Confidentiality Profile as a de-identifier shall always protect (e.g., encrypt and replace) the SOP Instance UID (0008,0018) Attribute as well as all references to other SOP Instances, whether contained in the main dataset or embedded in an Item of a Sequence of Items, that could potentially be used by unauthorized entities to identify the patient.

Note

In the case of a SOP Instance UID embedded in an item of a sequence, this means that the enclosing Attribute in the top-level data set must be encrypted in its entirety.

6. The attribute Patient Identity Removed (0012,0062) shall be replaced or added to the dataset with a value of YES, and one or more codes from CID 7050 “De-identification Method” corresponding to the profile and options used shall be added to De-identification Method Code Sequence (0012,0064). A text string describing the method used may also be inserted in or added to De-identification Method (0012,0063), but is not required.

7. If the Dataset being de-identified is being stored within a DICOM File, then the File Meta Information including the 128 byte preamble, if present, shall be replaced with a description of the de-identifying application. Otherwise, there is a risk that identity information may leak through unmodified File Meta Information or preamble. See PS3.10.

The Attributes listed in Table E.1-1 for each profile are contained in Standard IODs, or may be contained in Standard Extended IODs. An implementation claiming conformance to an Application Level Confidentiality Profile as a de-identifier shall protect or retain all instances of the Attributes listed in Table E.1-1, whether contained in the main dataset or embedded in an Item of a Sequence of Items. The following action codes are used in the table:

- D - replace with a non-zero length value that may be a dummy value and consistent with the VR
- Z - replace with a zero length value, or a non-zero length value that may be a dummy value and consistent with the VR
- X - remove
- K - keep (unchanged for non-sequence attributes, cleaned for sequences)
- C - clean, that is replace with values of similar meaning known not to contain identifying information and consistent with the VR
- U - replace with a non-zero length UID that is internally consistent within a set of Instances
- Z/D - Z unless D is required to maintain IOD conformance (Type 2 versus Type 1)
- X/Z - X unless Z is required to maintain IOD conformance (Type 3 versus Type 2)
- X/D - X unless D is required to maintain IOD conformance (Type 3 versus Type 1)
- X/Z/D - X unless Z or D is required to maintain IOD conformance (Type 3 versus Type 2 versus Type 1)
- X/Z/U* - X unless Z or replacement of contained instance UIDs (U) is required to maintain IOD conformance (Type 3 versus Type 2 versus Type 1 sequences containing UID references)

These action codes are applicable to both Sequence and non-Sequence attributes; in the case of Sequences, the action is applicable to the Sequence and all of its contents. Cleaning a sequence ("C" action) may entail either changing values of attributes within that Sequence when the meaning of the Sequence within the context of its use in the IOD is understood, or recursively applying the profile rules to each Dataset in each Item of the Sequence. Keeping a Sequence ("K" action) requires recursively applying the profile rules to each Dataset in each Item of the Sequence (for example, in order to remap any UIDs contained within that sequence).

A requirement for an Option, when implemented, overrides any requirement for the underlying Profile.

Note

1. The Attributes listed in Table E.1-1 may not be sufficient to guarantee confidentiality of patient identity. In particular, identifying information may be contained in Private Attributes, new Standard Attributes, Retired Standard Attributes and additional Standard Attributes not present in Standard Composite IODs (as defined in PS3.3) but used in Standard Extended SOP Classes. Table E.1-1 indicates those Attributes that are used in Standard Composite IODs as well as those Attributes that are Retired. Also included in Table E.1-1 are some Elements that are not normally found in a Dataset, but are used in Commands, Directories and Meta Information Headers, but that could be misused within Private Sequences. Textual Content Items of Structured Reports, textual annotations of Presentation States, Curves and Overlays are specifically addressed. It is the responsibility of the de-identifier to ensure that all identifying information is removed.

2. It should be noted that conformance to an Application Level Confidentiality Profile does not necessarily guarantee confidentiality. For example, if an attacker already has access to the original images, the Pixel Data could be matched,

though the probability and impact of such a threat may be deemed to be negligible. If the Encrypted Attributes Sequence is used, it should be understood that any encryption scheme may be vulnerable to attack. Also, an organization's Security Policy and Key Management policy are recognized to have a much greater impact on the effectiveness of protection.

3. National and local regulations, which may vary, might require that additional attributes be de-identified, though the Profiles and Options have been designed to be sufficient to satisfy known regulations without compromising the usefulness of the de-identified instances for their intended purpose.

4. Table E.1-1 is normative, but it is subject to extension as the DICOM Standard evolves and other similar Attributes are added to IODs. De-identifiers may take this extensibility into account, for example, by considering handling all dates and times on the basis of their Value Representation of DT, DA or TM, rather than just those date and time Attributes lists.

5. The Profiles and Options do not specify whether the design of a de-identifier should be to remove what is know to be a risk of identity leakage, or to retain only what is known to be safe. The former approach may fail when the standard is extended, or when a vendor adds unanticipated standard or private attributes, whilst the latter requires an extensive, if not complete, comparison of each instance with the Information Object Definitions in PS3.3 to avoid discarding required or useful information. Table E.1-1 defines the minimum actions required for conformance.

6. De-identification of Private SOP Classes is not defined.

7. The "C" (clean) action is specified not only for string VRs, but also for Code Sequences, since the use of private or local codes and non-standard code meanings may potentially cause identity leakage.

8. The Digital Signatures Sequences needs to be removed because it contains the certificate of the signer; theoretically the signature could be verified and the object re-signed by the de-identifier itself with its own certificate, but this is not required by the Standard.

9. In general, there are no CS VR Attributes in this table, since it is usually safe to assume that code strings do not contain identifying information.

10. In general, there are no Code Sequence Attributes in this table, since it is usually safe to assume that coded sequence entries, including private codes, do not contain identifying information. Exceptions are codes for providers and staff.

11. The Clean Pixel Data and Clean Recognizable Visual Features Options are not listed in this table, since they are defined by descriptions of operations on the Pixel Data itself. The Clean Pixel Data option may be applied to the Pixel Data within the Icon Image Sequence, or more likely the Icon Image Sequence may be recreated entirely once the Pixel Data of the main Dataset has been cleaned. The Icon Image Sequence is to be removed when its Pixel Data cannot be cleaned.

12. The Original Attributes Sequence (0400,0561) (which in turn contains the Modified Attributes Sequence (0400,0550)) generally needs to be removed, because it may contain unencrypted copies of other Attributes that may have been modified (e.g., coerced to use local identifiers and names during import of foreign images); an alternative approach would be to selectively modify its contents. This is distinct from the use of the Modified Attributes Sequence (0400,0550) within the Encrypted Attributes Sequence (0400,0500).

13. Table E.1-1 distinguishes Attributes that are in standard Composite IODs defined in PS3.3 from those that are not; some Attributes are defined in PS3.3 for other IODs, or have a specific usage other than in the top level Dataset of a Composite IOD, but are (mis-) used by implementers in instances as a Standard Extended SOP Class at other levels than as defined by the Standard. Any such Attributes encountered may be removed without compromising the conformance of the instance with the standard IOD. For example, Verifying Observer Sequence (0040,A073) is only defined in structured report IODs and hence is described in Table E.1-1 as D since it is Type 1C; if encountered in an image instance, it should simply be removed (treated as X).

Table E.1-1. Application Level Confidentiality Profile Attributes

Attribute Name	Tag	Retired (from PS3.6)	In Std. Comp. IOD (from PS3.3)	Basic Profile	Retain Safe Private Option	Retain UIDs Option	Retain Device Ident. Option	Retain Patient Chars. Option	Retain Long. Full Dates Option	Retain Long. Modif. Dates Option	Clean Desc. Option	Clean Struct. Cont. Option	Clean Graph. Option
Accession Number	(0008,0050)	N	Y	Z									
Acquisition Comments	(0018,4000)	Y	N	X							C		
Acquisition Context Sequence	(0040,0555)	N	Y	X								C	
Acquisition Date	(0008,0022)	N	Y	X/Z					K	C			
Acquisition DateTime	(0008,002A)	N	Y	X/D					K	C			
Acquisition Device Processing Description	(0018,1400)	N	Y	X/D							C		
Acquisition Protocol Description	(0018,9424)	N	Y	X							C		
Acquisition Time	(0008,0032)	N	Y	X/Z					K	C			
Actual Human Performers Sequence	(0040,4035)	N	N	X									
Additional Patient's History	(0010,21B0)	N	Y	X							C		
Address (Trial)	(0040,A353)	Y	N	X									
Admission ID	(0038,0010)	N	Y	X									
Admitting Date	(0038,0020)	N	N	X					K	C			
Admitting Diagnoses Code Sequence	(0008,1084)	N	Y	X							C		
Admitting Diagnoses Description	(0008,1080)	N	Y	X							C		
Admitting Time	(0038,0021)	N	N	X					K	C			
Affected SOP Instance UID	(0000,1000)	N	N	X		K							
Allergies	(0010,2110)	N	N	X				C			C		
Arbitrary	(4000,0010)	Y	N	X									
Author Observer Sequence	(0040,A078)	N	Y	X									
Branch of Service	(0010,1081)	N	N	X									
Cassette ID	(0018,1007)	N	Y	X			K						

Attribute Name	Tag	Retired (from PS3.6)	In Std. Comp. IOD (from PS3.3)	Basic Profile	Retain Safe Private Option	Retain UIDs Option	Retain Device Ident. Option	Retain Patient Chars. Option	Retain Long. Full Dates Option	Retain Long. Modif. Dates Option	Clean Desc. Option	Clean Struct. Cont. Option	Clean Graph. Option
Comments on the Performed Procedure Step	(0040,0280)	N	Y	X							C		
Concatenation UID	(0020,9161)	N	Y	U		K							
Confidentiality Constraint on Patient Data Description	(0040,3001)	N	N	X									
Consulting Physician Identification Sequence	(0008,009D)	N	Y	X									
Consulting Physician's Name	(0008,009C)	N	Y	Z									
Content Creator's Name	(0070,0084)	N	Y	Z									
Content Creator's Identification Code Sequence	(0070,0086)	N	Y	X									
Content Date	(0008,0023)	N	Y	Z/D					K	C			
Content Sequence	(0040,A730)	N	Y	X								C	
Content Time	(0008,0033)	N	Y	Z/D					K	C			
Context Group Extension Creator UID	(0008,010D)	N	Y	U		K							
Contrast Bolus Agent	(0018,0010)	N	Y	Z/D							C		
Contribution Description	(0018,A003)	N	Y	X							C		
Country of Residence	(0010,2150)	N	N	X									
Creator Version UID	(0008,9123)	N	Y	U		K							
Current Observer (Trial)	(0040,A307)	Y	N	X									
Current Patient Location	(0038,0300)	N	N	X									
Curve Data	(50xx,xxxx)	Y	N	X									C
Curve Date	(0008,0025)	Y	Y	X					K	C			
Curve Time	(0008,0035)	Y	Y	X					K	C			

Attribute Name	Tag	Retired (from PS3.6)	In Std. Comp. IOD (from PS3.3)	Basic Profile	Retain Safe Private Option	Retain UIDs Option	Retain Device Ident. Option	Retain Patient Chars. Option	Retain Long. Full Dates Option	Retain Long. Modif. Dates Option	Clean Desc. Option	Clean Struct. Cont. Option	Clean Graph. Option
Custodial Organization Sequence	(0040,A07C)	N	Y	X									
Data Set Trailing Padding	(FFFC,FFFC)	N	Y	X									
Derivation Description	(0008,2111)	N	Y	X							C		
Detector ID	(0018,700A)	N	Y	X/D			K						
Device Serial Number	(0018,1000)	N	Y	X/Z/D			K						
Device UID	(0018,1002)	N	Y	U		K	K						
Digital Signature UID	(0400,0100)	N	Y	X									
Digital Signatures Sequence	(FFFA,FFFA)	N	Y	X									
Dimension Organization UID	(0020,9164)	N	Y	U		K							
Discharge Diagnosis Description	(0038,0040)	Y	N	X							C		
Distribution Address	(4008,011A)	Y	N	X									
Distribution Name	(4008,0119)	Y	N	X									
Dose Reference UID	(300A,0013)	N	Y	U		K							
End Acquisition DateTime	(0018,9517)	N	Y	X/D					K	C			
Ethnic Group	(0010,2160)	N	Y	X				K					
Expected Completion DateTime	(0040,4011)	N	N	X					K	C			
Failed SOP Instance UID List	(0008,0058)	N	N	U		K							
Fiducial UID	(0070,031A)	N	Y	U		K							
Filler Order Number / Imaging Service Request	(0040,2017)	N	Y	Z									
Frame Comments	(0020,9158)	N	Y	X							C		
Frame of Reference UID	(0020,0052)	N	Y	U		K							

Attribute Name	Tag	Retired (from PS3.6)	In Std. Comp. IOD (from PS3.3)	Basic Profile	Retain Safe Private Option	Retain UIDs Option	Retain Device Ident. Option	Retain Patient Chars. Option	Retain Long. Full Dates Option	Retain Long. Modif. Dates Option	Clean Desc. Option	Clean Struct. Cont. Option	Clean Graph. Option
Gantry ID	(0018,1008)	N	Y	X			K						
Generator ID	(0018,1005)	N	Y	X			K						
Graphic Annotation Sequence	(0070,0001)	N	Y	D									C
Human Performers Name	(0040,4037)	N	N	X									
Human Performers Organization	(0040,4036)	N	N	X									
Icon Image Sequence(see Note 12)	(0088,0200)	N	Y	X									
Identifying Comments	(0008,4000)	Y	N	X							C		
Image Comments	(0020,4000)	N	Y	X							C		
Image Presentation Comments	(0028,4000)	Y	N	X									
Imaging Service Request Comments	(0040,2400)	N	N	X							C		
Impressions	(4008,0300)	Y	N	X							C		
Instance Coercion DateTime	(0008,0015)	N	Y	X					K	C			
Instance Creator UID	(0008,0014)	N	Y	U		K							
Institution Address	(0008,0081)	N	Y	X									
Institution Code Sequence	(0008,0082)	N	Y	X/Z/D									
Institution Name	(0008,0080)	N	Y	X/Z/D									
Institutional Department Name	(0008,1040)	N	Y	X									
Insurance Plan Identification	(0010,1050)	Y	N	X									
Intended Recipients of Results Identification Sequence	(0040,1011)	N	N	X									

Attribute Name	Tag	Retired (from PS3.6)	In Std. Comp. IOD (from PS3.3)	Basic Profile	Retain Safe Private Option	Retain UIDs Option	Retain Device Ident. Option	Retain Patient Chars. Option	Retain Long. Full Dates Option	Retain Long. Modif. Dates Option	Clean Desc. Option	Clean Struct. Cont. Option	Clean Graph. Option
Interpretation Approver Sequence	(4008,0111)	Y	N	X									
Interpretation Author	(4008,010C)	Y	N	X									
Interpretation Diagnosis Description	(4008,0115)	Y	N	X							C		
Interpretation ID Issuer	(4008,0202)	Y	N	X									
Interpretation Recorder	(4008,0102)	Y	N	X									
Interpretation Text	(4008,010B)	Y	N	X							C		
Interpretation Transcriber	(4008,010A)	Y	N	X									
Irradiation Event UID	(0008,3010)	N	Y	U		K							
Issuer of Admission ID	(0038,0011)	N	Y	X									
Issuer of Patient ID	(0010,0021)	N	Y	X									
Issuer of Service Episode ID	(0038,0061)	N	Y	X									
Large Palette Color Lookup Table UID	(0028,1214)	Y	N	U		K							
Last Menstrual Date	(0010,21D0)	N	N	X					K	C			
MAC	(0400,0404)	N	Y	X									
Media Storage SOP Instance UID	(0002,0003)	N	N	U		K							
Medical Alerts	(0010,2000)	N	N	X							C		
Medical Record Locator	(0010,1090)	N	N	X									
Military Rank	(0010,1080)	N	N	X									
Modified Attributes Sequence	(0400,0550)	N	N	X									
Modified Image Description	(0020,3406)	Y	N	X									
Modifying Device ID	(0020,3401)	Y	N	X									

Attribute Name	Tag	Retired (from PS3.6)	In Std. Comp. IOD (from PS3.3)	Basic Profile	Retain Safe Private Option	Retain UIDs Option	Retain Device Ident. Option	Retain Patient Chars. Option	Retain Long. Full Dates Option	Retain Long. Modif. Dates Option	Clean Desc. Option	Clean Struct. Cont. Option	Clean Graph. Option
Modifying Device Manufacturer	(0020,3404)	Y	N	X									
Name of Physician(s) Reading Study	(0008,1060)	N	Y	X									
Names of Intended Recipient of Results	(0040,1010)	N	N	X									
Observation Date (Trial)	(0040,A192)	Y	N	X					K	C			
Observation Subject UID (Trial)	(0040,A402)	Y	N	U		K							
Observation Time (Trial)	(0040,A193)	Y	N	X					K	C			
Observation UID	(0040,A171)	N	Y	U		K							
Occupation	(0010,2180)	N	Y	X							C		
Operators' Identification Sequence	(0008,1072)	N	Y	X/D									
Operators' Name	(0008,1070)	N	Y	X/Z/D									
Original Attributes Sequence	(0400,0561)	N	Y	X									
Order Callback Phone Number	(0040,2010)	N	N	X									
Order Callback Telecom Information	(0040,2011)	N	N	X									
Order Entered By	(0040,2008)	N	N	X									
Order Enterer Location	(0040,2009)	N	N	X									
Other Patient IDs	(0010,1000)	N	Y	X									
Other Patient IDs Sequence	(0010,1002)	N	Y	X									
Other Patient Names	(0010,1001)	N	Y	X									
Overlay Comments	(60xx,4000)	Y	N	X									C
Overlay Data	(60xx,3000)	N	Y	X									C
Overlay Date	(0008,0024)	Y	Y	X					K	C			

Attribute Name	Tag	Retired (from PS3.6)	In Std. Comp. IOD (from PS3.3)	Basic Profile	Retain Safe Private Option	Retain UIDs Option	Retain Device Ident. Option	Retain Patient Chars. Option	Retain Long. Full Dates Option	Retain Long. Modif. Dates Option	Clean Desc. Option	Clean Struct. Cont. Option	Clean Graph. Option
Overlay Time	(0008,0034)	Y	Y	X					K	C			
Palette Color Lookup Table UID	(0028,1199)	N	Y	U		K							
Participant Sequence	(0040,A07A)	N	Y	X									
Patient Address	(0010,1040)	N	N	X									
Patient Comments	(0010,4000)	N	Y	X							C		
Patient ID	(0010,0020)	N	Y	Z									
Patient Sex Neutered	(0010,2203)	N	Y	X/Z				K					
Patient State	(0038,0500)	N	N	X				C			C		
Patient Transport Arrangements	(0040,1004)	N	N	X									
Patient's Age	(0010,1010)	N	Y	X				K					
Patient's Birth Date	(0010,0030)	N	Y	Z									
Patient's Birth Name	(0010,1005)	N	N	X									
Patient's Birth Time	(0010,0032)	N	Y	X									
Patient's Institution Residence	(0038,0400)	N	N	X									
Patient's Insurance Plan Code Sequence	(0010,0050)			X									
Patient's Mother's Birth Name	(0010,1060)	N	N	X									
Patient's Name	(0010,0010)	N	Y	Z									
Patient's Primary Language Code Sequence	(0010,0101)			X									
Patient's Primary Language Modifier Code Sequence	(0010,0102)			X									
Patient's Religious Preference	(0010,21F0)	N	N	X									
Patient's Sex	(0010,0040)	N	Y	Z				K					

Attribute Name	Tag	Retired (from PS3.6)	In Std. Comp. IOD (from PS3.3)	Basic Profile	Retain Safe Private Option	Retain UIDs Option	Retain Device Ident. Option	Retain Patient Chars. Option	Retain Long. Full Dates Option	Retain Long. Modif. Dates Option	Clean Desc. Option	Clean Struct. Cont. Option	Clean Graph. Option
Patient's Size	(0010,1020)	N	Y	X				K					
Patient's Telecom Information	(0010,2155)	N	N	X									
Patient's Telephone Numbers	(0010,2154)	N	N	X									
Patient's Weight	(0010,1030)	N	Y	X				K					
Performed Location	(0040,0243)	N	N	X									
Performed Procedure Step Description	(0040,0254)	N	Y	X							C		
Performed Procedure Step End Date	(0040,0250)	N	Y	X					K	C			
Performed Procedure Step End DateTime	(0040,4051)	N	N	X					K	C			
Performed Procedure Step End Time	(0040,0251)	N	Y	X					K	C			
Performed Procedure Step ID	(0040,0253)	N	Y	X									
Performed Procedure Step Start Date	(0040,0244)	N	Y	X					K	C			
Performed Procedure Step Start DateTime	(0040,4050)	N	N	X					K	C			
Performed Procedure Step Start Time	(0040,0245)	N	Y	X					K	C			
Performed Station AE Title	(0040,0241)	N	N	X			K						
Performed Station Geographic Location Code Sequence	(0040,4030)	N	N	X			K						
Performed Station Name	(0040,0242)	N	N	X			K						
Performed Station Name Code Sequence	(0040, 4028)	N	N	X			K						

Attribute Name	Tag	Retired (from PS3.6)	In Std. Comp. IOD (from PS3.3)	Basic Profile	Retain Safe Private Option	Retain UIDs Option	Retain Device Ident. Option	Retain Patient Chars. Option	Retain Long. Full Dates Option	Retain Long. Modif. Dates Option	Clean Desc. Option	Clean Struct. Cont. Option	Clean Graph. Option
Performing Physician Identification Sequence	(0008,1052)	N	Y	X									
Performing Physicians' Name	(0008,1050)	N	Y	X									
Person Address	(0040,1102)	N	Y	X									
Person Identification Code Sequence	(0040,1101)	N	Y	D									
Person Name	(0040,A123)	N	Y	D									
Person's Telecom Information	(0040,1104)	N	Y	X									
Person's Telephone Numbers	(0040,1103)	N	Y	X									
Physician Approving Interpretation	(4008,0114)	Y	N	X									
Physician(s) Reading Study Identification Sequence	(0008,1062)	N	Y	X									
Physician(s) of Record	(0008,1048)	N	Y	X									
Physician(s) of Record Identification Sequence	(0008,1049)	N	Y	X									
Placer Order Number / Imaging Service Request	(0040,2016)	N	Y	Z									
Plate ID	(0018,1004)	N	Y	X			K						
Pre-Medication	(0040,0012)	N	N	X				C					
Pregnancy Status	(0010,21C0)	N	N	X				K					
Presentation Display Collection UID	(0070,1101)	N	Y	U		K							
Presentation Sequence Collection UID	(0070,1102)	N	Y	U		K							

Attribute Name	Tag	Retired (from PS3.6)	In Std. Comp. IOD (from PS3.3)	Basic Profile	Retain Safe Private Option	Retain UIDs Option	Retain Device Ident. Option	Retain Patient Chars. Option	Retain Long. Full Dates Option	Retain Long. Modif. Dates Option	Clean Desc. Option	Clean Struct. Cont. Option	Clean Graph. Option
Procedure Step Cancellation DateTime	(0040,4052)	N	N	X					K	C			
Private attributes	*(gggg,eeee) where gggg is odd*	N	N	X	C								
Protocol Name	(0018,1030)	N	Y	X/D							C		
Reason for Omission Description	(300C,0113)	N	Y	X							C		
Reason for the Imaging Service Request	(0040,2001)	Y	N	X							C		
Reason for Study	(0032,1030)	Y	N	X							C		
Referenced Digital Signature Sequence	(0400,0402)	N	Y	X									
Referenced Frame of Reference UID	(3006,0024)	N	Y	U		K							
Referenced General Purpose Scheduled Procedure Step Transaction UID	(0040,4023)	Y	N	U		K							
Referenced Image Sequence	(0008,1140)	N	Y	X/Z/U*		K							
Referenced Observation UID (Trial)	(0040,A172)	Y	N	U		K							
Referenced Patient Alias Sequence	(0038, 0004)	N	N	X									
Referenced Patient Photo Sequence	(0010,1100)	N	Y	X									
Referenced Patient Sequence	(0008,1120)	N	Y	X		X							
Referenced Performed Procedure Step Sequence	(0008,1111)	N	Y	X/Z/D		K							

Attribute Name	Tag	Retired (from PS3.6)	In Std. Comp. IOD (from PS3.3)	Basic Profile	Retain Safe Private Option	Retain UIDs Option	Retain Device Ident. Option	Retain Patient Chars. Option	Retain Long. Full Dates Option	Retain Long. Modif. Dates Option	Clean Desc. Option	Clean Struct. Cont. Option	Clean Graph. Option
Referenced SOP Instance MAC Sequence	(0400,0403)	N	Y	X									
Referenced SOP Instance UID	(0008,1155)	N	Y	U		K							
Referenced SOP Instance UID in File	(0004,1511)	N	N	U		K							
Referenced Study Sequence	(0008,1110)	N	Y	X/Z		K							
Referring Physician's Address	(0008,0092)	N	N	X									
Referring Physician Identification Sequence	(0008,0096)	N	Y	X									
Referring Physician's Name	(0008,0090)	N	Y	Z									
Referring Physician's Telephone Numbers	(0008,0094)	N	N	X									
Region of Residence	(0010,2152)	N	N	X									
Related Frame of Reference UID	(3006,00C2)	N	Y	U		K							
Request Attributes Sequence	(0040,0275)	N	Y	X							C		
Requested Contrast Agent	(0032,1070)	N	N	X							C		
Requested Procedure Comments	(0040,1400)	N	N	X							C		
Requested Procedure Description	(0032,1060)	N	Y	X/Z							C		
Requested Procedure ID	(0040,1001)	N	N	X									
Requested Procedure Location	(0040,1005)	N	N	X									

Attribute Name	Tag	Retired (from PS3.6)	In Std. Comp. IOD (from PS3.3)	Basic Profile	Retain Safe Private Option	Retain UIDs Option	Retain Device Ident. Option	Retain Patient Chars. Option	Retain Long. Full Dates Option	Retain Long. Modif. Dates Option	Clean Desc. Option	Clean Struct. Cont. Option	Clean Graph. Option
Requested SOP Instance UID	(0000,1001)	N	N	U		K							
Requesting Physician	(0032,1032)	N	N	X									
Requesting Service	(0032,1033)	N	N	X									
Responsible Organization	(0010,2299)	N	Y	X									
Responsible Person	(0010,2297)	N	Y	X									
Results Comments	(4008,4000)	Y	N	X							C		
Results Distribution List Sequence	(4008,0118)	Y	N	X									
Results ID Issuer	(4008,0042)	Y	N	X									
Reviewer Name	(300E,0008)	N	Y	X/Z									
Scheduled Human Performers Sequence	(0040,4034)	N	N	X									
Scheduled Patient Institution Residence	(0038,001E)	Y	N	X									
Scheduled Performing Physician Identification Sequence	(0040,000B)	N	N	X									
Scheduled Performing Physician Name	(0040,0006)	N	N	X									
Scheduled Procedure Step End Date	(0040,0004)	N	N	X					K	C			
Scheduled Procedure Step End Time	(0040,0005)	N	N	X					K	C			
Scheduled Procedure Step Description	(0040,0007)	N	Y	X							C		
Scheduled Procedure Step Location	(0040,0011)	N	N	X			K						

Attribute Name	Tag	Retired (from PS3.6)	In Std. Comp. IOD (from PS3.3)	Basic Profile	Retain Safe Private Option	Retain UIDs Option	Retain Device Ident. Option	Retain Patient Chars. Option	Retain Long. Full Dates Option	Retain Long. Modif. Dates Option	Clean Desc. Option	Clean Struct. Cont. Option	Clean Graph. Option
Scheduled Procedure Step Modification DateTime	(0040,4010)	N	N	X					K	C			
Scheduled Procedure Step Start Date	(0040,0002)	N	N	X					K	C			
Scheduled Procedure Step Start DateTime	(0040,4005)	N	N	X					K	C			
Scheduled Procedure Step Start Time	(0040,0003)	N	N	X					K	C			
Scheduled Station AE Title	(0040,0001)	N	N	X			K						
Scheduled Station Geographic Location Code Sequence	(0040,4027)	N	N	X			K						
Scheduled Station Name	(0040,0010)	N	N	X			K						
Scheduled Station Name Code Sequence	(0040,4025)	N	N	X			K						
Scheduled Study Location	(0032,1020)	Y	N	X			K						
Scheduled Study Location AE Title	(0032,1021)	Y	N	X			K						
Series Date	(0008,0021)	N	Y	X/D					K	C			
Series Description	(0008,103E)	N	Y	X							C		
Series Instance UID	(0020,000E)	N	Y	U		K							
Series Time	(0008,0031)	N	Y	X/D					K	C			
Service Episode Description	(0038,0062)	N	Y	X							C		
Service Episode ID	(0038,0060)	N	Y	X									
Smoking Status	(0010,21A0)	N	N	X				K					
SOP Instance UID	(0008,0018)	N	Y	U		K							
Source Image Sequence	(0008,2112)	N	Y	X/Z/U*		K							

Attribute Name	Tag	Retired (from PS3.6)	In Std. Comp. IOD (from PS3.3)	Basic Profile	Retain Safe Private Option	Retain UIDs Option	Retain Device Ident. Option	Retain Patient Chars. Option	Retain Long. Full Dates Option	Retain Long. Modif. Dates Option	Clean Desc. Option	Clean Struct. Cont. Option	Clean Graph. Option
Source Serial Number	(3008,0105)	N	Y	X			K						
Special Needs	(0038,0050)	N	N	X				C					
Start Acquisition DateTime	(0018,9516)	N	Y	X/D					K	C			
Station Name	(0008,1010)	N	Y	X/Z/D			K						
Storage Media File-set UID	(0088,0140)	N	Y	U		K							
Study Comments	(0032,4000)	Y	N	X							C		
Study Date	(0008,0020)	N	Y	Z					K	C			
Study Description	(0008,1030)	N	Y	X							C		
Study ID	(0020,0010)	N	Y	Z									
Study ID Issuer	(0032,0012)	Y	N	X									
Study Instance UID	(0020,000D)	N	Y	U		K							
Study Time	(0008,0030)	N	Y	Z					K	C			
Synchronization Frame of Reference UID	(0020,0200)	N	Y	U		K							
Target UID	(0018,2042)	N	Y	U		K							
Telephone Number (Trial)	(0040,A354)	Y	N	X									
Template Extension Creator UID	(0040,DB0D)	Y	N	U		K							
Template Extension Organization UID	(0040,DB0C)	Y	N	U		K							
Text Comments	(4000,4000)	Y	N	X									
Text String	(2030,0020)	N	N	X									
Timezone Offset From UTC	(0008,0201)	N	Y	X					K	C			
Topic Author	(0088,0910)	Y	N	X									
Topic Keywords	(0088,0912)	Y	N	X									
Topic Subject	(0088,0906)	Y	N	X									
Topic Title	(0088,0904)	Y	N	X									
Tracking UID	(0062,0021)	N	Y	U		K							
Transaction UID	(0008,1195)	N	N	U		K							
UID	(0040,A124)	N	Y	U									

Attribute Name	Tag	Retired (from PS3.6)	In Std. Comp. IOD (from PS3.3)	Basic Profile	Retain Safe Private Option	Retain UIDs Option	Retain Device Ident. Option	Retain Patient Chars. Option	Retain Long. Full Dates Option	Retain Long. Modif. Dates Option	Clean Desc. Option	Clean Struct. Cont. Option	Clean Graph. Option
Verbal Source (Trial)	(0040,A352)	Y	N	X									
Verbal Source Identifier Code Sequence (Trial)	(0040,A358)	Y	N	X									
Verifying Observer Identification Code Sequence	(0040,A088)	N	Y	Z									
Verifying Observer Name	(0040,A075)	N	Y	D									
Verifying Observer Sequence	(0040,A073)	N	Y	D									
Verifying Organization	(0040,A027)	N	Y	X									
Visit Comments	(0038,4000)	N	N	X							C		

E.1.2 Re-identifier

An Application may claim conformance to an Application Level Confidentiality Profile as a re-identifier if it is capable of removing the protection from a protected SOP instance given that the recipient keys required for the decryption of one or more of the Encrypted Content (0400,0520) Attributes within the Encrypted Attributes Sequence (0400,0500) of the SOP instance are available. Removal of protection in this context is defined as the following process:

1. The application shall decrypt, using its recipient key, one instance of the Encrypted Content (0400,0520) Attribute within the Encrypted Attributes Sequence (0400,0500) and decode the resulting block of bytes into a DICOM dataset using the Transfer Syntax specified in the Encrypted Content Transfer Syntax UID (0400,0510). Re-identifiers claiming conformance to this profile shall be capable of decrypting the Encrypted Content using either AES or Triple-DES in all possible key lengths specified in this profile.

   Note

   If the application is able to decode more than one instance of the Encrypted Content (0400,0520) Attribute within the Encrypted Attributes Sequence (0400,0500), it is at the discretion of the application to choose any one of them.

2. The application shall move all Attributes contained in the single item of the Modified Attributes Sequence (0400,0550) of the decoded dataset into the main dataset, replacing "dummy value" Attributes that may be present in the main dataset.

   Note

   1. Re-identification does not imply a complete reconstruction of the original SOP Instance, since it is not required that all Attributes being protected be part of the Encrypted Attributes Data Set. If the original UIDs are part of the Encrypted Attributes Data Set, they might be usable to gain access to the original, unprotected SOP Instance.

   2. The presence of an encrypted data set that cannot be decrypted indicates that some or all of the attribute values in the message may not be real (they are dummies). Therefore, the recipient must not assume that any value in the message is diagnostically relevant.

3. The attribute Patient Identity Removed (0012,0062) shall be replaced or added to the dataset with a value of NO and De-identification Method (0012,0063) and De-identification Method Code Sequence (0012,0064) shall be removed.

E.1.3 Conformance Requirements

The Conformance Statement of an application that claims conformance to an Application Level Confidentiality Profile shall describe:

- which Attributes are removed during protection;
- which Attributes are replaced by dummy values and how the dummy values are generated;
- which Attributes are included in Encrypted Attributes Data Sets for later re-identification, and any pertinent details about how keys are selected for performing the encryption;
- the scope across which the application is able to ensure referential integrity of replacement values for references such as SOP Instance UID, Frame of Reference UID, etc. if multiple SOP instances are protected (e.g., across multiple Studies, consistent replacement if the same Study processed more than once, etc.);
- which Attributes and Attribute values are inserted during protection of a SOP instance;
- which Transfer Syntaxes are supported for encoding/decoding of the Encrypted Attributes Data Set;
- which Options are supported;
- any additional restrictions (e. g. key sizes for public keys).

E.2 Basic Application Level Confidentiality Profile

This profile is intended for use in clinical trials, and other scenarios in which de-identification may be required, such as creation of teaching files, other types of publication, as well as submission of images and associated information to registries, such as oncology or radiation dose registries.

This Basic Application Level Confidentiality Profile defines an extremely conservative approach that removes all information related to:

- the identity and demographic characteristics of the patient
- the identity of any responsible parties or family members
- the identity of any personnel involved in the procedure
- the identity of the organizations involved in ordering or performing the procedure
- additional information that could be used to match instances if given access to the originals, such as UIDs, dates and times
- private attributes

when that information is present in the non-Pixel Data Attributes, including graphics or overlays, as described in Table E.1-1.

Note

Unless the Clean Pixel Data Option is also specified, this profile does not address information burned-in to the pixels.

The Attribute Longitudinal Temporal Information Modified (0028,0303) shall be added to the Dataset with a value of "REMOVED" if none of the Retain Longitudinal Temporal Information Options is applied.

E.3 Basic Application Level Confidentiality Options

Various options are defined to be applicable to the Basic Application Level Confidentiality Profile. Some of these options require removal of additional information, and some of these options require retention of information that would otherwise be removed.

The following options are defined that require removal of additional information:

- Clean Pixel Data Option
- Clean Recognizable Visual Features Option

- Clean Graphics Option
- Clean Structured Content Option
- Clean Descriptors Option

The following options are defined that require retention of information that would otherwise be removed but that is needed for specific uses:

- Retain Longitudinal Temporal Information with Full Dates Option
- Retain Longitudinal Temporal Information with Modified Dates Option
- Retain Patient Characteristics Option
- Retain Device Identity Option
- Retain UIDs
- Retain Safe Private Option

E.3.1 Clean Pixel Data Option

When this Option is specified in addition to an Application Level Confidentiality Profile, any information burned in to the Pixel Data (7FE0,0010) corresponding to the Attribute information specified to be removed by the Profile and any other Options specified shall also be removed, as described in Table E.1-1.

This may require intervention of or approval by a human operator.

The Attribute Burned In Annotation (0028,0301) shall be added to the Dataset with a value of "NO".

Note

1. This capability is called out as a specific option, since it may be extremely burdensome in practice to implement and is unnecessary for the vast majority of modalities that do not burn in such annotation in the first place. For example, CT images do not normally contain such burned in annotation, whereas Ultrasound images routinely do.

2. Though image processing and optical character recognition techniques can be used to detect the presence of and location of burned in text, and matching against known identifying information can be applied, deciding whether or not that text is identifying information or some other type of information may be non-trivial. Compliance with this option requires that identifying information is removed, regardless of how that is achieved. It is not required that information specified to be retained in the non-pixel data by other Options (e.g., physical characteristics, dates or descriptors) also be retained burned-in to the pixel data. Thus the most conservative approach of removing any and all burned in text would be compliant. This may involve sacrificing additional potentially useful information such as localizer posting and manual graphic annotations.

3. The stored pixel values are to be changed (blacked out); it is not sufficient to superimpose an overlay or graphic annotation or shutter to obscure the pixel data values, since those may not be ignored by the receiving system.

4. This option is intended to apply to the Pixel Data (7FE0,0010) Attribute that occurs in the top level Dataset of an Image Storage SOP Instance. The other standard use of Pixel Data (7FE0,0010) is within Icon Image Sequence (0088,0200), which is already described in Table E.1-1 and the accompanying note as requiring removal. This option does not require the ability to manually or automatically process the pixel values of Pixel Data (7FE0,0010) occurring in any other location than the top level dataset, but it does not prohibit it. Pixel Data (7FE0,0010) occurring within private Attributes will be removed because such Attributes will not be known to be safe.

E.3.2 Clean Recognizable Visual Features Option

When this Option is specified in addition to an Application Level Confidentiality Profile, if there is sufficient visual information within the Pixel Data of a set of instances to allow an individual to be recognized from the instances themselves or a reconstruction of a set of instances, then sufficient removal or distortion of the Pixel Data shall be applied to prevent recognition.

This may require intervention of or approval by a human operator.

The Attribute Recognizable Visual Features (0028,0302) shall be added to the Dataset with a value of "NO".

Note

1. This capability is called out as a specific option, since it may be extremely burdensome in practice to implement and is unnecessary for the vast majority of anatomic sites and modalities.

2. In the case of full-face photographs, the risk of visual identification is obvious, and numerous techniques are well established for de-identification, such as applying black rectangles over the eyes, etc.

3. In the case of high-resolution cross-sectional imaging of the entire head and neck, it has been suggested that a 3D volume or surface rendering of the pixel data may be sufficient to allow identification (or matching against a constrained subset of individuals) under some circumstances.

4. Application of this option may render the pixel data unusable for the purpose for which it has been collected, and hence its use may require a compromise between de-identification and utility based on obtaining appropriate ethical approval and informed consent. Consider for example, the case of dental images.

5. Since the Referenced Patient Photo Sequence is removed as part of the Basic Profile, support of the Clean Recognizable Visual Features option does not add requirements for that attribute.

E.3.3 Clean Graphics Option

Instances of various Standard and Standard Extended SOP Classes, including Images, Presentation States and other Composite SOP Instances, may contain identification information encoded as graphics, text annotations or overlays. This does not include information contained in Structured Report SOP Classes.

When this Option is specified in addition to an Application Level Confidentiality Profile, any information encoded in graphics, text annotations or overlays corresponding to the Attribute information specified to be removed by the Profile and any other Options specified shall also be removed, as described in Table E.1-1.

This may require intervention of a human operator.

Note

1. This capability is called out as a specific option, since it may be more practical to simply remove all such graphics, text annotations or overlays (as required by the profile without this option).

2. As with burned-in pixel data annotation, deciding whether or not text is identifying information or some other type of information may be non-trivial. It is not required that information specified to be retained in the non-pixel data by other Options (e.g., physical characteristics, dates or descriptors) also be retained in graphics, text annotations or overlays.

E.3.4 Clean Structured Content Option

Instances of Structured Report SOP Classes may contain identifiable information in a Content Sequence (0040,A730) encoded in Content Items. Instances of other SOP Classes may contain structured content encoded in a similar manner in the Acquisition Context Sequence (0040,0555) or Specimen Preparation Sequence (0040,0610).

When this Option is specified in addition to an Application Level Confidentiality Profile, any information encoded in SR Content Items or Acquisition Context or Specimen Preparation Sequence Items corresponding to the Attribute information specified to be removed by the Profile and any other Options specified shall also be removed.

Note

1. For example, the "observer" responsible for a diagnostic imaging report may be explicitly identified in Observation Content related Content Items in an SR.

2. A de-identifier that does not implement this option creates significant risk when attempting to de-identity a Structured Report unless it is only used to de-identify instances that are known to have no identifying information in the Content Sequence.

E.3.5 Clean Descriptors Option

Even though many Attributes are defined in the DICOM Standard for specific purposes, such as to describe a Study or a Series, those that contain plain text over which an operator has control may contain unstructured information that includes identities.

When this Option is specified in addition to an Application Level Confidentiality Profile, any information that is embedded in text or string Attributes corresponding to the Attribute information specified to be removed by the Profile and any other Options specified shall also be removed, as described in Table E.1-1.

Note

1. For example, an operator may include a person's name or a patient's demographics or physical characteristics in the Study Description (0008,1030), perhaps because their modality user interface does not provide other fields or because other systems do not display them. E.g., the description might contain "CT chest abdomen pelvis - 55F Dr. Smith".

2. One approach to cleaning such text strings without human intervention is to extract and retain only values known to be useful and safe and discard all others. For example, in the string "CT chest abdomen pelvis - 55F Dr. Smith" are found in Study Description (0008,1030), then it would be feasible to detect and retain "CT chest abdomen pelvis" and discard the remainder. In an international setting, this may require an extensive dictionary of words that are safe to retain, e.g., to detect "Buik" for abdomen in Dutch or "λεκάνη" for pelvis in Greek. Another possibility is to extract such information and attempt to code the information in other Attributes (if otherwise absent or empty) such as Anatomic Region Sequence (0008,2218). However, the possibility of string values being both identifying and descriptive in different uses needs to be considered, e.g., "Dr. Hand" or "M. Genou".

3. Table E.1-1 calls out specific Attributes known to be at risk, but an implementer may want to consider any attribute that could potential contain character data, though this Option does not require that this be done. For example, all SH, LO, ST, LT and UT Value Representations could perhaps be misused. Code strings, CS, are not generally at risk, but a check against known Defined Terms and Enumerated Values could be performed. Though extremely unusual, it is conceivable that even a DS or IS string could be misused, and a check could be made that only legal numeric characters were used. Any PN Attribute is obviously at risk. The OB VR is discussed in the Retain Safe Private Option.

4. This Option specifies what needs to be removed, not what needs to be retained. Depending on the application, it may be desirable to retain some information, such as technique description, but discard other information, such as diagnosis, for example because it may bias the interpretation in a clinical trial. For example, one approach is to remove all description and comment attributes except Series Description (0008,103E), since this Attribute rarely contains identifying or diagnosis information yet is typically a reliable source of useful information about the acquisition technique populated automatically from modality device protocols, though it still could be cleaned as described in Note 2.

5. It should be recognized that if any descriptor contains information about a particularly unusual procedure or condition, then in conjunction with other demographic information it might reduce the number of possible individuals that could be the imaging subject. However, this is to some extent true also if the condition or other unusual physical features are obvious from visual examination of the images themselves. E.g., how many conjoined twins born in a particular month in Philadelphia might there be?

The manner of cleaning shall be described in the Conformance Statement.

E.3.6 Retain Longitudinal Temporal Information Options

Dates and times are recognized as having a potential for leakage of identity because they constrain the number of possible individuals that could be the imaging subject, though only if there is access to other information about the individuals concerned to match it against.

However, there are applications that require dates and times to be present to able to fulfill the objective. This is particularly true in therapeutic clinical trials in which the objective is to measure change in an outcome measure over time. Further, it is often necessary to correlate information from images with information from other sources, such as clinical and laboratory data, and dates and times need to be consistent.

Two options are specified to address these requirements:

- Retain Longitudinal Temporal Information With Full Dates Option

- Retain Longitudinal Temporal Information With Modified Dates Option

When the Retain Longitudinal Temporal Information With Full Dates Option is specified in addition to an Application Level Confidentiality Profile, any dates and times present in the Attributes shall be retained, as described in Table E.1-1. The Attribute Longitudinal Temporal Information Modified (0028,0303) shall be added to the Dataset with a value of "UNMODIFIED".

When the Retain Longitudinal Temporal Information With Modified Dates Option is specified in addition to an Application Level Confidentiality Profile, any dates and times present in the Attributes listed in Table E.1-1 shall be modified. The modification of the dates and times shall be performed in a manner that:

- aggregates or transforms dates so as to reduce the possibility of matching for re-identification
- preserves the gross longitudinal temporal relationships between images obtained on different dates to the extent necessary for the application
- preserves the fine temporal relationships between images and real-world events to the extent necessary for analysis of the images for the application

The Attribute Longitudinal Temporal Information Modified (0028,0303) shall be added to the Dataset with a value of "MODIFIED".

Note

1. Aggregation of dates may be performed by various means such as setting all dates to the first day of the month, all months to the first month of the year, etc., depending on the precision required for the application.
2. It is possible to modify all dates and times to dummy values by shifting them relative to an arbitrary epoch, and hence retain the precise longitudinal temporal relationships amongst a set of studies, when either de-identification of the entire set is performed at the same time, or some sort of mapping or database is kept to repeat this process on separate occasions.
3. Transformation of dates and times should be considered together, in order to address studies that span midnight.
4. Any transformation of times should be performed in such a manner as to not disrupt computations needed for analysis, such as comparison of start of injection time to the acquisition time for PET SUV, or extraction of time-intensity values from dynamic contrast enhanced studies.

The manner of date modification shall be described in the Conformance Statement.

E.3.7 Retain Patient Characteristics Option

Physical characteristics of the patient, which are descriptive rather than identifying information per se, are recognized as having a potential for leakage of identity because they constrain the number of possible individuals that could be the imaging subject, though only if there is access to other information about the individuals concerned to match it against.

However, there are applications that require such physical characteristics in order to perform the computations necessary to analyze the images to fulfill the objective. One such class of applications is those that are related to metabolic measures, such as computation of PET Standard Uptake Values (SUV) or DEXA or MRI measures of body composition, which are based on body weight, body surface area or lean body mass.

When this Option is specified in addition to an Application Level Confidentiality Profile, information about age, sex, height and weight and other characteristics present in the Attributes shall be retained, as described in Table E.1-1.

The manner of cleaning of retained attributes shall be described in the Conformance Statement.

E.3.8 Retain Device Identity Option

Information about the identity of the device that was used to perform the acquisition is recognized as having a potential for leakage of identity because it may constrain the number of possible individuals that could be the imaging subject, though only if there is access to other information about the individuals concerned to match it against.

However, there are applications that require such device information to perform the analysis or interpretation. The type of correction for spatial or other inhomogeneity may require knowledge of the specific device serial number. Confirmation that specific devices that

have been previously qualified (e.g., with phantoms) may be required. Further, there may be a need to maintain a record of the device used for regulatory or registry purposes, yet the acquisition site may not maintain an adequate electronic audit trail.

When this Option is specified in addition to an Application Level Confidentiality Profile, information about the identity of the device in the Attributes shall be retained, as described in Table E.1-1.

E.3.9 Retain UIDs Option

Though individuals do not have unique identifiers themselves, studies, series, instances and other entities in the DICOM model are assigned globally unique UIDs. Whilst these UIDs cannot be mapped directly to an individual out of context, given access to the original images, or to a database of the original images containing the UIDs, it would be possible to recover the individual's identity.

However, there are applications that require the ability to maintain an audit trail back to the original images and though there are other mechanisms they may not scale well or be reliably implemented. This Option is provided for use when it is judged that the risk of gaining access to the original information via the UIDs is small relative to the benefit of retaining them.

When this Option is specified in addition to an Application Level Confidentiality Profile, UIDs shall be retained, as described in Table E.1-1.

Note

1. A UID of a DICOM entity is not the same as a unique identifier of an individual, such as would be proscribed by some privacy regulations.

2. UIDs are generated using a hierarchical scheme of "roots", which may be traceable by a knowledgeable person back to the original assignee of the root, typically the device manufacturer, but sometimes the organization using the device.

3. When evaluating the risk of matching UIDs with the original images or PACS database, one should consider that even if the UIDs are changed, the pixel data itself presents a similar risk. Specifically, the pixel data of the de-identified image can be matched against the pixel data of the original image. Such matching can be greatly accelerated by comparing pre-computed hash values of the pixel data. Removal of burned-in identification may change the pixel data but then matching against a sub-region of the pixel data is almost certainly possible (e.g., the central region of an image). Even addition of noise to an image is not sufficient to prevent re-identification since statistical matching techniques can be used. Ultimately, if any useable pixel data is retained during de-identification, then re-identification is nearly always possible if one has access to the original images. Ergo, replacement of UIDs should not give rise to a false confidence that the images have been more thoroughly de-identified than if the UIDs are retained.

4. Regardless of this option, implementers should take care not to remove UIDs that are structural and defined by the standard as opposed to those that are instance-related. E.g., one would never remove or replace the SOP Class UID for de-identification purposes.

5. The Implementation Class UID (0002,0012) is not included in the list of UID attributes to be retained, since it is part of the File Meta Information (see PS3.10), which is entirely replaced whenever a file is stored or modified during de-identification. See Section E.1.1.

E.3.10 Retain Safe Private Option

By definition, Private Attributes contain proprietary information, in many cases the nature of which is known only to the vendor and not publicly documented.

However, some Private Attributes may be necessary for the desired application. For example, specific technique information such as CT helical span pitch, or pixel value transformation, such as PET SUV rescale factors, may only be available in Private Attributes since the information is either not defined in Standard Attributes, or was added to the DICOM Standard after the acquisition device was manufactured.

When this Option is specified in addition to an Application Level Confidentiality Profile, Private Attributes that are known by the de-identifier to be safe from identity leakage shall be retained, together with the Private Creator IDs that are required to fully define the retained Private Attributes; all other Private Attributes shall be removed or processed in the element-specific manner recommended by Deidentification Action (0008,0307), if present within Private Data Element Characteristics Sequence (0008,0300) (see PS3.3 Section C.12.1).

Whether or not an Attribute is known to be safe may be determined by:

- its presence in a block of Private Data Elements with a value of "SAFE" in Block Identifying Information Status (0008,0303) or individually listed in Nonidentifying Private Elements (gggg,0004) (within Private Data Element Characteristics Sequence (0008,0300); see PS3.3 Section C.12.1)
- its presence in Table E.3.10-1 Safe Private Attributes
- documentation in the Conformance Statement
- some other means.

When this Option is not specified, all Private Attributes shall be removed, as described in Table E.1-1.

Note

1. A sample list of Private Attributes thought to be safe is provided here. Vendors do not guarantee them to be safe, and do not commit to sending them in any particular software version (including future products).

Table E.3.10-1. Safe Private Attributes

Data Element	Private Creator	VR	VM	Meaning
(7053,xx00)	Philips PET Private Group	DS	1	SUV Factor - Multiplying stored pixel values by Rescale Slope then this factor results in SUVbw in g/l
(7053,xx09)	Philips PET Private Group	DS	1	Activity Concentration Factor - Multiplying stored pixel values by Rescale Slope then this factor results in MBq/ml.
(00E1,xx21)	ELSCINT1	DS	1	DLP
(01E1,xx26)	ELSCINT1	CS	1	Phantom Type
(01E1,xx50)	ELSCINT1	DS	1	Acquisition Duration
(01F1,xx01)	ELSCINT1	CS	1	Acquisition Type
(01F1,xx07)	ELSCINT1	DS	1	Table Velocity
(01F1,xx26)	ELSCINT1	DS	1	Pitch
(01F1,xx27)	ELSCINT1	DS	1	Rotation Time
(0019,xx23)	GEMS_ACQU_01	DS	1	Table Speed [mm/rotation]
(0019,xx24)	GEMS_ACQU_01	DS	1	Mid Scan Time [sec]
(0019,xx27)	GEMS_ACQU_01	DS	1	Rotation Speed (Gantry Period)
(0019,xx9E)	GEMS_ACQU_01	LO	1	Internal Pulse Sequence Name
(0043,xx27)	GEMS_PARM_01	SH	1	Scan Pitch Ratio in the form "n.nnn:1"
(0045,xx01)	GEMS_HELIOS_01	SS	1	Number of Macro Rows in Detector
(0045,xx02)	GEMS_HELIOS_01	FL	1	Macro width at ISO Center
(0903,xx10)	GEIIS PACS	US	1	Reject Image Flag
(0903,xx11)	GEIIS PACS	US	1	Significant Flag
(0903,xx12)	GEIIS PACS	US	1	Confidential Flag
(2001,xx03)	Philips Imaging DD 001	FL	1	Diffusion B-Factor
(2001,xx04)	Philips Imaging DD 001	CS	1	Diffusion Direction
(0019,xx0C)	SIEMENS MR HEADER	IS	1	B Value
(0019,xx0D)	SIEMENS MR HEADER	CS	1	Diffusion Directionality
(0019,xx0E)	SIEMENS MR HEADER	FD	3	Diffusion Gradient Direction

Data Element	Private Creator	VR	VM	Meaning
(0019,xx27)	SIEMENS MR HEADER	FD	6	B Matrix
(0043,xx39)	GEMS_PARM_01	IS	4	1st value is B Value
(0043,xx6F)	GEMS_PARM_01	DS	3-4	Scanner Table Entry + Gradient Coil Selected
(0025,xx07)	GEMS_SERS_01	SL	1	Images in Series
(7E01,xx01)	HOLOGIC, Inc.	LO	1	Codec Version
(7E01,xx02)	HOLOGIC, Inc.	SH	1	Codec Content Type
(7E01,xx10)	HOLOGIC, Inc.	SQ	1	High Resolution Data Sequence
(7E01,xx11)	HOLOGIC, Inc.	SQ	1	Low Resolution Data Sequence
(7E01,xx12)	HOLOGIC, Inc.	OB	1	Codec Content
(0099,xx01)	NQHeader	UI	1	Version
(0099,xx02)	NQHeader	UI	1	Analyzed Series UID
(0099,xx04)	NQHeader	SS	1	Return Code
(0099,xx05)	NQHeader	LT	1	Return Message
(0099,xx10)	NQHeader	FL	1	MI
(0099,xx20)	NQHeader	SH	1	Units
(0099,xx21)	NQHeader	FL	1	ICV
(0199,xx01)	NQLeft	FL	1	Left Cortical White Matter
(0199,xx02)	NQLeft	FL	1	Left Cortical Gray Matter
(0199,xx03)	NQLeft	FL	1	Left 3rd Ventricle
(0199,xx04)	NQLeft	FL	1	Left 4th Ventricle
(0199,xx05)	NQLeft	FL	1	Left 5th Ventricle
(0199,xx06)	NQLeft	FL	1	Left Lateral Ventricle
(0199,xx07)	NQLeft	FL	1	Left Inferior Lateral Ventricle
(0199,xx08)	NQLeft	FL	1	Left Inferior CSF
(0199,xx09)	NQLeft	FL	1	Left Cerebellar White Matter
(0199,xx0a)	NQLeft	FL	1	Left Cerebellar Gray Matter
(0199,xx0b)	NQLeft	FL	1	Left Hippocampus
(0199,xx0c)	NQLeft	FL	1	Left Amygdala
(0199,xx0d)	NQLeft	FL	1	Left Thalamus
(0199,xx0e)	NQLeft	FL	1	Left Caudate
(0199,xx0f)	NQLeft	FL	1	Left Putamen
(0199,xx10)	NQLeft	FL	1	Left Pallidum
(0199,xx11)	NQLeft	FL	1	Left Ventral Diencephalon
(0199,xx12)	NQLeft	FL	1	Left Nucleus Accumbens
(0199,xx13)	NQLeft	FL	1	Left Brain Stem
(0199,xx14)	NQLeft	FL	1	Left Exterior CSF
(0199,xx15)	NQLeft	FL	1	Left WM Hypo
(0199,xx16)	NQLeft	FL	1	Left Other
(0299,xx01)	NQRight	FL	1	Right Cortical White Matter
(0299,xx02)	NQRight	FL	1	Right Cortical Gray Matter
(0299,xx03)	NQRight	FL	1	Right 3rd Ventricle

Data Element	Private Creator	VR	VM	Meaning
(0299,xx04)	NQRight	FL	1	Right 4th Ventricle
(0299,xx05)	NQRight	FL	1	Right 5th Ventricle
(0299,xx06)	NQRight	FL	1	Right Lateral Ventricle
(0299,xx07)	NQRight	FL	1	Right Inferior Lateral Ventricle
(0299,xx08)	NQRight	FL	1	Right Inferior CSF
(0299,xx09)	NQRight	FL	1	Right Cerebellar White Matter
(0299,xx0a)	NQRight	FL	1	Right Cerebellar Gray Matter
(0299,xx0b)	NQRight	FL	1	Right Hippocampus
(0299,xx0c)	NQRight	FL	1	Right Amygdala
(0299,xx0d)	NQRight	FL	1	Right Thalamus
(0299,xx0e)	NQRight	FL	1	Right Caudate
(0299,xx0f)	NQRight	FL	1	Right Putamen
(0299,xx10)	NQRight	FL	1	Right Pallidum
(0299,xx11)	NQRight	FL	1	Right Ventral Diencephalon
(0299,xx12)	NQRight	FL	1	Right Nucleus Accumbens
(0299,xx13)	NQRight	FL	1	Right Brain Stem
(0299,xx14)	NQRight	FL	1	Right Exterior CSF
(0299,xx15)	NQRight	FL	1	Right WM Hypo
(0299,xx16)	NQRight	FL	1	Right Other
(2005,xx0D)	Philips MR Imaging DD 001	FL	1	Scale Intercept
(2005,xx0E)	Philips MR Imaging DD 001	FL	1	Scale Slope

2. One approach to retaining Private Attributes safely, either when the VR is encoded explicitly or known from a data dictionary (such as may be derived from published DICOM Conformance Statements or previously encountered instances, perhaps by adaptively extending the data dictionary as new explicit VR instances are received), is to retain those Attributes that are numeric only. For example, one might retain US, SS, UL, SS, FL and FD binary values, and IS and DS string values that contain only valid numeric characters. One might assume that other string Value Representations are unsafe in the absence of definite confirmation from the vendor to the contrary; code strings (CS) may be an exception. Bulk binary data in OB Value representations is particularly unsafe, and may often contain entire proprietary format headers in binary or text or XML form that includes the patient's name and other identifying information.

The safe private attributes that are retained shall be described in the Conformance Statement.

F Network Address Management Profiles

F.1 Basic Network Address Management Profile

The Basic Network Address Management Profile utilizes DHCP to provide services to assign and manage IP parameters for machines remotely. The DHCP server is manually configured to establish the rules for assigning IP addresses to machines. The rules may be explicit machine by machine assignments and may be assignment of a block of IP addresses to be assigned dynamically as machines are attached and removed from the network. The DHCP client can obtain its IP address and a variety of related parameters such as NTP server address from the DHCP server during startup. The DHCP server may dynamically update the DNS server with new relationships between IP addresses and DNS hostnames.

The DNS Client can obtain the IP number for another host by giving the DNS hostname to a DNS Server and receive the IP number in response. This transaction may be used in other profiles or in implementations that do not conform to the Basic Network Address Management Profile.

The Basic Network Address Management Profile applies to the actors DHCP Server, DHCP Client, DNS Server, and DNS Client. The mandatory and optional transactions are described in the table and sections below.

Table F.1-1. Basic Network Address Management Profile

Actor	Transaction	Optionality	Section
DHCP Server	Configure DHCP Server	M	F.1.2
	Find and Use DHCP Server	M	F.1.3
	Maintain Lease	M	F.1.4
	Resolve Hostname	M	F.1.1
	DDNS Coordination	O	F.1.5
DHCP Client	Find and Use DHCP Server	M	F.1.3
	Maintain Lease	M	F.1.4
DNS Server	DDNS Coordination	O	F.1.5
	Resolve Hostname	M	F.1.1
DNS Client	Resolve Hostname	M	F.1.1

F.1.1 Resolve Hostname

F.1.1.1 Scope

The DNS Client can obtain the IP number for a host by giving the DNS hostname to a DNS Server and receive the IP number in response.

F.1.1.2 Use Case Roles

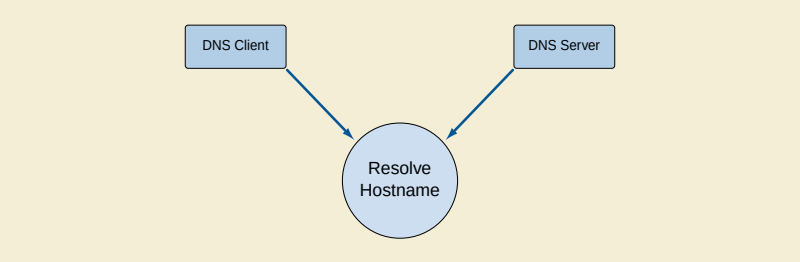

Figure F.1-1. Resolve Hostname

Actor: DNS Client

Role: Needs IP address, has the DNS Hostname

Actor: DNS Server

Role: Provides current IP address when given the DNS Hostname

F.1.1.3 Referenced Standards

The standards and their relationships for the family of DNS protocols are shown in Figure F.1-2. The details of transactions, transaction diagrams, etc. are contained within the referenced RFC's.

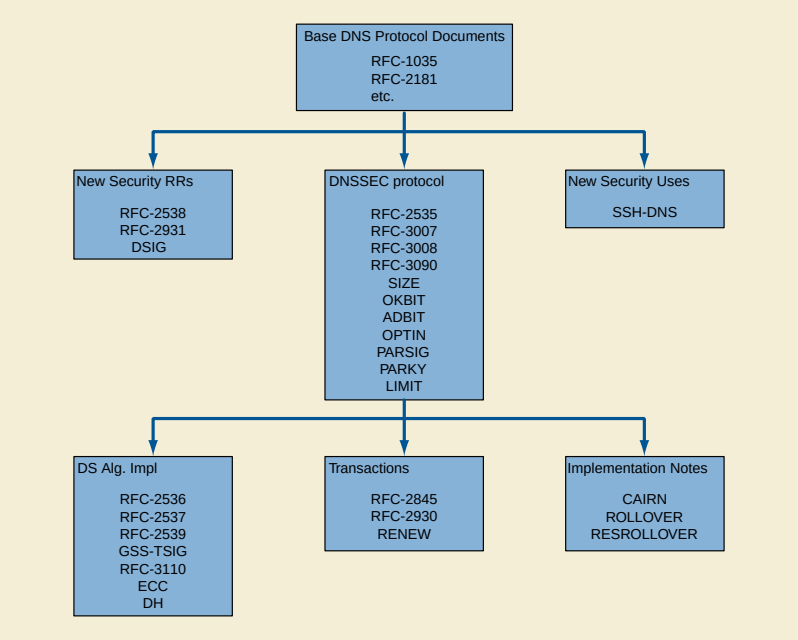

Figure F.1-2. DNS Referenced Standards

F.1.1.4 DNS Security Considerations (Informative)

The issue of security is under active development by the Internet Engineering Task Force and its various working groups. The security related RFCs and drafts are identified in Figure F.1-2. Some of these are completed. Others are still in the draft stage. The Basic Network Address Management Profile does not include specific requirements for support of DNS security extensions by the DNS Client.

The Basic Network Address Management profile should not be used outside a secured environment. At a minimum there should be:

a. Firewall or router protections to ensure that only approved external hosts are used for DNS services.

b. Agreements for VPN and other access should require that DNS clients use only approved DNS servers over the VPN.

Other network security procedures such as automated intrusion detection may be appropriate in some environments. Security features beyond this minimum should be established by the local security policy and are beyond the scope of DICOM.

The purpose of the selected security is to limit the scope of the threat to insider attacks. The DNS system discloses only hostnames and IP addresses, so there is little concern about eavesdropping. The protections are to limit the exposure to denial of service attacks by counterfeit servers or clients.

F.1.1.5 DNS Implementation Considerations (Informative)

Client caches may cause confusion during updates. Many DNS clients check for DNS updates very infrequently and might not reflect DNS changes for hours or days. Manual steps may be needed to trigger immediate updates. Details for controls of cache and update vary for different DNS clients and DNS servers, but DNS caching and update propagation delays are significant factors and implementations have mechanisms to manage these issues.

DNS Server failure management should be considered. Redundant servers and fallback host files are examples of possible error management tools.

F.1.1.6 Support For Service Discovery

The DNS server may provide additional optional information in support of configuration management. See Section H.2 for the specification of this information and additional RFC's to be supported.

F.1.2 Configure DHCPserver

F.1.2.1 Scope

The DHCP server shall be configurable by site administration so that

a. DHCP clients can be added and removed.

b. DHCP clients configurations can be modified to set values for attributes used in later transactions.

c. pre-allocation of fixed IP addresses for DHCP clients is supported

This standard does not specify how this configuration is to be performed.

Note

Most DHCP servers support the pre-allocation of fixed IP addresses to simplify the transition process for legacy systems. This permits a particular device to switch to DHCP while retaining the previously assigned IP address. This enables the use of a central site management of IP addresses without breaking compatibility with older systems that require fixed IP addresses.

F.1.2.2 Use Case Roles

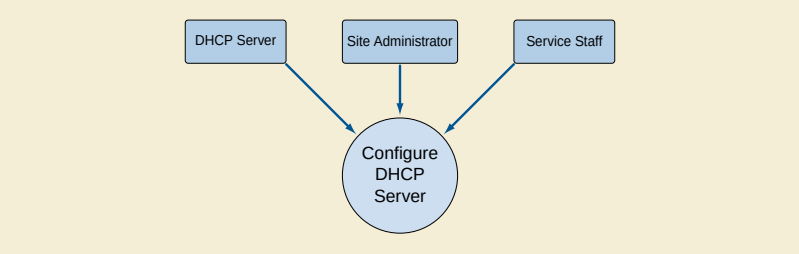

Figure F.1-3. Configure DHCP Server

Actor: DHCP Server

Role: Maintains internal configuration files.

Actor: Site Administrator

Role: Updates configuration information to add, modify, and remove descriptions of clients and servers.

Actor: Service Staff

Role: Provides initial configuration requirements for many devices when installing a new network, and for individual devices when installing or modifying a single device.

F.1.2.3 Referenced Standards

None

F.1.3 Find and Use DHCP Server

F.1.3.1 Scope

This is the support for the normal startup process. The DHCP client system boots up, and very early in the booting process it finds DHCP servers, selects one of the DHCP servers to be its server, queries that server to obtain a variety of information, and continues DHCP client self-configuration using the results of that query. DHCP servers may optionally provide a variety of information, such as server locations, normal routes. This transaction identifies what information shall be provided by a compliant DHCP server, and identifies what information shall be requested by a compliant DHCP client. A compliant DHCP server in not required to provide this optional information.

F.1.3.2 Use Case Roles

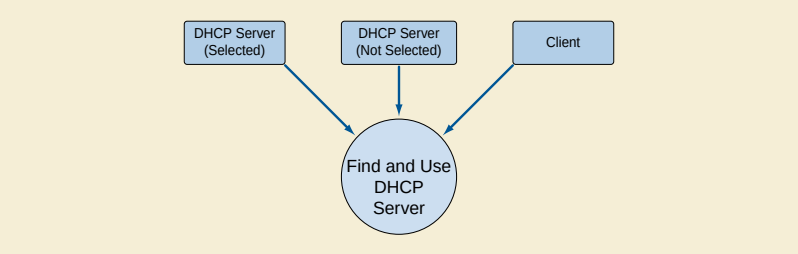

Figure F.1-4. Find and Use DHCP Server

Actor: DHCP Server

Role: Responds to DHCP acquisition queries. Multiple actors may exist. The DHCP client will select one.

Actor: DHCP client

Role: Queries for DHCP Servers. Selects one responding server.

F.1.3.3 Referenced Standards

RFC-2131 DHCP Protocol

RFC-2132 DHCP Options

RFC-2563 Auto Configuration control

F.1.3.4 Interaction Diagram

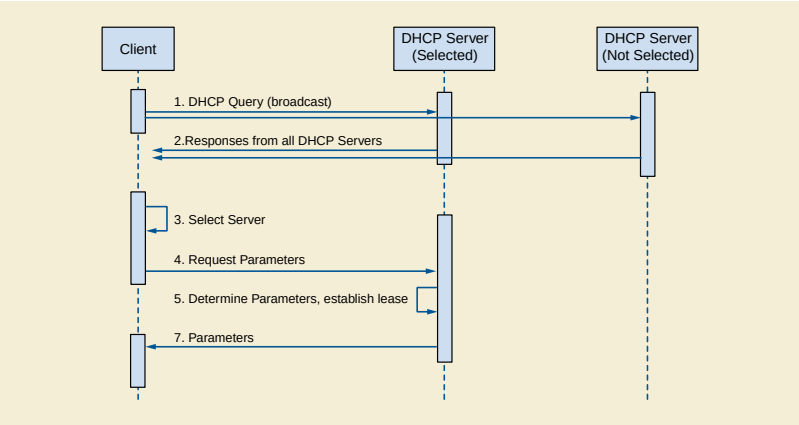

Figure F.1-5. DHCP Interactions

The DHCP client shall comply with RFC-2131 (DHCP Protocol), RFC-2132 (DHCP Options), RFC-2563 (Auto Configuration Control), and their referenced RFCs.

The DHCP client shall query for available DHCP servers. It shall select the DHCP server to use.

The DHCP client shall query for an IP assignment. The DHCP Server shall determine the IP parameters in accordance with the current DHCP configuration, establish a lease for these parameters, and respond with this information. (See below for lease maintenance and expiration.) The DHCP client shall apply these parameters to the TCP/IP stack. The DHCP client shall establish internal lease maintenance activities.

The DHCP client shall query for the optional information listed in Table F.1-2 when required by additional profiles used by the client system. If the DHCP server does not provide this information, the default values shall be used by the DHCP client.

Table F.1-2. DHCP Parameters

DHCP Option	Description	Default
NTP	List of NTP servers	Empty list
DNS	List of DNS servers	Empty list
Router	Default router	Empty list
Static routes		Nil
Hostname		Requested machine name
Domain name		Nil
Subnet mask		Derived from network value
Broadcast address		Derived from network value
Default router		Nil
Time offset		Site configurable
MTU		Hardware dependent
Auto-IP permission		From NVRAM

The DHCP client shall make this information available for other actors within the DHCP client machine.

F.1.4 Maintain Lease

F.1.4.1 Scope

The DHCP client normally maintains the IP lease in compliance with the RFCs. Sometimes the server will not renew the lease. Non-renewal is usually part of network service operations. The loss of the IP lease requires connections using that IP address to cease.

F.1.4.2 Use Case Roles

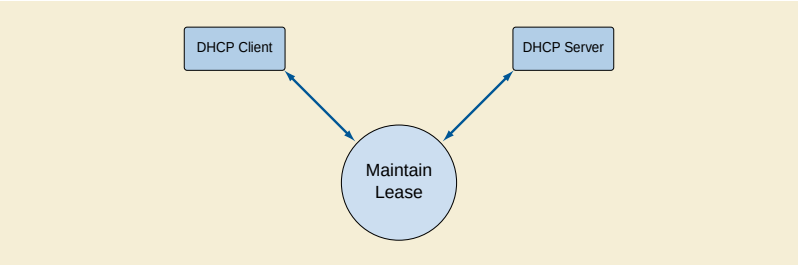

Figure F.1-6. Maintain Lease

Actor: DHCP client

Role: Deals with lease renewal and expiration.

Actor: DHCP Server

Role: Renewing or deliberately letting leases expire (sometimes done as part of network service operations).

F.1.4.3 Referenced Standards

RFC-2131 DHCP Protocol

RFC-2132 DHCP Options

F.1.4.4 Normal Interaction

The DHCP client shall maintain a lease on the IP address in accordance with the DHCP protocol as specified in RFC-2131 and RFC-2132. There is a possibility that the DHCP Server may fail, or may choose not to renew the lease.

In the event that the DHCP lease expires without being renewed, any still active DICOM connections may be aborted (AP-Abort).

Note

There is usually a period (typically between several minutes and several days) between the request for lease extension and actual expiration of the lease. The application might take advantage of this to perform a graceful association release rather than the abrupt shutdown of an AP-Abort.

F.1.5 DDNS Coordination

F.1.5.1 Scope

DHCP servers may coordinate their IP and hostname assignments with a DNS server. This permits dynamic assignment of IP addresses without interfering with access to DHCP Clients by other systems. The other systems utilize the agreed hostname (which DHCP can manage and provide to the client) and obtain the current IP address by means of DNS lookup.

A DHCP Server is in compliance with this optional part of the Basic Network Address Management Profile profile if it maintains and updates the relevant DNS server so as to maintain the proper hostname/IP relationships in the DNS database.

F.1.5.2 Use Case Roles

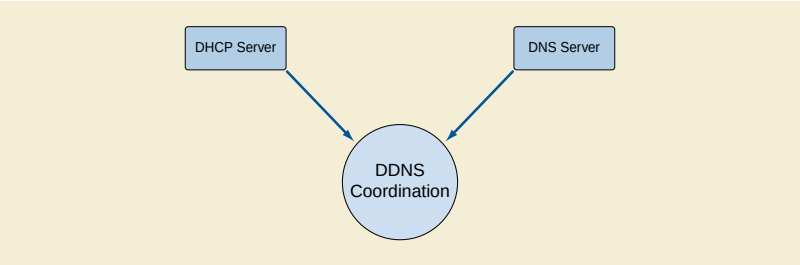

Figure F.1-7. DDNS Coordination

Actor: DHCP Server

Role: Responded to DHCP acquisition queries and assigned IP address to client.

Actor: DNS Server

Role: Maintains the DNS services for the network.

F.1.5.3 Referenced Standards

RFC-2136 Dynamic Updates in the Domain Name System

F.1.5.4 Basic Course of Events

After the DHCP server has assigned an IP address to a DHCP client, the DHCP server uses DDNS to inform the DNS server that the hostname assigned to the DHCP client has been given the assigned IP address. The DNS Server updates the DNS database so that subsequent DNS queries for this hostname are given the assigned IP address. When the lease for the IP address expires without renewal, the DHCP server informs the DNS server that the IP address and hostname are no longer valid. The DNS server removes them from the DNS database.

F.1.6 DHCP Security Considerations (Informative)

The Basic Network Address Management Profile Profile has two areas of security concerns:

a. Protection against denial of service attacks against the DHCP client/server traffic.

b. Protection against denial of service attacks against the DHCP server to DDNS server update process.

The Basic Network Address Management Profile Profile should not be used outside a secured environment. At a minimum there should be:

a. Firewall and or router protections to ensure that only approved hosts are used for DHCP and DNS services.

b. Agreements for VPN and other access should require that DNS clients on the hospital network use only approved DHCP or DNS servers over the VPN.

Other network security procedures such as automated intrusion detection may be appropriate in some environments. Security features beyond this minimum should be established by the local security policy and are beyond the scope of DICOM.

The purpose of the selected security is to limit the scope of the threat to insider attacks. The DHCP and DNS systems disclose only hostnames and IP addresses, so there is little concern about eavesdropping. The protections are to limit the exposure to denial of service attacks by counterfeit servers or clients. The specific DNS security extensions are described in Section F.1.1.4. This profile does not utilize the DHCP security extensions because they provide very limited added security and the attacks are insider denial of service attacks. Intrusion detection and other network level protection mechanisms are the most effective next level of protections for the DHCP process.

The DNS update is optional in this profile to accommodate the possibility that the DHCP server and DNS server cannot reach a mutually acceptable security process. Support of this option may require support of the DNS security protocols that are in the process of development. See Section F.1.1.4 for a discussion of the DNS security profile standards and drafts.

F.1.7 DHCP Implementation Considerations (Informative)

The DHCP configuration file can be a very useful form of documentation for the local network hardware configuration. It can be prepared in advance for new installations and updated as clients are added. Including information for all machines, including those that do not utilize DHCP, avoids accidental IP address conflicts and similar errors.

Most DHCP servers have a configuration capability that permits control of the IP address and other information provided to the client. These controls can pre-allocate a specific IP address, etc. to a machine based on the requested machine name or MAC address. These pre-allocated IP addresses then ensure that these specific machines are always assigned the same IP address. Legacy systems that do not utilize DNS can continue to use fixed tables with IP addresses when the DHCP server has pre-allocated the IP addresses for those services.

F.1.8 Conformance

The Conformance Statement for an LDAP Client shall describe its use of LDAP to configure the local AE titles. Any conformance to the Update LDAP Server option shall be specified, together with the values for all component object attributes in the update sent to the LDAP Server. Any use of LDAP to configure the remote device addresses and capabilities shall be described. The LDAP queries used to obtain remote device component object attributes shall be specified.

Note

In particular, use of LDAP to obtain the AE Title, TCP port, and IP address for specific system actors (e.g., an Image Archive, or a Performed Procedure Step Manager) should be detailed, as well as how the LDAP information for remote devices is selected for operational use.

G Time Synchronization Profiles

G.1 Basic Time Synchronization Profile

The Basic Time Synchronization Profile defines services to synchronize the clocks on multiple computers. It employs the Network Time Protocol (NTP) services that have been used for this purpose by many other disciplines. NTP permits synchronization to a local server that provides a local time source, and synchronization to a variety of external time services. The accuracy and precision controls are not explicitly part of the protocol. They are determined in large part by the selection of clock hardware and network topology.

An extensive discussion of implementation strategies for NTP can be found at http://www.ntp.org.

The Basic Time Synchronization Profile applies to the actors DHCP Client, DHCP Server, SNTP Client, NTP Client and NTP Server. The mandatory and optional transactions are described in the table and sections below.

Table G.1-1. Basic Time Synchronization Profile

Actor	Transaction	Optionality	Section
NTP Server	Maintain Time	M	G.1.2
	Find NTP Servers	O	G.1.1
NTP Client	Maintain Time	M	G.1.2
	Find NTP Servers	O	G.1.1
SNTP Client	Maintain Time	M	G.1.2
DHCP Server	Find NTP Servers	O	G.1.1
DCHP Client	Find NTP Servers	M	G.1.1

G.1.1 Find NTP Servers

The optional NTP protocol elements for NTP autoconfiguration and NTP autodiscovery can significantly simplify installation. The NTP specification for these is defined such that they are truly optional for both client and server. In the event that a client cannot find an NTP server automatically using these services, it can use the DHCP optional information or manually configured information to find a server. Support for these services is recommended but not mandatory.

This transaction exists primarily as a means of documenting whether particular models of equipment support the automatic discovery. This lets installation and operation plan their DHCP and equipment installation procedures in advance.

G.1.1.1 Scope

This applies to any client that needs the correct time, or that needs to have its time stamps synchronized with those of another system. The accuracy of synchronization is determined by details of the configuration and implementation of the network and NTP servers at any specific site.

Both the NTP and SNTP clients shall utilize the NTP server information if it is provided by DHCP and NTP services have not been found using autodiscovery. Manual configuration shall be provided as a backup. Autodiscovery or DHCP are preferred.

G.1.1.2 Use Case Roles

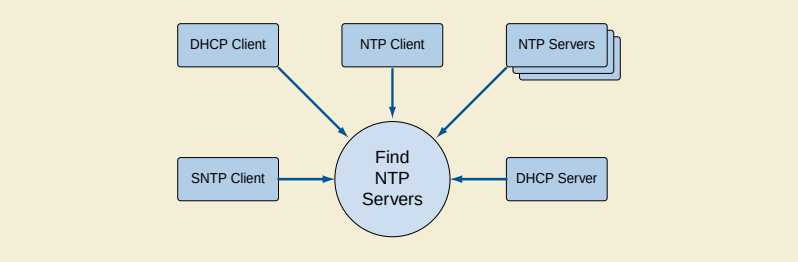

Figure G.1-1. Find NTP Servers

DHCP Server	Provides UTC offset, provides list of NTP servers
DHCP Client	Receives UTC offset and list of NTP servers
NTP Client	Maintains client clock
SNTP Client	Maintains client clock
NTP Servers	External time servers. These may have connections to other time servers, and may be synchronized with national time sources.

G.1.1.3 Referenced Standards

RFC-1305 Network Time Protocol (NTP) standard specification

RFC-2030 Simple NTP

G.1.1.4 Basic Course of Events.

The DHCP server may have provided a list of NTP servers or one may be obtained through optional NTP discovery mechanisms. If this list is empty and no manually configured NTP server address is present, the client shall select its internal clock as the time source (see below). If the list is not empty, the client shall attempt to maintain time synchronization with all those NTP servers. The client may attempt to use the multi-cast, manycast, and broadcast options as defined in RFC-1305. It shall utilize the point to point synchronization option if these are not available. The synchronization shall be in compliance with either RFC-1305 (NTP) or RFC-2030 (SNTP).

If the application requires time synchronization of better than 1s mean error, the client should use NTP. SNTP cannot ensure a more accurate time synchronization.

The DHCP server may have provided a UTC offset between the local time at the machine and UTC. If this is missing, the UTC offset will be obtained in a device specific manner (e.g., service, CMOS). If the UTC offset is provided, the client shall use this offset for converting between UTC and local time.

G.1.1.5 Alternative Paths

If there is no UTC offset information from the DHCP server, then the NTP client will use its preset or service set UTC offset.

If there is no NTP time server, then the NTP client will select its internal battery clock as the source of UTC. These may have substantial errors. This also means that when there are multiple systems but no NTP source, the multiple systems will not attempt to synchronize with one another.

G.1.1.6 Assumptions

The local battery clock time is set to UTC, or the local operating system has proper support to manage both battery clock time, NTP clock time, and system clock time. The NTP time is always in UTC.

G.1.1.7 Postconditions

The client will remain synchronized with its selected time source. In an environment with one or more NTP servers, this will be good time synchronization. In the absence of NTP servers, the selected source will be the internal client clock, with all its attendant errors.

G.1.2 Maintain Time

G.1.2.1 Scope

This applies to any client that needs the correct time, or that needs to have its time stamps synchronized with those of another system. The accuracy of synchronization is determined by details of the configuration and implementation of the network and NTP servers at any specific site.

G.1.2.2 Use Case Roles

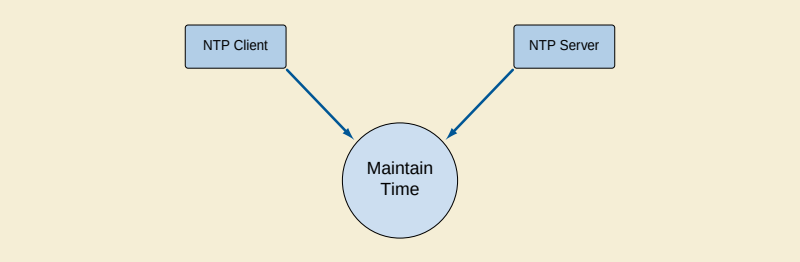

Figure G.2-1. Maintain Time

NTP/SNTP Client	Maintains client clock
NTP Servers	External time servers. These may have connections to other time servers, and may be synchronized with national time sources.

G.1.2.3 Referenced Standards

RFC-1305 Network Time Protocol (NTP) standard specification

RFC-2030 Simple NTP

G.1.2.4 Basic Course of Events.

All the full detail is in RFC-1305 and RFC-2030. The most common and mandatory minimum mode for NTP operation establishes a ping pong of messages between client and servers. The client sends requests to the servers, which fill in time related fields in a response, and the client performs optimal estimation of the present time. The RFCs deal with issues of lost messages, estimation formulae, etc. Once the clocks are in synchronization these ping pong exchanges typically stabilize at roughly 1000 second intervals.

The client machine typically uses the time estimate to maintain the internal operating system clock. This clock is then used by applications that need time information. This approach eliminates the application visible difference between synchronized and unsynchronized time. The RFCs provide guidance on proper implementations.

G.1.3 NTP Security Considerations (Informative)

The Basic Time Synchronization profile should not be used outside a secured environment. At a minimum there should be:

a. Firewall and or router protections to ensure that only approved hosts are used for NTP services.

b. Agreements for VPN and other access should require that use only approved NTP servers over the VPN.

This limits the risks to insider denial of service attacks. The service denial is manipulation of the time synchronization such that systems report the incorrect time. The NTP protocols incorporate secure transaction capabilities that can be negotiated. This profile assumes

that the above protections are sufficient and does not require support of secure transactions, but they may be supported by an implementation. The SNTP client does not support the use of secured transactions.

Sites with particular concerns regarding security of external network time sources may choose to utilize a GPS or radio based time synchronization. Note that when selecting GPS and radio time sources, care must be taken to establish the accuracy and stability provided by the particular time source. The underlying time accuracy of GPS and radio sources is superb, but some receivers are intended for low accuracy uses and do not provide an accurate or stable result.

G.1.4 NTP Implementation Considerations (Informative)

NTP servers always support both NTP and SNTP clients. The difference is one of synchronization accuracy, not communications compatibility. Although in theory both NTP and SNTP clients could run at the same time on a client this is not recommended. The SNTP updates will simply degrade the time accuracy. When other time protocol clients, such as IRIG, are also being used these clients must be coordinated with the NTP client to avoid synchronization problems.

RFC-1305 includes specifications for management of intermittent access to the NTP servers, broken servers, etc. The NTP servers do not need to be present and operational when the NTP process begins. NTP supports the use of multiple servers to provide backup and better accuracy. RFC-1305 specifies the mechanisms used by the NTP client. The site www.ntp.org provides extensive guidance and references regarding the most effective configurations for backups and multiple server configurations.

The local battery clock and client operating system must be properly UTC aware. NTP synchronization is in UTC. This can be a source of confusion because some computers are configured with their hardware clocks set to local time and the operating system set (incorrectly) to UTC. This is a common error that only becomes apparent when the devices attempt to synchronize clocks.

G.1.5 Conformance

The Conformance Statement for the NTP Server and NTP Client shall state whether secure transactions are supported.

The Conformance Statement for the NTP Server shall state whether it is also an NTP Client.

H Application Configuration Management Profiles

H.1 Application Configuration Management Profile

The Application Configuration Management Profile applies to the actors LDAP Server, LDAP Client, and DNS Server. The mandatory and optional transactions are described in the table and sections below.

Table H.1-1. Application Configuration Management Profiles

Actor	Transaction	Optionality	Section
LDAP Server	Query LDAP Server	M	H.1.4.2
	Update LDAP Server	O	H.1.4.3
	Maintain LDAP Server	M	H.1.4.4
LDAP Client	Find LDAP Server	M	H.1.4.1
	Query LDAP Server	M	H.1.4.2
	Update LDAP Server	O	H.1.4.3
DNS Server	Find LDAP Server	M	H.1.4.1

H.1.1 Data ~~ModelcomponentModel Component~~ Objects

The normative definition of the schema can be found in Section H.1.3. This section gives additional informative descriptions of the objects and information defined in that schema and makes normative statements regarding DICOM system behavior.

The Application Configuration Data Model has the following component objects:

Device The description of the device

Network AE The description of the network application entity

Network Connection The description of the network interface

Transfer Capability The description of the SOP classes and syntaxes supported by a Network AE.

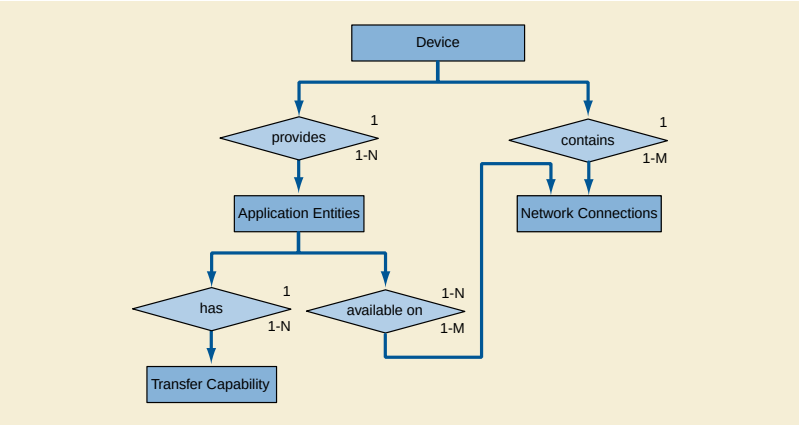

Figure H.1-1. Application Configuration Data Model

In addition there are a number of other objects used in the LDAP schema (see Section H.1.2 and Figure H.1-2) :

DICOM Configuration Root –The root of DICOM Configuration Hierarchy

DICOM Devices Root –The root of the DICOM Devices Hierarchy

DICOM Unique AE-Title Registry Root –The root of the Unique DICOM AE-Title Registry

DICOM Unique AE Title –A unique AE Title within the AE Title Registry

LDAP permits extensions to schema to support local needs (i.e., an object may implement a single structural and multiple auxiliary LDAP classes). DICOM does not mandate client support for such extensions. Servers may support such extensions for local purposes. DICOM Clients may accept or ignore extensions and shall not consider their presence an error.

H.1.1.1 Device

The "device" is set of components organized to perform a task rather than a specific physical instance. For simple devices there may be one physical device corresponding to the Data Model device. But for complex equipment there may be many physical parts to one "device".

The "device" is the collection of physical entities that supports a collection of Application Entities. It is uniquely associated with these entities and vice versa. It is also uniquely associated with the network connections and vice versa. In a simple workstation with one CPU, power connection, and network connection the "device" is the workstation.

An example of a complex device is a server built from a network of multiple computers that have multiple network connections and independent power connections. This would be one device with one application entity and multiple network connections. Servers like this are designed so that individual component computers can be replaced without disturbing operations. The Application Configuration Data Model does not describe any of this internal structure. It describes the network connections and the network visible Application Entities. These complex devices are usually designed for very high availability, but in the unusual event of a system shutdown the "device" corresponds to all the parts that get shut down.

Table H.1-2. Attributes of Device Object

Information Field	Multiplicity	Description
Device Name	1	A unique name (within the scope of the LDAP database) for this device. It is restricted to legal LDAP names, and not constrained by DICOM AE Title limitations.
Description	0..1	Unconstrained text description of the device.
Manufacturer	0..1	Should be the same as the value of Manufacturer (0008,0070) in SOP instances created by this device.
Manufacturer Model Name	0..1	Should be the same as the value of Manufacturer Model Name (0008,1090) in SOP instances created by this device.
Software Version	0..N	Should be the same as the values of Software Versions (0018,1020) in SOP instances created by this device.
Station Name	0..1	Should be the same as the value of Station Name (0008,1010) in SOP instances created by this device.
Device Serial Number	0..1	Should be the same as the value of Device Serial Number (0018,1000) in SOP instances created by this device.
Primary Device Type	0..N	Represents the kind of device and is most applicable for acquisition modalities. Types should be selected from the list of code values (0008,0100) for CID 30 “DICOM Devices” when applicable.
Institution Name	0..N	Should be the same as the value of Institution Name (0008,0080) in SOP Instances created by this device.
Institution Address	0..N	Should be the same as the value of Institution Address (0008,0081) attribute in SOP Instances created by this device.
Institutional Department Name	0..N	Should be the same as the value of Institutional Department Name (0008,1040) in SOP Instances created by this device.

Information Field	Multiplicity	Description
Issuer of Patient ID	0..1	Default value for the Issuer of Patient ID (0010,0021) for SOP Instances created by this device. May be overridden by the values received in a worklist or other source.
Related Device Reference	0..N	The DNs of related device descriptions outside the DICOM Configuration hierarchy. Can be used to link the DICOM Device object to additional LDAP objects instantiated from other schema and used for separate administrative purposes.
Authorized Node Certificate Reference	0..N	The DNs for the certificates of nodes that are authorized to connect to this device. The DNs need not be within the DICOM configuration hierarchy.
This Node Certificate Reference	0..N	The DNs of the public certificate(s) for this node. The DNs need not be within the DICOM configuration hierarchy.
Vendor Device Data	0..N	Device specific vendor configuration information
Installed	1	Boolean to indicate whether this device is presently installed on the network. (This is useful for pre-configuration, mobile vans, and similar situations.)

The "Authorized Node Certificate Reference" is intended to allow the LDAP server to provide the list of certificates for nodes that are authorized to communicate with this device. These should be the public certificates only. This list need not be complete. Other network peers may be authorized by other mechanisms.

The "This Node Certificate Reference" is intended to allow the LDAP server to provide the certificate(s) for this node. These may also be handled independently of LDAP.

Note

A device may have multiple Primary Device Type entries. It may be a multifunctional device, e.g., combined PET and CT. It may be a cascaded device, e.g., image capture and ultrasound.

Table H.1-3. Child Objects of Device Object

Information Field	Multiplicity	Description
Network Application Entity	1..N	The application entities available on this device (see Section H.1.1.2)
Network Connection	1..N	The network connections for this device (see Section H.1.1.3)

H.1.1.2 Network Application Entity

A Network AE is an application entity that provides services on a network. A Network AE will have the same functional capability regardless of the particular network connection used. If there are functional differences based on selected network connection, then these are separate Network AEs. If there are functional differences based on other internal structures, then these are separate Network AEs.

Table H.1-4. Attributes of Network AE Object

Information Field	Multiplicity	Description
AE Title	1	Unique AE title for this Network AE
Description	0..1	Unconstrained text description of the application entity.
Vendor Data	0..N	AE specific vendor configuration information
Application Cluster	0..N	Locally defined names for a subset of related applications. E.g. "neuroradiology".
Preferred Called AE Title	0..N	AE Title(s) that are preferred for initiating associations.
Preferred Calling AE Title	0..N	AE Title(s) that are preferred for accepting associations.

Information Field	Multiplicity	Description
Association Acceptor	1	A Boolean value. True if the Network AE can accept associations, false otherwise.
Association Initiator	1	A Boolean value. True if the Network AE can accept associations, false otherwise.
Network Connection Reference	1..N	The DNs of the Network Connection objects for this AE
Supported Character Set	0..N	The Character Set(s) supported by the Network AE for data sets it receives. The value shall be selected from the Defined Terms for Specific Character Set (0008,0005) in PS3.3. If no values are present, this implies that the Network AE supports only the default character repertoire(ISO IR 6).
Installed	0..1	A Boolean value. True if the AE is installed on network. If not present, information about the installed status of the AE is inherited from the device

The "Application Cluster" concept provides the mechanism to define local clusters of systems. The use cases for Configuration Management require a "domain" capability for DICOM applications that would be independent of the network topology and administrative domains that are used by DNS and other TCP level protocols. The Application Cluster is multi-valued to permit multiple clustering concepts for different purposes. It is expected to be used as part of a query to limit the scope of the query.

The "Preferred Called AE Title" concept is intended to allow a site administrator to define a limited default set of AEs that are preferred for use as communication partners when initiating associations. This capability is particularly useful for large centrally administered sites to simplify the configuration possibilities and restrict the number of configured AEs for specific workflow scenarios. For example, the set of AEs might contain the AE Titles of assigned Printer, Archive, RIS and QA Workstations so that the client device could adapt its configuration preferences accordingly. The "Preferred Called AE Title" concept does not prohibit association initiation to unlisted AEs. Associations to unlisted AEs can be initiated if necessary.

The "Preferred Calling AE Title" concept is intended to allow a site administrator to define a default set of AEs that are preferred when accepting assocations. The "Preferred Calling AE Title" concept does not prohibit accepting associations from unlisted AEs.

The "Network Connection Reference" is a link to a separate Network Connection object. The referenced Network Connection object is a sibling the AE object (i.e., both are children of the same Device object).

Table H.1-5. Child Objects of Network AE Object

Information Field	Multiplicity	Description
Transfer Capability	1..N	The Transfer Capabilities for this Network AE. See Section H.1.4

H.1.1.3 Network Connection

The "network connection" describes one TCP port on one network device. This can be used for a TCP connection over which a DICOM association can be negotiated with one or more Network AEs. It specifies the hostname and TCP port number. A network connection may support multiple Network AEs. The Network AE selection takes place during association negotiation based on the called and calling AE-titles.

Table H.1-6. Attributes of Network Connection Object

Information Field	Multiplicity	Description
Common Name	0..1	An arbitrary name for the Network Connections object. Can be a meaningful name or any unique sequence of characters. Can be used as the RDN. Note The "cn" attribute type is a basic LDAP defined type and is a synonym for Common Name.

Information Field	Multiplicity	Description
Hostname	1	This is the DNS name for this particular connection. This is used to obtain the current IP address for connections. Hostname must be sufficiently qualified to be unambiguous for any client DNS user.
Port	0..1	The TCP port that the AE is listening on. (This may be missing for a network connection that only initiates associations.)
TLS CipherSuite	0..N	The TLS CipherSuites that are supported on this particular connection. TLS CipherSuites shall be described using an RFC-2246 string representation (e.g., "TLS_RSA_WITH_RC4_128_SHA")
Installed	0..1	A Boolean value. True if the Network Connection is installed on the network. If not present, information about the installed status of the Network Connection is inherited from the device.

Inclusion of a TLS CipherSuite in a Network Connection capable of accepting associations implies that the TLS protocol must be used to successfully establish an association on the Network Connection.

A single Network AE may be available on multiple network connections. This is often done at servers for availability or performance reasons. For example, at a hospital where each floor is networked to a single hub per floor, the major servers may have direct connections to each of the hubs. This provides better performance and reliability. If the server does not change behavior based on the particular physical network connection, then it can be described as having Network AEs that are available on all of these multiple network connections. A Network AE may also be visible on multiple TCP ports on the same network hardware port, with each TCP port represented as a separate network connection. This would allow, e.g., a TLS-secured DICOM port and a classical un-secured DICOM port to be supported by the same AE.

H.1.1.4 Transfer Capabilities

Each Network AE object has one or more Transfer Capabilities. Each transfer capability specifies the SOP class that the Network AE can support, the mode that it can utilize (SCP or SCU), and the Transfer Syntax(es) that it can utilize. A Network AE that supports the same SOP class in both SCP and SCU modes will have two Transfer Capabilities objects for that SOP class.

Table H.1-7. Attributes of Transfer Capability Object

Information Field	Multiplicity	Description
Common Name	0..1	An arbitrary name for the Transfer Capability object. Can be a meaningful name or any unqiue sequence of characters. Can be used as the RDN.
SOP Class	1	SOP Class UID
Role	1	Either "SCU" or "SCP"
Transfer Syntax	1..N	The transfer syntax(es) that may be requested as an SCU or that are offered as an SCP.

H.1.1.5 DICOM Configuration Root

This structural object class represents the root of the DICOM Configuration Hierarchy. Only a single object of this type should exist within an organizational domain. Clients can search for an object of this class to locate the root of the DICOM Configuration Hierarchy.

Table H.1-8. Attributes of the DICOM Configuration Root Object

Information Field	Multiplicity	Description
Common Name	1	The Name for the Configuration Root. Should be used as the RDN. The name shall be "DICOM Configuration".
Description	0..1	Unconstrained text description.

Table H.1-9. Child Objects of DICOM Configuration Root Object

Information Field	Multiplicity	Description
Devices Root	1	The root of the DICOM Devices Hierarchy
Unique AE Titles Registry Root	1	The root of the Unique AE Titles Registry

H.1.1.6 Devices Root

This structural object class represents the root of the DICOM Devices Hierarchy. Only a single object of this type should exist as a child of DICOM Configuration Root. Clients can search for an object of this class to locate the root of the DICOM Devices Hierarchy.

Table H.1-10. Attributes of the Devices Root Object

Information Field	Multiplicity	Description
Common Name	1	The Name for the Devices Root. Should be used as the RDN. The name shall be "Devices".
Description	0..1	Unconstrained text description.

Table H.1-11. Child Objects of Devices Root Object

Information Field	Multiplicity	Description
Device	0..N	The individual devices installed within this organizational domain.

H.1.1.7 Unique AE Titles Registry Root

This structural object class represents the root of the Unique AE-Titles Registry Hierarchy. Only a single object of this type should exist as a child of the DICOM Configuration Root. Clients can search for an object of this class to locate the root of the Unique AE Titles Registry.

Table H.1-12. Attributes of the Unique AE Titles Registry Root Object

Information Field	Multiplicity	Description
Common Name	1	The Name for the Unique AE Titles Registry Root. Should be used as the RDN. The name shall be "Unique AE Titles Registry".
Description	0..1	Unconstrained text description.

Table H.1-13. Child Objects of Unique AE Titles Registry Root Object

Information Field	Multiplicity	Description
Unique AE Title	0..N	The unique AE Titles installed within this organizational domain (see Section H.1.1.8)

H.1.1.8 Unique AE Title

This structural object class represents a Unique Application Entity Title. Objects of this type should only exist as children of the Unique AE-Titles Registry Root. The sole purpose of this object class is to enable allocation of unique AE Titles. All operational information associated with an AE Title is maintained within a separate Network AE object.

Table H.1-14. Attributes of the Unique AE Title Object

Information Field	Multiplicity	Description
AE Title	1	The Unique AE Titles.

H.1.2 Application Configuration Data Model Hierarchy

The LDAP structure is built upon a hierarchy of named objects. This hierarchy can vary from site to site. The DICOM configuration management function needs to find its objects within this hierarchy in a predictable manner. For this reason, three specific object classes are defined for the three objects at the top of the DICOM hierarchy. These three object classes must not be used in this tree relationship anywhere else in the LDAP hierarchy.

The DICOM portion of the hierarchy shall begin at a root object of class dicomConfigurationRoot with a Common Name of "DICOM Configuration". Below this object shall be two other objects:

a. An object of class dicomDevicesRoot with a Common Name of "Devices". This is the root of the tree of objects that correspond to the Application Configuration Data Model structure of Section H.1.1.

b. An object of class dicomUniqueAETitlesRegistryRoot with a common name of "Unique AE Titles Registry". This is the root of a flat tree of objects. Each of these objects is named with one of the AE titles that are presently assigned. This is the mechanism for finding available AE titles.

The three object classes dicomConfigurationRoot, dicomDevicesRoot, and dicomUniqueAETitleRegistryRoot are used by LDAP clients to establish the local root of the DICOM configuration information within an LDAP hierarchy that may be used for many other purposes.

Note

During system startup it is likely that the DICOM configuration application will do an LDAP search for an entry of object class dicomConfigurationRoot and then confirm that it has the dicomDevicesRoot and dicomUniqueAETitlesRegistryRoot entries directly below it. When it finds this configuration, it can then save the full location within the local LDAP tree and use that as the root of the DICOM tree.

The objects underneath the dicomUniqueAETitlesRegistryRoot are used to provide the uniqueness required for DICOM AE-titles. The dicomUniqueAETitle objects have a single attribute representing a unique AE Title. When a new AE-Title is required, a tentative new name is selected. The new name is reserved by using the LDAP create facility to create an object of class dicomUniqueAETitle with the new name under the AE-Title object. If this name is already in use, the create will fail. Otherwise, this reserves the name. LDAP queries can be used to obtain the list of presently assigned AE-titles by obtaining the list of all names under the dicomUniqueAE-TitlesRegistryRoot object.

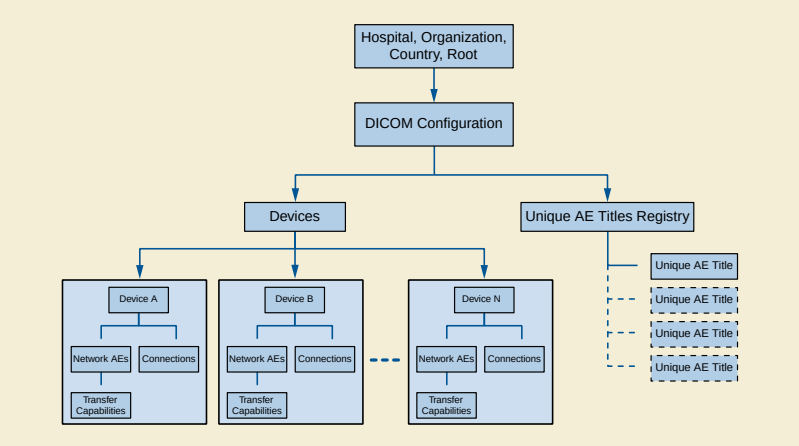

Figure H.1-2. DICOM Configuration Hierarchy

Note

1. LDAP uses a root and relative hierarchical naming system for objects. Every object name is fully unique within the full hierarchy. This means that the names of the objects beneath "Unique AE Titles Registry" will be unique. It also means that the full names of Network AEs and Connections will be within their hierarchy context. E.g., the DN for one of the Network AEs in Figure H.1-2 would be:

dicomAETitle=CT_01, dicomDeviceName=Special Research CT, cn=Devices, cn=DICOM Configuration, o=Sometown Hospital

2. In theory, multiple independent DICOM configuration hierarchies could exist within one organization. The LDAP servers in such a network should constrain local device accesses so that DICOM configuration clients have only one DICOM Configuration Hierarchy visible to each client.

3. The merger of two organizations will require manual configuration management to merge DICOM Configuration hierarchies. There are likely to be conflicts in AE-titles, roles, and other conflicts.

H.1.3 LDAP Schema For Objects and Attributes

The individual LDAP attribute information is summarized in the comments at the beginning of the schema below. The formal definition of the objects and the attributes is in the schema below. This schema may be extended by defining an additional schema that defines auxiliary classes, sub-classes derived from this schema, or both.

The formal LDAP schema for the Application Configuration Data Model and the DICOM Configuration Hierarchy is:

```
# 3 Attribute Type Definitions
#
#    The following attribute types are defined in this document:
#
# Name                                Syntax    Multiplicity
# ---------------------------------       ------    ------------
# dicomDeviceName                         string    Single
# dicomDescription                        string    Single
# dicomManufacturer                       string    Single
# dicomManufacturerModelName              string    Single
# dicomSoftwareVersion                    string    Multiple
# dicomVendorData                         binary    Multiple
# dicomAETitle                            string    Single
# dicomNetworkConnectionReference         DN        Multiple
# dicomApplicationCluster                 string    Multiple
# dicomAssociationInitiator               bool      Single
# dicomAssociationAcceptor                bool      Single
# dicomHostname                           string    Single
# dicomPort                               integer   Single
# dicomSOPClass                           OID       Single
# dicomTransferRole                       string    Single
# dicomTransferSyntax                     OID       Multiple
# dicomPrimaryDeviceType                  string    Multiple
# dicomRelatedDeviceReference             DN        Multiple
# dicomPreferredCalledAETitle             string    Multiple
# dicomTLSCipherSuite                     string    Multiple
# dicomAuthorizedNodeCertificateReference DN        Multiple
# dicomThisNodeCertificateReference       DN        Multiple
# dicomInstalled                          bool      Single
# dicomStationName                        string    Single
# dicomDeviceSerialNumber                 string    Single
# dicomInstitutionName                    string    Multiple
# dicomInstitutionAddress                 string    Multiple
# dicomInstitutionDepartmentName          string    Multiple
# dicomIssuerOfPatientID                  string    Single
# dicomPreferredCallingAETitle            string    Multiple
# dicomSupportedCharacterSet              string    Multiple
#


# 3.1 dicomDeviceName                     string    Single
#
```

```
#   This attribute stores the unique name (within the scope of the LDAP database)
#   for a DICOM Device.
#
#   It is a single-valued attribute.
#   This attribute's syntax is 'Directory String'.
#   Its case is not significant for equality and substring matches.
#
attributetype ( 1.2.840.10008.15.0.3.1
 NAME 'dicomDeviceName'
 DESC 'The unique name for the device'
 EQUALITY caseIgnoreMatch
 SUBSTR caseIgnoreSubstringsMatch
 SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
 SINGLE-VALUE )

# 3.2 dicomDescription                  string    Single
#
#   This attribute stores the (unconstrained) textual description for a DICOM entity.
#
#   It is a single-valued attribute.
#   This attribute's syntax is 'Directory String'.
#   Its case is not significant for equality and substring matches.
#
attributetype ( 1.2.840.10008.15.0.3.2
 NAME 'dicomDescription'
 DESC 'Textual description of the DICOM entity'
 EQUALITY caseIgnoreMatch
 SUBSTR caseIgnoreSubstringsMatch
 SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
 SINGLE-VALUE )

# 3.3 dicomManufacturer                 string    Single
#
#   This attribute stores the Manufacturer name for a DICOM Device.
#   Should be identical to the value of the DICOM attribute Manufacturer (0008,0070) [VR=LO]
#   contained in SOP Instances created by this device.
#
#   It is a single-valued attribute.
#   This attribute's syntax is 'Directory String'.
#   Its case is not significant for equality and substring matches.
#
attributetype ( 1.2.840.10008.15.0.3.3
 NAME 'dicomManufacturer'
 DESC 'The device Manufacturer name'
 EQUALITY caseIgnoreMatch
 SUBSTR caseIgnoreSubstringsMatch
 SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
 SINGLE-VALUE )

# 3.4 dicomManufacturerModelName        string    Single
#
#   This attribute stores the Manufacturer Model Name for a DICOM Device.
#   Should be identical to the value of the DICOM attribute Manufacturer
#   Model Name (0008,1090) [VR=LO]
#   contained in SOP Instances created by this device.
#
#   It is a single-valued attribute.
#   This attribute's syntax is 'Directory String'.
#   Its case is not significant for equality and substring matches.
#
```

```
attributetype ( 1.2.840.10008.15.0.3.4
 NAME 'dicomManufacturerModelName'
 DESC 'The device Manufacturer Model Name'
 EQUALITY caseIgnoreMatch
 SUBSTR caseIgnoreSubstringsMatch
 SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
 SINGLE-VALUE )

# 3.5 dicomSoftwareVersion              string    Multiple
#
#    This attribute stores the software version of the device and/or its subcomponents.
#    Should be the same as the values of Software Versions (0018,1020) in
#    SOP instances created by this device.
#
#    It is a multi-valued attribute.
#    This attribute's syntax is 'Directory String'.
#    Its case is not significant for equality and substring matches.
#
attributetype ( 1.2.840.10008.15.0.3.5
 NAME 'dicomSoftwareVersion'
 DESC 'The device software version. Should be the same as the values of Software
      Versions (0018,1020) in SOP instances created by this device.'
 EQUALITY caseIgnoreMatch
 SUBSTR caseIgnoreSubstringsMatch
 SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 )

# 3.6 dicomVendorData                   binary    Multiple
#
#    This attribute stores vendor specific configuration information.
#
#    It is a multi-valued attribute.
#    This attribute's syntax is 'Binary'.
#    Neither equality nor substring matches are applicable to binary data.
#
attributetype ( 1.2.840.10008.15.0.3.6
 NAME 'dicomVendorData'
 DESC 'Arbitrary vendor-specific configuration information (binary data)'
 SYNTAX 1.3.6.1.4.1.1466.115.121.1.5 )

# 3.7 dicomAETitle                      name      Single
#
#    This attribute stores an Application Entity (AE) title.
#
#    It is a single-valued attribute.
#    This attribute's syntax is 'IA5 String'.
#    Its case is significant.
#
attributetype ( 1.2.840.10008.15.0.3.7
 NAME 'dicomAETitle'
 DESC 'Application Entity (AE) title'
 EQUALITY caseExactIA5Match
 SYNTAX 1.3.6.1.4.1.1466.115.121.1.26
 SINGLE-VALUE )

# 3.8 dicomNetworkConnectionReference     DN        Multiple
#
#    This attribute stores the DN of a dicomNetworkConnection object
#    used by an Application Entity.
#
#    It is a multi-valued attribute.
```

```
#   This attribute's syntax is 'Distinguished Name'.
#
attributetype ( 1.2.840.10008.15.0.3.8
 NAME 'dicomNetworkConnectionReference'
 DESC 'The DN of a dicomNetworkConnection object used by an Application Entity'
 EQUALITY distinguishedNameMatch
 SYNTAX 1.3.6.1.4.1.1466.115.121.1.12 )

# 3.9 dicomApplicationCluster            string    Multiple
#
#   This attribute stores an application cluster name for an Application
#   Entity (e.g., "Neuroradiology Research")
#
#   It is a multi-valued attribute.
#   This attribute's syntax is 'Directory String'.
#   Its case is not significant for equality and substring matches.
#
attributetype ( 1.2.840.10008.15.0.3.9
 NAME 'dicomApplicationCluster'
 DESC 'Application cluster name for an Application Entity (e.g., "Neuroradiology Research")'
 EQUALITY caseIgnoreMatch
 SUBSTR caseIgnoreSubstringsMatch
 SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 )

# 3.10 dicomAssociationInitiator         bool      Single
#
#   This attribute indicates if an Application Entity is capable of initiating
#   network associations.
#
#   It is a single-valued attribute.
#   This attribute's syntax is 'Boolean'.
#
attributetype ( 1.2.840.10008.15.0.3.10
 NAME 'dicomAssociationInitiator'
 DESC 'Indicates if an Application Entity is capable of initiating network associations'
 EQUALITY booleanMatch
 SYNTAX 1.3.6.1.4.1.1466.115.121.1.7
 SINGLE-VALUE )

# 3.11 dicomAssociationAcceptor          bool      Single
#
#   This attribute indicates if an Application Entity is capable of accepting
#   network associations.
#
#   It is a single-valued attribute.
#   This attribute's syntax is 'Boolean'.
#
attributetype ( 1.2.840.10008.15.0.3.11
 NAME 'dicomAssociationAcceptor'
 DESC 'Indicates if an Application Entity is capable of accepting network associations'
 EQUALITY booleanMatch
 SYNTAX 1.3.6.1.4.1.1466.115.121.1.7
 SINGLE-VALUE )

# 3.12 dicomHostname                     string    Single
#
#   This attribute stores a DNS hostname for a connection.
#
#   It is a single-valued attribute.
#   This attribute's syntax is 'Directory String'.
```

```
#    Its case is not significant for equality and substring matches.
#
attributetype ( 1.2.840.10008.15.0.3.12
 NAME 'dicomHostname'
 DESC 'DNS hostname'
 EQUALITY caseIgnoreMatch
 SUBSTR caseIgnoreSubstringsMatch
 SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
 SINGLE-VALUE )

# 3.13 dicomPort                    integer   Single
#
#    This attribute stores a TCP port number for a connection.
#
#    It is a single-valued attribute.
#    This attribute's syntax is 'Integer'.
#
attributetype ( 1.2.840.10008.15.0.3.13
 NAME 'dicomPort'
 DESC 'TCP Port number'
 EQUALITY  integerMatch
 SYNTAX 1.3.6.1.4.1.1466.115.121.1.27
 SINGLE-VALUE )

# 3.14 dicomSOPClass                OID       Single
#
#    This attribute stores a SOP Class UID
#
#    It is a single-valued attribute.
#    This attribute's syntax is 'OID'.
#
attributetype ( 1.2.840.10008.15.0.3.14
 NAME 'dicomSOPClass'
 DESC 'A SOP Class UID'
 EQUALITY  objectIdentifierMatch
 SYNTAX 1.3.6.1.4.1.1466.115.121.1.38
 SINGLE-VALUE )

# 3.15 dicomTransferRole            String    Single
#
#    This attribute stores a transfer role (either "SCU" or "SCP").
#
#    It is a single-valued attribute.
#    This attribute's syntax is 'Directory String'.
#    Its case is not significant for equality and substring matches.
#
attributetype ( 1.2.840.10008.15.0.3.15
 NAME 'dicomTransferRole'
 DESC 'Transfer role (either "SCU" or "SCP")'
 EQUALITY caseIgnoreMatch
 SUBSTR caseIgnoreSubstringsMatch
 SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
 SINGLE-VALUE )

# 3.16 dicomTransferSyntax          OID       Multiple
#
#    This attribute stores a Transfer Syntax UID
#
#    It is a multi-valued attribute.
#    This attribute's syntax is 'OID'.
```

```
#
attributetype ( 1.2.840.10008.15.0.3.16
 NAME 'dicomTransferSyntax'
 DESC 'A Transfer Syntax UID'
 EQUALITY  objectIdentifierMatch
 SYNTAX 1.3.6.1.4.1.1466.115.121.1.38 )

# 3.17 dicomPrimaryDeviceType            string    Multiple
#
#    This attribute stores the primary type for a DICOM Device.
#    Types should be selected from the list of code values (0008,0100)
#    for Context ID 30 in DICOM Part 16 when applicable.
#
#    It is a multiple-valued attribute.
#    This attribute's syntax is 'IA5 String'.
#    Its case is significant.
#
attributetype ( 1.2.840.10008.15.0.3.17
 NAME 'dicomPrimaryDeviceType'
 DESC 'The device Primary Device type'
 EQUALITY caseExactIA5Match
 SYNTAX 1.3.6.1.4.1.1466.115.121.1.26 )

# 3.18 dicomRelatedDeviceReference       DN        Multiple
#
#    This attribute stores a reference to a related device description outside
#    the DICOM Configuration Hierachy.  Can be used to link the DICOM Device object to
#    additional LDAP objects instantiated from other schema and used for
#    separate administrative purposes.
#
#    This attribute's syntax is 'Distinguished Name'.
#    It is a multiple-valued attribute.
#
attributetype ( 1.2.840.10008.15.0.3.18
 NAME 'dicomRelatedDeviceReference'
 DESC 'The DN of a related device description outside the DICOM Configuration Hierachy'
 EQUALITY distinguishedNameMatch
 SYNTAX 1.3.6.1.4.1.1466.115.121.1.12 )

# 3.19 dicomPreferredCalledAETitle       string    Multiple
#
#    AE Title(s) to which associations may be preferably initiated.
#
#    It is a multiple-valued attribute.
#    This attribute's syntax is 'IA5 String'.
#    Its case is significant.
#
attributetype ( 1.2.840.10008.15.0.3.19
 NAME 'dicomPreferredCalledAETitle'
 DESC 'AE Title(s) to which associations may be preferably initiated.'
 EQUALITY caseExactIA5Match
 SYNTAX 1.3.6.1.4.1.1466.115.121.1.26 )

# 3.20 dicomTLSCipherSuite               string    Multiple
#
#    The attribute stores the supported TLS CipherSuites.
#    TLS CipherSuites shall be described using a RFC-2246 string representation
#    (e.g., "TLS_RSA_WITH_RC4_128_SHA").
#
#    It is a multiple-valued attribute.
```

```
#   This attribute's syntax is 'IA5 String'.
#   Its case is significant.
#
attributetype ( 1.2.840.10008.15.0.3.20
 NAME 'dicomTLSCipherSuite'
 DESC 'The supported TLS CipherSuites'
 EQUALITY caseExactIA5Match
 SYNTAX 1.3.6.1.4.1.1466.115.121.1.26 )

# 3.21  dicomAuthorizedNodeCertificateReference DN Multiple
#
#   This attribute stores a reference to a TLS public certificate for a DICOM
#   node that is authorized to connect to this node.  The certificate
#   is not necessarily stored within the DICOM Hierarchy
#
#   This attribute's syntax is 'Distinguished Name'.
#   It is a multiple-valued attribute.
#
attributetype ( 1.2.840.10008.15.0.3.21
 NAME 'dicomAuthorizedNodeCertificateReference'
 DESC 'The DN of a Certificate for a DICOM node that is authorized to connect to this node'
 EQUALITY distinguishedNameMatch
 SYNTAX 1.3.6.1.4.1.1466.115.121.1.12 )

# 3.22 dicomThisNodeCertificateReference DN Multiple
#
#   This attribute stores a reference to a TLS public certificate for
#   this node.  It is not necessarily stored as part of
#   the DICOM Configuration Hierachy.
#
#   This attribute's syntax is 'Distinguished Name'.
#   It is a multiple-valued attribute.
#
attributetype ( 1.2.840.10008.15.0.3.22
 NAME 'dicomThisNodeCertificateReference'
 DESC 'The DN of a related device description outside the DICOM Configuration Hierachy'
 EQUALITY distinguishedNameMatch
 SYNTAX 1.3.6.1.4.1.1466.115.121.1.12 )

# 3.23 dicomInstalled                bool      Single
#
#   This attribute indicates whether the object is presently installed.
#
#   It is a single-valued attribute.
#   This attribute's syntax is 'Boolean'.
#
attributetype ( 1.2.840.10008.15.0.3.23
 NAME 'dicomInstalled'
 DESC 'Indicates if the DICOM object (device, Network AE, or Port) is presently installed'
 EQUALITY booleanMatch
 SYNTAX 1.3.6.1.4.1.1466.115.121.1.7
 SINGLE-VALUE )

# 3.24 dicomStationName              string    Single
#
#   This attribute stores the station name of the device.
#   Should be the same as the value of Station Name (0008,1010) in
#   SOP instances created by this device.
#
#   It is a single-valued attribute.
```

```
#    This attribute's syntax is 'Directory String'.
#
attributetype ( 1.2.840.10008.15.0.3.24
 NAME 'dicomStationName'
 DESC 'Station Name of the device.  Should be the same as the value of Station
      Name (0008,1010) in SOP instances created by this device.'
 EQUALITY caseIgnoreMatch
 SUBSTR caseIgnoreSubstringsMatch
 SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
 SINGLE-VALUE)

# 3.25 dicomDeviceSerialNumber          string    Single
#
#    This attribute stores the serial number of the device.
#    Should be the same as the value of Device Serial Number (0018,1000)
#    in SOP instances created by this device.
#
#    It is a single-valued attribute.
#    This attribute's syntax is 'Directory String'.
#
attributetype ( 1.2.840.10008.15.0.3.25
 NAME 'dicomDeviceSerialNumber'
 DESC 'Serial number of the device. Should be the same as the value of Device Serial
      Number (0018,1000) in SOP instances created by this device.'
 EQUALITY caseIgnoreMatch
 SUBSTR caseIgnoreSubstringsMatch
 SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
 SINGLE-VALUE)

# 3.26 dicomInstitutionName             string    Multiple
#
#    This attribute stores the institution name of the device.
#    Should be the same as the value of Institution Name (0008,0080)
#    in SOP Instances created by this device.
#
#    It is a multi-valued attribute.
#    This attribute's syntax is 'Directory String'.
#
attributetype ( 1.2.840.10008.15.0.3.26
 NAME 'dicomInstitutionName'
 DESC 'Institution name of the device. Should be the same as the value of Institution
      Name (0008,0080) in SOP Instances created by this device.'
 EQUALITY caseIgnoreMatch
 SUBSTR caseIgnoreSubstringsMatch
 SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 )

# 3.27 dicomInstitutionAddress          string    Multiple
#
#    This attribute stores the institution address of the device.
#    Should be the same as the value of Institution Address (0008,0081)
#    attribute in SOP Instances created by this device.
#
#    It is a multi-valued attribute.
#    This attribute's syntax is 'Directory String'.
#
attributetype ( 1.2.840.10008.15.0.3.27
 NAME 'dicomInstitutionAddress'
 DESC 'Institution address of the device.  Should be the same as the value of Institution
      Address (0008,0081) attribute in SOP Instances created by this device.'
 EQUALITY caseIgnoreMatch
```

```
 SUBSTR caseIgnoreSubstringsMatch
 SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 )

# 3.28 dicomInstitutionDepartmentName    string   Multiple
#
#    This attribute stores the institution department name of the device.
#    Should be the same as the value of Institutional Department Name (0008,1040)
#    in SOP Instances created by this device.
#
#    It is a multi-valued attribute.
#    This attribute's syntax is 'Directory String'.
#
attributetype ( 1.2.840.10008.15.0.3.28
 NAME 'dicomInstitutionDepartmentName'
 DESC 'Institution department name of the device.  Should be the same as the value of Institutional
      Department Name (0008,1040) in SOP Instances created by this device.'
 EQUALITY caseIgnoreMatch
 SUBSTR caseIgnoreSubstringsMatch
 SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 )

# 3.29 dicomIssuerOfPatientID            string    Single
#
#    This attribute stores the Default value for the Issuer of Patient ID (0010,0021)
#    for SOP Instances created by this device.  May be overridden by the values
#    received in a worklist or other source.
#
#    It is a multi-valued attribute.
#    This attribute's syntax is 'Directory String'.
#
attributetype ( 1.2.840.10008.15.0.3.29
 NAME 'dicomIssuerOfPatientID'
 DESC 'Default value for the Issuer of Patient ID (0010,0021) for SOP Instances created by this device.
      May be overridden by the values received in a worklist or other source.'
 EQUALITY caseIgnoreMatch
 SUBSTR caseIgnoreSubstringsMatch
 SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 )

# 3.30 dicomPreferredCallingAETitle      string    Multiple
#
#    AE Title(s) to which associations may be preferably accepted.
#
#    It is a multiple-valued attribute.
#    This attribute's syntax is 'IA5 String'.
#    Its case is significant.
#
attributetype ( 1.2.840.10008.15.0.3.30
 NAME 'dicomPreferredCallingAETitle'
 DESC 'AE Title(s) to which associations may be preferably accepted.'
 EQUALITY caseExactIA5Match
 SYNTAX 1.3.6.1.4.1.1466.115.121.1.26 )

# 3.31 dicomSupportedCharacterSet        string    Multiple
#
#    The Character Set(s) supported by the Network AE for data sets it receives.
#    Contains one of the Defined Terms for Specific Character Set (0008,0005).
#    If not present, this implies that the Network AE supports only the default
#    character repertoire (ISO IR 6).
#
#    It is a multiple-valued attribute.
#    This attribute's syntax is 'IA5 String'.
```

```
#    Its case is significant.
#
attributetype ( 1.2.840.10008.15.0.3.31
 NAME 'dicomSupportedCharacterSet'
 DESC 'The Character Set(s) supported by the Network AE for data sets it receives.'
 EQUALITY caseExactIA5Match
 SYNTAX 1.3.6.1.4.1.1466.115.121.1.26 )


# 4 Object Class Definitions
#
#    The following object classes are defined in this document.  All are
#    structural classes.
#
# Name                        Description
# --------------------------    -------------------------
# dicomConfigurationRoot         root of the DICOM Configuration Hierarchy
# dicomDevicesRoot               root of the DICOM Devices Hierarchy
# dicomUniqueAETitlesRegistryRoot root of the Unique DICOM AE-Titles Registry Hierarchy
# dicomDevice                   Devices
# dicomNetworkAE                Network AE
# dicomNetworkConnection         Network Connections
# dicomUniqueAETitle             Unique AE Title
# dicomTransferCapability        Transfer Capability

#
# 4.1 dicomConfigurationRoot
#
#    This structural object class represents the root of the DICOM Configuration Hierarchy.
#    Only a single object of this type should exist within an organizational domain.
#    Clients can search for an object of this class to locate the root of the
#    DICOM Configuration Hierarchy.
#
objectclass ( 1.2.840.10008.15.0.4.1
 NAME 'dicomConfigurationRoot'
 DESC 'Root of the DICOM Configuration Hierarchy'
 SUP top
 STRUCTURAL
 MUST ( cn )
 MAY ( description ) )

#
# 4.2 dicomDevicesRoot
#
#    This structural object class represents the root of the DICOM Devices Hierarchy.
#    Only a single object of this type should exist as a child of dicomConfigurationRoot.
#
objectclass ( 1.2.840.10008.15.0.4.2
 NAME 'dicomDevicesRoot'
 DESC 'Root of the DICOM Devices Hierarchy'
 SUP top
 STRUCTURAL
 MUST ( cn )
 MAY ( description ) )

#
# 4.3 dicomUniqueAETitlesRegistryRoot
#
#    This structural object class represents the root of the Unique DICOM AE-Titles
#    Registry Hierarchy.
```

```
#    Only a single object of this type should exist as a child of dicomConfigurationRoot.
#
objectclass ( 1.2.840.10008.15.0.4.3
 NAME 'dicomUniqueAETitlesRegistryRoot'
 DESC 'Root of the Unique DICOM AE-Title Registry Hierarchy'
 SUP top
 STRUCTURAL
 MUST ( cn )
 MAY ( description ) )

#
# 4.4 dicomDevice
#
#    This structural object class represents a DICOM Device.
#
objectclass ( 1.2.840.10008.15.0.4.4
 NAME 'dicomDevice'
 DESC 'DICOM Device related information'
 SUP top
 STRUCTURAL
 MUST (
  dicomDeviceName $
  dicomInstalled )
 MAY  (
  dicomDescription $
  dicomManufacturer $
  dicomManufacturerModelName $
  dicomSoftwareVersion $
  dicomStationName $
  dicomDeviceSerialNumber $
  dicomInstitutionName $
  dicomInstitutionAddress $
  dicomInstitutionDepartmentName $
  dicomIssuerOfPatientID $
  dicomVendorData $
  dicomPrimaryDeviceType $
  dicomRelatedDeviceReference $
  dicomAuthorizedNodeCertificateReference $
  dicomThisNodeCertificateReference) )

#
# 4.5 dicomNetworkAE
#
#    This structural object class represents a Network Application Entity
#
objectclass ( 1.2.840.10008.15.0.4.5
 NAME 'dicomNetworkAE'
 DESC 'DICOM Network AE related information'
 SUP top
 STRUCTURAL
 MUST (
  dicomAETitle $
  dicomNetworkConnectionReference $
  dicomAssociationInitiator $
  dicomAssociationAcceptor )
 MAY (
  dicomDescription $
  dicomVendorData $
  dicomApplicationCluster $
  dicomPreferredCalledAETitle $
```

```
  dicomPreferredCallingAETitle $
  dicomSupportedCharacterSet $
  dicomInstalled ) )

#
# 4.6 dicomNetworkConnection
#
#    This structural object class represents a Network Connection
#
objectclass ( 1.2.840.10008.15.0.4.6
 NAME 'dicomNetworkConnection'
 DESC 'DICOM Network Connection information'
 SUP top
 STRUCTURAL
 MUST ( dicomHostname )
 MAY (
  cn $
  dicomPort $
  dicomTLSCipherSuite $
  dicomInstalled ) )

#
# 4.7 dicomUniqueAETitle
#
#    This structural object class represents a Unique Application Entity Title
#
objectclass ( 1.2.840.10008.15.0.4.7
 NAME 'dicomUniqueAETitle'
 DESC 'A Unique DICOM Application Entity title'
 SUP top
 STRUCTURAL
 MUST ( dicomAETitle ) )

#
# 4.8 dicomTransferCapability
#
#    This structural object class represents Transfer Capabilities for an Application Entity
#
objectclass ( 1.2.840.10008.15.0.4.8
 NAME 'dicomTransferCapability'
 DESC 'Transfer Capabilities for an Application Entity'
 SUP top
 STRUCTURAL
 MUST (
  dicomSOPClass $
  dicomTransferRole $
  dicomTransferSyntax)
 MAY (
  cn) )
```

H.1.4 Transactions

H.1.4.1 Find LDAP Server

H.1.4.1.1 Scope

The RFC-2782 *A DNS RR for specifying the location of services (DNS SRV)*specifies a mechanism for requesting the names and rudimentary descriptions for machines that provide network services. The DNS client requests the descriptions for all machines that are registered as offering a particular service name. In this case the service name requested will be "LDAP". The DNS server may respond with multiple names for a single request.

H.1.4.1.2 Use Case Roles

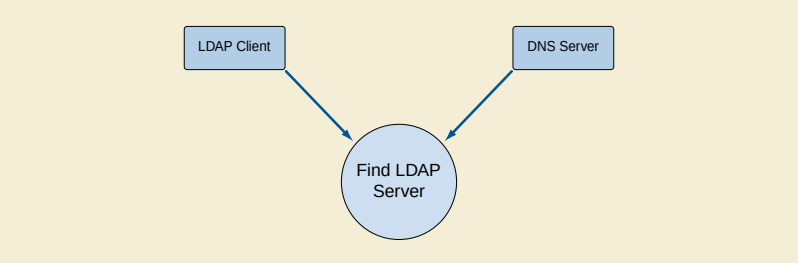

Figure H.1-3. Find LDAP Server

DNS Server Provides list of LDAP servers

LDAP Client Requests list of LDAP servers

H.1.4.1.3 Referenced Standards

RFC-2181 Clarifications to the DNS Specification

RFC-2219 Use of DNS Aliases for Network Services

RFC-2782 A DNS RR for specifying the location of services (DNS SRV)

other RFC's are included by reference from RFC-2181, RFC-2219, and RFC-2782.

H.1.4.1.4 Interaction Diagram

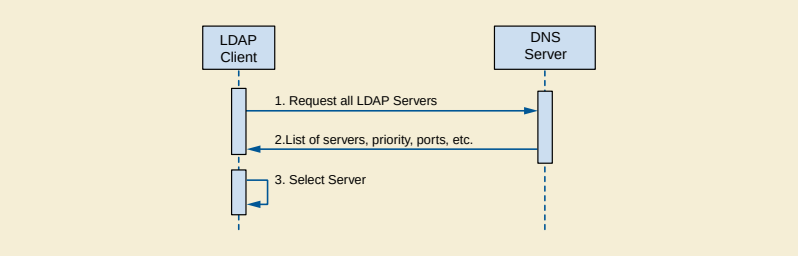

Figure H.1-4. Select LDAP Server

The DNS client shall request a list of all the LDAP servers available. It will use the priority, capacity, and location information provided by DNS to select a server. (RFC-2782 recommends the proper use of these parameters.) It is possible that there is no LDAP server, or that the DNS server does not support the SRV RR request.

Note

1. Multiple LDAP servers providing access to a common replicated LDAP database is a commonly supported configuration. This permits LDAP servers to be located where appropriate for best performance and fault tolerance. The DNS server response information provides guidance for selecting the most appropriate server.

2. There may also be multiple LDAP servers providing different databases. In this situation the client may have to examine several servers to find the one that supports the DICOM configuration database. Similarly a single LDAP server may support multiple base DNs, and the client will need to check each of these DNs to determine which is the DICOM supporting tree.

H.1.4.1.5 Alternative Paths

The client may have a mechanism for manual default selection of the LDAP server to be used if the DNS server does not provide an LDAP server location.

H.1.4.2 Query LDAP Server

H.1.4.2.1 Scope

The RFC-2251 "Lightweight Directory Access Protocol (v3) " specifies a mechanism for making queries of a database corresponding to an LDAP schema. The LDAP client can compose requests in the LDAP query language, and the LDAP server will respond with the results for a single request.

H.1.4.2.2 Use Case Roles

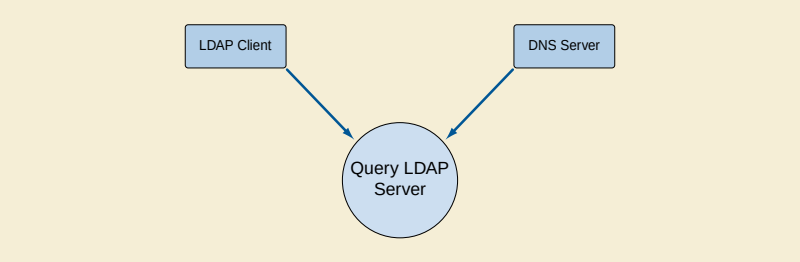

Figure H.1-5. Query LDAP Server

LDAP Server	Provides query response
LDAP Client	Requests LDAP information

H.1.4.2.3 Referenced Standards

RFC-2251 Lightweight Directory Access Protocol (v3). LDAP support requires compliance with other RFC's invoked by reference.

H.1.4.2.4 Interaction Description

The LDAP client may make a wide variety of queries and cascaded queries using LDAP. The LDAP client and server shall support the Application Configuration Data Model .

Note

Multiple LDAP servers providing access to a common replicated LDAP database is a commonly supported configuration. This permits LDAP servers to be located where appropriate for best performance and fault tolerance. The replications rules chosen for the LDAP servers affect the visible data consistency. LDAP permits inconsistent views of the database during updates and replications.

H.1.4.3 Update LDAP Server

H.1.4.3.1 Scope

The RFC-2251 "Lightweight Directory Access Protocol (v3) " specifies a mechanism for making updates to a database corresponding to an LDAP schema. The LDAP client can compose updates in the LDAP query language, and the LDAP server will respond with the results for a single request. Update requests may be refused for security reasons.

H.1.4.3.2 Use Case Roles

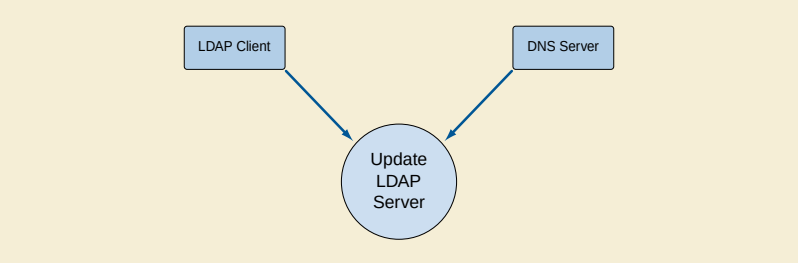

Figure H.1-6. Update LDAP Server

LDAP Server Maintains database

LDAP Client Updates LDAP information

H.1.4.3.3 Referenced Standards

RFC-2251 Lightweight Directory Access Protocol (v3). LDAP support requires compliance with other RFC's invoked by reference.

H.1.4.3.4 Interaction Description

The LDAP client may make a request to update the LDAP database. The LDAP client shall support the data model described above. The LDAP server may choose to refuse the update request for security reasons. If the LDAP server permits update requests, is shall support the data model described above.

Note

Multiple LDAP servers providing access to a common replicated LDAP database is a commonly supported configuration. This permits LDAP servers to be located where appropriate for best performance and fault tolerance. Inappropriate selection of replication rules in the configuration of the LDAP server will result in failure for AE-title uniqueness when creating the AE-titles objects.

H.1.4.3.5 Special Update For Network AE Creation

The creation of a new Network AE requires special action. The following steps shall be followed:

a. A tentative AE title shall be selected. Various algorithms are possible, ranging from generating a random name to starting with a preset name template and incrementing a counter field. The client may query the Unique AE Titles Registry sub-tree to obtain the complete list of names that are presently in use as part of this process.

b. A new Unique AE Title object shall be created in the Unique AE Titles Registry portion of the hierarchy with the tentative name. The LDAP server enforces uniqueness of names at any specific point in the hierarchy.

c. If the new object creation was successful, this shall be the AE Title used for the new Network AE.

d. If the new object creation fails due to non-unique name, return to a) and select another name.

H.1.4.4 Maintain LDAP Server

The LDAP server shall support a separate manual or automated means of maintaining the LDAP database contents. The LDAP server shall support the RFC-2849 file format mechanism for updating the LDAP database. The LDAP Client or service installation tools shall provide RFC-2849 formatted files to update LDAP server databases manually. The LDAP server may refuse client network updates for security reasons. If this is the case, then the maintenance process will be used to maintain the LDAP database.

The manual update procedures are not specified other than the requirement above that at least the minimal LDAP information exchange file format from RFC 2849 be supported. The exact mechanisms for transferring this information remain vendor and site specific. In some situations, for example the creation of AE-titles, a purely manual update mechanism may be easier than exchanging files.

The conformance statement shall document the mechanisms available for transferring this information. Typical mechanisms include:

a. floppy disk

b. CD-R

c. SSH

d. Secure FTP

e. FTP

f. email

g. HTTPS

Note

1. There are many automated and semi-automatic tools for maintaining LDAP databases. Many LDAP servers provide GUI interfaces and updating tools. The specifics of these tools are outside the scope of DICOM. The LDAP RFC-2849 requires at least a minimal data exchange capability. There are also XML based tools for creating and maintaining these files.

2. This mechanism may also be highly effective for preparing a new network installation by means of a single pre-planned network configuration setup rather than individual machine updates.

H.1.5 LDAP Security Considerations (Informative)

H.1.5.1 Threat Assessment

The threat and value for the LDAP based configuration mechanisms fall into categories:

a. AE-uniqueness mechanism

b. Finding (and updating) Network AE descriptions

c. Finding (and updating) device descriptions

These each pose different vulnerabilities to attack. These are:

a. Active Attacks

1. The AE-title uniqueness mechanism could be attacked by creating vast numbers of spurious AE-titles. This could be a Denial of Service (DoS) attack on the LDAP server. It has a low probability of interfering with DICOM operations.

2. The Network AE information could be maliciously updated. This would interfere with DICOM operations by interfering with finding the proper server. It could direct connections to malicious nodes, although the use of TLS authentication for DICOM connections would detect such misdirection. When TLS authentication is in place this becomes a DoS attack.

3. The device descriptions could be maliciously modified. This would interfere with proper device operation.

b. Passive Attacks

1. There is no apparent value to an attacker in obtaining the current list of AE-titles. This does not indicate where these AE-titles are deployed or on what equipment.

2. The Network AE information and device descriptions might be of value in determining the location of vulnerable systems. If it is known that a particular model of equipment from a particular vendor is vulnerable to a specific attack, then the Network AE Information can be used to find that equipment.

H.1.5.2 Available LDAP Security Mechanisms

The security mechanisms for LDAP are highly variable in actual implementations. They are a mixture of administrative restrictions and protocol implementations. The widely available options for security methods are:

a. Anonymous access, where there is no restriction on performing this function over the network.

b. Basic, where there is a username and password exchange prior to granting access to this function. The exchange is vulnerable to snooping, spoofing, and man in the middle attacks.

c. TLS, where there is an SSL/TLS exchange during connection establishment.

d. Manual, where no network access is permitted and the function must be performed manually at the server, or semi-automatically at the server. The semi-automatic means permit the use of independently exchanged files (e.g., via floppy) together with manual commands at the server.

The categories of functions that may be independently controlled are:

a. Read related, to read, query, or otherwise obtain a portion of the LDAP directory tree

b. Update related, to modify previously existing objects in the directory tree

c. Create, to create new objects in the directory tree.

Finally, these rules may be applied differently to different subtrees within the overall LDAP structure. The specific details of Access Control Lists (ACLs), functional controls, etc. vary somewhat between different LDAP implementations.

H.1.5.3 Recommendations (Informative)

The LDAP server should be able to specify different restrictions for the AE-Title list and for the remainder of the configuration information. To facilitate interoperability, Table H.1-15 defines several patterns for access control. They correspond to different assessments of risk for a network environment.

Table H.1-15. LDAP Security Patterns

	TLS	TLS-Manual	Basic	Basic-Manual	Anonymous	Anonymous-Manual
Read AE-title	Anonymous, TLS	Anonymous, TLS	Anonymous, Basic	Anonymous, Basic	Anonymous	Anonymous
Create AE-Title	TLS	Manual	Basic	Manual	Anonymous	Manual
Read Config	TLS	TLS	Basic	Basic	Anonymous	Anonymous
Update Config	TLS	Manual	Basic	Manual	Anonymous	Manual
Create Config	TLS	Manual	Basic	Manual	Anonymous	Manual

TLS This pattern provides SSL/TLS authentication and encryption between client and server. It requires additional setup during installation because the TLS certificate information needs to be installed onto the client machines and server. Once the certificates are installed the clients may then perform full updating operations.

TLS-Manual This pattern provides SSL/TLS controls for read access to information and require manual intervention to perform update and creation functions.

Basic This pattern utilizes the LDAP basic security to gain access to the LDAP database. It requires the installation of a password during client setup. It does not provide encryption protection. Once the password is installed, the client can then perform updates.

Basic-Manual This pattern utilizes basic security protection for read access to the configuration information and requires manual intervention to perform update and creation functions.

Anonymous This pattern permits full read/update access to all machines on the network.

Anonymous-Manual This pattern permits full read access to all machines on the network, but requires manual intervention to perform update and creation.

A client or server implementation may be capable of being configured to support multiple patterns. This should be documented in the conformance claim. The specific configuration in use at a specific site can then be determined at installation time.

H.1.6 Implementation Considerations (Informative)

The LDAP database can be used as a documentation tool. Documenting the configuration for both managed and legacy machines makes upgrading easier and reduces the error rate for manually configured legacy equipment.

There are various possible implementation strategies for clients performing lookups within the LDAP database. For example, before initiating a DICOM association to a specific AE, a client implementation could either:

a. Query the LDAP database to obtain hostname and port for the specific AE Title immediately prior to initiating a DICOM association.

b. Maintain a local cache of AE Title, hostname and port information and only query the LDAP database if the specific AE Title is not found in the local cache.

The advantages of maintaining a local cache include performance (by avoiding frequent lookups) and reliability (should the LDAP server be temporarily unavailable). The disadvantage of a cache is that it can become outdated over time. Client implementations should provide appropriate mechanisms to purge locally cached information.

Client caches may cause confusion during updates. Manual steps may be needed to trigger immediate updates. LDAP database replication also may introduce delays and inconsistencies. Database replication may also require manual intervention to force updates to occur immediately.

One strategy to reduce client cache problems is to re-acquire new DNS and LDAP information after any network association information. Often the first symptom of stale cache information is association failures due to the use of obsolete configuration information.

Some LDAP servers do not support a "modify DN" operation. For example, in the case of renaming a device on such a server, a tree copy operation may be needed to create a new object tree using the new name, followed by removal of the old object tree. After such a rename the device may need to search using other attributes when finding its own configuration information, e.g., the device serial number.

H.1.7 Conformance

The Conformance Statement for an LDAP Client or LDAP Server implementation shall specify the security pattern(s) that it supports.

H.2 DNS Service Discovery

H.2.1 Scope

Service discovery mechanisms provide a means for devices to announce their presence and seek information about the existence of other services on the network. Many of these mechanisms are DNS-based.

The exact use of such protocols as DNS Service Discovery (DNS-SD), Multi-cast DNS (mDNS) and DNS Dynamic Updates is defined in RFC's referenced by DICOM. This section standardizes the name to be used in DNS SRV records for such purposes, and the DNS TXT records that encode accompanying parameters.

Security issues associated with self discovery are out of scope. See Section F.1.1.4 for the informative discussion on DNS Security issues.

H.2.2 Use Case Roles

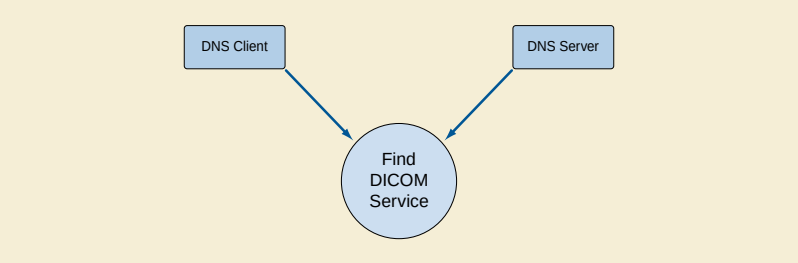

Figure H.2-1. Find DICOM Service

DNS Server Provides list of DICOM Association Acceptors

DNS Client Requests list of DICOM Association Acceptors

H.2.3 Referenced Standards

RFC 2136 DNS Dynamic Updates http://tools.ietf.org/html/rfc2136

RFC 2181 Clarifications to the DNS Specification http://tools.ietf.org/html/rfc2181

RFC 2219 Use of DNS Aliases for Network Services http://tools.ietf.org/html/rfc2219

RFC 2782 A DNS RR for specifying the location of services (DNS SRV) http://tools.ietf.org/html/rfc2782

RFC 6762 Multicast DNS http://tools.ietf.org/html/rfc6762

RFC 6763 DNS-Based Service Discovery http://tools.ietf.org/html/rfc6763

DNS Self-Discovery http://www.dns-sd.org/

The name to be used in the DNS SRV to advertise DICOM Association Acceptors, regardless of the SOP Class(es) supported, shall be

- "dicom" for unsecured DICOM communication
- "dicom-tls" for the Basic TLS Secure Transport Connection Profile
- "dicom-iscl" for ISCL Transport Connection Profile
- "dicomweb" for DICOM web services over unsecured http
- "dicomweb-tls" for DICOM web services over https

  Note

  These choices are consistent with the names registered with IANA to define the mapping of IP ports to services, which is conventional for this usage. The choice "dicom" is used rather than the "acr-nema" alternative for clarity. There is no implied port choice by the usage in the DNS SRV Service Type, since the port is explicitly conveyed.

The DNS TXT record may contain the following parameters:

- AET= <*application entity title*>, where the value <*application entity title*>is to be used as the Called Application Entity Title when initiating Associations to the device
- PrimaryDeviceType= <*primary device type*>, where the value <*primary device type*>is as defined Table H.1-2 Attributes of Device Object

- DICOMWebPath= <*service*>, where the value <*service*> is the *path* component of the DICOM Web Service root as defined in PS3.18

In the absence of a DNS TXT record, or the AET parameter of the DNS TXT record, then the Instance Name preceding the Service Type in the DNS SRV record used for DICOM service discovery shall be the AET.

Note

Further parameters are not specified, for example to indicate the SOP Classes supported or other information, since the size of DNS records encoded as UDP datagrams is strictly limited, and furthermore, the envisaged multicast usage encourages the exchange of the minimal information necessary. The existing DICOM association negotiation mechanism can be used to explore the SOP Classes offered once the IP address, port number and AET are known. The primary device type is supplied because it is useful to indicate to users the type of device, which is not conveyed during association establishment.

H.2.4 Examples

Example SRV record:

- _dicomweb-tls._tcp. examplehospital.org 86400 IN SRV 10 60 443 ~~dicomweb. examplehospital.org.~~dicomweb.examplehospital.org.

Example TXT record:

- ~~dicomweb. examplehospital.org~~dicomweb.examplehospital.org IN TXT "DICOMWebPath=apps/dicom-rs"

The above examples would combine to define a DICOM web service root of:

- "https://~~dicomweb. examplehospital.org~~dicomweb.examplehospital.org:443/apps/dicom-rs"