CODONICS

Integrity™ *Medical Image Import Station*

Powered by…

DICOM® Connectivity Framework

LAUREL BRIDGE

Providing DICOM Connectivity for the Medical Community

DICOM Conformance Statement

Part Number: 900-396-002 Rev. 01

Document / Software Version: v1.4.0

Date: 27 August, 2008

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

This page intentionally left blank.

0 TABLE OF CONTENTS

1 TABLE OF TABLES

0 INTRODUCTION

The Codonics Integrity Medical Image Import Station (MIIS) supports import of medical images and other instances stored on optical disc storage medium in the DICOM 3.0 protocol, and forwarding of these same entities to Dicom Store SCPs using the DICOM Connectivity Framework (DCF) software. The DCF software is a modular software component system used for storage, processing, printing or otherwise communicating medical image data, in this case, primarily for the purpose of media import into a hospital network.

0.1 Scope and Intended Audience

Conformance of the Integrity MIIS to the DICOM 3.0 Standard is discussed in this document. It specifies the Service Classes, Information Objects, and Communication Protocols supported by the implementation. This statement is intended to aid the system integrator in connecting the Codonics Integrity to other components which make use of the DICOM 3.0 Standard for inter-network communication and media exchange. The reader of this document should be familiar with the DICOM 3.0 Standard, the components being interconnected, and other references listed in Section 0.3 and Section 8 of this document.

0.2 Laurel Bridge Software Components

The Laurel Bridge Software DCF Storage Service Class User component is a software function of the Codonics Integrity product. It typically interfaces a PACS or other device on a TCP/IP network with the Codonics Integrity via the DCF Storage User (SCU) software, allowing the Integrity to forward medical images and related data from the optical storage medium to a Dicom Storage device on the hospital network after modifying the identifying medical image metadata to suit the conventions of the particular facility.

This conformance statement represents the functionality of Codonics' DCF-based system.

Because the DCF is highly configurable, the OEM conformance claim for a particular realization of the DCF should not be construed to completely represent the functions or limitations of the complete DCF software package. *Once customized, the OEM conformance claim only applies to the specific OEM implementation described within, in this case, that of the Codonics Integrity products.*

For further information on the complete DCF package, one should contact Laurel Bridge Software, Inc., 160 E. Main St., Newark, DE 19711, Telephone: 302-453-0222, http://www.laurelbridge.com. Under the terms of the DCF Software License Agreement, this notice is required to be present in all DICOM conformance claims covering the DCF software functionality.

0.3 References

ACR-NEMA DICOM 3.0 Standard, Parts 1 through 14 (PS 3.1–PS 3.14); ©2004.

See Section 8 of this document for additional reference information.

0.4 Important Considerations for the Reader

There is no concept in DICOM of a singular "monolithic" compliance with the Standard. The DICOM Conformance Statement, is a document whose organization and content are mandated by the Standard (PS 3.2-2004, Annex A through F) and which allows users to communicate how they comply with the Standard in their implementations. The presence of specific DICOM functionality in a Conformance Statement is not sufficient to guarantee inter-operability between components. When evaluating network inter-operability between the DCF and some other DICOM component, the following should be considered:

- The DCF Conformance Claim is an appropriate starting point for ascertaining whether the DCF software can communicate with a particular component on a protocol level.

- The only way to know for certain whether the DCF can inter-operate with other DICOM components is to perform a connectivity test. This test must be completed before a field installation can occur. The OEM normally does such testing in cooperation with the suppliers of other DICOM components.

- The DCF Conformance Claim represents a best effort at documenting the DICOM functionality of commercial versions of the Codonics Integrity, but is not a functional specification of any DCF component or product. Laurel Bridge Software reserves the right to make changes at any time to the functionality of DCF components described herein. Both Laurel Bridge Software and Codonics are committed to following the evolution of the DICOM Standard with either modifications or additions to the Codonics Integrity's DICOM functionality provided by the DCF.

Note: The section numbering in this document is fixed and conforms to the numbering scheme prescribed in DICOM PS 3.2-1999, Annex A and Annex B.

0.5 Revision History

Revision	Date	Author	Description of Changes
0.90	7 January 2008	Glenn Burke	Adapted from the Virtua Conformance Statement as first pre-release version.
0.91	10 January 2008	Glenn Burke	Added Original Attr. Seq. and Contributing Equip. Seq. to the table of updated/added values.
.101	13 January 2008	Steven K. Minner	Made comments to Glenn's todos. Removed some entries from the Glossary section.
1.0	22 February 2008	Glenn Burke	Updated based on Steve M's comments. Updated handling of duplicate UIDs. Updated document to use Word autonumbering.
1.01	25 February 2008	Glenn Burke	Changed MDIS to MIIS. Updated information about support of Extended Character Sets. Various updates to content.
1.02	25 February 2008	Ross Goodman	Updated format. Assigned part number
1.03	18 March 2008	Glenn Burke	Updated App. Data Flow Diagram. Removed Compressed Syntaxes from Store Client.
1.4.0	8 July 2008	Glenn Burke	Updated Store Client Syntaxes Added Store SCP section Fixed Heading number formatting

0.6 Symbols, Abbreviations and Definitions

Abstract Syntax: A DICOM term which is identical to a DICOM SOP Class; it identifies a set of SOPs which, when taken together, represent a logical grouping. An Abstract Syntax identifies one SOP Class or Meta SOP Class.

ACR: American College of Radiology.

ANSI: American National Standards Institute.

Application Entity (AE): A DICOM term for defining a particular user at an IP address.

Association: A DICOM term for a communication context which is used by two Application Entities that communicate to one another.

Association Negotiation: The software handshaking that occurs between two DICOM Application Entities to set up an Association.

Attribute: Each DICOM information object has its own set of characteristics or attributes. Each attribute has a name and may have a value (see IOD), depending on its category.

Big Endian: A term for encoding data where the most-significant byte appears first and remaining bytes follow in descending order of significance; sometimes known as “Motorola” format (see Little Endian). (The term is used because of an analogy with the story Gulliver's Travels, in which Jonathan Swift imagined a never-ending fight between the kingdoms of the Big-Endians and the Little-Endians, whose only difference is in where they crack open a hard-boiled egg.)

Calling (Requesting) AE Title: The name used by the receiver in a DICOM Association to indicate which Application Entity it received the data from. It is the AE Title of the AE that is initiating the transfer.

Called (Receiving) AE Title: The name used by the sender in a DICOM Association to indicate which Application Entity it wants to transmit its data to. It is the AE Title of the AE that is receiving the transfer.

Command Element: An encoding of a parameter of a command which conveys this parameter's value.

Command Stream: The result of encoding a set of DICOM Command Elements using the DICOM encoding scheme.

Composite Information Object: A DICOM information object (see IOD) whose attributes contain multiple real world objects.

Conformance: Conformance in the DICOM sense means to be in compliance with the parts of the DICOM Standard.

Conformance Statement: A document whose organization and content are mandated by the DICOM Standard, which allows users to communicate how they have chosen to comply with the Standard in their implementations (see Section 8).

Data Dictionary: A registry of DICOM Data Elements which assigns a unique tag, a name, value characteristics, and semantics to each Data Element (see the DICOM Data Element Dictionary in DICOM PS 3.6-2007).

Data Element: A unit of information as defined by a single entry in the data dictionary. An encoded Information Object Definition (IOD) Attribute that is composed of, at a minimum, three fields: a Data Element Tag, a Value Length, and a Value Field. For some specific Transfer Syntaxes, a

Data Element also contains a VR Field where the Value Representation of that Data Element is specified explicitly.

Data Set: Exchanged information consisting of a structured set of Attribute values directly or indirectly related to Information Objects. The value of each Attribute in a Data Set is expressed as a Data Element.

Data Stream: The result of encoding a Data Set using the DICOM encoding scheme (Data Element Numbers and representations as specified by the Data Dictionary).

DICOM: Digital Imaging and Communications in Medicine.

DICOM File: A DICOM File is a file with a content formatted according to the requirements of DICOM PS 3.10-1999.

DICOM File Format: The DICOM File Format provides a means to encapsulate in a File the Data Set representing a SOP Instance related to a DICOM Information Object.

DIMSE: DICOM Message Service Element. This represents an abstraction of a common set of things that a user would do to a data element, would likely use over and over, and would appear in various different contexts.

DIMSE-C: DICOM Message Service Element—Composite.

DIMSE-C services: A subset of the DIMSE services which supports operations on Composite SOP Instances related to composite Information Object Definitions with peer DIMSE-service-users.

DIMSE-N: DICOM Message Service Element—Normalized.

DIMSE-N services: A subset of the DIMSE services which supports operations and notifications on Normalized SOP Instances related to Normalized Information Object Definitions with peer DIMSE-service-users.

File Set Creator (FSC): Creates or modifies a DICOM file set (DICOMDIR file) and its corresponding DICOM data files.

File Set Reader (FSR): Reads a DICOM file set (DICOMDIR file) and its corresponding DICOM data files.

File Set Updater (FSU): Creates, modifies or deletes a DICOM file set (DICOMDIR file) and its corresponding DICOM data files.

Information Object Class or

Information Object [Definition] (IOD): A software representation of a real object (e.g., CT Image, Study, etc.). An Information Object is generally a list of characteristics (Attributes) which completely describe the object as far as the software is concerned. The formal description of an Information Object generally includes a description of its purpose and the Attributes it posseses.

Information Object Instance or

Instance (of an IOD): A software representation of a specific occurance of a real object or entity, including values for the Attributes of the Information Object Class to which the entity belongs..

IP (Internet Protocol) Address: A unique identifier for the network interface of a computer on a TCP/IP network. An IP address is typically comprised of four octets, separated by dots (.), with each octet capable of representing a number from 0 to 255. For example: 192.168.10.1

Little Endian: A term for encoding data where the least-significant byte appears first and remaining bytes follow in ascending order of significance; sometimes known as ”Intel” format (see Big Endian).

LUT: Lookup Table.

Message: A data unit of the Message Exchange Protocol exchanged between two cooperating DICOM Application Entities. A Message is composed of a Command Stream followed by an optional Data Stream.

Meta SOP Class: A collection or group of related SOP Classes identified by a single Abstract Syntax UID, which, when taken together, represent a logical grouping and which are used together to provide a high-level functionality, e.g., for the purpose of negotiating the use of the set with a single item.

Module: A logical group of the valid attributes of DICOM information objects.

NEMA: National Electrical Manufacturers Association.

Normalized Information Object: A DICOM Information Object (see IOD) whose attributes contain a single real world object. *Note: the differentiation of normalized versus composite information object definitions is not strongly enforced in DICOM 3.0.*

Presentation Context: A Presentation Context consists of an Abstract Syntax plus a list of acceptable Transfer Syntaxes. The Presentation Context defines both what data will be sent (Abstract Syntax) and how the data are encoded to be sent (Transfer Syntax).

Protocol Data Unit (PDU): A data object which is exchanged by software protocol devices (entities, machines) within a given layer of the protocol stack.

Real-World Activity: Something which exists in the real world and which pertains to specific area of information processing within the area of interest of the DICOM Standard. A Real-World Activity may be represented by one or more SOP Classes.

Real-World Object: Something which exists in the real world and upon which operations may be performed which are within the area of interest of the DICOM Standard. A Real-World Object may be represented through a SOP Instance.

Service Class: A group of operations that a user might want to perform on particular Information Objects. Formally, a structured description of a service which is supported by cooperating DICOM Application Entities using specific DICOM Commands acting on a specific class of Information Object.

Service Class Provider (SCP, Provider, Server): A device which provides the services of a DICOM Service Class or Classes which are utilized by another device (SCU) and which performs operations and invokes notifications on a specific Association.

Service Class User (SCU, User, Client): A device which utilizes the DICOM Service Class or Classes which are provided by another device (SCP) and which invokes operations and performs notifications on a specific Association.

Service-Object Pair (SOP): The combination of a DICOM Information Object and the Service Class which operates upon that object.

SOP Class: A DICOM term which is identical to an Abstract Syntax; it identifies a set of SOPs which, when taken together, represent a logical grouping (see Meta SOP Class).

Storage Service Class (SSC): A DICOM term for a logical grouping of Service Classes which all involve storage of images and other DICOM instances.

Tag: A unique identifier for an element of information composed of an ordered pair of numbers (a Group Number followed by an Element Number), which is used to identify Attributes and corresponding Data Elements.

TCP/IP: Transmission Control Protocol / Internet Protocol.

Transfer Syntax: A part of the DICOM Presentation Context which specifies a set of encoding rules that allow Application Entities to unambiguously negotiate the encoding techniques (e.g., Data Element structure, byte ordering, compression) they are able to support, thereby allowing these Application Entities to communicate.

Unique Identifier (UID): A globally unique identifier (based on the structure defined by ISO 8824 for OSI Object Identifiers) which is assigned to every DICOM information object as specified by the DICOM Standard (see Section 2.1.1.4) and which guarantees global unique identification for objects across multiple countries, sites, vendors and equipment.

Value Representation (VR): A VR is the defined format of a particular data element.

1 IMPLEMENTATION MODELS

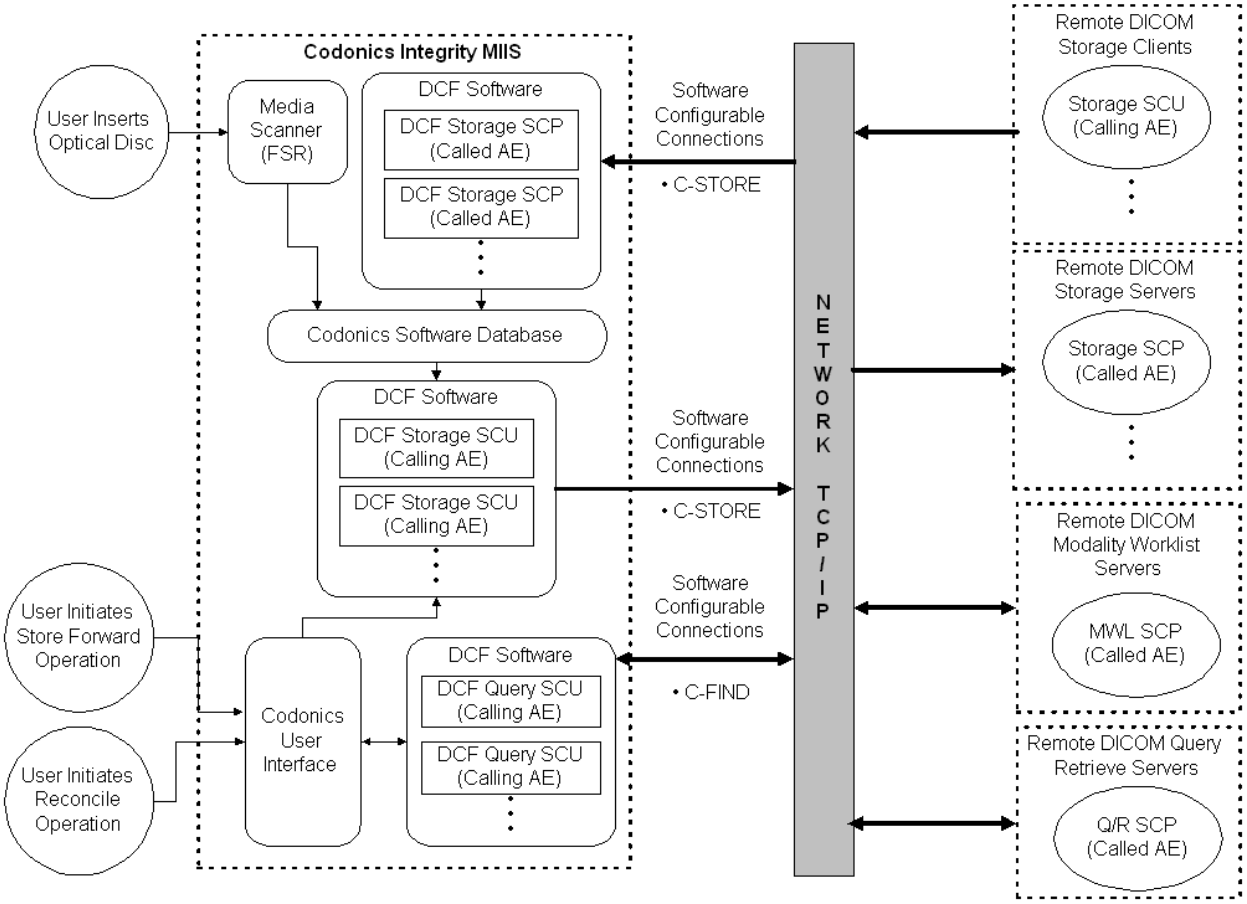
The DCF Media Scanner (Dicom File Set Reader) is implemented as a single process running on the Integrity MIIS. The number of Dicom File Sets that can be read in is currently limited to one at a time.

The DCF Storage Client is implemented as independent, functional, and configurable components. The DCF Storage Client supports multiple Application Entities. It may concurrently initiate and/or maintain associations to multiple DICOM Storage Servers. The number of associations that the DCF Storage Client uses simultaneously is limited to 24.

The DCF Query Client is implemented as independent, functional, and configurable components. The Codonics User Interface (UI) is web-based, and allows multiple users to simultaneously execute query operations to Dicom Query Retrieve (Q/R) SCPs or Dicom Modality Worklist (MWL) SCPs in order to obtain Patient Information. The number of associations initiated at one time by the Query Client is limited to 1.

1.1 Application Data Flow Diagram—Integrity MIIS

The implementation model of the Integrity MIIS is depicted in the following figure:



1.2 Functional Definitions of Application Entities (AEs)

The DCF Storage Server creates a StoreSCP (Application Entity or AE) to handle each requested association (unless the configurable maximum associations is exceeded). Each StoreSCP can be

configured independently, based on a flexible policy that takes both Called and Calling AE Titles into account.

Once the configuration for the StoreSCP is selected and the StoreSCP is created, the StoreSCP continues with the association negotiation, independent of the DCF Storage Server. The StoreSCP's configuration specifies which SOP classes are to be supported, which transfer syntaxes are to be supported, as well as many other parameters, such as what type of validation is to be performed on incoming messages.

If the StoreSCP accepts the association, then it will service requests from the client SCU until the association is ended. As the StoreSCPs receive storage requests from their corresponding SCUs they commit the stored entities to an internal database, grouping them by Patient, Study, Series and Instance identities. Once the SCU has completed its set of storage requests, it can close the association, or keep the association open for subsequent storage requests.

The association ends when either the SCU releases the association or there is an unrecoverable error. Optionally, if the SCU does not send a request for a period in excess of the StoreSCP configurable timeout, then the StoreSCP will terminate the association.

The DCF Query Client is created when a user requests to Reconcile a Study. The Query Client attempts to open an association with a Query/Retrieve SCP or with an Modality Worklist SCP. When the association is accepted, the Query Client will send one or more C-Find requests for Patient information matching particular criteria. The Query Client will collect any results returned by the SCP for later use by the Integrity MIIS.

After all required C-Find operations have been completed, the Query Client releases the association. The association ends when either the Query Client releases the association or there is an unrecoverable error.

The DCF Storage Client is created when a user requests to Store Forward a Study or Studies. The Storage Client attempts to open one association per Store Destination (Remote Storage Server) on which to perform C-Store operations. For each Server that accepts the association, the Storage Client will send Instances from each user-selected Study to the Storage SCP.

After all required C-Store operations to each Storage server have been completed, the Storage Client releases the association to that Storage Server. The association ends when either the Storage Client releases the association or there is an unrecoverable error.

1.3 Sequencing of Real World Activities—DCF Storage Server

The sequence of events for a typical transaction are listed below:

Storage Client (modality, workstation, or other device) requests association with Storage Server.

Storage Client stores DICOM Instances to Storage Server.

Storage Client terminates the association.

Storage Server releases any resources allocated during association.

1.4 Sequencing of Real World Activities—DCF Query Client

The sequence of events for a typical query transaction are listed below:

User initiates a query operation from the user interface of the Integrity device.

The following steps are repeated until all Patient Matching criteria have been queried with, or until any results are returned (configurable).

Query Client requests association with Q/R or MWL Server.

Query Client queries for matching patients from Q/R or MWL Server, based on the next set of configurable matching criteria.

Q/R or MWL Server returns matching patients to Query Client.

Query Client terminates the association.

User interface is updated with list of matching patients.

1.5 Sequencing of Real World Activities—DCF Storage Client

The sequence of events for a typical Storage transaction are listed below:

User initiates a Store operation from the user interface of the Integrity device.

For each selected Storage Server (SCP):

Storage Client requests association with Storage Server.

Storage Client stores Dicom Instances to Storage Server.

Storage Client terminates the association.

Storage Server releases any resources allocated during association.

2 AE SPECIFICATIONS

The DCF Storage Server supports multiple Application Entities or AEs. Each AE in this case is an instance of StoreSCP using a particular configuration.

The DCF Query Client supports multiple Application Entities or AEs. Each AE in this case is an instance of QuerySCU using a particular configuration.

The DCF Storage Client supports multiple Application Entities or AEs. Each AE in this case is a Store Destination.

Table 2.1 – Integrity Supported SOP Classes

SOP Class Name	SOP Class UID
Computed Radiography Image Storage	1.2.840.10008.5.1.4.1.1.1
Digital X-Ray Image Storage – For Presentation	1.2.840.10008.5.1.4.1.1.1.1
Digital X-Ray Image Storage – For Processing	1.2.840.10008.5.1.4.1.1.1.1.1
Digital Mammography X-Ray Image Storage – For Presentation	1.2.840.10008.5.1.4.1.1.1.2
Digital Mammography X-Ray Image Storage – For Processing	1.2.840.10008.5.1.4.1.1.1.2.1
Digital Intra-oral X-Ray Image Storage – For Presentation	1.2.840.10008.5.1.4.1.1.1.3
Digital Intra-oral X-Ray Image Storage – For Processing	1.2.840.10008.5.1.4.1.1.1.3.1
CT Image Storage	1.2.840.10008.5.1.4.1.1.2
Enhanced CT Image Storage	1.2.840.10008.5.1.4.1.1.2.1
Ultrasound Multi-frame Image Storage (Retired)	1.2.840.10008.5.1.4.1.1.3
Ultrasound Multi-frame Image Storage	1.2.840.10008.5.1.4.1.1.3.1
MR Image Storage	1.2.840.10008.5.1.4.1.1.4
Enhanced MR Image Storage	1.2.840.10008.5.1.4.1.1.4.1
MR Spectroscopy Storage	1.2.840.10008.5.1.4.1.1.4.2
Nuclear Medicine Image Storage (Retired)	1.2.840.10008.5.1.4.1.1.5
Ultrasound Image Storage	1.2.840.10008.5.1.4.1.1.6.1
Ultrasound Image Storage (Retired)	1.2.840.10008.5.1.4.1.1.6
Secondary Capture Image Storage	1.2.840.10008.5.1.4.1.1.7
Multi-frame Single Bit Secondary Capture Image Storage	1.2.840.10008.5.1.4.1.1.7.1
Multi-frame Grayscale Byte Secondary Capture Image Storage	1.2.840.10008.5.1.4.1.1.7.2
Multi-frame Grayscale Word Secondary Capture Image Storage	1.2.840.10008.5.1.4.1.1.7.3
Multi-frame True Color Secondary Capture Image Storage	1.2.840.10008.5.1.4.1.1.7.4
Standalone Overlay Storage	1.2.840.10008.5.1.4.1.1.8
Standalone Curve Storage	1.2.840.10008.5.1.4.1.1.9

ECG 12-Lead Waveform Storage	1.2.840.10008.5.1.4.1.1.9.1.1
ECG General Waveform Storage	1.2.840.10008.5.1.4.1.1.9.1.2
ECG Ambulatory Waveform Storage	1.2.840.10008.5.1.4.1.1.9.1.3
Hemodynamic Waveform Storage	1.2.840.10008.5.1.4.1.1.9.2.1
Cardiac Electrophysiology Waveform Storage	1.2.840.10008.5.1.4.1.1.9.3.1
Basic Void Audio Waveform Storage	1.2.840.10008.5.1.4.1.1.9.4.1
Standalone Modality LUT Storage	1.2.840.10008.5.1.4.1.1.10
Standalone VOI LUT Storage	1.2.840.10008.5.1.4.1.1.11
Grayscale Softcopy Presentation State Storage	1.2.840.10008.5.1.4.1.1.11.1
Color Softcopy Presentation State Storage SOP Class	1.2.840.10008.5.1.4.1.1.11.2
Pseudo-Color Softcopy Presentation State Storage SOP Class	1.2.840.10008.5.1.4.1.1.11.3
Blending Softcopy Presentation State Storage SOP Class	1.2.840.10008.5.1.4.1.1.11.4
X-Ray Angiographic Image Storage	1.2.840.10008.5.1.4.1.1.12.1
Enhanced XA Image Storage	1.2.840.10008.5.1.4.1.1.12.1.1
X-Ray Radiofluoroscopic Image Storage	1.2.840.10008.5.1.4.1.1.12.2
Enhanced XRF Image Storage	1.2.840.10008.5.1.4.1.1.12.2.1
X-Ray Angiographic Bi-Plane Image Storage (Retired)	1.2.840.10008.5.1.4.1.1.12.3
Nuclear Medicine Image Storage	1.2.840.10008.5.1.4.1.1.20
Raw Data Storage	1.2.840.10008.5.1.4.1.1.66
Spatial Registration Storage	1.2.840.10008.5.1.4.1.1.66.1
Spatial Fiducials Storage	1.2.840.10008.5.1.4.1.1.66.2
VL Endoscopic Image Storage	1.2.840.10008.5.1.4.1.1.77.1.1
Video Endoscopic Image Storage	1.2.840.10008.5.1.4.1.1.77.1.1.1
VL Microscopic Image Storage	1.2.840.10008.5.1.4.1.1.77.1.2
Video Microscopic Image Storage	1.2.840.10008.5.1.4.1.1.77.1.2.1
VL Slide-Coordinates Microscopic Image Storage	1.2.840.10008.5.1.4.1.1.77.1.3
VL Photographic Image Storage	1.2.840.10008.5.1.4.1.1.77.1.4
Video Photographic Image Storage	1.2.840.10008.5.1.4.1.1.77.1.4.1
Ophthalmic Photography 8 Bit Image Storage	1.2.840.10008.5.1.4.1.1.77.1.5.1
Ophthalmic Photography 16 Bit Image Storage	1.2.840.10008.5.1.4.1.1.77.1.5.2
Stereometric Relationship Storage	1.2.840.10008.5.1.4.1.1.77.1.5.3
Basic Text SR Storage	1.2.840.10008.5.1.4.1.1.88.11
Enhanced SR Storage	1.2.840.10008.5.1.4.1.1.88.22
Comprehensive SR Storage	1.2.840.10008.5.1.4.1.1.88.33
Procedure Log Storage	1.2.840.10008.5.1.4.1.1.88.40
Mammography CAD SR Storage	1.2.840.10008.5.1.4.1.1.88.50
Key Object Selection Document Storage	1.2.840.10008.5.1.4.1.1.88.59
Chest CAD SR Storage	1.2.840.10008.5.1.4.1.1.88.65
X-Ray Radiation Dose SR	1.2.840.10008.5.1.4.1.1.88.67

Encapsulated PDF Storage	1.2.840.10008.5.1.4.1.1.104.1
Positron Emission Tomography Image Storage	1.2.840.10008.5.1.4.1.1.128
Standalone PET Curve Storage	1.2.840.10008.5.1.4.1.1.129
RT Image Storage	1.2.840.10008.5.1.4.1.1.481.1
RT Dose Storage	1.2.840.10008.5.1.4.1.1.481.2
RT Structure Set Storage	1.2.840.10008.5.1.4.1.1.481.3
RT Beams Treatment Record Storage	1.2.840.10008.5.1.4.1.1.481.4
RT Plan Storage	1.2.840.10008.5.1.4.1.1.481.5
RT Brachy Treatment Record Storage	1.2.840.10008.5.1.4.1.1.481.6
RT Treatment Summary Record Storage	1.2.840.10008.5.1.4.1.1.481.7

2.1 DCF Storage Server (STORE-SCP) AE Specification

The DCF Storage Server provides standard conformance to the DICOM 3.0 SOP Classes in Table 2.1 as an SCP.

The StoreSCP Profile allows configuration for Storage support of Custom SOP Classes. Any SOP Class UIDs that are added to this profile will be accepted for Storage by the Integrity MIIS.

2.1.1 Association Establishment Policies

2.1.1.1 General

The DCF Storage Server (SCP) listens to the transport (TCP) port which has been configured and accepts associations from DICOM Storage Clients (SCUs). If the maximum number of unique IP addresses is exceeded then the association is refused and the A-ASSOCIATE-RJ PDU will specify result = rejected-transient, reason = temporary-congestion. An accepted association remains connected until the client disconnects by sending either an A-RELEASE-RQ or A-ABORT PDU, or there is an unrecoverable error detected by the Storage Server. If the association remains idle for a configurable period of time, the association will be broken by the DCF Storage Server. In the event of an idle timeout, the Storage Server will close the transport connection, but will not send any notification (e.g., P-ABORT PDU).

2.1.1.2 Number of Concurrent Associations

The DCF Storage Server can support multiple concurrent associations from multiple unique hosts. The total number of concurrent associations is limited to 24. Once this limit is reached, association requests are rejected until the number of active associations drops below this limit.

2.1.1.3 Asynchronous Nature

The DCF Storage Server does not support asynchronous operations.

2.1.1.4 Implementation Identifying Information

The implementation UID for the DCF Storage Server is returned in the A-ASSOCIATE-AC PDU. The value for that UID will be “1.2.840.114089.1.1.0.X.Y.Z”, where X.Y.Z is the version number (for example, 1.5.0). The implementation version name is also returned and has the form “DCF X.Y.Zz” where X.Y.Zz is the full version identifier (for example, 1.4.0b for beta version 1.4.0).

All internally generated UID's will be prefixed 1.2.840.xxxxxx, where the identification code “xxxxxx”="114089.1.1" is Laurel Bridge Software's ANSI registered organization identification code for the DCF software. See DICOM PS 3.5-1999, Section 9 for further information.

2.1.2 Association Initiation by Real-World Activity

The DCF Storage Server does not initiate associations.

2.1.3 Association Acceptance Policy

2.1.3.1 Real-World Activity—Verification

2.1.3.1.1 Associated Real World Activity—Verification

The Verification Service Class is a feature used for network diagnostic purposes to verify application level communication between peer DICOM AEs. The DCF Storage Server responds to Verification requests to provide an SCU with the ability to determine if the DCF Storage Server is receiving DICOM requests. This verification is accomplished on an established Association using the C-ECHO DIMSE-C service.

An example of a typical real world activity to initiate a Verification association is a service person invoking a DICOM-Echo client on a remote host, specifying the transport address and AE Title of an instance of the DCF Storage Server as the target.

2.1.3.1.2 Presentation Context Table—Verification

Table 2.2 – Supported Verification Presentation Contexts

Presentation Context Table					
Abstract Syntax		Transfer Syntax		Role	Extended Negotiation
Name	UID	Name	UID		
Verification	1.2.840.10008.1.1	Implicit VR Little Endian	1.2.840.10008.1.2	SCP	None
		Explicit VR Little Endian	1.2.840.10008.1.2.1	SCP	None
		Explicit VR Big Endian	1.2.840.10008.1.2.2	SCP	None

2.1.3.1.3 SOP Specific Conformance—Verification

The DCF Storage Server provides standard conformance to the DICOM Verification Service Class.

The Verification SOP Class consists of the C-ECHO DIMSE-C service. No associated Information Object Definition is defined. No Specialized SOP Classes and/or Meta SOP Classes are defined for the Verification SOP Class.

2.1.3.1.4 Presentation Context Acceptance Criterion

The Verification SOP class can be requested on its own, or in combination with other supported SOP classes.

2.1.3.1.5 Transfer Syntax Selection Policies

The transfer syntax for each DICOM presentation context is negotiated independently. The DCF Storage Server can be configured to support any or all of the transfer syntaxes listed in Table 2.1.3.1.2.1. The order of preference for selecting a transfer syntax is also configurable. This configuration may vary

between associations; however, for a given association, it is shared between all SOP classes or presentation contexts.

2.1.3.2 Real-World Activity—Storage

2.1.3.2.1 Associated Real World Activity—Storage

As instances are received they are copied to the local file system and a record inserted into the local database. If the received instance is a duplicate of a previously received instance, the old file and database record will be overwritten with the new one.

2.1.3.2.2 Presentation Context Table—Storage

The DCF Storage Server will accept association establishment, using one of the presentation contexts listed below. Dicom instances received over this association will be stored on Integrity in the Transfer Syntax they were originally received in.

Table 2.3 - Supported Storage Presentation Contexts

Presentation Context Table					
Abstract Syntax		**Transfer Syntax**		**Role**	**Extended Negotiation**
Name	**UID**	**Name**	**UID**		
See Table 2.1	See Table 2.1	Implicit VR Little Endian	1.2.840.10008.1.2	SCP	None
		Explicit VR Little Endian	1.2.840.10008.1.2.1	SCP	None
		Explicit VR Big Endian	1.2.840.10008.1.2.2	SCP	None
		JPEG Baseline (Process 1)	1.2.840.10008.1.2.4.50	SCP	None
		JPEG Extended (Process 2 & 4)	1.2.840.10008.1.2.4.51	SCP	None
		JPEG Lossless (Process 14)	1.2.840.10008.1.2.4.57	SCP	None
		JPEG Lossless First-Order Prediction	1.2.840.10008.1.2.4.70	SCP	None
		JPEG 2000 Lossless	1.2.840.10008.1.2.4.90	SCP	None
		JPEG 2000	1.2.840.10008.1.2.4.91	SCP	None

2.1.3.2.3 SOP Specific Conformance—Storage

The Integrity Storage Server organizes received SOP Instances into its internal database based on the Patient, Study, Series, and Instance level header information in the received SOP Instances. Integrity organizes SOP Instances into Study entities based on the Study Instance UID included in the SOP Instances. Integrity imposes the following restraint on Stored SOP Instances in order to prevent unintended combination of data for different Patients: received SOP Instances with the same Study UID must contain the exact same Dicom header information for 3 of the following 4 fields: Patient Name, Patient ID, Patient Birth Date, and Patient Sex. Which 3 fields of the 4 that are matched on is configurable. If a SOP Instance for a Study UID is received that has header information in any of the 3 configured fields that is different than header information in an existing (already Stored) Study, the SOP Instance will be rejected and the current Association will be aborted by the Integrity.

For every operation requested on a SOP class of the Storage Service Classes, a status code is returned. They are grouped into success, warning or failure categories (see DICOM PS 3.7-1999):

Success - Indicates that the SCP performed the requested operation as requested.

Warning - Indicates that the SCP has received the request and will process it. However, immediate processing of the request, or processing in the way specified by the SCU, may not be possible. The SCP expects to be able to complete the request without further action by the SCU across the DICOM interface. The exact behavior of the SCP is described within this Conformance Statement.

Failure - Indicates that the SCP is unable to perform the request. The request will not be processed unless it is repeated successfully by the SCU at a later time. The exact behavior of the SCP is described in this Conformance Statement.

Certain errors may be reported for any DIMSE message sent to any SOP Class, in some cases, failures or warnings will only be generated if the Storage Server has message validation enabled. Status codes that are unique to a particular DIMSE message for particular SOP classes are described for each SOP Class in its sub-section entitled DIMSE Specific Behavior. Statuses include:

Status	Code	Description
INVALID_ATTRIBUTE	0106H	Failure status—Indicates an attribute has been received that is not valid for this message. Processing of the message will fail.
UNRECOGNIZED_ATTRIBUTE	0107H	Warning status—Indicates an attribute has been received that is not valid for this message. The attribute will be discarded and processing of the message will continue
DUPLICATE_INSTANCE	0111H	Failure status—The SCU has specified an instance UID for an object that already exists (N-CREATE only). Processing of the message will fail
NO_SUCH_INSTANCE	0112H	Failure status—No object with this instance UID exists. Processing of the message will fail
ATTRIBUTE_OUT_OF_RANGE	0116H	Warning status—An attribute has been received whose value is not within the legal set of possible values (see tables below). If a default has been configured, it will be substituted for the offending value. The validation component can be configured to treat a missing attribute in this manner (i.e. warn and apply default)
INVALID_OBJECT_INSTANCE	0117H	Failure status—The SOP instance UID field in the message is invalid. Processing of the message will fail
NO_SUCH_CLASS	0118H	Failure status—The SOP class UID field in the message is invalid. Processing of the message will fail
MISSING_ATTRIBUTE	0120H	Failure status—A required attribute was not included in the message data set. Processing of the message will fail.
UNRECOGNIZED_OP	0211H	Failure status—The received DIMSE message is not valid for the specified presentation context (see SOP class specific interpretations for this error code below). Processing of the message will fail

2.2 DCF Query Client (FIND-SCU) AE Specification

The DCF FIND-SCU provides Standard Conformance to the following SOP Classes. The Integrity MIIS supports multiple simultaneous C-Find operations to different C-Find SCPs. Each operation is handled in its own thread by a unique C-Find SCU.

Table 2.4– FIND-SCU Supported SOP Classes

SOP Class Name	SOP Class UID	SCU	SCP
Patient Root Query/Retrieve Information Model – FIND	1.2.840.10008.5.1.4.1.2.1.1	Yes	No
Study Root Query/Retrieve Information Model – FIND	1.2.840.10008.5.1.4.1.2.2.1	Yes	No
Patient/Study Only Query/Retrieve Information Model – FIND	1.2.840.10008.5.1.4.1.2.3.1	Yes	No

2.2.1 Association Establishment Policies

2.2.1.1 General

The DCF FIND-SCU initiates but never accepts associations.

The maximum PDU size which can be received by the DCF FIND-SCU is configurable, with a default value of 32,768 (32K) bytes (see Table 5.3.3).

2.2.1.2 Number of Associations

Each FIND-SCU instance initiates a single association at a time.

2.2.1.3 Asynchronous Nature

FIND-SCU will only allow a single outstanding operation on an Association. Therefore, FIND-SCU will not perform asynchronous operations window negotiation.

2.2.1.4 Implementation Identifying Information

The implementation UID for the DCF FIND-SCU will be “1.2.840.114089.1.1.0.X.Y.Z”, where X.Y.Z is the version number (for example, 1.5.0). The implementation version name is also included and has the form “DCF X.Y.Zz” where X.Y.Zz is the full version identifier (for example, 1.4.0b for beta version 1.4.0).

2.2.2 Association Initiation by Real-World Activity

The DCF FIND-SCU attempts to initiate a new association when the user performs the Reconcile action from the user interface.

2.2.3 Real-World Activity – Query Remote AE

2.2.3.1 Description and Sequencing of Activities

A single attempt will be made to query the remote AE. If the query fails, for whatever reason, no retry will be performed.

2.2.3.2 Presentation Context Table – FIND-SCU

Table 2.5– Supported FIND-SCU Presentation Contexts

Presentation Context Table					
Abstract Syntax		Transfer Syntax		Role	Extended Negotiation
Name	UID	Name	UID		
See Table 2.1	See Table 2.1	Implicit VR Little Endian	1.2.840.10008.1.2	SCU	None
		Explicit VR Little Endian	1.2.840.10008.1.2.1	SCU	None
		Explicit VR Big Endian	1.2.840.10008.1.2.2	SCU	None

FIND-SCU will propose multiple Presentation Contexts, one for each of the supported Transfer Syntaxes, and an additional Presentation Context with all of the supported Transfer Syntaxes, in order to determine which Transfer Syntaxes the remote SCP supports, and which it prefers.

2.2.3.3 Extended Negotiation

No extended negotiation is performed.

In particular, relational queries are not supported.

2.2.3.4 SOP Specific Conformance – FIND-SCU

2.2.3.4.1 SOP Specific Conformance to C-FIND SOP Classes

FIND-SCU provides standard conformance to the supported C-FIND SOP Classes.

All queries are initiated at the highest level of the information model.

No CANCEL requests are ever issued.

Unexpected attributes returned in a C-FIND response (those not requested) are processed as if they were requested. Requested return attributes not returned by the SCP are ignored. Non-matching responses returned by the SCP due to unsupported (hopefully optional) matching keys are not filtered locally by the FIND-SCU and thus will still be presented to the user. Duplicate responses are filtered out and not presented to the user.

Specific Character Set is a configurable field that is included in Query operations. The user can define a set of candidate Specific Character Set values to be used when Querying a server. When the automated query is formulated internally, all or a subset of the configured Specific Character Set values will be

included as a multi-valued attribute in the Query request. The values of Specific Character Set supported for user configuration and querying is defined inTable 7.1.

If present in the response, Specific Character Set will be used to identify character sets other than the default character set for display of strings on the user interface.

Types of Matching supported by the C-FIND SCU:

Table 2.6- Study Root Request Identifier for FIND-SCU

Name	Tag	Types of Matching
STUDY Level		
Patient's Name	(0010,0010)	S,*,U
Patient's Birth Date	(0010,0030)	S,R
Patient's Sex	(0010,0040)	S,*,U

An 'S' indicates the identifier attribute uses Single Value Matching, an 'R' indicates Range Matching, an '*' indicates wildcard matching, a 'U' indicates Universal Matching, and an 'L' indicates that UID lists are sent. "NONE" indicates that no matching is supported, but that values for this Element are requested to be returned (i.e. universal matching), and "UNIQUE" indicates that this is the Unique Key for that query level, in which case Universal Matching or Single Value Matching is used depending on the query level.

2.2.3.4.2 Presentation Context Acceptance Criterion

FIND-SCU does not accept associations.

2.2.3.4.3 Transfer Syntax Selection Policies

FIND-SCU prefers explicit Transfer Syntaxes. If offered a choice of Transfer Syntaxes in the accepted Presentation Contexts, it will apply the following priority to the choice of Presentation Context to use for the C-FIND operation:

1. first encountered explicit Transfer Syntax,
2. default Transfer Syntax.

2.2.3.4.4 Response Status Behavior

FIND-SCU will behave as described in the table below in response to the status returned in the C-FIND response command message(s).

Table 2.7 - Response Status Behavior for FIND-SCU and Query Remote AE

Service Status	Further Meaning	Status Codes	Behavior
Refused	Out of Resources	A700	Current query is terminated
Error	Identifier does not match SOP Class	A900	Current query is terminated
	Unable to process	Cxxx	Current query is terminated
Cancel	Matching terminated	FE00	Ignored (should never occur, since

	due to Cancel request		cancels never issued)
Success	Matching is complete - No final Identifier is supplied	0000	Current query is terminated
Pending	Matches are continuing - Current Match is supplied and any Optional Keys were supported in the same manner as Required Keys	FF00	Current query continues
	Matches are continuing - Warning that one or more Optional Keys were not supported for existence and/or matching for this Identifier	FF01	Current query continues

2.2.3.4.5 Association Acceptance Policy

FIND-SCU does not accept associations.

2.3 DCF Worklist Client (MWL-SCU) AE Specification

The DCF MWL-SCU provides Standard Conformance to the following SOP Classes. The Integrity MIIS supports multiple simultaneous C-Find operations to different MWL C-FIND SCPs. Each operation is handled in its own thread by a unique MWL C-FIND SCU.

2.3.1 Association Establishment Policies

2.3.1.1 General

The DCF MWL-SCU initiates but never accepts associations.

The maximum PDU size which can be received by the DCF MWL-SCU is configurable, with a default value of 16,384 (16K) bytes (see Table 5.3.3).

2.3.1.2 Number of Associations

Each MWL-SCU instance initiates a single association at a time.

2.3.1.3 Asynchronous Nature

MWL-SCU will only allow a single outstanding operation on an Association. Therefore, MWL-SCU will not perform asynchronous operations window negotiation.

2.3.1.4 Implementation Identifying Information

The implementation UID for the DCF MWL-SCU will be "1.2.840.114089.1.1.0.X.Y.Z", where X.Y.Z is the version number (for example, 1.5.0). The implementation version name is also included and has the form "DCF X.Y.Zz" where X.Y.Zz is the full version identifier (for example, 1.4.0b for beta version 1.4.0).

2.3.2 Association Initiation by Real-World Activity

The DCF MWL-SCU attempts to initiate a new association when the user performs the Reconcile action from the user interface.

2.3.3 Real-World Activity – Query Remote AE

2.3.3.1 Description and Sequencing of Activities

A single attempt will be made to query the remote AE. If the query fails, for whatever reason, no retry will be performed.

2.3.3.2 Presentation Context Table – MWL-SCU

Table 2.8 – Supported MWL-SCU Presentation Contexts

Presentation Context Table					
Abstract Syntax		**Transfer Syntax**		**Role**	**Extended Negotiation**
Name	**UID**	**Name**	**UID**		
Modality Worklist Information Model – FIND	1.2.840.10008.5.1.4.31	Implicit VR Little Endian	1.2.840.10008.1.2	SCU	None
		Explicit VR Little Endian	1.2.840.10008.1.2.1	SCU	None
		Explicit VR Big Endian	1.2.840.10008.1.2.2	SCU	None

MWL-SCU will propose multiple Presentation Contexts, one for each of the supported Transfer Syntaxes, and an additional Presentation Context with all of the supported Transfer Syntaxes, in order to determine which Transfer Syntaxes the remote SCP supports, and which it prefers.

2.3.3.3 Extended Negotiation

No extended negotiation is performed.

In particular, relational queries are not supported.

2.3.3.4 SOP Specific Conformance – MWL-SCU

2.3.3.4.1 SOP Specific Conformance to C-FIND SOP Classes

MWL-SCU provides standard conformance to the supported C-FIND SOP Classes.

No CANCEL requests are ever issued.

Unexpected attributes returned in a C-FIND response (those not requested) are processed as if they were requested. Requested return attributes not returned by the SCP are ignored. Non-matching responses returned by the SCP due to unsupported (hopefully optional) matching keys are not filtered locally by the MWL-SCU and thus will still be presented to the user. Duplicate responses are filtered out and not presented to the user.

Specific Character Set is a configurable field that is included in Query operations. The user can define a set of candidate Specific Character Set values to be used when Querying a server. When the automated query is formulated internally, all or a subset of the configured Specific Character Set values will be included as a multi-valued attribute in the Query request. The values of Specific Character Set supported for user configuration and querying is defined in Table 7.1.

If present in the response, Specific Character Set will be used to identify character sets other than the default character set for display of strings on the user interface.

Types of Matching supported by the C-FIND SCU:

Table 2.9 – C-FIND Request Identifier for MWL-SCU

Name	Tag	Types of Matching
STUDY Level		
Patient's Name	(0010,0010)	S,*,U
Patient's Birth Date	(0010,0030)	S,R
Patient's Sex	(0010,0040)	S,*,U
Scheduled Procedure Step		
Scheduled Procedure Step Sequence	(0040,0100)	None
> Scheduled Station AET	(0040,001)	S
> Scheduled Procedure Step Start Date	(0040,002)	S,R
> Scheduled Procedure Step Start Time	(0040,003)	S,R
> Modality	(0008,0060)	S
> Scheduled Performing Physician's Name	(0040,0006)	None
> Scheduled Procedure Step Description	(0040,0007)	None
> Scheduled Station Name	(0040,0010)	None
> Scheduled Procedure Step Location	(0040,0011)	None
> Scheduled Protocol Code Sequence	(0040,0008)	None
> Pre-Medication	(0040,0012)	None
> Scheduled Procedure Step ID	(0040,0009)	None

An 'S' indicates the identifier attribute uses Single Value Matching, an 'R' indicates Range Matching, an '*' indicates wildcard matching, a 'U' indicates Universal Matching, and an 'L' indicates that UID lists are sent. "NONE" indicates that no matching is supported, but that values for this Element are requested to be returned (i.e. universal matching), and "UNIQUE" indicates that this is the Unique Key for that query level, in which case Universal Matching or Single Value Matching is used depending on the query level.

2.3.3.4.2 Presentation Context Acceptance Criterion

MWL-SCU does not accept associations.

2.3.3.4.3 Transfer Syntax Selection Policies

MWL-SCU prefers explicit Transfer Syntaxes. If offered a choice of Transfer Syntaxes in the accepted Presentation Contexts, it will apply the following priority to the choice of Presentation Context to use for the C-FIND operation:

1. first encountered explicit Transfer Syntax,
2. default Transfer Syntax.

2.3.3.4.4 Response Status Behavior

MWL-SCU will behave as described in the table below in response to the status returned in the C-FIND response command message(s).

Table 2.10 - Response Status Behavior for MWL-SCU and Query Remote AE

Service Status	Further Meaning	Status Codes	Behavior
Refused	Out of Resources	A700	Current query is terminated
Error	Identifier does not match SOP Class	A900	Current query is terminated
	Unable to process	Cxxx	Current query is terminated
Cancel	Matching terminated due to Cancel request	FE00	Ignored (should never occur, since cancels never issued)
Success	Matching is complete - No final Identifier is supplied	0000	Current query is terminated
Pending	Matches are continuing - Current Match is supplied and any Optional Keys were supported in the same manner as Required Keys	FF00	Current query continues
	Matches are continuing - Warning that one or more Optional Keys were not supported for existence and/or matching for this Identifier	FF01	Current query continues

2.3.3.4.5 Association Acceptance Policy

MWL-SCU does not accept associations.

2.4 DCF Store Client AE Specification

The DCF Storage Client provides standard conformance to the following DICOM 3.0 SOP Classes as an SCU.

2.4.1 Association Establishment Policies

2.4.1.1 General

The DCF Storage Client (SCU) connects to the transport (TCP) port which has been configured and initiates associations to DICOM Storage Servers (SCPs). An accepted association remains connected until the client disconnects by sending either an A-RELEASE-RQ or A-ABORT PDU, or there is an unrecoverable error.

The maximum PDU size which can be sent by the DCF Storage Client is configurable, with a default value of 3,276,800 (3M) bytes (see Table 5.3.3).

2.4.1.2 Number of Concurrent Associations

The DCF Storage Client can support multiple concurrent associations to multiple unique hosts. The total number of concurrent associations is limited to 24. Once this limit is reached, the Storage Client does not initiate any new associations until the number of active associations drops below this limit.

2.4.1.3 Asynchronous Nature

The DCF Storage Client does not support asynchronous operations.

2.4.1.4 Implementation Identifying Information

The implementation UID for the DCF Storage Client is given in the A-ASSOCIATE-RQ PDU. The value for that UID will be “1.2.840.114089.1.1.0.X.Y.Z”, where X.Y.Z is the version number (for example, 1.5.0). The implementation version name is also returned and has the form “DCF X.Y.Zz” where X.Y.Zz is the full version identifier (for example, 1.4.0b for beta version 1.4.0).

All internally generated UID's will be prefixed 1.2.840.xxxxxx, where the identification code “xxxxxx”="114089.1.1" is Laurel Bridge Software's ANSI registered organization identification code for the DCF software. See DICOM PS 3.5-1999, Section 9 for further information.

2.4.1.5 Called Titles

The DCF Storage Client uses a configurable Called AE Title for each Store Destination it opens an association with. See Section 5.4 for more details on this aspect of system configuration.

2.4.2 Association Initiation by Real-World Activity

2.4.3 Real-World Activity—Storage

2.4.3.1 Associated Real World Activity—Storage

A user can select images and presentation states and request them to be sent to multiple destinations (up to 10). Each request is forwarded to the job queue and processed individually.

The DCF Storage Client is invoked by the StoreJobProcessor daemon process that is responsible for processing Dicom Store jobs. A job consists of the instances of a Study or Studies and information about the Storage destination. The DCF Storage Client initiates a C-STORE request to the Storage Destination to store images. If the process successfully establishes an Association to the Storage Destination, it will transfer each instance one after another via the open Association. Status of the transfer is reported through the Integrity User Interface. Jobs are processed serially, rather than concurrently. If the C-STORE Response from the remote Application contains a status other than Success or Warning, the Association is aborted and the related Job is given a failure status. It can be restarted at any time by user interaction with the Integrity User Interface.

The DCF Storage Client attempts to initiate a new Association in order to issue a C-STORE request. If the job contains multiple instances then multiple C-STORE requests will be issued over the same Association.

If the Storage Destination is configured to support Storage Commitment, the DCF Storage Client will, after all images and presentation states have been sent, transmit a single Storage Commitment request (N-ACTION) over the same Association. Upon receiving the N-ACTION response the DCF Storage Client will delay releasing the Association for one second. If no N-EVENT-REPORT is received within this time period the Association will be immediately released. Notification of Storage Commitment success or failure can be received over a separate association at a later time.

Before performing a C-Store operation on a Study, the user of the Integrity MIIS can optionally perform an automated Reconciliation of patient information. The Reconciled patient information will be based on results from a MWL or Q/R Query, and can be manually entered/modified by a user.

The automated query or queries will be performed by the DCF Query Client, which will search for matches for the current Study based on predefined sets of rules in Codonics Matching Profiles. Once the query or queries have been performed, results will be displayed to the user and the user must manually choose to use the results of a particular query, or to enter/modify any of the Reconcilable information manually. The following tables specify which Dicom header fields have the opportunity to be modified before a Study is Stored.

Table 2.11 – Reconcilable Dicom Header Fields

Name	Tag	Source of Initial Value
Patient Name	(0010,0010)	Query
Patient ID	(0010,0020)	Query
Patient Birth Date	(0010,0030)	Query
Patient Sex	(0010,0040)	Query
Study ID	(0020,0010)	Imported Data
Study Date	(0008,0020)	Imported Data
Accession Number	(0008,0050)	Imported Data
Referring Physician Name	(0008,0090)	Imported Data
Study Description	(0008,1030)	Imported Data

Table 2.12 – Updated/Added Dicom Header Fields

Name	Tag	Value
Original Attributes Sequence	(0400,0561)	Original values of reconciled fields
Contributing Equipment Sequence	(0018,A001)	
> Manufacturer	(0008,0070)	Codonics
> Manufacturer's Model Name	(0008,1090)	Integrity
> Device Serial Number	(0008,1000)	<Serial Number>
> Software Version(s)	(0008,1020)	<Software Version>
> Contribution Date Time	(0008,A002)	<Time of Reconciliation>
> Contribution Description	(0008,A003)	Reconciliation

		of data read from disc.
> Purpose of Reference Code Sequence	(0040,A170)	
>Coding Scheme Designator	(0008,102)	DCM
> Code Value	(0008,100)	MEDIM
> Code Meaning	(0008,104)	Portable Media Importer Equipment

When a user of the Integrity MIIS requests that a Study or Studies be Stored, a Dicom association will be opened to each Store Destination. Dicom Instances are then transferred to each Store Destination. If the Store Destination returns a response code that is not Success, the association is aborted and the transfer is flagged as an error.

2.4.3.2 Presentation Context Table—Storage

When operating in pass-thru mode, the DCF Storage Client will attempt to establish an association using one of the presentation contexts listed in the table below. When operating in conversion mode, some transfer syntaxes from the table below are not available.

By default, the DCF Storage Client operates in pass-thru mode. In this mode, it will choose a presentation context based on the Abstract Syntax and Stored Transfer Syntax of the instances to be stored.

The DCF Storage Client can also operate in conversion mode. In this mode, it will convert Instances into a specific outgoing Transfer Syntax rather than preserving the on-disk syntax. Note: when operating in this mode, conversion to the following Transfer Syntaxes from the table below is not supported:

- JPEG Extended (Process 2 & 4) (1.2.840.10008.1.2.4.51)
- JPEG Lossless (Process 14) (1.2.840.10008.1.2.4.57)

Table 2.13 - Supported Storage Presentation Contexts

Presentation Context Table					
Abstract Syntax		**Transfer Syntax**		**Role**	**Extended Negotiation**
Name	**UID**	**Name**	**UID**		
See Table 2.1	See Table 2.1	Implicit VR Little Endian	1.2.840.10008.1.2	SCU	None
		Explicit VR Little Endian	1.2.840.10008.1.2.1	SCU	None
		Explicit VR Big Endian	1.2.840.10008.1.2.2	SCU	None
		JPEG Baseline (Process 1)	1.2.840.10008.1.2.4.50	SCU	None
		JPEG Extended (Process 2 & 4)	1.2.840.10008.1.2.4.51	SCU	None
		JPEG Lossless (Process 14)	1.2.840.10008.1.2.4.57	SCU	None
		JPEG Lossless First-Order Prediction	1.2.840.10008.1.2.4.70	SCU	None

		JPEG 2000 Lossless	1.2.840.10008.1.2.4.90	SCU	None
		JPEG 2000	1.2.840.10008.1.2.4.91	SCU	None

2.4.3.3 SOP Specific Conformance for Storage SOP Class

Table 2.14 - STORAGE C-STORE RESPONSE STATUS HANDLING BEHAVIOR

Service Status	Further Meaning	Error Code	Behavior
Success	Success	0000	The SCP has successfully stored the SOP Instance. If all SOP Instances in a send job have status success then the job is marked as complete.
Refused	Out of Resources	A700-A7FF	The Association is aborted using A-ABORT and the send job is marked as failed. The status meaning is logged and the job failure is reported to the user via the User Interface . This is a transient failure.
Error	Data Set does not match SOP Class	A900-A9FF	The Association is aborted using A-ABORT and the send job is marked as failed. The status meaning is logged and the job failure is reported to the user via the User Interface.
Error	Cannot Understand	C000-CFFF	The Association is aborted using A-ABORT and the send job is marked as failed. The status meaning is logged and the job failure is reported to the user via the User Interface.
Warning	Coercion of Data Elements	B000	Image transmission is considered successful but the status meaning is logged.
Warning	Data Set does not match SOP Class	B007	Image transmission is considered successful but the status meaning is logged.
Warning	Elements Discarded	B006	Image transmission is considered successful but the status meaning is logged.

The behavior of DCF Storage Client during communication failure is summarized in the Table below:

Table 2.15 - STORAGE COMMUNICATION FAILURE BEHAVIOR

Exception	Behavior
Timeout	The Association is aborted using A-ABORT and the send job is marked as failed. The reason is logged and the job failure is reported to the user via the User Interface.
Association aborted by the SCP or network layers	The send job is marked as failed. The reason is logged and the job failure is reported to the user via the User Interface.

A failed send job can be restarted by user interaction through the User Interface.

2.4.4 SOP Specific Conformance for Storage Commitment SOP Class

2.4.4.1 Storage Commitment Operations (N-ACTION)

The DCF Storage Client will request storage commitment for instances if the Remote AE is configured to support Storage Commitment and a presentation context for the Storage Commitment Push Model has been accepted.

The DCF Storage Client does not send the optional Storage Media FileSet ID & UID Attributes or the Referenced Study Component Sequence Attribute in the N-ACTION request.

The behavior of DCF Storage Client when encountering status codes in a N-ACTION response is summarized in the Table below:

Table 2.16 - STORAGE COMMITMENT N-ACTION RESPONSE STATUS HANDLING BEHAVIOR

Service Status	Further Meaning	Error Code	Behavior
Success	Success	0000	The request for storage comment is considered successfully sent. The DCF Storage Client will wait indefinitely for an N-EVENT-REPORT for the Transaction UID.
*	*	Any other status code.	The Association is aborted using A-ABORT and the request for storage comment is marked as failed. The status meaning is logged and reported to the user.

The behavior of DCF Storage Client during communication failure is summarized in the Table below:

Table 2.17 - STORAGE COMMITMENT COMMUNICATION FAILURE BEHAVIOR

Exception	Behavior
Timeout	The Association is aborted using A-ABORT and the send job is marked as failed. The reason is logged and the job failure is reported to the user via the User Interface.
Association aborted by the SCP or network layers	The send job is marked as failed. The reason is logged and the job failure is reported to the user via the User Interface.

2.4.4.2 Storage Commitment Notifications (N-EVENT-REPORT)

The DCF Storage Client is capable of receiving an N-EVENT-REPORT notification if it has successfully negotiated a Presentation Context for the Storage Commitment Push Model (i.e. only associations established with archive devices).

The behavior of DCF Storage Client when receiving Event Types within the N-EVENT-REPORT is summarized in the Table below.

Table 2.18 - STORAGE COMMITMENT N-EVENT-REPORT BEHAVIOUR

Event Type Name	Event Type ID	Behavior
Storage Commitment Request Successful	1	The Study which encompasses all Referenced SOP Instances under Referenced SOP Sequence (0008,1199) is marked with a Storage Commitment Success status.
Storage Commitment Request Complete – Failures Exist	2	The Study which encompasses all Referenced SOP Instances under Referenced SOP Sequence (0008,1199) is marked with a Storage Commitment Failure status. The Failure Reasons are logged and the job failure is reported to the user via the User Interface. A send job that failed storage commitment will not be automatically restarted but can be restarted by user interaction.

The reasons for returning specific status codes in a N-EVENT-REPORT response are summarized in the Table below.

Table 2.19 - STORAGE COMMITMENT N-EVENT-REPORT RESPONSE STATUS REASONS

Service Status	Further Meaning	Error Code	Reasons
Success	Success	0000	The storage commitment result has been successfully received.
Failure	Unrecognized Operation	0211H	The Transaction UID in the N-EVENT-REPORT request is not recognized (was never issued within an N-ACTION request).
Failure	Resource Limitation	0213H	The Transaction UID in the N-EVENT-REPORT request has expired (no N-EVENT-REPORT was received within a configurable time limit).
Failure	No Such Event Type	0113H	An invalid Event Type ID was supplied in the N-EVENT-REPORT request.
Failure	Processing Failure	0110H	An internal error occurred during processing of the N-EVENT-REPORT. A short description of the error will be returned in Error Comment (0000,0902).
Failure	Invalid Argument Value	0115H	One or more SOP Instance UIDs with the Referenced SOP Sequence (0008,1199) or Failed SOP Sequence (0008,1198) was not included in the Storage Commitment Request associated with this Transaction UID. The unrecognized SOP Instance UIDs will be returned within the Event Information of the N-EVENT-REPORT response.

2.4.4.3 Association Acceptance Policy

2.4.4.4 Activity – Receive Storage Commitment Response

2.4.4.4.1 Description and Sequencing of Activities

The DCF Storage Client will accept associations in order to receive responses to a Storage Commitment Request.

A possible sequence of interactions between the DCF Storage Client and an Image Manager (e.g. a storage or archive device supporting Storage Commitment SOP Classes as an SCP) is:

1. The Image Manager opens a new association with the DCF Storage Client.

2. The Image Manager sends an N-EVENT-REPORT request notifying the DCF Storage Client of the status of a previous Storage Commitment Request. The DCF Storage Client replies with a N-EVENT-REPORT response confirming receipt.

3. The Image Manager closes the association with the DCF Storage Client.

The DCF Storage Client may reject association attempts as shown in the Table below. The Result, Source and Reason/Diag columns represent the values returned in the appropriate fields of an ASSOCIATE-RJ PDU (see PS 3.8, Section 9.3.4). The contents of the Source column is abbreviated to save space and the meaning of the abbreviations are:

a) 1 – DICOM UL service-user

b) 2 – DICOM UL service-provider (ASCE related function)

c) 3 – DICOM UL service-provider (Presentation related function)

Table 2.20 - ASSOCIATION REJECTION REASONS

Result	Source	Reason/Diag	Explanation
2 – rejected transient	c	2 – local-limit-exceeded	The (configurable) maximum number of simultaneous associations has been reached. An association request with the same parameters may succeed at a later time.
2 – rejected transient	c	1 – application-context-name-not-supported	No associations can be accepted at this time due to the real-time requirements of higher priority activities (e.g. during image acquisition no associations will be accepted) or because insufficient resources are available (e.g. memory, processes, threads). An association request with the same parameters may succeed at a later time.
1 – rejected permanent	a	2 – temporary-congestion	The association request contained an unsupported Application Context Name. An association request with the same parameters will not succeed at a later time.
1 – rejected permanent	a	7 – called-AE-title-not-recognized	The association request contained an unrecognized Called AE Title. An association request with the same parameters will not succeed at a later time unless configuration changes are made. This rejection reason normally occurs when the association initiator is incorrectly configured and attempts to address the association acceptor using the wrong AE Title.
1 – rejected permanent	a	3 – calling-AE-title-not-recognized	The association request contained an unrecognized Calling AE Title. An association request with the same parameters will not succeed at a later time unless configuration changes are made. This rejection reason normally occurs when the association acceptor has not been configured to recognize the AE Title of the association initiator.
1 – rejected permanent	b	1 – no-reason-given	The association request could not be parsed. An association request with the same format will not succeed at a later time.

2.4.4.4.2 Accepted Presentation Contexts

The DCF Storage Client will accept Presentation Contexts as shown in the Table below.

Presentation Context Table					
Abstract Syntax		**Transfer Syntax**		**Role**	**Ext. Neg.**
Name	**UID**		**Name List**		**UID List**
Storage Commitment Push Model	1.2.840.10008.1.20.1	Implicit VR Little Endian Explicit VR Little Endian	1.2.840.10008.1.2 1.2.840.10008.1.2.1	SCU	None
Verification	1.2.840.10008.1.1	Implicit VR Little Endian Explicit VR Little Endian	1.2.840.10008.1.2 1.2.840.10008.1.2.1	SCP	None

The DCF Storage Client will prefer to select the Explicit VR Little Endian Transfer Syntax if multiple transfer syntaxes are offered. The DCF Storage Client will only accept the SCU role (which must be proposed via SCP/SCU Role Selection Negotiation) within a Presentation Context for the Storage Commitment Push Model SOP Class.

2.4.4.4.3 SOP Specific Conformance for Storage Commitment SOP Class

2.4.4.4.4 Storage Commitment Notifications (N-EVENT-REPORT)

The behavior of DCF Storage Client when receiving Event Types within the N-EVENT-REPORT is summarized in Table 2.18.

The reasons for returning specific status codes in a N-EVENT-REPORT response are summarized inTable 2.19.

2.4.4.4.5 SOP Specific Conformance for Verification SOP Class

The DCF Storage Client provides standard conformance to the Verification SOP Class as an SCP. If the C-ECHO request was successfully received, a 0000 (Success) status code will be returned in the C-ECHO response. Otherwise, a C000 (Error – Cannot Understand) status code will be returned in the C-ECHO response.

2.4.4.4.6 Association Acceptance Policy

The DCF Storage Client accepts associations for Storage Commitment as described above.

3 COMMUNICATION PROFILES

3.1 TCP/IP Stack

The DCF Storage Client and Query Client provide DICOM 3.0 TCP/IP Network Communication Support as defined in part 8 of the standard.

3.2 Physical Media Support

The DCF Storage Client and Query Client support DICOM over any IP network supported by the Operating System running on the Codonics device (computer) where they are installed and running. The typical medium is Ethernet.

4 EXTENSIONS/SPECIALIZATIONS/PRIVATIZATIONS

The DCF does not define any private elements.

5 CONFIGURATION

5.1 AE Title Presentation Address Mapping

AE Titles are used only during association negotiation with remote Storage Servers. That is, no DIMSE messages or data sets reference other hosts or servers using AE Titles as is common with certain other SOP classes. There is no need for AE Title to presentation address mapping with the Storage SOP classes.

5.2 DCF Storage Client Configurable Parameters—Global

The following items are configurable on a global basis and apply to all associations initiated by the DCF Storage Client.

Table 5.1 - Global Configuration Parameters

Parameter Name	Range	Defaults	Comments
debug_flags	N/A	0x00000	This parameter is intended for Codonics developer and field-service use only.

5.3 DCF Storage Client Configurable Parameters—Per Association

Each software component has debug flags that may be set for diagnostic purposes; these flags may be dynamically accessed via a browser based interface, but are not listed below. Other configuration parameters which are used to control SCU internal behavior are omitted from the lists as well.

The SOP Classes that the DCF Storage Client supports are configured by their presence in the appropriate configuration file. See Section 1.2 for additional description of the configuration process. Any of the SOP Classes from Table 2.1 can be individually enabled or disabled in this way.

The transfer syntax for each DICOM presentation context is negotiated independently. The DCF Storage Client can be configured to support any or all of the transfer syntaxes listed in Table 2.13. The order of preference for selecting a transfer syntax is also configurable. This configuration may vary between associations; however, for a given association, it is shared between all SOP classes or presentation contexts.

5.4 DCF Storage Client Configurable Parameters—Per Store Destination

The Codonics Integrity supports multiple parameter sets known as Store Destination Profiles, which affect the parameters associated with a given Store Job. These are general-purpose, configurable parameter sets that are described in detail in the Integrity User's Manual. When a Store Job is requested, the

Storage Client that is created to service a C-Store operation uses the IP Address, port, and Called AE Title specified in the Store Destination Profile when connecting to the remote host.

6 MEDIA INTERCHANGE

6.1 IMPLEMENTATION MODEL

6.1.1 Application Data Flow

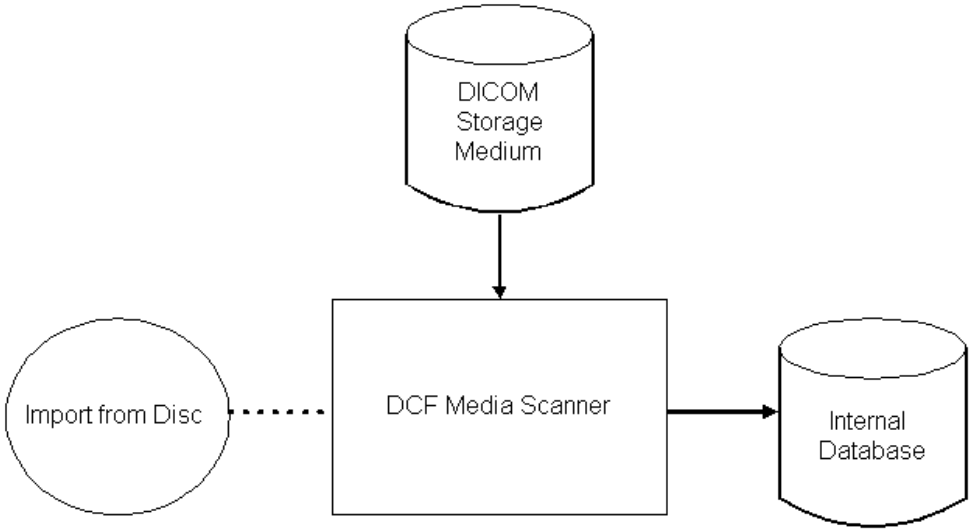


Figure B.6.1-1
APPLICATION DATA FLOW DIAGRAM FOR MEDIA IMPORT

— The DCF Media Scanner imports Dicom Instances from an optical disc Storage medium (CD or DVD) into an internal database. It is associated with the local real-world activity “Import from Disc”. The activity “Import from Disc” is performed automatically upon the user inserting an optical disc storage medium into the optical disc drive of the Integrity device.

6.1.2 Functional Definition of AEs

6.1.2.1 Functional Definition of DCF Media Scanner

The Media Scanner application acts as a Dicom File Set Reader (FSR). Activation of the “Import from Disc” function will cause the Media Scanner application to Read the Dicom data included on the Dicom Storage Medium and import whatever Dicom SOP Instances that it locates into an internal database. The database groups SOP Instances by Patient, Study, Series and Instance identities. When the full set of discovered files has been committed to the internal database, the optical disc is ejected.

6.1.3 Sequencing of Real-World Activities

The Media Scanner will wait indefinitely for a media to be inserted before starting to read the inserted media.

The sequence of events for a typical transaction are listed below:

User inserts optical disc.

Media Scanner discovers DICOM SOP Instances on the media.

Media Scanner imports DICOM SOP Instances to internal database.

Media Scanner ejects optical disc.

6.1.4 File Meta Information Options

File Meta Information (Group 2) tags found in imported data will be discarded when the SOP Instances are stored to another device.

6.2 AE SPECIFICATIONS

6.2.1 DCF Media Scanner Specification

The DCF Media Scanner provides standard conformance to the DICOM Interchange Option of the Media Storage Service Class. The Application Profiles and roles are listed below:

Table 6.1

APPLICATION PROFILES, ACTIVITIES AND ROLES FOR OFFLINE-MEDIA

Application Profiles Supported	Real World Activity	Role	SC Option
STD-GEN-CD	Import from CD-R	FSR	Interchange
STD-GEN-DVD-RAM	Import from DVD-R	FSR	Interchange

6.2.1.1 File Meta Information for the Application Entity

The Source Application Entity Title included in the File Meta Header is configurable (see section 5.4).

6.2.1.2 Real-World Activities

6.2.1.2.1 Activity – Import from Disc

The DCF Media Scanner acts as an FSR using the interchange option when requested to import SOP Instances from an optical disc medium to the local database.

If the DCF Media Scanner encounters Dicom Instances on the media for the same study that have the same SOP Class but different on-media Transfer Syntaxes, Media Scanner will convert one or both Instances to the same Transfer Syntax when imported to the Integrity database. If both Instances are originally in a lossy format, then both instances will be converted to Explicit Little Endian when importing.

If the DCF Media Scanner encounters Dicom Instances on the media that have the same Instance UID as other instances on the media, it will generate a new Instance UID for each duplicate before importing the Instances into its local database. Referenced Instance UIDs in other Instances on the media will not be modified to reflect the generated UID.

All internally generated UID's will be prefixed 1.2.840.xxxxxx, where the identification code “xxxxxx”="114089.1.1" is Laurel Bridge Software's ANSI registered organization identification code for the DCF software. See DICOM PS 3.5-1999, Section 9 for further information.

6.2.1.2.2 Media Storage Application Profiles

The Media Scanner supports the STD-GEN-CD and STD-GEN-DVD-RAM Application Profiles.

6.2.1.2.3 Options

Table 6.2 - Supported Data Medium Presentation Contexts

Abstract Syntax		Transfer Syntax	
Name	**UID**	**Name**	**UID**
See Table 2.1	See Table 2.1	Implicit VR Little Endian	1.2.840.10008.1.2
		Explicit VR Little Endian	1.2.840.10008.1.2.1
		Explicit VR Big Endian	1.2.840.10008.1.2.2
		JPEG Baseline	1.2.840.10008.1.2.4.50
		JPEG Extended	1.2.840.10008.1.2.4.51
		JPEG Lossless	1.2.840.10008.1.2.4.57
		JPEG Lossless First-Order Prediction	1.2.840.10008.1.2.4.70
		JPEG 2000 Lossless	1.2.840.10008.1.2.4.90
		JPEG 2000	1.2.840.10008.1.2.4.91

6.3 AUGMENTED AND PRIVATE APPLICATION PROFILES

Integrity does not support any augmented or private application profiles.

7 SUPPORT OF EXTENDED CHARACTER SETS

7.1 Overview

The Integrity MIIS supports all extended character sets defined in the DICOM 2004 standard, including single-byte and multi-byte character sets as well as code extension techniques using ISO 2022 escapes.

The Integrity MIIS will display the correct symbol for all names and strings found in the Query Data received over the network and in the SOP Instances imported into the local database.

The Integrity MIIS can be configured to use a particular Specific Character Set in Query requests sent to a Query or MWL SCP.

If the Integrity MIIS is configured to use a particular Specific Character Set in Query requests, the Integrity MIIS will also use that Specific Character set when Storing studies, replacing any Specific Character set that may already exist in the data of the study. Changing the Specific Character Set in this way will occur whether or not the study has been Reconciled.

7.2 Character Sets

In addition to the default character repertoire, the Defined Terms for Specific Character Set in the table below are supported:

Table 7.1 – SUPPORTED SPECIFIC CHARACTER SET DEFINED TERMS

Character Set Description	Defined Term
Latin alphabet No. 1	ISO_IR 100
Latin alphabet No. 2	ISO_IR 101
Latin alphabet No. 3	ISO_IR 109
Latin alphabet No. 4	ISO_IR 110
Cyrillic	ISO_IR 144
Arabic	ISO_IR 127
Greek	ISO_IR 126
Hebrew	ISO_IR 138
Latin alphabet No. 5	ISO_IR 148
Japanese	ISO_IR 13
Thai	ISO_IR 166
Default repertoire	ISO 2022 IR 6
Latin alphabet No. 1	ISO 2022 IR 100
Latin alphabet No. 2	ISO 2022 IR 101
Latin alphabet No. 3	ISO 2022 IR 109
Latin alphabet No. 4	ISO 2022 IR 110
Cyrillic	ISO 2022 IR 144
Arabic	ISO 2022 IR 127
Greek	ISO 2022 IR 126
Hebrew	ISO 2022 IR 138
Latin alphabet No. 5	ISO 2022 IR 148
Japanese	ISO 2022 IR 13
Thai	ISO 2022 IR 166
Japanese	ISO 2022 IR 87
Japanese	ISO 2022 IR 159
Korean	ISO 2022 IR 149
Chinese	GB18030
Unicode in UTF-8	ISO_IR 192

7.3 Character set Configuration

Whether or not characters are displayed correctly and stored to other devices correctly depends on the proper configuration of the Integrity MIIS profiles. Consult the Integrity User's Manual for information on configuring settings related to character sets in the Locale and Query Profiles.

8 CODES AND CONTROLLED TERMINOLOGY

The DCF uses the Baseline Context Groups defined in DICOM PS 3.3-1999. No alternative or private Context Groups or Coding Schemes are used.

9 SECURITY

9.1 Security Profiles

None supported.

9.2 Association level security

None supported.

9.3 Application level security

None supported.

10 REFERENCES

Quoted below are references to and portions of the sections of DICOM PS 3.0-1999 that relate to the preparation of a conformance statement. In addition, a list of DICOM Change Proposals that have been incorporated within this release of the DCF Storage Client is provided.

10.1 DICOM PS 3.2-1999, Annex A (Normative) DICOM Conformance Statement Template

This Annex is a template which shall be used to generate a DICOM Conformance Statement. A DICOM Conformance Statement shall begin with an introduction which sets the framework. The introduction shall describe the implementation and how, in general terms, it uses DICOM to achieve its purposes. …

10.2 DICOM PS 3.2-1999, Annex B (Informative) DICOM Conformance Statement Sample

This Annex is a sample DICOM Conformance Statement for a fictitious DICOM Implementation. It is presented as an example only. The viability of such an implementation should not be assumed as the purpose of this Annex is only to guide the writer of DICOM Conformance Statements by providing a Conformance Statement example. …

— End of Document —