Digital Imaging and Communications in Medicine (DICOM)

Supplement xxx: Conformance Requirements, Scenarios, Test Cases, and Conformity Assessment Reports

Prepared by WG-31 – Conformance

DICOM Standards Committee
1300 N. 17th Street Suite 900
Rosslyn, Virginia 22209 USA

VERSION: Draft

Table of Contents

Document History

Version	Date	Contents
01	2017-02-24	Initial version, includes a) setting up global structure and b) contents on requirements.
02	2017-06-23	Reworked comments. Split requirements over parts.
03	2017-09-28	Added sections for Web Services

Scope and Field of Application

This document is a Supplement to the DICOM Standard. It is an extension to the following parts of the published DICOM Standard:

PS 3.1	Introduction and Overview
PS 3.2	Conformance
PS 3.8	Network Communication Support for Message Exchange

This supplement to the DICOM Standard extends the standard with Conformity Assessment aspects, including an extension of the requirements, and new sections on test scenarios, test cases, and product conformity assessment reporting.

This together forms a test framework that, when used, will guarantee that a well verified product – conforming to its DICOM Conformance Statement – will be released, with proper evidence of the associated validation activities.

Limitations of the Current Standard

Currently, section 7 of PS3.2 is about Conformance Requirements. However, that part is quite short and incomplete. Furthermore, the DICOM Standard lists neither scenarios, test cases, nor the procedure of selecting applicable test cases given a DICOM Conformance Statement. Finally, no guidance is given on how to report on product Conformity Assessment.

To Do

What	Status	Notes
Revisit section 6.2 Conformance in PS3.1 Introduction and Overview	In progress	
Rewrite section on requirements.	In progress	To be split for every part
Write section on test scenarios.	To be started	
Write section on test cases.	To be started	
Write section on procedure to select applicable test cases given a DICOM Conformance Statement	To be started	
Write section on conformity assessment reporting.	To be started	

Open Issues

#	Description
1	How to ensure traceability from assessment to the requirements in the DICOM Standard? Can they be tagged in a certain way so that they can be extracted / referred to?
2	PS3.1 states, rightfully, that security measures are part of a DCS. Do we need a section of conformance requirements on security?
3	Can it be exhaustive, are we able to refer to all requirements? E.g. rules will be hard to have all separate tags. Do we need that?

Closed Issues

#	Description
1	

Changes to the Standard

Update PS3.1, Section 6.2 as follows:

PS3.1 – 6.2 PS3.2 Conformance

PS3.2 of the DICOM Standard defines principles that implementations claiming conformance to the Standard shall follow:

- Conformance requirements. PS3.2 specifies the general requirements that must be met by any implementation claiming conformance. It references the conformance sections of other parts of the Standard.
- Conformance Statement. PS3.2 defines the structure of a Conformance Statement. It specifies the information that must be present in a Conformance Statement. It references the Conformance Statement sections of other parts of the Standard.
- **Conformance test scenarios. PS3.2 defines different usage scenarios …**
- **Conformance test cases. PS3.2 defines the test cases …**
- **Conformance claim assessment. PS3.2 defines how to identify the test cases that have to be executed to assess a conformance claim.**
- **Conformity assessment reporting. PS3.2 defines how conformity assessment is reported by giving an assessment report template.**

Commented [MJ1]: No specifics, no system dependency.

Commented [MJ2]: E.g. MPPS as SCU, QR as SCP, Storage as SCU, …

Commented [MJ3]: E.g. duplicate image storage, storage with wrong system type, …

Commented [MJ4]: E.g. do duplicate image storage for CT, do duplicate image storage for MR, …

PS3.2 does not specify a testing/validation procedure to assess an implementation's conformance to the Standard**, although the requirements, scenarios, test cases, conformance claim assessment, and the conformity assessment report template are applicable ingredients of such a procedure**.

Figure 6.2-1 and Figure 6.2-2 depict the construction process for a Conformance Statement for both network communication and media exchange. A Conformance Statement consists of the following parts:

Commented [JM5]: Redraw as one picture, and include parts 18-20 (web services, application hosting, and imaging reports).

Commented [MJ6R5]: This is plain maintenance of this section, not related to the subject at hand.

- Set of Information Objects that is recognized by this implementation
- Set of Service Classes that this implementation supports
- Set of communications protocols or physical media that this implementation supports
- Set of security measures that this implementation supports.

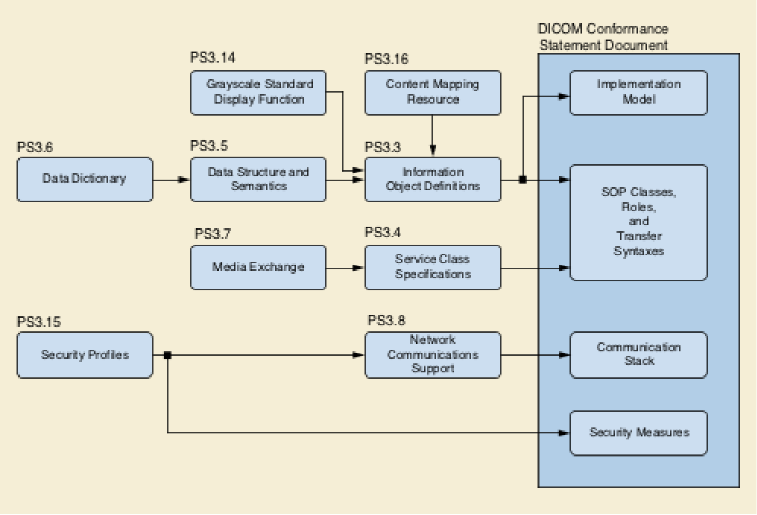
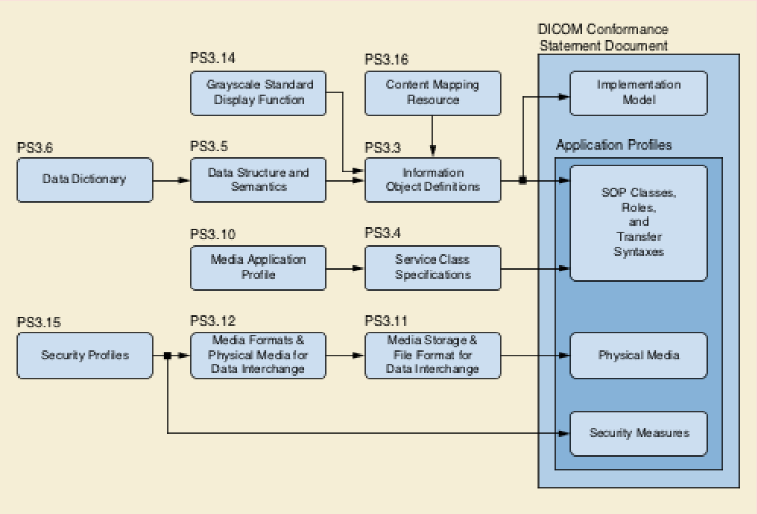

DICOM Conformance Statement Document
PS3.14
Grayscale Standard Display Function
PS3.16
Content Mapping Resource
Implementation Model
PS3.6
Data Dictionary
PS3.5
Data Structure and Semantics
PS3.3
Information Object Definitions
SOP Classes, Roles, and Transfer Syntaxes
PS3.7
Media Exchange
PS3.4
Service Class Specifications
PS3.15
Security Profiles
PS3.8
Network Communications Support
Communication Stack
Security Measures

Figure 6.2-1. Construction Process for a Network Conformance Claim


DICOM Conformance Statement Document
PS3.14
Grayscale Standard Display Function
PS3.16
Content Mapping Resource
Implementation Model
Application Profiles
PS3.6
Data Dictionary
PS3.5
Data Structure and Semantics
PS3.3
Information Object Definitions
SOP Classes, Roles, and Transfer Syntaxes
PS3.10
Media Application Profile
PS3.4
Service Class Specifications
PS3.15
Security Profiles
PS3.12
Media Formats & Physical Media for Data Interchange
PS3.11
Media Storage & File Format for Data Interchange
Physical Media
Security Measures

Commented [JM7]: Are application profiles only relevant for media? Or is this PS3.11? Should be in the picture!

Figure 6.2-2. Construction Process for a Media Conformance Claim

135

Replace PS3.2, Section 7 with:

PS3.2 – 7 Conformance Requirements

The DICOM Standard facilitates interoperability of medical imaging equipment by a three level specification:

- Exchange level services
- Application level services
- Information Object definitions

A system shall support all three levels in one or more ways to be DICOM conformant. Conformance of a system to these levels cannot be assessed in isolation, but should always be combined.

Note that not all combinations of exchange level services and application level services do apply. Table 7-1 shows the mapping and the relevant sections.

		Exchange level services (7.1)		
		Network Communication Services (7.1.1)	**Web services (7.1.2)**	**File Services (7.1.3)**
Application Level Services (7.2)	**Verification (7.2.1)**	PS 3.7, annex X.1	PS 3.18, annex X.1	*Not applicable*
	Query / Retrieve (7.2.2)	PS 3.7, annex X.2	PS 3.18, annex X.2	*Not applicable*
	Storage (7.2.3)	PS 3.7, annex X.3	PS 3.18, annex X.3	PS 3.10, annex X.1
	Storage Commit (7.2.4)	PS 3.7, annex X.4	*?*	*Not applicable*
	Study management (7.2.5)	PS 3.7, annex X.5	PS3.18, annex X.4	*Not applicable*
	Print (7.2.6)	PS3.7, annex X.6	*Not yet available*	*Not applicable*

Table 7-1 Support of Application Level Services by Exchange Level Services

7.1 Exchange Level Services

This section describes the different types of services that are used by the Exchange Level to transfer the information from the Application Level Services to the receiver of the information. The services that will be described are:

- Network Communication Services
- Web Services
- File Services

7.1.1 Network Communication Services

The Network Communication Services use the standard TCP/IP network protocol to exchange messages. This exchange is described in two layers: the TCP/IP transport layer and the DICOM Upper Layer protocol for TCP/IP (UL). The UL is specified as:

- Set up a connection between the two systems
  - A-ASSOCIATE
- Exchange the data that is required by the application level service
  - P-DATA
- Close the connection between the two systems
  - A-RELEASE
  - A-ABORT
  - A-P-ABORT

For every type of Application Level Service the sequence of calling the UL services is predefined. A full state machine, describing the possible states, actions and transitions, is given in PS3.8 Section 9.2:

Commented [JM8]: Given the amount of work, the current and envisioned structure, a rewrite is sensible. Naturally, all current items in section 7 need to be addressed.

Commented [MJ9]: Philosophy of this section: this describes the generic requirements; the test scenarios describe what to use in what role.

Commented [MJ10]: Open issue for WG27: We can use the capabilities interface here, but shouldn't we have a separate verification service?

Commented [MJ11]: Open issue: Should we have commit as a separate service is it part of study management?

Commented [MJ12]: Open issue for WG27: Not sure whether we have a storage commit with web services.

Commented [MJ13R12]: We do not have a commit using web services. This is a limitation.

Commented [MJ14]: Revisit this table to make references to new sections in each part.

Commented [MJ15]: Media exchange?

Commented [MJ16]: Too descriptive? Repetitive?

Commented [MJ17R16]: There should be some level of repetition, otherwise you will only have references. Not too much, but that is going to be a balancing act. We should come to a common understanding of what is the appropriate level.

- Machine states are defined in PS3.8 Section 9.2.1.
- State machine actions are defined in PS3.8 Section 9.2.2.
- State transition table is defined in PS3.8 Section 9.2.3.

In the State transition table, the normal order is shown next to the exceptional transitions. The Abort message is a message coming as exceptional message that can come from both systems involved.

At lower level each item has a specific set of messages to achieve its goal. For instance, setting up a connection requires the following steps in the A-ASSOCIATE:

- ASSOCIATE REQUEST, giving information about the calling application and its capabilities.
- ASSOCIATE ACCEPT, responding with the answer to the capabilities that the receiving system is able to support.
- ASSOCIATE REJECT, responding that the system cannot handle the association.

The A-ASSOCIATE is exchanging information on the capabilities for both systems. Based on this information it is known what data can be exchanged and how it should be encoded. Extended negotiation for a specific service class can be used to allow more detailed exchange on capabilities during the creation of the Association.

The P-DATA message is a container where the exchanged data is encoded which is based on requests and responses. The number of P-DATA messages is depending on the type of application service using the Network Communication Service.

The normal closure of an association is done by means of an A-RELEASE message. The A-ABORT and A-P-ABORT should only be used to close a connection when the normal message flow can't be completed by either of the two systems.

The A-ABORT is coming from Application Level Services. The A-P-ABORT is coming from the lower levels and is used to indicate problems in services at the lower levels.

The different commands that build the Network Exchange Level are specified in detail in PS3.8.

7.1.1.1 A-ASSOCIATE

Association setup is depending on the application and it is necessary to test this for the different types of service classes. The requirement is correct setting up of the association for all types of service classes. The full specification can be found in PS3.8 Section 7.1 A-ASSOCIATE Service.

7.1.1.2 P-DATA

P-DATA exchange can be repeated multiple times. Test aspects are the different types of P-Data block their sequence, usage and handling. The full specification can be found in PS3.8 Section 7.6 P-DATA Service.

7.1.1.3 A-RELEASE

A-RELEASE shall close the connection and end the application service. The full specification can be found in PS3.8 Section 7.2 A-RELEASE Service.

7.1.1.4 A-ABORT

A-ABORT shall close the connection and end the application service. After this the system shall be in the initial state. The full specification can be found in PS3.8 Section 7.3 A-ABORT Service.

7.1.1.5 A-P-ABORT

A-P-ABORT shall close the connection and end the application service. After this the system shall be in the initial state. The full specification can be found in PS3.8 Section 7.4 A-P-ABORT Service.

7.1.2 Web Services

The Web Services use the standard HTTP network protocol to exchange messages.

…

7.1.3 File Services

…

7.2 Application Level Services

The application exchange of data can take place through Network, Web of File Services.

Network and web connections require a direct connection between the Storage SCU and the Storage SCP. Therefore, it is immediately known whether the data needs a specific format to allow the Storage SCP to handle it correctly (for storage).

For files, the data is stored without interaction with the system reading the data; hence, only a SCU can be identified. Therefore, there might be a problem at the moment of usage, as it is unknown whether the system can handle the format used during storage.

7.2.1 Verification

…

7.2.2 Query / Retrieve

…

7.2.3 Storage

The Storage Service enables systems to exchange information objects. There are many kinds of objects, all defined in PS3.3 Information Objects Definition. They include, for instance images and waveforms captured of a patient.

7.2.4 Storage Commit

…

7.2.2 Study Management

…

7.2.6 Print

…

7.4 Data Object Definitions

Commented [MJ18]: Move entire section to an Annex in PS 3.3?

7.4.1 Data Encoding

7.4.1.1 Value Encoding

A Data Set is constructed by encoding the values of Attributes specified in the Information Object Definition (IOD) of a Real-World Object. The specific content and semantics of these Data Elements are specified in Information Object Definitions (see PS3.3 Section 6).

The Value Representation of Data Elements is an essential item of the DICOM Standard. The Value Representation is describing how the content of the Data Element shall be encoded in the data stream. The full set of VR's is described in PS 3.5 Section 6.2, which includes the Definition, Character Repertoire and Length of each VR. During the testing it is important to check that the correct encoding is used for all VRs.

Other items that are important in this context are:

- Support of Character Repertoires to be able to support all languages (PS 3.5 Section 6.1)
- Difference between Enumerated Values and Defined Terms (PS 3.5 Section 6.3)
- Value Multiplicity and Delimitation (PS 3.5 Section 6.4)

- Maximum length of Data Elements (PS 3.5 Table 6.2-1)

7.4.1.1.1 Value Representation

Attributes shall be encoded according the applicable Value Representation.

7.4.1.1.2 Character Sets used

The used Character Sets shall match the Character Set information encoded in the object.

7.4.1.1.3 Enumerated Values

Attributes specified as Enumerated Value shall use only the specified values.

7.4.1.1.4 Defined Terms

Attributes specified as Defined Terms might contain additional values, additional values defined in the DCS shall be accepted.

7.4.1.1.5 Value Multiplicity

Attributes shall adhere to their specified multiplicity.

7.4.1.1.6 Attribute Delimiters

Attributes with multiple values shall use the Delimitation defined for the specific Value Representation.

7.4.1.1.7 Attribute Length

Attributes shall adhere to the length rules specified for the specific Value Representation.

7.4.1.2 Data Set

A Data Set represents an instance of a real world Information Object and is constructed of Data Elements. Data Elements contain the encoded Values of Attributes of that object. The specific content and semantics of these Attributes are specified in Information Object Definitions.

For assessing the conformance, the encoding structure of the individual data elements is the lowest level that needs to be assessed.

7.4.1.2.1 Standard Groups

Standard groups (0000,*eeee*), (0002,*eeee*), (0004,*eeee*) and (0006,*eeee*) shall not be used in objects.

7.4.1.2.2 Private Groups

Private groups (0001,*eeee*), (0003,*eeee*), (0005,*eeee*), (0007,*eeee*) and (FFFF,*eeee*) shall not be used in objects.

7.4.1.2.3 Private Data Elements

Private Data elements shall use the identification of the Private Group mechanism according the standard.

Commented [JM19]: Insert reference.

7.4.1.2.4 Explicit Value Representation

Explicit Value Representation encoding shall store the VR information in the element structure in the objects.

7.4.1.2.5 Implicit Value Representation

Implicit Value Representation encoding shall not store the VR information in the element structure in the objects.

7.4.1.2.6 Implicit and Explicit coexistence

Implicit and Explicit Value Representation of Data Elements shall not coexist.

7.4.1.2.7 Little Endian

Encoding of Little Endian byte ordering shall be according the standard.

7.4.1.2.8 Big Endian

Big Endian byte ordering shall be according the standard.

7.4.1.2.9 Group Length

The system shall be able to handle elements with Group Length present as well as absent.

7.4.1.2.10 Sequence Length

The system shall be able to handle elements with Sequence Length defined as well as undefined format.

7.4.1.2.11 Data Element Type

Presence of Data elements shall be as specified in the Data object according the rules for presence of type 1, 1C, 2, 2C and 3.

7.4.1.2.12 Sequence multiplicity

System shall handle Sequence Elements in accordance with the specified multiplicity

7.4.1.2.13 Classic objects

The system shall be able to encode Classic (single frame) objects according the standard.

7.4.1.2.14 Enhanced Multiframe Objects

The system shall be able to encode Enhanced Multi frame objects according the standard.

7.4.1.3 Encoding of Pixel, Overlay and Waveform Data

Correct Encoding of Pixel, Overlay and Waveform Data have special rules that are described in PS 3.5 Section 8.

More details on how the Transfer Syntax is used to encode Data Sets can be found in PS 3.5 Section 10 and Annex A.

7.4.1.3.1 Overlay Plane

The system shall be able to handle Overlay Planes as per the standard.

7.4.1.3.2 Curve

The system shall be able to handle Curve information as per the standard.

7.4.1.3.3 Pixel Data

Pixel Data shall be encoded according the transfer syntax.

7.4.1.3.4 Waveform

The system shall be able to handle Waveform information as per the standard.

7.4.2 Information Object Definitions

An IOD shall conform to what has been described about it in PS3.3.

Add to PS3.2, Section 8:

PS3.2 – 8 Test Scenarios

…

Commented [MJ20]: Propose to structure it as per the DICOM parts structure. Any other options?

8.18 Web Services

…

8.18.x QIBA

1. QIBA as User Agent
2. QIBA as Origin Server

…

Add to PS3.2, Section 9:

PS3.2 – 9 Test Cases

…

9.18.x QIBA

Add to PS3.2, Section 10:

PS3.2 – 10 Assessing the Conformance Claim

Which tests have to be executed based on the conformance claim? This can for instance mean to execute multiple times the same test case for different supported IODs or character sets.

Add to PS3.2, Section 11:

PS3.2 – 11 Reporting Conformity Assessment

…

Add to PS 3.8, Annex X

P.S 3.8, Annex X – Conformance Requirements

X.1 Verification Service using Network Communication Services

…

X.2 Query/Retrieve Service using Network Communication Services

…

X.3 Storage Service using Network Communications Service

The Storage Service shall be able to execute a Network Store operation.

Commented [MJ21]: Requirement; next subsections are subrequirements.

The Storage Service using Network Communication Services will have three stages:

1. Set-up of the Association
2. Exchange of the Data Objects
3. Closure of the Association

X.3.1 Storage Network Association

Association establishment is used to negotiate the type of data to be exchanged and how the data will be encoded. The full description of the Association Negotiation is specified in PS3.7 Annex D. The Storage Service as SCU will be using the Association Request. The Storage Service as SCP will respond with either an Association Accept or an Association Reject message.

The following items are important variation points for the Association Request Negotiation:

1. Presentation Context(s)
   - Proposed (Meta) SOP Classes
   - Associated Transfer Syntaxes
2. DIMSE parameters (such as max PDU length supported and Implementation Class UID)
3. Extended Negotiation parameters as specified in PS 3.4 Annex B.3.1

Allowed Standard SOP classes can be found in PS 3.4 Annex B.5 Standard SOP Classes.

The specification of the Transfer Syntaxes can be found in PS3.5 Annex A Transfer Syntax Specifications.

The Association Response from the Storage Service SCP will give an overview of the SOP Classes and Transfer Syntaxes that are supported by the SCP. The Storage Service SCU will decide based on the reply which data can be send and which Transfer Syntax will be used.

X..3.1.1 Storage Network SOP Classes

The system shall be able to build up the association for different SOP Classes

X.3.1.2 Storage Network Transfer Syntaxes

The system shall be able to build up the association for different Transfer Syntaxes

X.3.1.3 Storage Network DIMSE parameters

The system shall be able to build up the association taking into account the different DIMSE parameters

X.3.1.4 Storage Extended Negotiation

During association setup it should be possible to perform extended negotiation on the created connection.

This requirement will be out of scope currently as none of the Philips products is supporting extended negotiation.

X.3.2 Storage Network Store

The C-STORE service is used by the Storage Service SCU to store a composite SOP Instance on the peer Storage Service SCP. It is a confirmed service that can be repeated one or more times within a single Association. This way allowing the transfer of a full series of images in a single association.

Commented [MJ22]: N-STORE too

The full description and associated parameters of the C-STORE Message can be found in PS 3.7 section 9.1.1.

PS 3.4 Annex B gives a normative description of the Storage Service Class, here items like the level of storage as SCP (0 (Local), 1(Base) or 2 (Full)) is described here. Also more details on Association Negotiation can be found in this Annex.

Normal flow will be that after transferring an object the Storage Service SCP will process that and return the appropriate response. The Storage Service SCP may return a C-STORE response with the status of Failed or Refused before the entire object has been transmitted by the Storage Service SCU. A C-STORE response with the status of Success or Warning shall not be returned until the entire object has been received by the Storage Service SCP. A Storage Service SCP can give and immediate answer after receiving or process the object first before acknowledge the correct receipt of the object. This is up to the receiving application.

X.3.2.1 Storage Network single store

The system shall be able to handle a single Store request

X.3.2.2 Storage Network multi store single association

The system shall be able to handle multiple Store requests within a single association

X.3.2.3 Storage Network with Failure status result

The system shall be able to handle the failure of a Store request

X.3.2.4 Storage Network with Warning status result

The system shall be able to handle a Store request with Warning status result

X.3.3 Storage Network Close Association

The A-RELEASE Service is invoked by the Storage Service SCU to request the orderly termination of the Association with the Storage Service SCP.

The Storage Service SCU and SCP can use the A-ABORT Service to terminate the Association anywhere during the C-STORE operation.

The A-P-ABORT will be used by lower level services to finalize the association at any moment during the connection if needed.

X.3.3.1. Storage Network Association closure

The system shall end the Store application and return to a state where the used association is closed and there are no open or pending activities.

X.3.3.2. Storage Network Association closure with an A-P-ABORT

After a A-P-ABORT the system shall end in a state where the used association is closed and there are no open or pending activities

X.3.3.3. Storage Network Association closure with an A-ABORT

After an A-ABORT the system shall end in a state where the used association is closed and there are no open or pending activities

X.4 Storage Commit Service using Network Communication Services

…

X.5 Study Management Service using Network Communication Services

…

X.6 Print Service using Network Communications Services

…

Add to PS 3.10, Annex X

PS 3.10, Annex X – Conformance Requirements

X.1 Verification Service using Web Services

…

X.2 Query/Retrieve Service using Web Services

…

X.3 Storage Service using Web Services

…

X.4 Study Management Service using Web Services

…

Add to PS 3.18, Annex X

PS3.18 Annex X – Conformance Requirements

An implementation may conform to DICOM Web Services by supporting the role of user agent, origin server or both, for any of the Services defined in this Part.

X.1 Message Syntax

The syntax of the request and response messages for transactions are defined using the ABNF Grammar used in [RFC7230], which is based on the ABNF defined in [RFC5234]. This Standard also supports the ABNF extensions in [RFC7405], which defines '%s' prefix for denoting case sensitive strings.

The syntax rules defined herein are valid for the US-ASCII character set or character sets that are supersets of US-ASCII, e.g., Unicode UTF-8.

X.1.1 Syntax for Data Types

Data types shall be encoded according the Common Syntactic Rules for Data Types.

X.2 HyperText Transfer Protocol

The system shall support HTTP for data transfer as origin server and/or user agent. (add reference to versions supported)

X.3 Transactions

Each transaction is composed of a request message and a response message, sometimes referred to as a request/response pair. When used in PS3.18 the term "request" means "request message", and "response" means "response-message", unless clearly stated otherwise. Figure X.3-1 is an interaction diagram that shows the message flow of a transaction. The user agent always initiates a transaction by sending a request to the origin server. When it receives the request, the origin server processes it and returns a response.

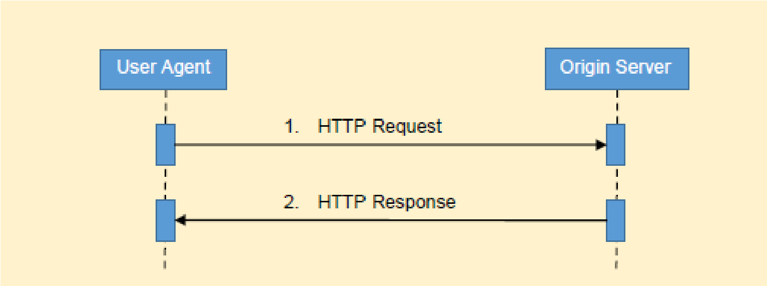


Figure X.3-1: Interaction Diagram for Transactions

X.3.1 OPTIONS

The system shall be able to handle the OPTIONS method.

X.3.2 DELETE Method

The system shall be able to handle the DELETE method.

X.3.3 GET

The system shall be able to handle the GET method.

X.3.4 HEAD

The system shall be able to handle the HEAD method.

X.3.5 POST

The system shall be able to handle the POST method.

X.3.6 PUT

The system shall be able to handle the PUT method.

X.4 Target Resource URI

Each service defines the format of its target resource URIs (aka Target URIs) and Query Parameters using URI Templates; and each transaction specifies which target resources it can reference. The target resource is also known as the request target or the target URI.

X.4.1 Support Target Resource URI

The system shall use the defined format for the target resource URI without query parameters

X.4.2 Support Target Resource URI with Query Parameters

The system shall use the defined format for the target resource URI with query parameters

X.5 Query Parameters

The query component of a request URI may be used to specify one or more Query Parameters. These parameters are referred to as Query Parameters in order to distinguish them from header field parameters or other types of parameters that may be contained in the payload.

X.5.1 Query Parameter Syntax

The system shall form the query part of the resource URI according to the query parameter syntax.

X.5.2 Content Negotiation Query Parameters

The system shall create Resource URIs in accordance with the content negotiation query parameters specification.

X.5.3 Search Query Parameters

The system shall create Resource URIs in accordance with the search query parameters specification.

X.5.4 Standard Rendering Query Parameters

The system shall create Resource URIs in accordance with the standard rendering query parameters specification.

X.6 Header Fields

The DICOM specification makes use of standard HTTP header fields, however the requirements on these header fields might be stronger than specified by the HTTP Standard.

X.6.1 Content Negotiation Header Fields

The system shall create Resource URIs in accordance with the content negotiation header fields specification.

X.6.2 Content Representation Header Fields

The system shall create Resource URIs in accordance with the content representation header fields specification.

X.6.3 Payload Header Fields

The system shall create Resource URIs in accordance with the payload header fields specification.

X.6.4 Conditional Request Header Fields

The system shall create Resource URIs in accordance with the conditional request header fields specification.

X.6.5 Caching Header Fields

The system shall create Resource URIs in accordance with the caching header fields specification.

X.7 Status Codes

The system can use several response message ranging from Success to Error.

X.7.1 Success

The system shall be able to handle a Status Code Success.

X.7.2 Warning

The system shall be able to handle a Status Code Warning.

X.7.3 Redirection

The system shall be able to handle a Status Code Redirection.

X.7.4 Client Error

The system shall be able to handle a Status Code Client Error.

X.7.5 Server Error

The system shall be able to handle a Status Code Server Error.

X.8 Payload

Both request and response messages may have message bodies. The message body (if any) of an HTTP message is used to carry the payload of the message. The message body is identical to the payload unless a transfer coding has been applied, as described in [RFC7230, Section 3.3.1]. This standard uses the term 'payload' to denote the message body before any transfer coding has been applied to it.

X.8.1 Absent Payload

The system shall be able to handle a message that has no payload.

X.8.2 Single Part Payload

The system shall be able to handle a message with a Single Part payload.

X8.3 Multi Part Payload

The system shall be able to handle a message with a Multi Part payload.

X.9 Media Types

Media types are the basis for both content negotiation and data typing of message payloads. Each PS3.18 service and/or transaction defines the media types and associated representations that are default, required and optional.

X.9.1 Multipart Media Types

The system shall create Resource URIs in accordance with the multipart media types specification.

X.9.2 DICOM Resource Catergories

The system shall create Resource URIs in accordance with the DICOM resource categories specification.

X.9.3 DICOM Media Types and Media Types for Bulk Data

The system shall create Resource URIs in accordance with the DICOM Media Types and Media types for bulk data specification.

X.9.4 Rendered Media Types

The system shall create Resource URIs in accordance with the rendered media types specification.

X.9.5 Acceptable Media Types

The system shall create Resource URIs in accordance with the acceptable media types specification.

X.9.6 Accept Query Parameter

The system shall create Resource URIs in accordance with the accept query parameter specification.

X.9.7 Accept Header Field

The system shall create Resource URIs in accordance with the accept header field specification.

X.9.8 Selected Media Type

The system shall create Resource URIs in accordance with the selected media types specification.

X.9.9 Content-Type Header Field

The system shall create Resource URIs in accordance with the content-type header field specification.

X.10 Character Sets

HTTP uses charset names to indicate or negotiate the character encoding of textual content in representations [RFC6365, Section 3.3 <https://tools.ietf.org/html/rfc6365#section-3.3>].

Character sets may be identified using the value in the IANA Preferred MIME Name column in the IANA Character Set Registry <http://www.iana.org/assignments/character-sets/character-sets.xhtml>.

Character sets may be identified by using the DICOM Defined Terms for the character set. See PS3.3, Section C.12.1.1.2, and PS3.5, Section 6.1.2.3.

X.10.1 Acceptable Character Sets

The system shall create Resource URIs in accordance with the acceptable character sets specification.

X.10.2 Character Set Query Parameter

The system shall create Resource URIs in accordance with the character set query parameter specification.

X.10.3 Character Set Media Type Parameters

The system shall create Resource URIs in accordance with the character set media type parameters specification.

X.10.4 Accept-Charset Header Field

The system shall create Resource URIs in accordance with the accept-charset header field specification.

X.10.5 Selected Character Ste

The system shall create Resource URIs in accordance with the selected character set specification.

X.11 Security

This standard does not introduce any security-related requirements.

The HTTPS protocol can be used to protect information contained in request and/or response messages.

As such no requirement is defined for security support.

7.3.11 Storage Service using Files Services

…

Original Text of PS3.2:

7 Conformance Requirements

An implementation claiming DICOM conformance may choose to support one of the following:

- network conformance according to Section 7.1 (DICOM Network Conformance Requirements);
- media storage conformance according to Section 7.2 (DICOM Media Storage Conformance Requirements);
- both of the above.

7.1 DICOM Network Conformance Requirements

An implementation claiming DICOM network conformance shall:

- conform to the minimum conformance requirements defined in this section;
- provide with the implementation a Conformance Statement structured according to the rules and policies in this Part including Annex A;
- conform to at least one Standard or Standard Extended SOP class as defined in PS3.4;

  Note

  Conformance to a Standard or Standard Extended SOP class implies conformance to the related IOD outlined in PS3.3, the Data Elements defined in PS3.6, and the operations and notifications defined in PS3.7.
- comply with the rules governing SOP Class types outlined in Section 7.3;
- accept a Presentation Context for the Verification SOP Class as an SCP if the implementation accepts any DICOM association requests;
- produce and/or process Data Sets as defined in PS3.5;

  Note

  Conformance to PS3.5 also implies conformance to PS3.6.
- obtain legitimate right to a registered <org id> for creating UIDs (see PS3.5) if an implementation utilizes Privately Defined UIDs (i.e., UIDs not defined in the DICOM Standard);
- support the following communication mode:
- TCP/IP (See PS3.8),

7.2 DICOM Media Interchange Conformance Requirements

An implementation claiming DICOM Media Interchange conformance shall:

- conform to the minimum conformance requirements defined in this section;
- provide with the implementation a Conformance Statement structured according to the rules and policies in this Part including Annex C;
- conform to at least one Standard Application Profile as defined in PS3.11;
- support one of the Physical Media and associated Media Format, as specified by PS3.12;
- comply with the rules governing SOP Class types outlined in Section 7.3;
- comply with the specific rules governing media storage Application Profile according to their types as specified in Section 7.4. No other types of Application Profiles may be used;

- read as an FSR or FSU all SOP Classes defined as mandatory by each of the supported Application Profiles encoded in any of the mandatory Transfer Syntaxes.
- write as an FSC or FSU all SOP Classes defined as mandatory by each of the supported Application Profiles in one of the mandatory Transfer Syntaxes;
- be able to gracefully ignore any Standard, Standard Extended, specialized or Private SOP Classes that may be present on the Storage Medium but are not defined in any of the Application Profiles to which conformance is claimed.

  Note

  There may be more than one Application Profile used to create or read a File-set on a single physical medium (e.g., a medium may have a File-set created with Standard and Augmented Application Profiles).
- be able to gracefully ignore Directory Records in the DICOMDIR file that do not correspond to Directory Records defined in any of the Application Profiles to which conformance is claimed.
- access the File-set(s) on media using the standard roles defined in PS3.10;
- produce and/or process Data Sets as defined in PS3.5 encapsulated in DICOM Files;

  Note

  Conformance to PS3.5 also implies conformance to PS3.6
- obtain legitimate right to a registered <org id> for creating UIDs (see PS3.5) if an implementation utilizes Privately Defined UIDs (i.e., UIDs not defined in the DICOM Standard).

An implementation that does not meet all the above requirements shall not claim conformance to DICOM for Media Storage Interchange.

7.3 Rules Governing Types of SOP Classes

Each SOP Class published in a Conformance Statement is one of four basic types. Each SOP Class in an implementation claiming conformance to the DICOM Standard shall be handled in accordance with the following rules, as dictated by the type of SOP Class.

Standard SOP Classes conform to all relevant Parts of the DICOM Standard with no additions or changes.

To claim conformance to a Standard SOP Class, an implementation shall make a declaration of this fact in its Conformance Statement, and identify its selected options, roles, and behavior.

Standard Extended SOP Classes shall:

a. be a proper super set of one Standard SOP Class;

b. not change the semantics of any Standard Attribute of that Standard SOP Class;

c. not contain any Private Type 1, 1C, 2, or 2C Attributes, nor add additional Standard Type 1, 1C, 2 or 2C Attributes;

d. not change any Standard Type 3 Attributes to Type 1, 1C, 2, or 2C;

e. use the same UID as the Standard SOP Class on which it is based.

A Standard Extended SOP Class may include Standard and/or Private Type 3 Attributes beyond those defined in the IOD on which it is based as long as the Conformance Statement identifies the added Attributes and defines their relationship with the PS3.3 information model.

An implementation claiming conformance with a Standard Extended SOP Class shall identify in its Conformance Statement the Standard SOP Class being extended, the options, roles, and behavior selected, and describe the Attributes being added with the Standard SOP Class's IOD Model and Modules.

Specialized SOP Classes shall:

a. be completely conformant to relevant Parts of the DICOM Standard;

b. be based on a Standard SOP Class, i.e.:

- contain all the Type 1, 1C, 2, and 2C Attributes of Standard SOP Class on which it is based;
- not change the semantics of any Standard Attribute;
- use a Privately Defined UID for its SOP Class (i.e., shall not be identified with a DICOM Defined UID);

c. be based on the DICOM Information Model in PS3.3 and PS3.4.

Specialized SOP Classes may:

a. contain additional Standard and/or Private Type 1, 1C, 2, or 2C Attributes;

b. add Private and Standard Type 3 Attributes, which may or may not be published in the Conformance Statement.

> Note
>
> The usage of any unpublished Attributes may be ignored by other users and providers of the Specialized SOP Class.

c. enumerate the permitted values for Attributes within the set allowed by the Standard SOP Class;

d. enumerate the permitted Templates for Content Items within the set allowed by the Standard SOP Class.

An implementation claiming conformance with a Specialized SOP Class shall include in its Conformance Statement the identity of the Standard SOP Class being specialized, a description of usage of all Standard and Private Type 1, 1C, 2, and 2C Attributes in the Specialized SOP Class, a description of the constraints on Attributes values and Templates, and the associated Privately Defined UID.

Private SOP Classes shall:

a. be completely conformant to relevant Parts of the DICOM Standard with the possible exception that support of the DICOM Default Transfer Syntax or a Transfer Syntax mandated by a media storage Application Profile is not required;

b. not change the PS3.6 specification of any Standard Attributes;

c. use a Privately Defined UID for its SOP Class (i.e., shall not be identified with a DICOM Defined UID);

d. not change existing DIMSE Services or create new ones;

e. not change existing DICOM File Services defined in PS3.10 or extend them in a manner that jeopardizes interoperability.

Private SOP Classes may:

a. use or apply DIMSE Services to privately defined or altered IODs (i.e., not necessarily be based on a Standard SOP Class);

b. use or apply Media Storage Operations to privately defined or altered IODs (i.e., not necessarily be based on a Standard SOP Class);

c. designate any Standard Attribute as Type 1, 1C, 2, or 2C regardless of the Type of the Attribute in other IODs;

d. define Private Attributes as Type 1, 1C, 2, or 2C;

e. include Private and Standard Type 3 Attributes, which may or may not be published in the Conformance Statement.

An implementation claiming conformance with a Private SOP Class shall provide a PS3.3, PS3.4, and PS3.6-like description of the Private SOP Class in the implementation's Conformance Statement, including descriptions of the usage of all Standard and Private Type 1, 1C, 2, or 2C Attributes in the SOP Class, the DICOM Information Model, and the Privately Defined UIDs.

Note

Unpublished SOP Classes (i.e., SOP Classes that are not defined in the DICOM Standard and are not defined in the Conformance Statement) are permitted in order to allow an implementation to support other abstract syntaxes within the DICOM Application Context. Such unpublished SOP Classes would utilize Privately Defined UIDs. The presence of an unpublished SOP Class does not prevent the implementation from being DICOM conformant but would have no meaning to other implementations and may be ignored.

7.4 Rules Governing Types of Application Profiles

Application Profile used in a Conformance Statement shall be of one of three basic types. Each Application Profile in an implementation claiming conformance to the DICOM Standard shall be handled in accordance with the following rules, as dictated by the type of Application Profile.

7.4.1 Standard Application Profile

A Standard Application Profile shall:

a. conform to all relevant Parts of DICOM with no changes;

b. support only one of the Physical Media and associated Media Format, as specified by PS3.12.

To claim conformance to a Standard Application Profile, an implementation shall make a declaration of this fact in its Conformance Statement, and identify its selected options, roles, and behavior.

An implementation of a Standard Application Profile may extend Standard SOP Classes of this Standard application profile. Such Standard Extended SOP Classes shall meet the requirements specified in Section 7.3.

7.4.2 Augmented Application Profile

An Augmented Application Profile shall:

a. be a proper super set of the Standard Application Profile. It adds the support of additional Standard or Standard Extended SOP Classes;

b. use the same Physical Media and its associated Media Format specified in the corresponding Standard Application Profile;

c. not include Specialized or Private SOP Classes.

An Augmented Application Profile may:

a. include one or more Standard or Standard Extended SOP Classes in addition to those of the corresponding Standard Application Profile. These additional SOP Classes may be mandatory or optional;

b. include the extensions (e.g., additional required keys, additional directory records) to the Basic Directory Information Object corresponding to the SOP Classes defined in a);

c. add one or more new roles (FSC, FSR, FSU).

To claim conformance to an Augmented Application Profile, an implementation shall make a declaration of this fact in its Conformance Statement, and shall identify the Standard Application Profile from which it is derived and specify the augmentations. The implementation shall also identify its selected options, roles, and behavior.

An implementation of a Augmented Application Profile may:

a. extend Standard SOP Classes of the corresponding Standard application profile. Such Standard Extended SOP Classes shall meet the requirements specified in Section 7.3;

b. also claim conformance to the Standard Application Profile on which this Augmented Profile is based. In this case, FSC and FSU implementations shall be able to restrict their behavior to the Standard Application Profile (i.e., provide a means to write only the Standard or Standard Extended SOP Classes defined in the corresponding Standard Application Profile).

7.4.3 Private Application Profile

A Private Application Profile:

- conforms to PS3.10 and to the Media Storage Service Class specified in PS3.4;

- support only one of the Physical Media and associated Media Format, as specified by PS3.12;

  Note

  The intent of these two conditions is to ensure that at least the DICOMDIR is readable by other APs.

- complies with the rules governing SOP Classes in Section 7.3.

To claim conformance to a Private Application Profile, an implementation shall make a declaration of this fact in its Conformance Statement, and shall provide a description of the Application Profile patterned after the descriptions in PS3.11. The implementation shall also identify its selected options, roles, and behavior.

> Note
>
> An implementation that does not meet the provisions of Section 7, including the types of Application Profile, is not conformant to DICOM and so is outside the scope of DICOM conformance. Such an implementation is not an Application Profile in DICOM terminology. For example, if an implementation chooses to write DICOM files onto media that is not in PS3.12, or use a file system not defined for a specific media type in PS3.12, then that implementation cannot claim that it conforms to the DICOM Standard using that media or file system.

7.5 Conformance of DICOM Media

DICOM does not define conformance of a piece of medium in a generic sense. DICOM conformance of a piece of medium can only be evaluated within the scope of one or more media storage Application Profiles that define specific contexts for interoperability.

> Note
>
> One may accept the statement "this is a DICOM CD-R" when pointing to a storage medium. However, one should not state "this CD-R is DICOM conformant", but rather "this CD-R conforms to the Basic Cardiac X-ray Angiographic DICOM Application Profile".

7.6 Security Profiles

DICOM specifies methods for providing security at different levels of the ISO OSI Basic Reference Model through the use of mechanisms specific to a particular layer. The methods for applying these mechanisms are described in the various parts of the DICOM Standard. Some mechanisms and algorithms are specified in PS3.15 as Security Profiles. An implementation's Conformance Statement describes which Security Profiles can be used by that application.

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

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

An implementation shall list in its Conformance Statement any additional use of the User Identity association negotiation sub-item that is not specified in a standard Security Profile.

7.7 Transformation of DICOM SR to CDA

DICOM specifies the transformation of DICOM SR objects to CDA documents in PS3.20.

This transformation is unidirectional (DICOM SR to HL7 CDA). Conformance statements shall at a minimum state conformance to the top level templates used for the SR document and the CDA document.