

# X-Tray

## DICOM Conformance Statement

Version 2.2.0  
2019-02-26

krucom

## Overview

X-Tray is a healthcare Workflow Manager that handles data-flow related to diagnostic imaging. This document covers X-Tray's interfaces for DICOM Modality Worklist services.

SOP Classes	User of Service (SCU)	Provider of Service (SCP)
Workflow Management		
Modality Worklist	Option	Yes

Table 1 Networking Service Class specification

X-Tray can be used in a vast number of scenarios to provide connectivity. The general connectivity possibilities of X-Tray are out of the scope of this document. An example from Enterprise Imaging is provided below in order to help the reader better understand the context that X-Tray works in:

In the Enterprise Imaging scenario, X-Tray connects the EHR, VNA and Imaging Acquisition Equipment (modalities) with regards to order information, patient demographics and image notification. Concerning DICOM, X-Tray functions as a worklist SCP providing the Imaging Acquisition Equipment with worklists for either encounter or order based imaging.

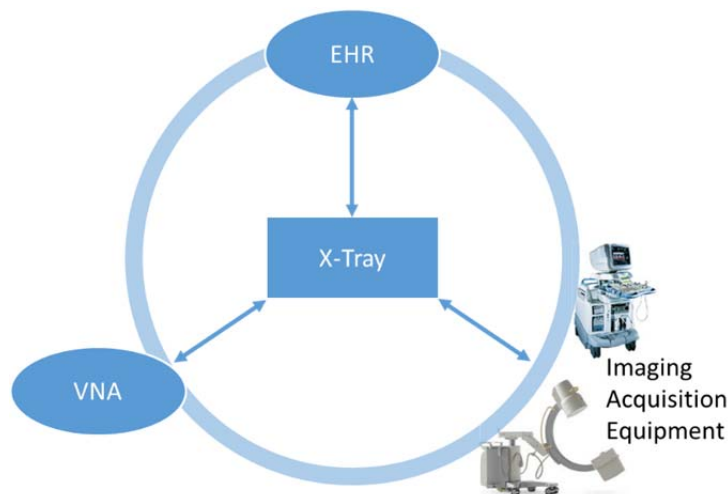


Figure 1: X-Tray in the Enterprise Imaging scenario

The equipment described in this document has been validated in accordance with the DICOM standard. Krucom AB shall not be liable for errors contained herein or consequential damages concerning the furnishing, performance or use of this document. Krucom AB reserves the right to revise this publication and to make changes to its content at any time, without obligation to notify any person or entity of such revisions and changes.

## Table of Contents

Overview .....	2
1. Introduction.....	5
1.1 Revision History.....	5
1.2 Audience.....	5
1.3 Remarks.....	5
1.4 Terms and Definitions .....	5
1.5 Basics of DICOM Communication.....	7
1.6 Abbreviations and Acronyms .....	8
1.7 References.....	8
1.8 Trademarks.....	8
2. Implementation Model .....	9
2.1 Application Data Flow Diagram.....	9
2.2 Functional Definition of AE.....	9
2.2.1 X-Tray SCP Application Entity .....	9
2.2.2 Associated Real World Activity - Query for Worklist.....	9
2.3 Sequencing of Real-World Activities .....	10
3. AE Specifications .....	11
3.1 X-Tray SCP.....	11
3.1.1 SOP Classes.....	11
3.1.2 Association Policies .....	11
3.1.3 Association Initiation Policy.....	11
3.1.4 Association Acceptance Policy .....	12
3.2 X-Tray SCU .....	15
3.2.1 SOP Classes.....	15
3.2.2 Association Policies .....	15
3.2.3 Association Initiation Policy.....	15
3.2.4 Association Acceptance Policy .....	16
3.3 Network Interfaces.....	17
3.3.1 Physical Network Interface.....	17
3.3.2 Additional Protocols .....	17
3.3.3 IPv4 and IPv6 Support .....	17
3.4 Configuration.....	17
3.4.1 AE Title/Presentation Address Mapping .....	17
3.4.2 Parameters .....	18

---

4. Media Interchange .....	19
5. Support of Character Sets .....	20
6. Security .....	21
6.1 Security Profiles .....	21
6.2 Association Level Security .....	21
6.3 Application Level Security .....	21

## 1. Introduction

This document is intended to describe X-Tray's conformance to DICOM.

### 1.1 Revision History

Revision	Date	Comments
1.0	2001-01-16	Initial Release
1.1	2003-09-02	Layout Rearrangements
1.2	2005-10-12	Change of document base
1.3	2006-02-06	Worklist SCU capabilities included in DCS
1.9.0	2016-02-16	Major revision with change of document base. Added new X-Tray attributes. Harmonized DCS revision number with X-Tray major and minor version number i.e. this DCS revision (1.9.0) applies to all X-Tray 1.9.x releases.

**Table 2:** Revision History

### 1.2 Audience

This document is written for the people that need to understand how X-Tray will integrate into their healthcare facility. This includes both those responsible for overall imaging network policy and architecture, as well as integrators who need to have a detailed understanding of the DICOM features of the product. This document contains some basic DICOM definitions so that any reader may understand how this product implements DICOM features. However, integrators are expected to fully understand all the DICOM terminology, how the tables in this document relate to the product's functionality, and how that functionality integrates with other devices that support compatible DICOM features.

### 1.3 Remarks

The scope of this DICOM Conformance Statement is to facilitate integration between X-Tray and other DICOM products. The Conformance Statement should be read and understood in conjunction with the DICOM Standard. DICOM by itself does not guarantee interoperability. The Conformance Statement does, however, facilitate a first-level comparison for interoperability between different applications supporting compatible DICOM functionality.

This Conformance Statement is not supposed to replace validation with other DICOM equipment to ensure proper exchange of intended information. In fact, the user should be aware of the following important issues:

- The comparison of different Conformance Statements is just the first step towards assessing interconnectivity and interoperability between the product and other DICOM conformant equipment.
- Test procedures should be defined and executed to validate the required level of interoperability with specific compatible DICOM equipment, as established by the healthcare facility.

### 1.4 Terms and Definitions

Informal definitions are provided for the following terms used in this Conformance Statement. The DICOM Standard is the authoritative source for formal definitions of these terms.

Abstract Syntax	The information agreed to be exchanged between applications, generally equivalent to a Service/Object Pair (SOP) Class. Examples: Verification SOP Class, Modality Worklist Information Model Find SOP Class, Computed Radiography Image Storage SOP Class.
Application Entity (AE)	An end point of a DICOM information exchange, including the DICOM network or media interface software; i.e., the software that sends or receives DICOM information objects or messages. A single device may have multiple Application Entities.
Application Entity Title (AET)	The externally known name of an Application Entity, used to identify a DICOM application to other DICOM applications on the network.
Application Context	The specification of the type of communication used between Application Entities. Example: DICOM network protocol.
Association Attribute	A network communication channel set up between Application Entities. A unit of information in an object definition; a data element identified by a tag. The information may be a complex data structure (Sequence), itself composed of lower level data elements. Examples: Patient ID (0010,0020), Accession Number (0008,0050), Photometric Interpretation(0028,0004), Procedure Code Sequence (0008,1032).
Information Object Definition(IOD)	The specified set of Attributes that comprise a type of data object; does not represent a specific instance of the data object, but rather a class of similar data objects that have the same properties. The Attributes may be specified as Mandatory (Type 1), Required but possibly unknown (Type2), or Optional (Type 3), and there may be conditions associated with the use of an Attribute (Types 1C and 2C). Examples: MR Image IOD, CT Image IOD, Print Job IOD.
Module	A set of Attributes within an Information Object Definition that are logically related to each other. Example: Patient Module includes Patient Name, Patient ID, Patient Birth Date, and Patient Sex.
Negotiation	First phase of Association establishment that allows Application Entities to agree on the types of data to be exchanged and how that data will be encoded.
Presentation Context	The set of DICOM network services used over an Association, as negotiated between Application Entities; includes Abstract Syntaxes and Transfer Syntaxes.
Protocol Data Unit (PDU)	A packet (piece) of a DICOM message sent across the network. Devices must specify the maximum size packet they can receive for DICOM messages.
Service Class Provider (SCP)	Role of an Application Entity that provides a DICOM network service; typically, a server that performs operations requested by another Application Entity (Service Class User). Examples: Picture Archiving and Communication System (image storage SCP, and image query/retrieve SCP), Radiology Information System (modality worklist SCP).
Service Class User (SCU)	Role of an Application Entity that uses a DICOM network service; typically, a client. Examples: imaging modality (image storage SCU, and modality worklist SCU), imaging workstation (image query/retrieve SCU)
Service/Object Pair Class (SOPClass)	The specification of the network or media transfer (service) of a particular type of data (object); the fundamental unit of DICOM interoperability specification. Examples: Ultrasound Image Storage Service, Basic Grayscale Print Management.
Service/Object Pair Instance (SOP Instance)	An information object; a specific occurrence of information exchanged in a SOP Class. Examples: a specific x-ray image.

Tag	A 32-bit identifier for a data element, represented as a pair of four digit hexadecimal numbers, the "group" and the "element". If the "group" number is odd, the tag is for a private (manufacturer-specific) data element. Examples: (0010,0020) [Patient ID], (07FE,0010) [Pixel Data], (0019,0210) [private data element]
Transfer Syntax	The encoding used for exchange of DICOM information objects and messages. Examples: JPEG compressed (images), little endian explicit value representation.
Unique Identifier (UID)	A globally unique "dotted decimal" string that identifies a specific object or a class of objects; anISO-8824 Object Identifier. Examples: Study Instance UID, SOP Class UID, SOP Instance UID.
Value Representation (VR)	The format type of an individual DICOM data element, such as text, an integer, a person's name, or a code. DICOM information objects can be transmitted with either explicit identification of the type of each data element (Explicit VR), or without explicit identification (Implicit VR); with Implicit VR, the receiving application must use a DICOM data dictionary to look up the format of each data element.

## 1.5 Basics of DICOM Communication

This section describes terminology used in this Conformance Statement for the non-specialist. The key terms used in the Conformance Statement are highlighted in *italics* below. This section is not a substitute for training about DICOM, and it makes many simplifications about the meanings of DICOM terms.

Two *Application Entities* (devices) that want to communicate with each other over a network using DICOM protocol must first agree on several things during an initial network "handshake". One of the two devices must initiate an *Association* (a connection to the other device), and ask if specific services, information, and encoding can be supported by the other device (*Negotiation*).

DICOM specifies a number of network services and types of information objects, each of which is called an *Abstract Syntax* for the Negotiation. DICOM also specifies a variety of methods for encoding data, denoted *Transfer Syntaxes*. The Negotiation allows the initiating Application Entity to propose combinations of Abstract Syntax and Transfer Syntax to be used on the Association; these combinations are called *Presentation Contexts*. The receiving Application Entity accepts the Presentation Contexts it supports.

For each Presentation Context, the Association Negotiation also allows the devices to agree on *Roles* - which one is the *Service Class User* (SCU - client) and which is the *Service Class Provider* (SCP - server). Normally the device initiating the connection is the SCU, i.e., the client system calls the server.

The Association Negotiation finally enables exchange of maximum network packet (*PDU*) size, security information, and network service options (called *Extended Negotiation* information).

The Application Entities, having negotiated the Association parameters, may now commence exchanging data. Common data exchanges include queries for worklists and lists of stored images, transfer of image objects and analyses (structured reports), and sending images to film printers. Each exchangeable unit of data is formatted by the sender in accordance with the appropriate *Information Object Definition*, and sent using the negotiated Transfer Syntax. There is a Default Transfer Syntax that all systems must accept, but it may not be the most efficient for some use cases. Each transfer is explicitly acknowledged by the receiver with a *Response Status* indicating success, failure, or that query or retrieve operations are still in process.

## 1.6 Abbreviations and Acronyms

ADT	Admit Discharge Transfer	MTU	Maximum Transmission Unit (IP)
AE	Application Entity	MWL	Modality Worklist
AET	Application Entity Title	NTP	Network Time Protocol
CDA	Clinical Document Architecture	O	Optional (Key Attribute)
DCS	DICOM Conformance Statement	ORM	Order Message
DHCP	Dynamic Host Configuration Protocol	ORU	Observation Result
DICOM	Digital Imaging and Communications in Medicine	OSI	Open Systems Interconnection
DIMSE	DICOM Message Service Element	PACS	Picture Archiving and Communication System
DNS	Domain Name System	PDU	Protocol Data Unit
EHR	Electronic Health Record	R	Required (Key Attribute)
EI	Enterprise Imaging	RDN	Relative Distinguished Name (LDAP)
EMR	Electronic Medical Record	RIS	Radiology Information System
EPR	Electronic Patient Record	SCP	Service Class Provider
HIS	Hospital Information System	SCU	Service Class User
HL7	Health Level 7 Standard	SOAP	Simple Object Access Protocol
IHE	Integrating the Healthcare Enterprise	SOP	Service-Object Pair
IOD	Information Object Definition	SPS	Scheduled Procedure Step
IPv4	Internet Protocol version 4	SR	Structured Reporting
IPv6	Internet Protocol version 6	TCP/IP	Transmission Control Protocol/Internet Protocol
ISO	International Organization for Standards	U	Unique (Key Attribute)
JSON	JavaScript Object Notation	UL	Upper Layer
LDAP	Lightweight Directory Access Protocol	US	Ultrasound
LDIF	LDAP Data Interchange Format	VNA	Vendor Neutral Archive
MPPS	Modality Performed Procedure Step	VR	Value Representation
MSPS	Modality Scheduled Procedure Step	UID	Unique Identifier
		UML	Unified Modelling Language

## 1.7 References

NEMA PS3 Digital Imaging and Communications in Medicine (DICOM) Standard, available free at <http://medical.nema.org/>

## 1.8 Trademarks

X-Tray is a registered trademark of Krucom AB.

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

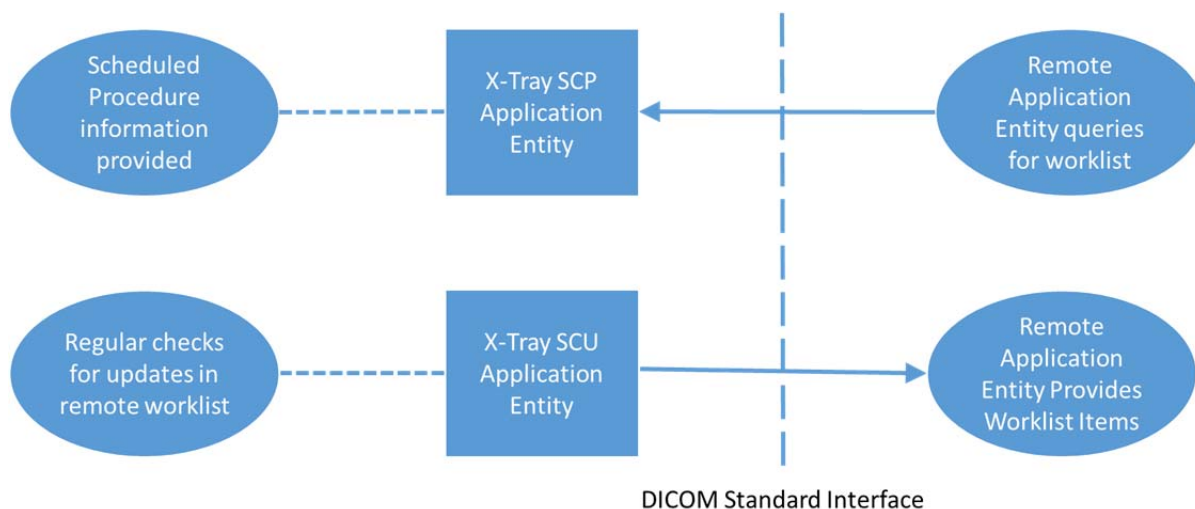


## 2. Implementation Model

X-Tray provides the following functionality:

- SCP and SCU for Verification.
- SCP and SCU for Modality Worklist.

### 2.1 Application Data Flow Diagram



**Figure 2:** Application Data Flow Diagram

- The X-Tray SCP Application Entity accepts Association Requests for Modality Worklist and Verification from Remote Application Entities. X-Tray SCP spawns additional threads as necessary to handle incoming connections.
- The X-Tray SCU Application Entity queries Remote Application Entities (e.g. RIS ) for Modality Worklist or Verification. A new association is opened each time X-Tray performs a worklist query.

### 2.2 Functional Definition of AE

X-Tray can be configured to perform the functions outlined in Figure 2. This section describes the sequences of real-world activities that are involved in performing these functions.

#### 2.2.1 X-Tray SCP Application Entity

The X-Tray SCP Application Entity accepts Association Requests for Modality Worklist from MWL SCUs and responds to queries from these SCUs. When a query is received, X-Tray responds to the MWL SCU with the scheduled procedures matching the query and the rules configured in X-Tray. Additionally, the X-Tray SCP Application Entity accepts associations for Verification from SCUs and responds automatically with Success status.

#### 2.2.2 Associated Real World Activity - Query for Worklist

The X-Tray SCU Application Entity regularly queries remote Application Entities (e.g. RIS ) for scheduled procedures using Modality Worklist. The contents of the query and time between queries is configurable in X-Tray. A new association is opened each time X-Tray performs a worklist query. Furthermore, the X-Tray SCU Application Entity may request associations for Verification in order to test validity of the DICOM connection to Remote Application Entities. Verification can be initiated

from the real-world activity of a service engineer (via X-Tray's test-tool) or in conjunction with the regular worklist queries (configurable, disabled by default).

### 2.3 Sequencing of Real-World Activities

All X-Tray SCP activities are performed asynchronously in the background and not dependent on any sequencing.

During normal operation, X-Tray SCU activities are initiated sequentially.

## 3. AE Specifications

### 3.1 X-Tray SCP

#### 3.1.1 SOP Classes

X-Tray SCP provides Standard Conformance to the following SOP Classes:

SOP Class Name	SOP Class UID
Verification SOP Class	1.2.840.10008.1.1
Modality Worklist Information Model - FIND	1.2.840.10008.5.1.4.31

**Table 3:** SOP Classes supported by X-Tray SCP

#### 3.1.2 Association Policies

##### *General*

X-Tray SCP accepts but never initiates associations.

##### *Number of Associations*

X-Tray SCP can receive an unlimited number of simultaneous associations. However, the licencing policy may restrict the maximum number of connectable devices.

##### *Asynchronous Nature*

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

##### *Implementation Identifying Information*

X-Tray SCP is identified by:

- Implementation Class UID **1.2.752.48.1.1.1.20000228**
- Implementation Version Name **KRUCOM**

#### 3.1.3 Association Initiation Policy

X-Tray SCP does not initiate associations.

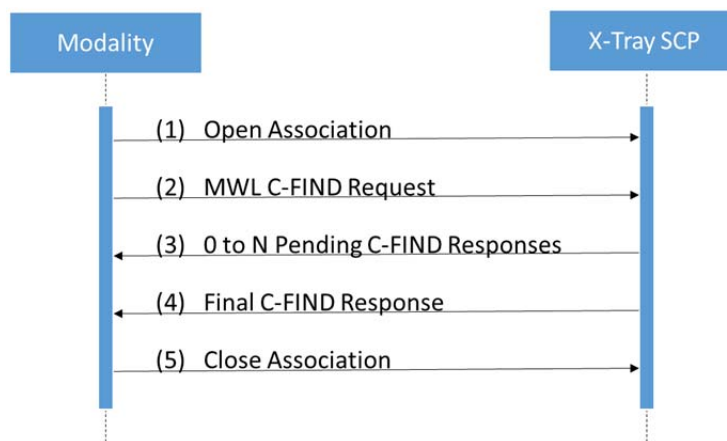
### 3.1.4 Association Acceptance Policy

X-Tray SCP will accept associations in order to receive worklist queries and verification requests. The process runs in the background and spawns a new thread for each connection request from a Remote AE.

#### Activity - Modality Requests Worklist from X-Tray SCP

Figure 3 below is a possible sequence of messages between a Modality Worklist SCU and X-Tray SCP.

1. The Modality opens an Association with X-Tray SCP for the purpose of querying for a Modality Worklist. X-Tray logs the IP address and AE Title of the connecting Modality.
2. The Modality sends an MWL C-FIND query to X-Tray SCP. X-Tray logs the latest request received from each IP address and AE Title.
3. X-Tray SCP queries its worklist cache using the attributes from the C-FIND Request and returns 0 to N C-FIND responses depending on matches returned from the worklist cache and the rules configured in X-Tray. If the Modality is not recognised (e.g. not configured in X-Tray) it will receive an empty worklist from X-Tray SCP.
4. X-Tray SCP sends the final C-FIND response and writes the total number of returned worklist items (query hits).
5. The Modality closes the Association.



**Figure 3:** Sequencing Diagram for Activity: Modality Requests Worklist from X-Tray SCP

#### Accepted Presentation Contexts

X-Tray SCP uses the following Transfer Syntax with all SOP Classes.

Name-list	UID-list
DICOM Implicit VR Little Endian Transfer Syntax	1.2.840.10008.1.2

**Table 4:** Transfer Syntax acceptable to X-Tray

#### Extended Negotiation

No extended negotiation is performed.

*SOP Specific Conformance for Modality Worklist SOP Class*

X-Tray SCP supports required and optional matching and return key attributes as described in table 5 below.

Attribute Description	Tag	Remark
Specific Character Set	(0008,0005)	Always returned with value "ISO_IR 100"
Scheduled Procedure Step Sequence	(0040,0100)	
> Modality	(0008,0060)	Single Value Matching
> Requested Contrast Agent	(0032,1070)	
> Scheduled Station AE Title	(0040,0001)	Single Value Matching
> Scheduled Procedure Step Start Date	(0040,0002)	Single Value Matching or Range Matching
> Scheduled Procedure Step Start Time	(0040,0003)	Single Value Matching or Range Matching
> Scheduled Performing Physician's Name	(0040,0006)	Single Value Matching or Wild Card Matching
> Scheduled Procedure Step Description	(0040,0007)	
> Scheduled Protocol Code Sequence	(0040,0008)	
>> Code Value	(0008,0100)	
>> Coding Scheme Version	(0008,0103)	
>> Coding Scheme Designator	(0008,0102)	
>> Code Meaning	(0008,0104)	
> Scheduled Procedure Step ID	(0040,0009)	Single Value Matching
> Scheduled Station Name	(0040,0010)	Single Value Matching
> Scheduled Procedure Step Location	(0040,0011)	
> Pre-Medication	(0040,0012)	
> Scheduled Procedure Step Status	(0040,0020)	
> Comments on the Scheduled Procedure Step	(0040,0400)	
Study Instance UID	(0020,000D)	Single Value Matching
Requested Procedure Description	(0032,1060)	
Requested Procedure Code Sequence	(0032,1064)	
> Code Value	(0008,0100)	
> Coding Scheme Designator	(0008,0102)	
> Coding Scheme Version	(0008,0103)	
> Code Meaning	(0008,0104)	
Requested Procedure ID	(0040,1001)	
Requested Procedure Priority	(0040,1003)	
Names of Intended Recipients of Results	(0040,1010)	
Requested Procedure Comments	(0040,1400)	
Accession Number	(0008,0050)	Single Value Matching
Requesting Physician	(0032,1032)	
Requesting Service	(0032,1033)	Single Value Matching
Placer Order Number / Imaging Service Request	(0040,2016)	
Filler Order Number / Imaging Service Request	(0040,2017)	
Institution Name	(0008,0080)	
Admission ID	(0038,0010)	
Current Patient Location	(0038,0300)	
Referring Physician's Name	(0008,0090)	
Referring Physician's Address	(0008,0092)	
Admitting Diagnoses Description	(0008,1080)	
Admitting Date	(0038,0020)	
Patient's Name	(0010,0010)	Single Value Matching or Wild Card Matching
Patient ID	(0010,0020)	Single Value Matching
Other Patient IDs	(0010,1000)	
Patients Birth Date	(0010,0030)	

Attribute Description	Tag	Remark
Patient's Sex	(0010,0040)	
Patient's Age	(0010,1010)	
Patient's Size	(0010,1020)	
Patient's Weight	(0010,1030)	
Patient's Address	(0010,1040)	
Patient's Telephone Numbers	(0010,2154)	
Patient Comments	(0010,4000)	
Confidentiality Constraint on Patient Data Description	(0040,3001)	
Medical Alerts	(0010,2000)	
Allergies	(0010,2110)	
Pregnancy Status	(0010,21C0)	
Special Needs	(0038,0050)	
Patient State	(0038,0500)	

**Table 5:** X-Tray SCP return and matching key attributes

Comments:

- X-Tray SCP interprets all worklist queries, performs matching and returns datasets using Character Set ISO\_IR 100.
- Scheduled Step Start Date (0040,0002) and Scheduled Step Start Time (0040,0003) are subject to Range Matching. If both keys are specified for Range Matching, e.g. the date range July 5 to July 7 and the time range 10am to 6pm specifies the time period starting on July 5, 10am until July 7, 6pm.
- X-Tray SCP does not support:
  - case-insensitive nor fuzzy semantic matching of person names
  - time zone offset from UTC (0008,0201)
  - priority requests
  - cancel request

## 3.2 X-Tray SCU

### 3.2.1 SOP Classes

X-Tray SCU provides Standard Conformance to the following SOP Classes:

SOP Class Name	SOP Class UID
Verification SOP Class	1.2.840.10008.1.1
Modality Worklist Information Model - FIND	1.2.840.10008.5.1.4.31

**Table 6:** SOP Classes supported by X-Tray SCU

### 3.2.2 Association Policies

#### General

X-Tray SCU initiates but does not accept associations.

#### Number of Associations

During normal operation, X-Tray SCU uses a maximum of one simultaneous association.

#### Asynchronous Nature

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

#### Implementation Identifying Information

X-Tray SCU is identified by:

- Implementation Class UID **1.2.752.48.1.1.1.20000228**
- Implementation Version Name **KRUCOM**

### 3.2.3 Association Initiation Policy

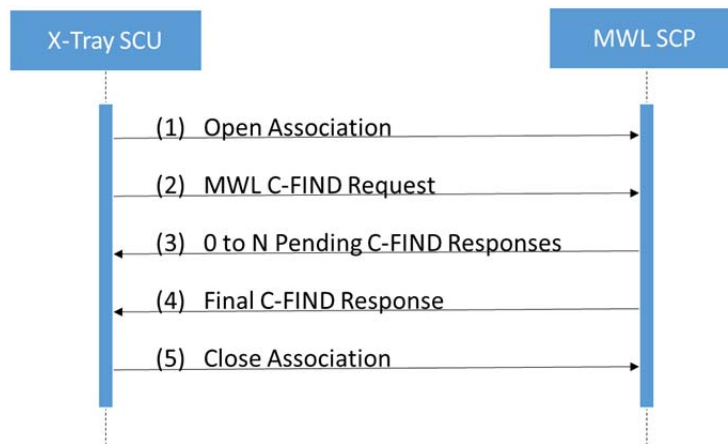
The X-Tray SCU Application Entity regularly queries remote Application Entities (e.g. RIS ) for scheduled procedures using Modality Worklist. The time between queries from X-Tray SCU is configurable. A new association is opened each time X-Tray SCU performs a worklist query.

Furthermore, the X-Tray SCU Application Entity may request associations for Verification in order to test validity of the DICOM connection to Remote Application Entities. Verification can be initiated from the real-world activity of a service engineer (via X-Tray's test-tool) or in conjunction with the regular worklist queries (configurable, disabled by default).

*Activity - X-Tray SCU Requests Worklist from MWL SCP*

Figure 4 below is a possible sequence of messages between X-Tray SCU and a MWL SCP.

1. X-Tray SCU opens an Association with DMWL SCP for the purpose of querying for a Modality Worklist.
2. X-Tray SCU sends an MWL C-FIND query to DMWL SCP.
3. DMWL SCP returns 0 to N C-FIND responses (worklist items).
4. DMWL SCP sends the final C-FIND response.
5. X-Tray SCU closes the Association.



**Figure 4:** Sequencing Diagram for Activity: X-Tray SCU Requests Worklist from MWL SCP

*Accepted Presentation Contexts*

X-Tray SCU uses the following Transfer Syntax with all SOP Classes.

Name-list	UID-list
DICOM Implicit VR Little Endian Transfer Syntax	1.2.840.10008.1.2

**Table 7:** Transfer Syntax proposed by X-Tray

*Extended Negotiation*

No extended negotiation is performed.

*SOP Specific Conformance for Modality Worklist SOP Class*

X-Tray SCU is highly configurable with regards to requested matching and return key attributes. By default, X-Tray SCP queries for all the return keys supported by X-Tray SCP, see table 5.

By default, X-Tray SCU uses Character Set ISO\_IR 100.

Scheduled Step Start Date (0040,0002) and Scheduled Step Start Time (0040,0003) are subject to Range Matching. If both keys are specified for Range Matching, e.g. the date range July 5 to July 7 and the time range 10am to 6pm specifies the time period starting on July 5, 10am until July 7, 6pm.

X-Tray SCU does not support:

- fuzzy semantic matching of person names
- Timezone Offset From UTC (0008,0201)
- priority requests
- cancel request

**3.2.4 Association Acceptance Policy**

X-Tray SCU does not accept associations.



## 3.3 Network Interfaces

### 3.3.1 Physical Network Interface

X-Tray is indifferent to the physical medium over which TCP/IP executes, which is dependent on the underlying operating system and hardware.

### 3.3.2 Additional Protocols

When host names rather than IP addresses are used in the configuration properties to specify presentation addresses for remote AEs, the X-Tray is dependent on the name resolution mechanism of the underlying operating system.

### 3.3.3 IPv4 and IPv6 Support

X-Tray only supports IPv4 connections.

## 3.4 Configuration

### 3.4.1 AE Title/Presentation Address Mapping

#### *Local AE Titles*

The local AE Title used by each individual X-Tray AE can be configured independently of the AE Title used by other local applications. If so configured, all local AEs are capable of using the same AE Title. If it is required, X-Tray SCU is capable of appearing using numerous different AE Titles.

Application Entity	Default AE Title	Default TCP/IP Port
X-Tray SCP	X-TRAY	104
X-Tray SCU	X-TRAY	104

**Table 8:** Default local AE configuration

#### *Remote AE Title/Presentation Address Mapping*

For X-Tray SCP, the AE Titles and host names or IP address of remote applications are set in X-Tray Configuration Manager.

For X-Tray SCU the AE Titles, ports and host names or IP address of remote applications are specified in a configuration file.

### 3.4.2 Parameters

Parameter	Configurable (Yes/No)	Default Value
<b>General Parameters</b>		
Time-out waiting for acceptance or rejection Response to an Association Open Request. (Application Level timeout)	No	None
General DIMSE level time-out values	No	None
Time-out waiting for response to TCP/IP connect request. (Low-level timeout)	No	None
Time-out waiting for acceptance of a TCP/IP message over the network. (Low-level timeout)	No	None
Time-out for waiting for data between TCP/IP packets. (Low-level timeout)	No	None
Any changes to default TCP/IP settings, such as configurable stack parameters.	No	None
<b>AE Specific Parameters (all AEs)</b>		
Maximum PDU size the AE can receive	No	16 kB
Maximum PDU size the AE can send	No	16 kB
AE specific DIMSE level time-out values	No	None
Number of simultaneous Associations by Service and/or SOP Class	No	X-Tray SCP: Unlimited <sup>1</sup> X-Tray SCU: 1
SOP Class support	No	All supported SOP Classes always proposed and accepted
Transfer Syntax support	No	Implicit VR Little Endian Transfer Syntax always proposed and accepted

**Table 9:** General Configuration Parameters

<sup>1</sup> The licencing policy may restrict the maximum number of connectable devices.

## 4. Media Interchange

X-Tray does not support Media Storage

## 5. Support of Character Sets

X-Tray supports the character sets specified in table 10 below.

Defined Term	Description
ISO_IR 6	Default Repertoire
ISO_IR 100	8-bit character set for west European languages. Also known as ISO 8859-1, Latin-1 or ECMA-94

**Table 10:** Character sets supported by X-Tray

## 6. Security

X-Tray does not support any specific security measures.

It is assumed that X-Tray is used within a secured environment. It is assumed that a secured environment includes at a minimum:

- a. Firewall or router protections to ensure that only approved external hosts have network access to X-Tray.
- b. Firewall or router protections to ensure that X-Tray only has network access to approved external hosts and services.
- c. Any communication with external hosts and services outside the locally secured environment use appropriate secure network channels (e.g., such as a Virtual Private Network (VPN) )

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

### 6.1 Security Profiles

None supported.

### 6.2 Association Level Security

None supported. Any Calling AE Titles and/or IP addresses may open an Association.

### 6.3 Application Level Security

None supported.