

DICOM Correction Item

Correction Number	CP-884
Log Summary: DNS self-discovery for secure DICOM services	
Type of Modification	Name of Standard
Clarification	PS 3.15 2008
Rationale for Correction	
DNS self discovery supports announcement of ordinary DICOM service (service name of "dicom"), but a separate service name is needed to announce secure DICOM services, which may be listening on different ports of the same machine.	
Sections of documents affected	
PS 3.15 H.2	
Correction Wording:	

Amend PS 3.15:

H.2 DNS SERVICE DISCOVERY

H.2.1 Scope

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

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

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

H.2.2 Use Case Roles

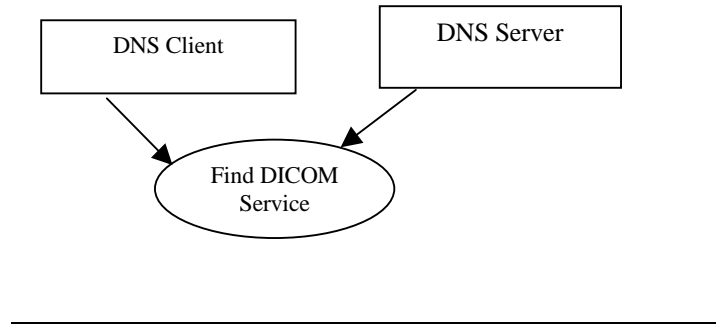


Figure H.2-1 Find DICOM Service

DNS Server	Provides list of DICOM Association Acceptors
DNS Client	Requests list of DICOM Association Acceptors

H.2.3 Referenced Standards

- RFC-2181 Clarifications to the DNS Specification
- RFC-2219 Use of DNS Aliases for Network Services
- RFC-2782 A DNS RR for specifying the location of services (DNS SRV)
- RFC 2136 DNS Dynamic Updates <<http://www.rfc-editor.org/rfc/rfc2136.txt>>
- RFC 2782 A DNS RR for specifying the location of services (DNS SRV) <<http://www.rfc-editor.org/rfc/rfc2136.txt>>
- DNS SRV (RFC 2782) Service Types <<http://www.dns-sd.org/ServiceTypes.html>>
- DNS-Based Service Discovery <<http://files.dns-sd.org/draft-cheshire-dnsext-dns-sd.txt>>
- DNS Self-Discovery <<http://www.dns-sd.org/>>
- Multicast DNS <<http://files.multicastdns.org/draft-cheshire-dnsext-multicastdns.txt>>
- Multicast DNS <<http://www.multicastdns.org/>>

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

- “dicom” **for unsecured DICOM communication**
- “dicom-tls” **for the Basic TLS Secure Transport Connection Profile**
- “dicom-iscl” **for ISCL Transport Connection Profile.**

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

The DNS TXT record may contain the following parameters:

- AET=<*application entity title*>, where the value <*application entity title*> is to be used as the Called Application Entity Title when initiating Associations to the device

- PrimaryDeviceType=*<primary device type>*, where the value *<primary device type>* is as defined Table H.1-2 Attributes of Device Object

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

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