DICOM Correction Proposal

STATUS	Final Text
Date of Last Update	2020/01/17
Person Assigned	
Submitter Name	William R. Jacqmein, bill.jacqmein@agfa.com
Submission Date	

Correction Number CP- 1946
Log Summary: Update Part 15 Annex H (add conformance)
Name of Standard PS3.15 2019e
Rationale for Correction: A small editorial edit in H.2.1is required. Need to add RFC8553. Need to add a Conformance section.
Correction Wording:

Modify PS3.15, Section 2 Normative references to add the following:

RFC 4033. IETF. March 2005. DNS Security Introduction and Requirements.

RFC 4034. IETF. March 2005. Resource Records for the DNS Security Extensions.

RFC 4035. IETF. March 2005. Protocol Modifications for the DNS Security Extensions.

RFC8553 DNS AttrLeaf Changes https://tools.ietf.org/html/rfc8553

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

Modify PS 3, Part 15, Annex H, Section H.2 as shown (and hyperlink references in H.2.3 to Section 2 entries):

H Application Configuration Management Profiles

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**~~ **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

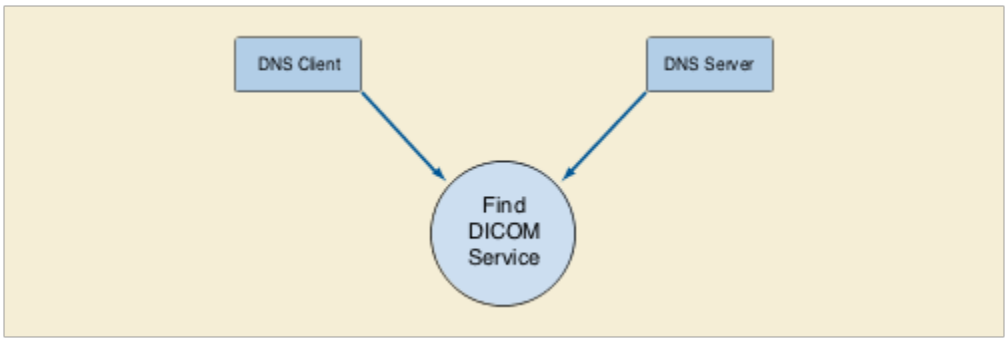

Figure H.2-1. Find DICOM Service

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

H.2.3 Referenced Standards

RFC2136 DNS Dynamic Updates http://tools.ietf.org/html/rfc2136

RFC2181 Clarifications to the DNS Specification http://tools.ietf.org/html/rfc2181

RFC2219 Use of DNS Aliases for Network Services http://tools.ietf.org/html/rfc2219

RFC2782 A DNS RR for specifying the location of services (DNS SRV) http://tools.ietf.org/html/rfc2782

RFC6762 Multicast DNS http://tools.ietf.org/html/rfc6762

RFC6763 DNS-Based Service Discovery http://tools.ietf.org/html/rfc6763

RFC8553 DNS AttrLeaf Changes https://tools.ietf.org/html/rfc8553

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

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

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

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

The DNS TXT record may contain the following parameters:

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

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

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

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

H.2.4 Examples

Example SRV record:

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

Example TXT record:

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

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

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

H.2.5 Conformance

An implementation that supports this profile shall state in its Conformance Statement whether it supports reading (DNS Client) or writing DNS (DNS Server) records.

An implementation that supports this profile shall state in its Conformance Statement whether it supports DNSSEC [RFC 4033], [RFC 4034], [RFC 4035] for the interactions described in this profile, in which case either the options supported shall be stated or a reference provided to the DNSSEC support for this product.