DICOM Correction Proposal

STATUS	Final Text
Date of Last Update	2020/01/17
Person Assigned	
Submitter Name	rjhorniii@gmail.com
Submission Date	2019/05/14

Correction Number CP-1942
Log Summary: DDNS/DHCP updates
Name of Standard PS3.15 2019e
Rationale for Correction: The description of DDNS is unclear and causes confusion. The conformance requirements were for LDAP, not for DDNS.
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.

Modify PS3.15, Section F.1.5 DDNS Coordination through F.1.8 Conformance as shown

F.1.5 DDNS Coordination

F.1.5.1 Scope

DHCP servers may coordinate their IP and hostname assignments with a DNS server. This permits dynamic assignment of IP addresses without interfering with access to DHCP Clients by other systems. The other systems utilize the agreed hostname (which DHCP can manage and provide to the client) and obtain the current IP address by means of DNS lookup.

Dynamic DNS (DDNS) provides the capability to the client to update DNS records hosted on the DNS server. The client can be a DHCP server, Active Directory or LDAP servers, or even an application announcing the systems IP address and optionally any available services.

A DHCP Server ~~**is in compliance**~~ **complies** with this optional part of the Basic Network Address Management Profile ~~**profile**~~ if it maintains and updates the relevant DNS ~~**server**~~ **entry** so as to maintain the ~~**proper**~~ hostname~~/~~ **and** IP relationships in the DNS database **when they change**.

F.1.5.2 Use Case Roles

Figure F.1-7. DDNS Coordination

Actor: DHCP Server

Role: Responded to DHCP acquisition queries and assigned IP address to client.

Actor: DNS Server

Role: Maintains the DNS services for the network.

F.1.5.3 Referenced Standards

RFC2136 Dynamic Updates in the Domain Name System

F.1.5.4 Basic Course of Events

~~**After the DHCP server has assigned**~~**The DHCP server assigns** an IP address to a DHCP client~~**,. the DHCP server uses DDNS to inform**~~**then informs** the **D**DNS server that the hostname ~~**assigned**~~ **associated with**~~**to**~~ the DHCP client has been given ~~**the**~~ **an** assigned IP address. The **D**DNS **s**~~**S**~~erver updates the DNS database **and links the IP address to the hostname.** ~~**so that subsequent**~~ DNS queries for this hostname are ~~**given**~~ **directed to** the assigned IP address. ~~**When**~~ **If** the ~~**lease for the**~~**assigned** IP address ~~**expires without renewal**~~**changes or expires**, the DHCP server informs the **D**DNS server**, which updates the DNS database.** ~~**that the IP address and hostname are no longer valid. The DNS server removes them from the DNS database.**~~

F.1.6 DHCP Security Considerations (Informative)

The Basic Network Address Management Profile Profile has two areas of security concerns:

a. Protection against denial of service attacks against the DHCP client/server traffic.

b. Protection against denial of service attacks against the DHCP server to DDNS server update process.

The Basic Network Address Management Profile Profile should not be used outside a secured environment. At a minimum there should be:

a. Firewall and or router protections to ensure that only approved hosts are used for DHCP and DNS services.

b. Agreements for VPN and other access should require that DNS clients on the hospital network use only approved DHCP or DNS servers over the VPN.

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

The purpose of the selected security is to limit the scope of the threat to insider attacks. The DHCP and DNS systems disclose only hostnames and IP addresses, so there is little concern about eavesdropping. The protections are to limit the exposure to denial of service attacks by counterfeit servers or clients. The specific DNS security extensions are described in Section F.1.1.4. This profile does not utilize the DHCP security extensions because they provide very limited added security and the attacks are insider denial of service attacks. Intrusion detection and other network level protection mechanisms are the most effective next level of protections for the DHCP process.

The DNS update is optional in this profile to accommodate the possibility that the DHCP server and DNS server cannot reach a mutually acceptable security process. Support of this option may require support of the DNS security protocols that are in the process of development. See Section F.1.1.4 for a discussion of the DNS security profile standards and drafts.

F.1.7 DHCP Implementation Considerations (Informative)

The DHCP configuration file can be a very useful form of documentation for the local network hardware configuration. It can be prepared in advance for new installations and updated as clients are added. Including information for all machines, including those that do not utilize DHCP, avoids accidental IP address conflicts and similar errors.

Most DHCP servers have a configuration capability that permits control of the IP address and other information provided to the client. These controls can pre-allocate a specific IP address, etc. to a machine based on the requested machine name or MAC address. These pre-allocated IP addresses then ensure that these specific machines are always assigned the same IP address. Legacy systems that do not utilize DNS can continue to use fixed tables with IP addresses when the DHCP server has pre-allocated the IP addresses for those services.

F.1.8 Conformance

An implementation that supports this profile shall state in its Conformance Statement whether it supports DHCP as DHCP Client or DHCP Server.

An implementation that supports this profile as a DHCP Client shall state in its Conformance Statement how the DHCP Server is discovered (see F.1.3).

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.

~~**The Conformance Statement for an LDAP Client shall describe its use of LDAP to configure the local AE titles. Any conformance to the Update LDAP Server option shall be specified, together with the values for all component object attributes in the update sent to the LDAP Server. Any use of LDAP to configure the remote device addresses and capabilities shall be described. The LDAP queries used to obtain remote device component object attributes shall be specified.**~~

> ~~**Note In particular, use of LDAP to obtain the AE Title, TCP port, and IP address for specific system actors (e.g., an Image Archive, or a Performed Procedure Step Manager) should be detailed, as well as how the LDAP information for remote devices is selected for operational use.**~~