DICOM Correction Proposal

STATUS	Final Text
Date of Last Update	2020/03/10
Person Assigned	Rob Horn
Submitter Name	R Horn, rjhorniii@gmail.com
Submission Date	2019/08/21

Correction Number CP-1965
Log Summary: Update NTP profile in PS3.15
Name of Standard PS3.15 2020a
Rationale for Correction: Preparation of revised conformance claim revealed obsolete and missing RFC references, clarifications needed, non-requirement advice that is obsolete, etc. Major changes: - Update to RFC5905 and RFC5906 from RFC1305. RFC5905 and RFC5906 were issued in 2010 and clarify some confusions in 1305. 5905 servers are interoperable with old 1305 clients (if any still exist). 1305 servers should all have been updated to 5905. Some of those clarifications make discussions and explanations in this profile unnecessary. - Clarified explanation of NTP server list - Removed explanation of fall back when no NTP servers found. This is covered in RFC5905. - Revised security section to simplify and refer to RFC5905 and RFC5906 as appropriate. - Added references to ntp.org and nwtime.org. These are the sites for the network time foundation. They maintain the reference implementation, RFCs, and coordinate operational activities like network servers and security notifications.
Correction Wording:

Update PS 3.15 Annex G, Section G.1.1.3 Referenced Standards through G.1.1.7 as shown

G.1.1.3 Referenced Standards

~~**RFC1305 Network Time Protocol (NTP) standard specification**~~

RFC2030 ~~**Simple NTP**~~ **Simple Network Time Protocol (SNTP) Version 4**

RFC5905 Network Time Protocol Version 4: Protocol and Algorithms Specification

RFC5906 Network Time Protocol Version 4: Autokey Specification

RFC8633 Network Time Protocol Best Current Practices

G.1.1.4 Basic Course of Events.

~~**The DHCP server may have provided a list of NTP servers or one may be obtained through optional NTP discovery mechanisms. If this list is empty and no manually configured NTP server address is present, the client shall select its internal clock as the time source (see below). If the**~~

~~list is not empty, the client shall attempt to maintain time synchronization with all those NTP servers. The client may attempt to use the multi-cast, manycast, and broadcast options as defined in [RFC1305]. It shall utilize the point to point synchronization option if these are not available. The synchronization shall be in compliance with either [RFC1305] (NTP) or [RFC2030] (SNTP).~~

The NTP Client uses a list of NTP Servers, which may be:

- **obtained through optional NTP discovery mechanisms (see RFC5905 Section 3.1),**
- **provided by a DHCP Server, see Annex F on DHCP, and/or**
- **manually configured.**

If the list is not empty, the client shall attempt to maintain time synchronization with at least one of the NTP servers. The client synchronization shall be in compliance with either [RFC5905] (NTP) or [RFC2030] (SNTP). If the list is empty, the client may choose an alternative method of time synchronization.

~~If the application requires time synchronization of better than 1s mean error, the client should use NTP. SNTP cannot ensure a more accurate time synchronization.~~

SNTP provides much lower accuracy than NTP. If time synchronization of better than 1s mean error is required, the client should use NTP. [RFC5905] and [RFC8633] discuss implementation and accuracy considerations.

~~The~~**A** DHCP server may ~~have~~ provide~~d~~ **to the DHCP Client** a UTC offset between the local time at the machine and UTC ~~If this is missing, the UTC offset will be obtained in a device specific manner (e.g., service, CMOS). If the UTC offset is provided,~~**which** the client shall use ~~this offset~~ for converting between UTC and local time.

G.1.1.5 Alternative Paths

If there is no UTC offset information from the DHCP **or NTP** server, then **the UTC offset will be obtained in a device specific manner (e.g., service, CMOS, internal battery clock)** ~~the NTP client will use its preset or service set UTC offset~~.

~~If there is no NTP time server, then the NTP client will select its internal battery clock as the source of UTC. These may have substantial errors. This also means that when there are multiple systems but no NTP source, the multiple systems will not attempt to synchronize with one another.~~

G.1.1.6 Assumptions

The local battery clock time is set to UTC, or the local operating system has proper support to manage both battery clock time, NTP clock time, and system clock time. The NTP time is always in UTC.

G.1.1.7 Postconditions

The client will remain synchronized with its selected time source. In an environment with one or more NTP servers, this will be good time synchronization. In the absence of NTP servers, the selected source will be the internal client clock~~, with all its attendant errors~~.

Modify PS 3.15 Annex G, Section G.1.2 Maintain Time as shown

G.1.2 Maintain Time

G.1.2.1 Scope

This applies to any client that needs the correct time, or that needs to have its time stamps synchronized with those of another system. The accuracy of synchronization is determined by details of the configuration and implementation of the network and NTP servers at any specific site.

G.1.2.2 Use Case Roles

Editorial instruction: Add SNTP Client to Figure G.2-1

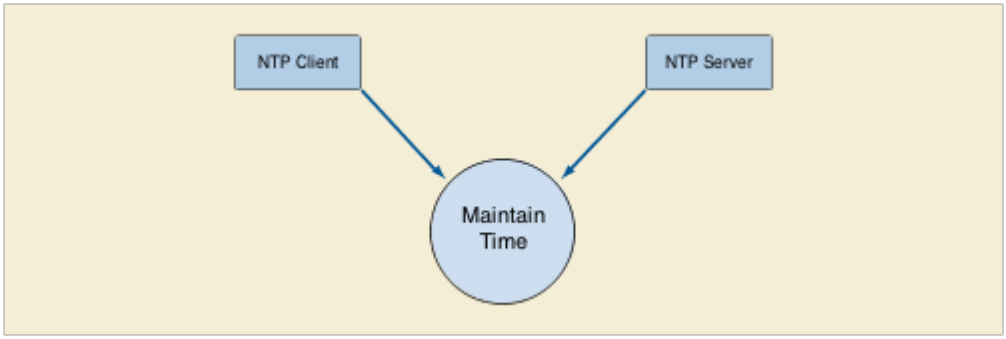

Figure G.2-1. Maintain Time

NTP/SNTP Client Maintains client clock

NTP Servers External time servers. These may have connections to other time servers, and may be synchronized with national time sources.

G.1.2.3 Referenced Standards

~~**RFC1305 Network Time Protocol (NTP) standard specification**~~

RFC2030 ~~**Simple NTP**~~ **Simple Network Time Protocol (SNTP) Version 4**

RFC2827 Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing

RFC5905 Network Time Protocol Version 4: Protocol and Algorithms Specification

RFC5906 Network Time Protocol Version 4: Autokey Specification

RFC8633 Network Time Protocol Best Current Practices

G.1.2.4 Basic Course of Events.

~~**All the full**~~ **The** detail **on Maintain Time transactions** is **described** in [RFC~~**1305**~~**5905**] and [RFC2030]. The most common and **the** mandatory minimum mode for NTP operation ~~**establishes**~~ **uses** a ~~**ping pong**~~ **series** of messages between client and servers. The client sends ~~**a**~~ request**s** to the servers, which fill in time related fields in a response, and the client performs optimal estimation of the present time **based on that information**. The RFCs deal with issues of lost messages, estimation formulae, etc. Once the clocks are in synchronization**,** these ~~**ping pong**~~**message** exchanges typically stabilize at roughly 1000 second intervals.

The client machine ~~**typically**~~ uses the time estimate to maintain the internal operating system clock. This clock is then used by applications that need time information. This approach eliminates the application visible difference between synchronized and unsynchronized time. The RFCs provide guidance on proper implementations.

G.1.3 NTP Security Considerations (Informative)

~~**The Basic Time Synchronization 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 NTP services.**~~

~~b. Agreements for VPN and other access should require that use only approved NTP servers over the VPN.~~

~~This limits the risks to insider denial of service attacks. The service denial is manipulation of the time synchronization such that systems report the incorrect time. The NTP protocols incorporate secure transaction capabilities that can be negotiated. This profile assumes that the above protections are sufficient and does not require support of secure transactions, but they may be supported by an implementation. The SNTP client does not support the use of secured transactions.~~

~~Sites with particular concerns regarding security of external network time sources may choose to utilize a GPS or radio based time synchronization. Note that when selecting GPS and radio time sources, care must be taken to establish the accuracy and stability provided by the particular time source. The underlying time accuracy of GPS and radio sources is superb, but some receivers are intended for low accuracy uses and do not provide an accurate or stable result.~~

NTP security considerations (RFC5905 Section 8, RFC5906, and RFC8633) may be applicable based on site-specific environment and threat considerations. Locations with NTP Servers should also consider RFC2827 and implementing access controls on the use of the server.

Security Policies and Procedures for NTP are maintained at https://www.nwtime.org/security-policy/ as part of the Network Time Foundation.

G.1.4 NTP Implementation Considerations (Informative)

NTP **compliant** servers always support both NTP and SNTP clients. The difference is one of synchronization accuracy, not communications compatibility. Although in theory both NTP and SNTP clients could run at the same time on ~~a client~~**the same system,** this is not recommended. The SNTP updates will simply degrade the time accuracy. When other time protocol clients, such as IRIG, are also being used these clients must be coordinated with the NTP client to avoid synchronization problems.

These and other considerations, such as multiple clock types, accuracy implications, and configuration alternatives, are documented at http://www.ntp.org.

~~RFC1305 includes specifications for management of intermittent access to the NTP servers, broken servers, etc. The NTP servers do not need to be present and operational when the NTP process begins. NTP supports the use of multiple servers to provide backup and better accuracy. RFC1305 specifies the mechanisms used by the NTP client. The site www.ntp.org provides extensive guidance and references regarding the most effective configurations for backups and multiple server configurations.~~

~~The local battery clock and client operating system must be properly UTC aware. NTP synchronization is in UTC. This can be a source of confusion because some computers are configured with their hardware clocks set to local time and the operating system set (incorrectly) to UTC. This is a common error that only becomes apparent when the devices attempt to synchronize clocks.~~

G.1.5 Conformance

The Conformance Statement for the NTP Server and NTP Client shall state whether secure transactions **(RFC5906)** are supported.

The Conformance Statement for the NTP Server shall state whether it is also an NTP Client.

The Conformance Statement for the NTP Client shall state how it manages time when no NTP Server is available.