**Maintaining Integrity in System Date/Time**

**5.7.5.1 FPT\_STM.1 Reliable Time Stamps**

Proposal:

**FPT\_STM.1.1** The TSF shall be able to provide reliable time stamps.

Reliable time stamps are expected to be used with other TSF, e.g. for the generation of audit data to allow the Security Administrator to investigate incidents by checking the order of events and to determine the actual local time when events occurred. The decision about the required level of accuracy of that information is up to the administrator. The TOE depends on external time and date information, either provided manually by the Security Administrator or through the use of an NTP server. The use of a local real-time clock and the automatic synchronization with an NTP server is recommended but not mandated. The ST Author specifies the means which are used to update system time in FMT\_MTD.1/SystemTime Management of TSF Data. The ST author describes in the TSS how the external time and date information is received by the TOE and how this information is maintained.

#### FMT\_MTD.1/SystemTime Management of TSF Data

**FMT\_MTD.1/SystemTime Management of TSF Data**

**FMT\_MTD.1.1/SystemTime** The TSF shall restrict the ability to *modify* the *System Time* to[selection: *Security Administrators* *(locally or remotely),* an *NTP Server authorized by the Security Administrator].*

If a Security Administrator is modifying the system time remotely, they will, of course, have to use a protected communication path as specified in FPT\_TRP.1/Admin. If the ST Author selects the NTP Server option, then the ST Author must select the **FPT\_STM\_EXT.1** in Appendix X, or they must include “NTP Server” in the open assignment in FTP\_ITC.1.1.

[The following is a selection-based SFR]

**FPT\_STM\_EXT.1 Protection of System Time updates**

**FPT\_STM\_EXT.1/Autokey** The TSF shall use Network Time Protocol version 4 (NTPv4) as specified in RFC 5905, configuring the optional message authentication code (MAC) for symmetric key authentication scheme and Autokey as specified in RFC 5906 using the following identity schemes: [selection: private certificate (PC), trusted certificate (TC), a modified Schnorr algorithm (IFF - Identify Friend or Foe), a modified Guillou-Quisquater (GQ) algorithm, a modified Mu-Varadharajan (MV) algorithm].

Use of this SFR indicates the TOE provides an NTP client that implements NTPv4 and complies with the corresponding standard. From RFC 5906 “There are five schemes now implemented in the NTPv4 reference implementation to prove identity: (1) private certificate (PC), (2) trusted certificate (TC), (3) a modified Schnorr algorithm (IFF aka Identify Friendly or Foe), (4) a modified Guillou-Quisquater (GQ) algorithm, and (5) a modified Mu-Varadharajan (MV) algorithm. Not all of these provide the same level of protection and one, TC, provides no protection but is included for comparison.”

**FPT\_STM\_EXT.1/Presharedkey** tbd

[If in **FMT\_MTD.1.1/SystemTime** NTP is selected, either the above SFR, **FPT\_STM\_EXT.1, is used, or this version of FTP\_ITC.1 is used]**

#### FTP\_ITC.1 Inter-TSF trusted channel (Refinement)

**FTP\_ITC.1 Inter-TSF trusted channel**

**FTP\_ITC.1.1** The TSF shall be **capable of using [selection: *IPsec, SSH, TLS, HTTPS*] to** provide a trusted communication channel between itself and **authorized IT entities supporting the following capabilities: audit server, NTP Server, [selection: *authentication server, assignment: [other capabilities]*]** that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from disclosure and detection of modification of the channel data.

**FTP\_ITC.1.2** The TSF shall permit **the TSF, or the authorized IT entities** to initiate communication via the trusted channel.

**FTP\_ITC.1.3** The TSF shall initiate communication via the trusted channel for **updating system time (NTP)** [assignment: *list of* ***services for which the TSF is able to initiate communications***].

The ST Author may need to iterate this requirement for clarity if multiple protocols are used for multiple purposes (e.g., IPSec is used to protect the communication path with the NTP server, and TLS is used to protect the path to the audit server).