**Maintaining Integrity in System Date/Time**

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

CURRENT:

**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.

…

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.

#### 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 *Security Administrators* *(locally or remotely)*, *and by* [selection: an *NTP Server authorized by the Security Administrator, no other means].*

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.

[The following is a selection-based SFR]

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

**FPT\_STM\_EXT.1** The TSF shall update its system time using [selection:

* Network Time Protocol version 4 (NTPv4) as specified in RFC 5905, using Symmetric Cryptography [selection: SHA1, AES-CBC-256, [assignment: other ISO approved cryptographic algorithm]] as the cryptographic algorithm(s);
* Network Time Protocol version 4 (NTPv4) as specified in RFC 5905, using Autokey as specified in RFC 5906 using the following identity schemes: [selection: trusted certificate (TC), a modified Schnorr algorithm (IFF - Identify Friend or Foe), a modified Guillou-Quisquater (GQ) algorithm, a modified Mu-Varadharajan (MV) algorithm].
* The TSF shall be capable of using [selection: *IPsec, SSH, TLS, DTLS*] to provide a trusted channel between itself and an NTP Server

]

Use of this SFR indicates the TOE provides an NTP client that implements NTPv4 and complies with the corresponding standard. While RFC 5906 identifies 5 schemes available in the reference implementation, there are only three schemes that use a cryptographically strong challenge-response exchange: (1) a modified Schnorr algorithm (IFF aka Identify Friendly or Foe), (2) a modified Guillou-Quisquater (GQ) algorithm, and (3) a modified Mu-Varadharajan (MV) algorithm. The Trusted Certificate (TC) uses a certificate trail and is not considered an identity scheme according to RFC 5906. The Private Certificate scheme described in RFC 5906 is not intended to be used in an operational environment.

It is noted that for this requirement and FMT\_MTD.1.1/SystemTime that “NTP Server” also includes an entity acting as an NTP peer.