**Maintaining Integrity in System Date/Time**

*Guidelines for applicability of this SFR:*

* *This is a selection-based SFR, to be included in the ST if “synchronise time with an NTP server” is selected within FPT\_STM\_EXT.1.2.*
* *This SFR is required when the TOE can be configured to receive (as a client or peer) NTP clock updates from a non-TOE source (server or peer).*
* *This SFR is not applicable when/where NTP is being used between/among TOE components (such communications would be implicitly covered by FPT\_ITT.1).*
* *This SFR is not applicable if the TOE cannot be configured to operate as an NTP time recipient (client or peer), even if the TOE can operate as an NTP time source (server or peer) for non-TOE entities.  Such communications could potentially be listed as a capability within FTP\_ITC.1.*

**FCS\_NTP\_EXT.1** NTP Protocol

**FCS\_NTP\_EXT.1.1** The TSF shall implement [selection: NTP v3 (RFC 1305), NTP v4 (RFC 5905)].

**FCS\_NTP\_EXT.1.2** The TSF shall be able to update its system time using [selection:

* NTP messages authenticated with [assignment: list of algorithms consistent with selections made in FCS\_COP.1];
* NTP secured within [assignment: list of protocols consistent with selections made in FTP\_ITC.1].

] to provide trusted communication between itself and an external NTP time source.

*Application Note*

*The external time source can be an NTP server or NTP peer.*

**FCS\_NTP\_EXT.1.3** The TSF shall not participate in use of [selection: Broadcast, Multicast, Manycast, no other] NTP modes [selection: except where secured within an FTP\_ITC.1 protocol as noted above, with no exceptions].

*Application Note*

*The Multicast and Manycast NTP modes are discouraged for the same reason that Broadcast mode is prohibited; because they are intended to be used where a relatively high (compared with client/server and symmetric (peer) modes) number of NTP nodes share the same authentication credentials, thus increasing the potential for a malicious agent (another NTP node on the network) to use valid credentials to transmit faulty time data.*

**FCS\_NTP\_EXT.1.4** The TSF shall support concurrent configuration of one or more external NTP time sources.

*Application Note*

*As a best practice, supporting at least three (3) time sources is recommended for redundancy across unreliable networks, but one (1) is sufficient for the SFR.*

**Allocation of Requirements in Distributed TOEs**

|  |  |  |
| --- | --- | --- |
| **Requirement** | **Description** | **Distributed TOE SFR Allocation** |
| FCS\_NTP\_EXT.1 | NTP Protocol | One |

**NTP Subgroup response:** The NTP subgroup adapted the guidelines, application note and the allocation for distributed TOEs, though may have been modified for clarity. All other changes are noted in the Background information.