DATASHEET

ELECTRONIC TRADING RTS-25: CLOCK SYNC

It's Time to Clock-Sync Your Data

RTS-25: Clock-Synchronization of Trade Data

MiFID II requirements for clock-synchronization, as summarized in RTS-25, require firms and venues to timestamp events accurately relative to Coordinated Universal Time (UTC) and to an appropriate level of granularity. Specifically, Article 4 of RTS-25 states "Operators of trading venues and their members or participants shall establish a system of traceability to UTC. They shall be able to demonstrate traceability to UTC by documenting the system design, functioning and specifications. They shall be able to identify the exact point at which a timestamp is applied and demonstrate that the point within the system where the timestamp is applied remains consistent. Reviews of the compliance with this Regulation of the traceability system shall be conducted at least once a year." ESMA/2015/1909 Section 3.1 further clarifies the use of UTC clock-synchronization for "reportable events".

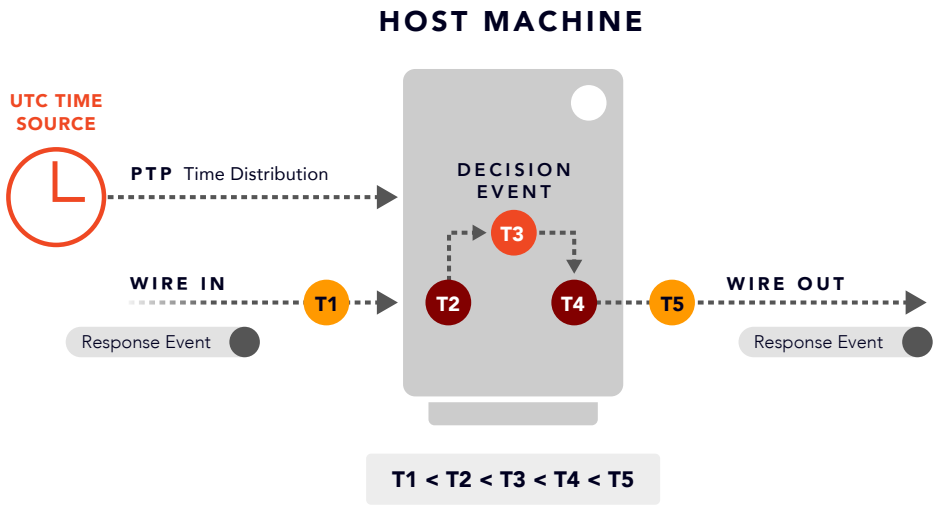

Figure 1: Wire, host timestamps, and application timestamps for measurement and recording of reportable electronic trading events.

TIMESTAMPS

- Host
- Wire
- Application

UTC Time Sources, Distribution and Timestamps

Over the past several years we have worked with the leading venues, participants and market makers throughout the world to develop robust, cost effective and accurate methods to record the timing of electronic trading events. We have found that accurate and precise timestamps of electronic trading events are a critical first step in making sense of these events in terms of latency measurement, forensic investigation and surveillance of trading activity.

Time-keeping technologies such as NTP and PTP are readily available today. Both technologies can deliver time signals to well within the tightest divergences specified in MiFID II (100 microseconds). However, achieving tight divergences reliably and consistently is not always easy. NTP and PTP each have strengths and weakness when it comes to reliably and consistently achieving the tightest divergences specified. Reliability and consistency of reporting should be a key requirement for any regulatory reporting system.

NTP STRENGTHS	PTP STRENGTHS	NTP WEAKNESSES	PTP WEAKNESSES
Mature protocol	Standardizes aspects of network time synchronization for much tighter divergences	Requires extensive modifications for tighter divergences	Not supported by older hardware and OSs
Most systems use the same implementation for divergences within 1 millisecond	Can achieve well below a micro second of divergence with right hardware deployment	Modifications may become un-supportable by anyone but the original engineer	Leaves the disciplining of local clocks up to the implementation
			Implementation of clock disciplining can vary widely in sophistication

Given these strengths and weaknesses, we have found that it is often not sufficient to deploy a network-based time-keeping protocol and assume it will work correctly.

Timestamp Methods for Trade Event Measurement

Methods for measuring and applying timestamps to electronics trading events fit into two broad categories:

Software Timestamps – these are timestamps applied to a specific event of interest using software running on a host machine that is synchronized to a reliable clock source.

Hardware Timestamps – these are timestamps applied to a specific event of interest using special purpose hardware in a network switch or a network interface card (NIC) in a host machine.

In general, hardware based timestamps are more reliable, have higher time precision (i.e., nanoseconds) and are less ambiguous. However, some complex trading events involving decision to trade require the use of software timestamps that are accurately synchronized to a UTC time source.

These two time-stamping measurement methods (hardware and software) can be used to create three timestamp data sources for trade execution events:

Application Timestamps - These are timestamps that are used to record the time at which a specific decision was made by the trading application.

Host Timestamps – These timestamps are made inline by software running on a host machine such as the kernel or network drivers

Wire Timestamps – These timestamps are made passively by hardware that takes a copy of the network packets, timestamps the packets and then decodes the underlying messages to recreate the trading context of the traffic, e.g., orders and/or market data.

IN PRACTICE THE THREE DATA SOURCES LEND THEMSELVES TO SPECIFIC USE CASES

Application Timestamps
Generally used to record the time at which a specific decision was made by the trading application. For example, the time at which a matching engine made a trade. This event time would be when the matching engine software made a match decision between buyer and seller. Typically, this time is recorded in the log file and inserted into the order execution response message for third parties to retrieve and use in their operations.

Host Timestamps
Generally used to record the time a specific message was received or sent by the host machine. For example, the time a gateway receives an order or sends an order response. The exact location where this measurement is made in the host stack can vary. It can happen at the socket layer or deeper within the software stack. This can introduce some level of variability and ambiguity in comparing event times between host machines.

Wire Timestamps
Most often used to unambiguously determine when a specific message was received and when it was sent by a trading function. In practice, wire timestamps tend to be more reliable and precise as there is no variability and ambiguity as to where in the host stack the measurement is made. Wire timestamps are broadly used throughout the industry for troubleshooting potential causality issues with application and host based timestamps.

CDS-190321