

Using Provenance to satisfy MiFID 2 regulatory timing demands

When MiFID 2 takes final effect in January 2018, traders face a raft of new technical requirements imposed by new MiFID 2 regulatory technology standards (known as RTS).

One of these – RTS 25 – regulates the technical standards covering the accuracy of clocks used to timestamp trade data as it is recorded for archiving. The purpose of this standard is ensure that events relating to an order can be reconstructed accurately from the recorded history throughout the lifetime of each order – even when individual trade events may be separated by just microseconds, as is the case in high-speed algorithmic trading (HFT) environments.

Under MiFID 2's proposed RTS 25 regulations, clocks used for timestamping must be accurately synchronized to Coordinated Universal Time (UTC), and timestamps must be accurate to within levels specified for different types of trades. For high-frequency algorithmic trading, the precision of timestamps applied to trade data must be 1 microsecond or better, and the maximum allowable divergence from UTC is 100 microseconds.

The benefits of wire capture and hardware-based timestamps

Commonly, high-frequency traders have implemented network packet capture solutions in order to ensure complete capture of trade data for archival and the accuracy of timestamps that are applied as that trade data is recorded.

Endace's DAG[™] Data Capture Cards are capable of 100% accurate capture and recording of network packets at line speed even on high-speed links such as those commonly found in HFT environments. Additionally, they record highly accurate timestamps for captured traffic.

THE CHALLENGE

- MiFID 2 imposes tough new standards on traders to ensure trade data is accurately time stamped as it is recorded
- High-speed, algorithmic traders must ensure timestamp accuracy to within 100 microseconds of UTC at 1 microsecond granularity, and be able to demonstrate this accuracy for audit purposes

THE SOLUTION - PROVENANCE

- Allows automatic recording of timing environment information and status as trade data is recorded
- Provides an embedded, easily referenceable record of timing accuracy for all recorded trade data
- Offers a way to satisfy MiFID 2's tough new regulatory demands with little or no compliance overhead.
- Ensures recording infrastructure is future-proofed -Provenance data can be extended and customized to meet new regulatory or business requirements

When synchronized with an accurate time source, such as a GPS receiver, DAG cards can timestamp captured packets to within 100 nanoseconds accuracy at a resolution of four nanoseconds – well within the accuracy levels dictated by MiFID 2's RTS 25 directive, and providing future proofing for future regulatory regimes.

However, providing a sufficiently accurate timestamping source for recorded trade data and ensuring that source is accurately synchronized with UTC is just the first part of satisfying RTS 25's timing requirements.



Why continuous monitoring of time accuracy is critical

Article 4 of the proposed RTS 25 standard outlines the obligations for timing traceability that traders must satisfy:

"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."¹

The key point to note in the above paragraph is that traders are required to document the functioning of their system of traceability to UTC and be able to demonstrate that.

Because timing accuracy can vary due to a host of variables such as system and network load, cross traffic, temperature variation, configuration changes, and clock drift, that means traders must continually monitor and record the performance of their timing system so they can prove it was functioning correctly at any given point in time. This is the only way traders can prove that the timestamps applied to recorded trade data were accurate to within the required tolerance at the time that trade data was captured and thus satisfy the requirements of RTS 25.

How Provenance can help traders satisfy MiFID 2 requirements easily

Provenance[™], is a new feature that Endace is introducing across its network recording products to help customers to solve exactly the sort of problem that complying with MiFID 2's new regulations introduces.

Put simply, Provenance enables recorded network traffic to be automatically "watermarked" every second with a rich set of additional data fields that describe the environment and the status of that environment at the time the capture occurred. This enriched data is embedded into the stream of the captured network data, forming a permanent and easily referenceable record of the status of the environment as packets were captured. This Provenance data includes things such as the hostname, link name, capture port, capture location, link type and link speed just to name a few. Critical to satisfying MiFID 2's RTS 25 directives, Provenance data also includes a wide variety of data about the type of timing infrastructure in place at the time of capture. For example, what the timing source was, what method of time synchronization was used (PTP, 1PPS or IRIG-B) and what the accuracy of that time source was at the time of capture.

This additional Provenance data forms an embedded record of the timing infrastructure and accuracy at the time that trade data is recorded. It allows traders to address MiFID 2 directives simply and easily – without requiring a separate system or process for monitoring timing systems or imposing any overhead in correlating recorded trade data with timing data. The relevant timing data is monitored and generated automatically, and embedded in the recorded trade data as it is captured – ensuring full context is maintained. Embedded Provenance data can be easily examined using standard packet analysis tools, such as Wireshark[™], enabling easy historical analysis of trade data to ensure that MiFID 2 timing accuracy requirements were met as that trade data was recorded.

Provenance also ensures that your recording infrastructure is future-proofed. As regulatory demands or business needs evolve in the future, Provenance data can be extended to add additional data fields to enrich recorded network traffic – including custom fields that might be required for specific application usage.

A quick look at Provenance in action

The screenshots below show some of the additional information available in a Provenance record as viewed in Wireshark. As outlined above, these records are embedded in captured network traffic every second – forming a continuous record of the environment as traffic is captured.

Regulatory technical and implementing standards – Annex I. MiFID II / MiFIR. Available for download from: https://www.esma.europa.eu/sites/default/files/library/2015/11/2015esma-1464_annex_i_-_draft_rts_and_its_on_mifid_ii_and_mifir.pdf, page 505.



SOLUTION BRIEF

provenance, example, ptp.erf	- 0 ×
File Edit View Go Capture Analyze Statistics Telephony Wireless Jools Help	
∡ ≡ ∴ Ø <mark>. 3</mark> ⊠ A ⇔ ∞ ⊠ ₹ £ 3 Q Q Q <u>B</u>	
Apply a display filter <ch-></ch->	Expression +
No. Time Source Destination Protocil Length Info	^
220 36.600000057 192.168.10.18 192.168.10.120 UDP 271 14067→24863 Len=225	
221 36.770411652 ERF 1424 MetaERF Record	
222 36.800000676 192.168.10.85 192.168.10.201 HTTP 1518 HTTP/1.1 200 OK (text/html)	
223 37.000000058 192.168.10.15 192.168.10.126 UDP 271 21918⇒34572 Len=225	
224 37.200000686 192.168.10.82 192.168.10.155 TCP 1518 [TCP segment of a reassembled PDU]	
225 37.400000474 192.168.10.82 192.168.10.155 HTTP 1099 HTTP/1.1 200 OK (text/html)	
	, ≡ *
> Clock Source: PTP (5)	^
> Clock Input Port Protocol: Ethernet (4)	
> Clock State: Synchronized (2)	
> Clock Threshold: 596 nanoseconds	
> Clock PHC Index: 7	
> Clock PHC Offset: 36,00000000 seconds	
> Clock Timebase: UTC	
> Clock Description: Symmetricom XLi IEEE 1588 Grandmaster	
> Clock Output Source: Internal (6)	
> Clock Link Cable Mode: Disabled Master (3)	
> PTP Domain Number: 0	
> PTP Steps Removed: 1	
> PTP Offset From Master: -11 nanoseconds	
> PTP Mean Path Delay: 1520 nanoseconds	
> PTP Parent Clock Identity: Symmetri ff:fe:01:c1:7a (00:a0:69:ff:fe:01:c1:7a)	
> PTP Parent Port Number: 1	
> PTP Grandmaster Identity: Symmetri ff:fe:01:c1:7a (00:a0:69:ff:fe:01:c1:7a)	
✓ PTP Grandmaster Clock Quality: 0x062142ba, Clock Class: 6, Clock Accuracy: The time is accurate to within 100 ns, Offset Scaled Log Variance: 17082	
0000 0110	
0010 0001	
Tag Type: ptp gm clock quality (406)	
Tag Length: 4	
> PTC current UTC Offset: 36.00000000 seconds	
> PTP Time Properties: 0x00000003c, Current UTC Offset Valid, PTP Timescale, Time Traceable, Frequency Traceable	
> PTP Time Source: GPS (32)	
> PTP Clock Identity: EndaceTe ff:fe:01:70:a8 (00:0e:a7:ff:fe:01:70:a8)	
> PTP Port Number: 1	
> PTP For State: SLAVE (9)	
> PTP Foll State. SAKE (5)	
→ FT DC and y DC	Profile: Default
🔍 🔍 Lexx nem (nex), 12 oyee	Profile: Default

grovenance_example_ptp.ef			- 0 ×	
Eile Edit View Go Capture Analyze Statistics Telephony Wireless Iools Help				
🗶 🗏 🕲 📘 🛅 🗙 🖻 🔍 🐡 🕾 🕾 🚊 📰 🍳 Q. Q. A. A.				
R Apply a display filter <ctrl-></ctrl->			Expression +	
No. Time Source Destination Protocol Length Info			^	
88 14.59890… 192.168.10.12 192.168.10.110 TCP 723 55619→988 [ACK] Seq=7981 Ack=1 Win=5792 Len=665			_	
89 14.77041 ERF 14 MetaERF Record			^	
90 14.79647 192.168.10.24 192.168.10.125 UDP 271 5660→10370 Len=225				
91 14.99742 192.168.10.54 192.168.10.164 TCP 11 [TCP Retransmission] 9304+380 [ACK] Seq=2148767033 Ack=	214620171	3 Win=56472 Len=1119 TSval=703761991 TSecr=70376151	.2	
92 15.19838 192.168.10.12 192.168.10.110 TCP 723 55619-988 [ACK] Seq=8646 Ack=1 Win=5792 Len=665				
93 15.39934… 192.168.10.28 192.168.10.112 TCP 74 27269→80 [<none>] Seq=1 Win=5792 Len=0 MSS=1460 TSval=703762033 TSecr=0</none>				
94 15.60029… 192.168.10.12 192.168.10.110 TCP 723 55619+988 [ACK] Seq=9311 Ack=1 Win=5792 Len=665				
 MetaERF Capture Section 	^ 0000		U.wW ^	
> Capture Section Header	0010		Example	
> Name: Example capture	0020		capture/Publ	
> Description: Public exmaple capture with Provenance and PTP	0030		ic exmap le captu	
> User: admin	0040		re with Provenan	
> Application Name: dagmeta	0050		ce and P TP admindagm	
> Application Version: 5.5.1	0000		eta/ 5.5.1	
> Timezone Offset: 46800	0080		NZDT	
> Timezone Name: NZDT	0090			
✓ MetaERF Host Section	00a0		sys8000- 2	
> Host Section Header	00b0	53 79 73 74 65 6d 73 20 74 65 73 74 20 38 30 30	Systems test 800	
> Name: sys8000-2	0000	30 2d 32 00 00 0b 00 07 45 6e 64 61 63 65 00 00	0-2 Endace	
> Description: Systems test 8000-2	00d0	00 22 00 0d 48 61 6d 69 6c 74 6f 6e 2c 20 4e 5a	."Hami lton, NZ	
> Organisation: Endace	00e0		Endace H	
> Location Name: Hamilton, NZ	00f0		amilton Systems	
> Location Description: Endace Hamilton Systems Lab	0100		Lab sys8000-	
> Hostname: sys8000-2.endace.com	0110		2.endace .com	
> Model: Intel Corporation NPB8000	0120		Inte l Corpor ation NP B8000	
> Serial Number: SYS8000-2	0140		SYS8 000-2	
> Memory: 127 GiB (137356386304 bytes)	0140		.(
> CPU Model: Intel(R) Xeon(R) CPU E5-2680 v2 @ 2.80GHz	0160		Intel(R) Xeon(R)	
> CPU Physical Cores: 20	0170		CPU E5- 2680 V2	
> CPU NUMA Nodes: 2	0180		@ 2.80GH z2	
> Operating System: CentOS Linux release 7.2.1511 (Core)	0190	00 00 00 14 00 33 00 04 00 00 00 02 00 11 00 26	&	
> DAG Software Version: 5.5.1	01a0	43 65 6e 74 4f 53 20 4c 69 6e 75 78 20 72 65 6c	CentOS L inux rel	
v MetaERF Module Section	01b0		ease 7.2 .1511 (C	
> Module Section Header	01c0		ore)55.5.	
> Card Number: 1		31 00 00 00 ff 02 00 04 00 00 01 ac 00 1e 00 04	1	
> Model: DAG 10X4-P	01e0		DAG 10X4	
Einmunno Vancion: diava ataci ath dago 52 10 5000070275252 2016/00/26 16:01:06	01f0		-P= d10x4-a7 pci eth- 40ge S2. ∨	
2 Text item (text), 156 bytes	0200	70 03 09 5T 05 74 08 20 34 30 07 05 5T 53 32 2e Packets: 385 Displayed: 385 (100.0%) - Load time: 0:0.19	pc1_etn- 40ge_52. v	





How do I get Provenance?

Provenance was introduced as a new feature in the DAG 5.5.1 software release in October 2016, and is supported on all DAG 10X capture cards including the 2-port DAG 10X2-S and DAG 10X2-P cards and the quad-port DAG 10X4-P.

DAG 5.5.1 is available free to customers with DAG support.

As a key new feature of Endace's network recording technology, Provenance will also be introduced on EndaceProbe network recorders with the release of OSm 6.3, a new version of the EndaceProbe operating system, in Q1, 2017.

Conclusion

Provenance offers an easy-to-implement, and automated mechanism for continuously monitoring and recording timing accuracy data alongside recorded trade data.

Coupled with the timestamp accuracy offered by Endace DAG technology, Provenance allows traders to be confident they can ensure accurate timestamps on all recorded trades and collect and archive the data needed to meet regulatory demands that will come into force with MiFID 2's RTS 25 directive.

Endace[™], the Endace logo and DAG[™] are registered trademarks in New Zealand and/or other countries of Endace Technology Limited. Other trademarks used may be the property of their respective holders. Use of the Endace products described in this document is subject to the Endace Terms of Trade and the Endace End User License Agreement (EULA).

For more information on the Endace portfolio of products, visit: endace.com/products

For further information, email: info@endace.com