Compliance with Regulatory Mandates Demand Accurate Time Synchronization in Financial Networks

Abstract: This white paper looks at the importance of accurate and synchronized time in the financial sector and offers guidelines on implementing network time synchronization that can provide the accuracy needed for financial organizations to stay compliant with regulatory mandates.

Today, businesses increasingly rely on a globally connected network to communicate internally and externally. Using devices such as workstations, PCs, laptops and emerging smart devices companies exchange confidential, private, financial, and corporate information. With the ever increasing volume of confidential and sensitive information traversing networks and crossing geographic time zones, the need for accuracy of time synchronization of all connected elements is a much needed but difficult challenge. If time stamping is not accomplished, logs and audit trails become impossible to establish when a certain event took place. This inability to time stamp events could impact the overall productivity and efficiency of the corporation. Furthermore, with increased regulatory constraints and compliances in a highly volatile sector whose business is to track financial transactions, an inaccurate time source can cause significant problems.

IT organizations in financial institutions are mandated to keep accurate records of all transactions such as when a transaction was initiated and completed along with the real-time date and time stamps for each transaction.

In general, clocks on computers that serve as the time source are notorious for drifting. A typical clock in most computers' is based on an inexpensive oscillator circuit or a battery backed quartz crystal clock which could easily drift seconds or even minutes per day depending on the type of oscillator. The oscillator is usually priced based on its quality which in turn dictates the performance. To overcome this, time synchronization can be accomplished by different means using time synchronization protocols such as NTP (Network Time Protocol) or PTP (Precision Time Protocol), typically from a GPS-based receiver.

Additionally, a financial institution must plan and implement a timing infrastructure that is protected against malicious attacks wherein an attacker modifies the network clock that can end up compromising the integrity of the financial system.

Regulatory mandates and the need for time accuracy in the financial industry

Compliance to regulatory mandates demand that the network time synchronization be very accurate. Highlights of a few regulatory mandate requirements are shown below.

- Accuracy of financial reporting based on proper time and event synchronization
- Elimination of fraudulent security trades. Accuracy of time and time stamping provides proof of when a transaction occurred or did not occur, which helps in digital forensics
- Protection of consumer information from being modified wherein every access of sensitive information is recorded for auditing with real time date and time stamp details
- Security of cardholder data in online or retail transaction networks

The risk associated with inaccurate time in an organization's network and the impact of this error in time on financial applications may include legal liability for negligence. Network time synchronization supports many laws and standards that demand network accuracy, security and reliability. Below are highlights of some of these standards and standard bodies that use time synchronization to meet compliance mandates.

Compliance with Regulatory Mandates Demand Accurate Time Synchronization in Financial Networks

Sarbanes-Oxley (SOX) Compliance

SOX compliance addresses the regulatory issues related to any backdating of stock grant date accuracy. Accurate timing of transaction, stock or otherwise, is fundamental to any SOX report.

Sarbanes-Oxley Compliance (SOX)	
What is it?	Validity of Financial statements with strict internal audit and control
Who does it apply?	All U.S. publicly traded companies
Requirements	Support authentication, **time stamping** for audits, security policies

Gramm-Leach-Bliley Act (GLBA)

GLBA ensures the protection of consumers' private financial data with accurate date and time stamping details from unauthorized use of access.

Gramm-Leach-Bliley Act (GLBA)	
What is it?	Protect consumer's private information at financial institutions from modifications
Who does it apply?	Banks, Security firms, insurance and other institutions providing financial products and services
Requirements	Provide reports with clear audit trail with user access date and **time stamp** details

Order Audit Trail System (OATS)

This is a process for all securities firms doing business in the US, where each order event is recorded and stored for data analysis and auditing thus providing market transparency. It includes strict guidelines on clock synchronization and the time source used for synchronization.

Order Audit Trail System (OATS)	
What is it?	Integrated audit trail of order, quote, and trade information for NASD* and OTC equity securities
Who does it apply?	All securities firms doing business in US under FINRA** regulation
Requirements	Electronically capturing and reporting of specific data elements related to handling or execution of orders with **time stamping** using a synchronized clock

Payment Card Industry-Data Security Standard (PCI-DSS)

PCI-DSS is the governance established for the Credit Card Industry whereby all access to the cardholder data has to be time stamped using a highly accurate time source. A detailed specification related to time synchronization was updated to version 1.2 in October 2008. In Section 10.4 of this governance requires an entity to "synchronize all critical system clocks and time".

Payment Card Industry – Data Security Standard (PCI-DSS)	
What is it?	Comply and log all access attempts to the cardholder data environment in real-time with data and time stamp
Who does it apply?	Any business that stores and transacts payments using cardholder data
Requirements	Implement automated audit trails to verify use of identification and authentication methods with real-time date and **time stamps**

*NASD – National Association of Securities Dealers
**FINRA – Financial Industry Regulatory Authority

Compliance with Regulatory Mandates Demand Accurate Time Synchronization in Financial Networks

Importance of a Network Time Synchronization System

To ensure that the above mandates and compliance requirements are met, financial institutions should develop a detailed architecture requirement around time synchronization and ensure proper deployment as part of their IT architecture. The cost of implementing a time service infrastructure to an organization is small while the benefits are far more significant. To make time both pervasive and accurate, implementing some key basic elements will go a long way in achieving synchronization throughout any organization.

Five essentials for implementing highly accurate time synchronization in the network are show below.

- An Accurate Time Source
- A Robust Timekeeping Architecture
- Efficient Server Management
- Robust Network Time Management Policy that is Secure, Verifiable, and Auditable

A brief description of each of the essentials and its impact on Time Synchronization is given below.

Accurate Time Source is a Must

Ultimately, accurate time must come from a reliable time source. How accurate that time needs to be depends on the financial applications and operations performed. Most network operations (e.g., online security, log files updates) require accuracy on the order of 1 to 10 milliseconds. Most financial business applications require accuracy in the 100 millisecond to 10 microsecond range—even if only to accurately establish the order of events. Financial institutions typically acquire time in one of two ways: 1) over the Internet from the National Institute of Standards and Technology, NIST, or a third-party time service; 2) from GPS satellites. If time is acquired over the Internet, organizations may use NTP (Network Time Protocol), or PTP (Precision Time Protocol) protocols used for synchronizing the clock on client machines with clocks on network time servers. If using time from GPS satellites, this usually is in the form of a GPS referenced time server that delivers time to the local network which in turn is distributed to client machines within the network. A GPS time source is highly accurate and is usually within a few microseconds to UTC.

Robust Time Keeping Architecture

Acquiring UTC from GPS requires taking the signal off the air and delivering it to the clients (PCs, workstations, servers, controllers, etc.) that rely on accurate time for event synchronization and time stamping. Since very few clients come equipped with reliable network time synchronization software, this implies that besides the GPS receiver itself there has to be a way to distribute time from the GPS receiver to the clients. In other words, the organization needs a time distribution network—ideally an architecture of deployed time servers and time clients. Time servers acquire time from GPS receivers and distribute time in response to client requests. Depending on the size and topology of the financial network, there may be a need to install multiple time servers in a certain configuration:

- To support multiple LANs
- As a backup
- To handle peak load volumes of client requests
- To handle special time-sensitive applications

The choice of GPS receiver, the choice of network time servers, and the architecture of the network are key to delivering an accurate time to the network.

Below are a few factors to consider when making choices about the server:

- Server performance
- 10/100/1000 Base-T Ethernet
- Redundant Time Sources
- Built-in time reference

Efficient Server Management

How should a financial institution control a network time server? The answer probably is: Any way it prefers to. Some organizations might prefer to access devices via a web interface; some through a comprehensive network management suite, such as OpenView, while others might rather just work with the device using a built-in keypad. Or the same organization may, from time to time, employ more than one of these methods, depending on the specific situation. A web or telnet interface offers a light client "footprint" and easy accessibility from any networked computer. The virtues of network management solution are that it allows the operator to monitor all network devices from a single console. In such a scenario, the device must offer SNMP (Simple Network Management Protocol) support so managers can monitor the device via any management software that also supports the same protocol. They can then control the device remotely via the web or telnet interface, or control the device locally using its keypad.

Compliance with Regulatory Mandates Demand Accurate Time Synchronization in Financial Networks

Robust Network Time Management

Managing a set of devices within a network is different from managing specific devices. The availability and reliability of accurate time across the entire network—not just a part of it—must be guaranteed. Network time servers must work in sync, their operation should be centrally controlled, the processing load should be balanced, and financial governance policies on issues such as security and confidentiality should be enforced. Nor should providing network-level management be so burdensome to network administrators that it interferes with other priorities they would normally have to attend to as part of their daily routine.

The network management would typically run on a central workstation, from which it would connect securely to a trusted network time source (such as a dedicated GPS referenced time server) and to clients. It in turn then distributes that time accurately and verifiably to every time-aware machine on the network. All time servers and clients should be individually identified using a unique serial number that is assigned when the management layer software is installed on the workstation. Administrators at this workstation are then able to perform the following activities.

- Perform core setup functions such as installation, monitoring, configuration and trouble shooting on all time servers
- Monitor time synchronization financial enterprise-wide
- Implement network wide time-keeping mitigation strategies such as time-source averaging, clock training, skewing
- Automatic failover of servers
- Safeguard against malicious or inadvertent tampering of network time keeping

Secure, Verifiable Audit Trail

A time synchronization infrastructure requires an audit capability. The whole point of a timekeeping infrastructure is to provide assurance that events happen on time and that the actual time of events can be verified. The audit trail is that assurance. This capability would typically take the form of a dedicated audit server—which makes sense given the fact that good auditors usually stand apart from the entities that they audit. This ensures integrity of the process—because time can be verified independently of the clocks subject to the audit—and because the process can be better isolated from security threats. The function of the audit server is to prove conclusively (and on demand) whether the time on any monitored system was correctly synchronized at a particular time and date with the specified time source. Below are four requirements that must be met for successful time auditing:

- Monitored machines must be reliable and individually identifiable
- Time on individual machines must be synchronized regularly and accurately with a known time source
- Vital information must be easily retrievable
- Synchronization information must be collected and compiled into concise and complete audit trails on a regular basis
- Immediate alerts must be generated when any monitored machine fails to be synchronized with acceptable intolerances

It is this type of audit capability that is typically required by federal regulations (e.g., SOX, PCI-DSS, GLBA and OATS described earlier) as well as by major securities organizations like NASD to prevent fraud and establish the validity of financial transactions.

Microsemi® Network Time Servers Offers Performance And Accuracy to Support Compliance And Governance Needs Of Financial Enterprise Networks

Timekeeping is not something financial organizations—in particular, network administrators in those organizations—want to spend a lot of time thinking about. If they start with a simple timekeeping infrastructure—based on specifics presented here—they will not have to. And neither will their users. Microsemi's current generation of GPS NTP/PTP network time synchronization products with atomic clock accuracy that is also available with a Rubidium atomic clock option ensures that time is synchronized and accurate throughout the financial enterprise network. Microsemi time servers protect network log file accuracy, security, billing systems, electronic transactions, database integrity, and many other essential applications needed by financial institutions to claim compliance to regulatory mandates. The Microsemi SyncServer Network Appliances make it easy to manage and monitor time synchronization through workstations, servers and routers, thus assuring the highest integrity of the time source throughout the network.

Microsemi

Microsemi Corporate Headquarters
One Enterprise, Aliso Viejo, CA 92656 USA
Within the USA: +1 (949) 380-6100
Sales: +1 (949) 380-6136
Fax: +1 (949) 215-4996

Microsemi Corporation (Nasdaq: MSCC) offers a comprehensive portfolio of semiconductor solutions for aerospace, defense and security; enterprise and communications; and industrial and alternative energy markets. Products include high-performance, high-reliability analog and RF devices, mixed signals and RF integrated circuits, customizable SoCs, FPGAs, and complete subsystems. Microsemi is headquartered in Aliso Viejo, Calif. Learn more at
www.microsemi.com

©2014 Microsemi Corporation. All rights reserved. Microsemi and the Microsemi logo are trademarks of Microsemi Corporation. All other trademarks and service marks are the property of their respective owners.