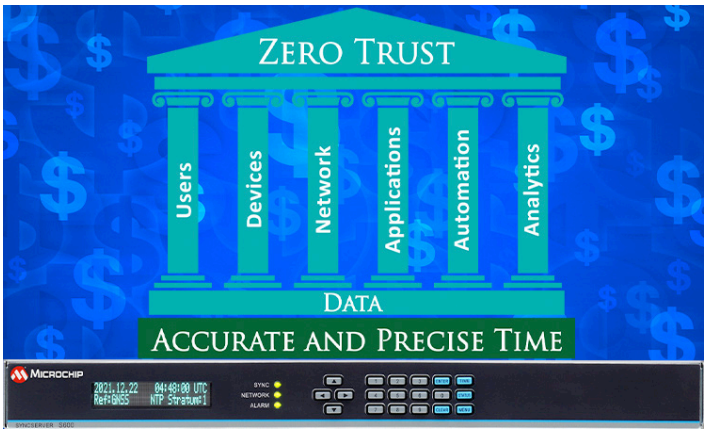
What Is Trusted Time for Zero Trust Financial Networks and Why Does it Matter?

Summary

A financial/banking firm that is rolling out a Zero Trust Architecture should care a great deal about accurate time synchronization of the network and the time server that provides it. Accurate time is essential for network operations, and the security aspects of the time server which is attached to the network, must be trusted in many respects. The SyncServer is unsurpassed in both its ability to deliver accurate time, as well as its compliance to the principles of Zero Trust.



Why Time Matters

Information Technology (IT) security at a bank is responsible to protect data, resources, money, personal information and much more. Part of that role is managing the who, what, where and ***when*** of all network activity as well as validating every device allowed to connect to the bank's network. The Zero Trust Architecture and the Payment Card Industry Data Security Standard (PCI-DSS) were created to help address these security challenges.

Timestamp Chaos Avoidance

Network-wide time synchronization accuracy and the essential role it plays in network management and security are often taken for granted. Imagine what would happen if every network device had a different time. Chaos would break out across the bank's network. Log files and network telemetry would be useless as logs and telemetry timestamps would not correlate. For example, syslogs that would be received in real time but backdated to the previous week would not be helpful. Dashboards would fault, or at least present incorrect data, and would most likely trigger alarms. Critical processes would either start too soon or too late. Network forensics would be nearly impossible, audits would be meaningless, video timestamps would be incorrect, etc. Time accuracy across a bank's network, or any organization's network, is important and it does matter.

Network Time Source Matters

Because time is so important, you need to consider the who, what, where and ***when*** of the source of time for network time synchronization. Time servers providing the Network Time Protocol (NTP) timestamps are the "what." If the "who" and "where" are merely an IP address of a time server from the Internet or Internet NTP server pool, then consideration needs to be given to the validity and vulnerability of the "when" of the NTP timestamps that are received. Time from the Internet violates just about every principle of Zero Trust and cannot be considered trusted time.

What Is Trusted Time?

Assuming you're getting time using NTP from somewhere for your network, Zero Trust raises two key questions. Is the time implicitly or explicitly trusted? And is the time server itself, as a device connected to the bank's network, compatible with Zero Trust networking technologies?

Trusted time means the time server is trusted with respect to the accuracy and legitimacy of the time. It also means the time server is trusted as a device connected to the network and is compliant with the company's Zero Trust security requirements.

Why the SyncServer® Time Server is a Trusted Time™ Server.

As the most secure Trusted Time™ network device available, a SyncServer® time server complies with the fundamental pillars of the Zero Trust model*, which include users, devices, network, applications and analytics, Figure 1.

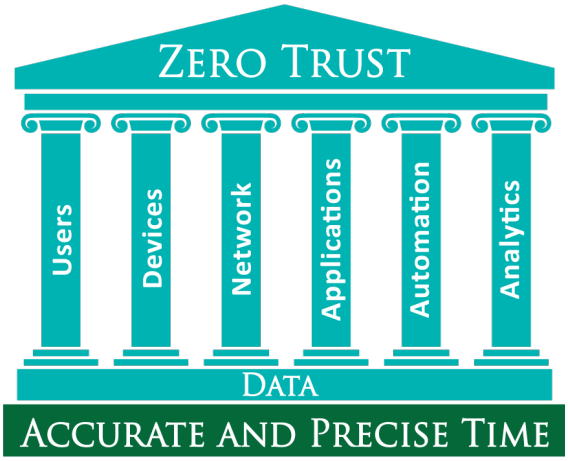


Figure 1. Accurate and precise time are foundational to Zero Trust networks

The SyncServer time server also conforms to the core components outlined in *NIST Special Publication 800-207: Zero Trust Architecture*. Figure 2 is a simplified representation of applicable core components showing how the SyncServer interoperates between the NIST data plane and control plane.

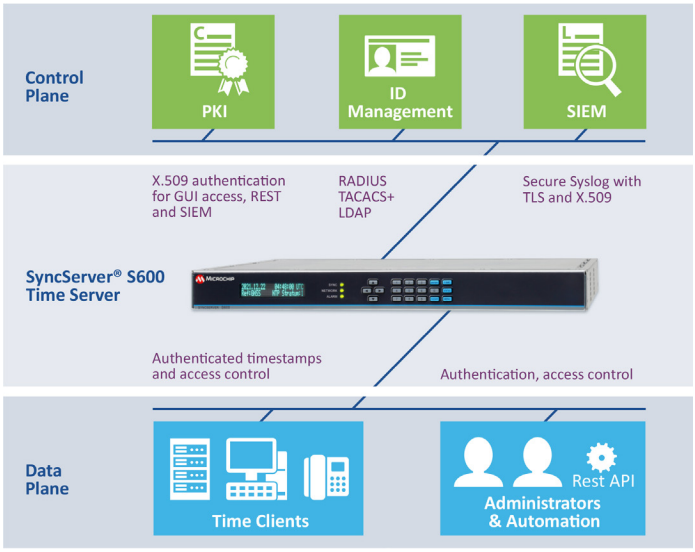


Figure 2. Interoperability of the SyncServer between the NIST defined Data Plane and Control Plane

The base Zero Trust premise is no implicit trust of anything, which includes the time and the time server. There are a number of scenarios for implementing trusted time in a Zero Trust architecture using a SyncServer time server. We have created infographics for many of these scenarios. In each graphic, the security technology in the SyncServer time server and the related Zero Trust pillars are highlighted for easy reference. You can view all the infographics here.

Learn More About Trusted Time

If your organization is moving towards a Zero Trust Architecture, we have created a focused application note that explains why trusted time is so important in a Zero Trust network. This short document explains how the SyncServer network time server ensures the security of time and complies with Zero Trust principles. It includes a detailed list of the SyncServer's security features and how they align with the Zero Trust model's pillars. Your bank's security team can use this helpful checklist, Figure 3, for determining SyncServer S600/S650 compliance to your network's security requirements.

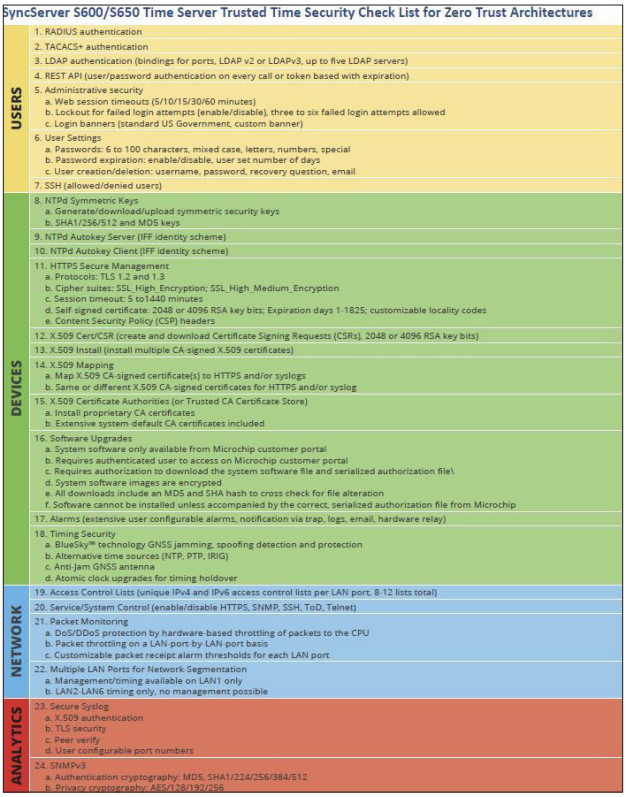


Figure 3. SyncServer S600/S650 Time Server Trusted Time Security Check List for Zero Trust Architectures

Be Zero Trust Time Compliant

As the most secure Trusted Time network device, the SyncServer time server is best suited to support Zero Trust initiatives at banks and financial institutions. It ensures the security of time and its sources, as well as complies with the fundamental pillars of Zero Trust.

Links to Resources

Web Page: Trusted Time for Zero Trust Networks

Application Note: Trusted Time for Zero Trust Networks

**American Council for Technology-Industry Advisory Council (ACT-IAC), Zero Trust Cybersecurity Current Trends April 18, 2019*

MICROCHIP