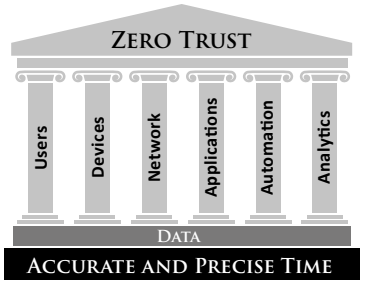
Trusted Time for Zero Trust Networks

The TimeProvider® 4100 grandmaster clock is the foundational source of Trusted Time to enable smooth operation of zero trust networks.



Summary

Time is central to accurate log files that define the who, what, when and where of all activity in a zero trust network.

Accurate, reliable and secure Trusted Time is foundational to zero trust networks. Without it, authentication mechanisms will fail, essential log file time stamps will not align, zero trust analytics will be unreliable and forensics will be hampered, among other possible issues.

Not only must the time be correct, but the PTP grandmaster must also comply with zero trust principles and fit into a zero trust architecture.

As the most secure Trusted Time™ network device, the TimeProvider 4100 IEEE® PTP 1588 grandmaster is well suited to support zero trust initiatives. It ensures the security of time and its sources and complies with the fundamental pillars of zero trust including users, devices, network and analytics.

Key Features of TimeProvider 4100 Grandmaster

- Support for the Authentication, Authorization and Accounting (AAA) framework
- Support for RADIUS and TACACS+ protocols
- Two-factor authentication (2FA)
- Hardened user interface
- Latest security standards in IEEE 1588-2019
- Time source validation
- Network segmentation support

Accurate time is the foundation of zero trust. Time in a zero trust network delivers an accurate time stamp in a log file. The National Institute of Standards and Technology (NIST) standard on zero trust includes time stamps for logs and recent White House executive orders for implementing zero trust and remediation capabilities related to cyber security incidents define the log file time stamp format and the source of the time[iii].

Cyber security relies on log files with accurate and precise time stamps.

Security Information and Event

Monitoring (SIEM) systems used in zero trust analytics rely on accurate and timely network telemetry. This includes accurate log file time stamps to help in identifying security incidents, policy violations, fraudulent activity and operational problems, auditing, forensic analysis, internal investigations, the establishment of baselines and the identification of operational trends and long-term problems[iv].

Time stamps originate from time-synchronized servers and systems. At a minimum, the systems generating the log files for the SIEM must be time synchronized with each other to prevent timeline chaos and the hampering of rapid incident response and fault diagnosis.

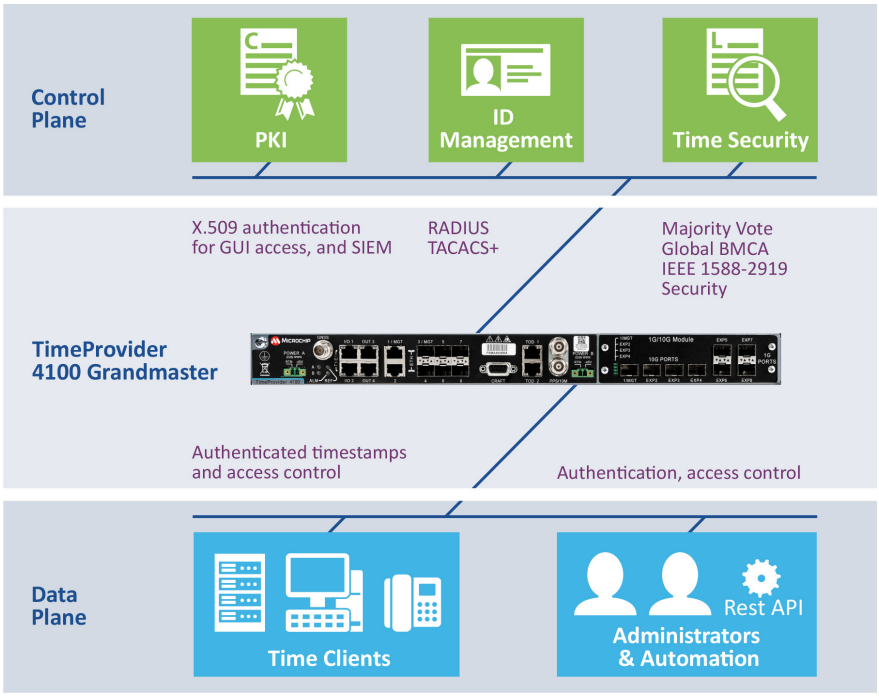
PTP grandmasters provide the time synchronization for network servers. A device such as the TimeProvider 4100 PTP grandmaster is the accurate, reliable and secure source of time for critical network servers that generate vital log files for the SIEM.

The TP4100 grandmaster is security hardened to reside on the zero trust network as a time service provider to the zero trust network and to incorporate zero trust user, device and network pillar principles in its design.

Authenticated time is essential. Network Time Protocol (NTP) packets are, by definition, sent in the clear, which makes them subject to easy manipulation in transit. For zero trust time synchronization, NTP authentication must be enabled to ensure the TP4100 grandmaster and NTP client association are trusted and to confirm the time stamps are unaltered.

PTP grandmasters must fit in the zero trust paradigm. Trusted Time is an essential aspect of a properly functioning and hardened zero trust network. Without the most basic notion of accurate and synchronized time across the zero trust network, many of the pillars of zero trust will not function reliably.

The TimeProvider 4100 PTP grandmaster delivers the trusted time for zero trust networks. The TP4100 grandmaster is foundational in supporting the pillars of zero trust networking and enabling accurate log file time stamps through secure, accurate and reliable network-wide time synchronization.



Users With Management Access to the PTP grandmaster Must Be Authenticated and Authorized

Users

The first line of defense in the TimeProvider 4100 PTP grandmaster is the physical segmentation of management and service ports on the network. Because PTP grandmasters must be configured by either humans or machines, protocols such as RADIUS or TACACS+ provide the robust authentication and authorization needed for access. TimeProvider 4100 grandmaster supports two-factor authentication with RADIUS, which requires an additional login credential beyond just the username and password to gain account access. Also with TACACS, the TP4100 grandmaster allows the definition of a specific port for more secured access and flexibility.

PTP grandmasters also need strict control over local access including robust password requirements, rotation and more.

The PTP Grandmaster is a Device on the Zero Trust Network Where Everything About It Must Be Authenticated and Trusted

Devices

At the most basic level, symmetric key authentication used between time clients and the TP4100 grandmaster ensures time packets are not altered in transit. Strong keys, such as MD5, SHA-1 and SHA-512, should be used to create the hashes to authenticate the timing packets.

While the feature-rich TP4100 grandmaster web GUI used to monitor and upgrade the unit is easy to use, that interface must be extremely hardened. To harden the interface, X.509 certificates should be used to authenticate the TP4100 grandmaster to the user's browser in addition to using secure TLS 1.2-based encryption of the link.

Zero trust also includes software updates for the PTP grandmaster. Only authenticated and authorized users are allowed access to TP4100 grandmaster software downloads. Software images are encrypted to prevent modifications and hashes are provided to ensure there are no modifications in transit. These downloads also include encrypted authorization files that control TP4100 grandmaster software installation. Before software installation, the TP4100 grandmaster authenticates versions and software integrity.

The TimeProvider PTP grandmaster system software is a custom tailored, hardened, current and embedded Linux® distribution that includes only what is needed to operate the custom hardware. This decreases any potential attack surface as software that might be found connected to a Common Vulnerability and Exposure (CVE) in a broad Linux distribution is not even present/loaded in the TP4100 grandmaster .

The PTP Grandmaster Should Provide Timing Security

The GNSS satellite system, from which the Stratum 1 TP4100 grandmaster obtains its time, can no longer be assumed

to be trustworthy. GNSS jamming and spoofing threats are becoming more prevalent, which means that a zero trust approach must now be taken.

GNSS validation takes the form of monitoring the local RF environment for anomalies and validating the data in the received GNSS signals. The TP4100 grandmaster interoperates with BlueSky™ firewall jamming and spoofing detection and protection capabilities to continuously validate GNSS.

At the core of the network, enhanced PRTC (ePRTC) units use local Cesium atomic clock systems and time of day input from National Laboratories to compare with GNSS signals with the goal of identifying potential jamming or spoofing of the time reference.

Multi-band receiver technology is included in every TP4100 grandmaster device to help mitigate issues on a specific frequency that can potentially be due to a security threat as well.

If a GNSS input is showing anomalous timing or other suspicious behavior, the TP4100 grandmaster does not disqualify this time reference immediately but enters into intermediate persistence and bridging phases before deciding to transition to holdover.

The TP4100 grandmaster also implements mechanisms to leverage other grandmasters in the network as a back-up to GNSS. This is called Assisted Partial Time Support (APTS) with Automated Asymmetry Correction (AAC), which allows the TP4100 grandmaster to keep operating if GNSS is deemed unreliable.

The TP4100 grandmaster also implements security mechanisms introduced as part of IEEE 1588-2019, the latest PTP standard. PTP 2019 defined a majority vote to eliminate some reference inputs into the device if they appear to be unreliable. In addition, a Global Best Master Clock Algorithm (G-BMCA) can then select the best input while considering the quality and performance of the network and the most efficient back-up.

The PTP Grandmaster Should Segment the Network Physically and Logically and Defend Against DoS Attacks

Facilitating segmented perimeters of the zero trust network, TP4100 grandmasters incorporate eight to sixteen physically isolated LAN ports to provide NTP/PTP timing services. Logical separation using VLANs allows for 256 unique interfaces. There is no cross traffic between ports and all ports have unique network configurations. Management access is limited to a single LAN port for further isolation from the network.

For Denial of Service (DoS) attack protection, TP4100 grandmasters incorporate unique NTP reflector technology that provides line speed, high-capacity NTP service and packet limits to prevent host overrun and alarms. Network traffic above user-set thresholds trips alarms while the TP4100 grandmaster services only timing packets. If there is a threat, the Dos load will not fault the TP4100 grandmaster CPU.

PTP Grandmasters Provide the Reliable Timeline Foundation Analytics Required to Manage Defenses in Real Time

Analytics rely on network telemetry data to provide the insights that enforce zero trust. These data are log files that contain time stamps providing the "when" of the event or activity. In addition to time synchronizing all devices on the network that are sending logs, the TP4100 grandmaster also provides essential logs. The TP4100 grandmaster supports exporting system logs to up to four remote log servers and integrates with the TimePictra® management platform to monitor and check the last configuration changes via autonomous messages and validate firmware versions.

Irrational Implicit Trust of "Free Time From the Internet"

Acquiring time from a public Internet PTP grandmaster breaks every principle and tenet of zero trust and grants implicit trust to an IP address somewhere on the Internet that happens to return an NTP request for time.

This unauthenticated, publicly advertised PTP grandmaster, which is outside every zero trust security perimeter in a pool with other publicly advertised PTP grandmasters, provides a time stamp that can be manipulated easily in transit, is subject to DoS attacks that can curtail service, can potentially be used in DoS amplification attacks or be subject to GNSS jamming and spoofing.

In addition to the difficulty of tracing a bad time stamp, there is no visibility or control over where the remote PTP grandmaster is getting its time or any of the controls surrounding its management, which makes it an unsuitable time service resource for use in a zero trust network.

Zero trust requires that the critical and essential PTP grandmaster be inside the perimeter, protected, authenticated and monitored to assure security, accuracy and reliability of foundational time services to the network.

Pass Your Next Zero Trust Audit With the TimeProvider 4100 Series PTP Grandmaster

TheTimeProvider 4100 PTP grandmaster, when properly configured in a zero trust network, meets all the applicable foundational pillars to provide accurate, reliable, secure and Trusted Time to the zero trust network.

References

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

ii NIST Special Publication 800-207 Zero Trust Architecture, August 2020

iii The White House, Executive Order on Improving the Nation's Cybersecurity, May 12, 2021; Executive Office of The President, Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents, M-21-31, August 27, 2021; Executive Office of The President, Moving the U.S. Government Toward Zero Trust Cybersecurity Principles, M-22-09, January 26, 2022

iv NIST Special Publication 800-92, Guide to Computer Security Log Management

v National Security Agency Cybersecurity Report, Hardening SIEM Solutions, A Technical Report from Network Infrastructure Security, October 29, 2019

TimeProvider 4100 Trusted Time Security Checklist for Zero Trust Architectures

USERS	1. RADIUS Authentication, Authorization and Accounting (AAA) and two-factor authentication
	2. TACACS+ authentication AAA and configurable port
	5. Administrative security
	a. Web session timeouts (5/10/15/30/60 minutes)
	b. Lockout for failed login attempts with five failed login attempts allowed
	c. Custom login banners
	6. User settings
	a. Passwords: 6 to 100 characters, letters, numbers, special characters
	b. User creation/deletion: username, password
	c. Multiple user privilege levels
	7. Full SSH config. with high/medium config. security suite
	8. AAA, accounting/logging, used commercial authentication servers
DEVICES	8. NTPd symmetric keys
	a. Auto-generate/edit/symmetric security keys
	b. MD5, SHA-1, SHA-256 and SHA-512 keys
	9. HTTPS secure management
	a. Protocols: TLS 1.2
	a. Cipher suites: SSL_High_Encryption; SSL_High_Medium_Encryption
	b. Session timeout: five to 1440 minutes
	c. Self-signed certificate: 2048 or 4096 RSA key bits; expiration days 1-1825; customizable locality codes
	16. Software upgrades
	a. System software only available from Microchip customer portal
	b. Requires authenticated user to access on Microchip customer portal
	c. Requires authorization to download the system software file and authorization file
	d. System software images are encrypted
	e. All downloads include an MD5 and SHA hash to cross-check for file alteration
	f. Software cannot be installed unless accompanied by the correct authorization file from Microchip
	17. Alarms (extensive user configurable alarms, notification via trap, logs)
	18. Timing security
	a. Alternative time sources (NTP, PTP)
	b. Atomic clock upgrades for timing holdover
	c. Bridging/persistence/holdover mechanisms
	d. ePRTC uses long term local Cesium and ToD from National Labs vs GNSS
	e. Global BMCA and Majority Vote (1588 2019)—up to three PTP client instances
	f. APTS and AAC as alternatives to GNSS
	g. Multi-band GNSS
	h. Physical signal monitoring with configurable alarm thresholds
NETWORK	20. Service/system control (enable/disable HTTPS, SNMP, SSH, ToD)
	21. Network timing security with configurable alarm thresholds
	22. Packet monitoring
	a. DoS/DDoS protection by hardware-based throttling of packets to the CPU
	b. Packet throttling on a LAN-port-by-LAN-port basis
	23. Multiple LAN Ports for network segmentation
	a. Management/timing available on ETH1/ETH3 and EXP1
	a. ETH1-8 and EXP1-8 timing service ports only; no management possible (enabled/disabled)
ANALYTICS	23. Syslog
	a. User configurable port numbers
	24. TimePictra® platform monitoring checks last configuration changes, autonomous messaging and firmware versions
	25. SNMPv3
	a. Authentication cryptography: MD5, SHA1
	b. Privacy cryptography: AES/128/192/256

DS00004788A

MICROCHIP