TimeSource Master Clock

SECURE VERIFIABLE TIME DELIVERY

PRODUCT | DATA SHEET

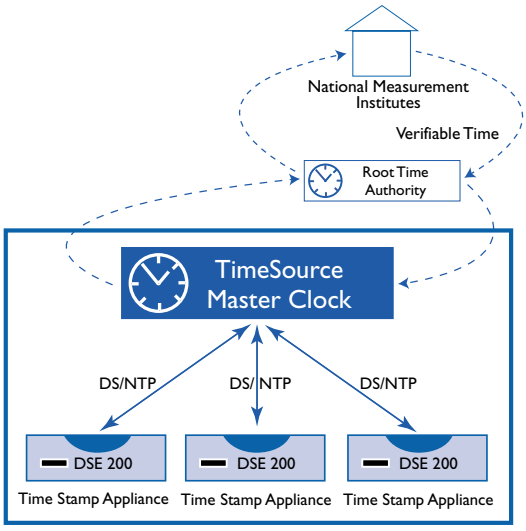
nCipher's TimeSource Master Clock (TMC200) is a network appliance incorporating a Rubidium atomic clock that can securely distribute accurate time throughout an organization. Deploying an authenticated and encrypted version of the industry-standard NTP protocol ensures the secure delivery of auditable time to multiple DSE200 time stamp appliances from a single source. For organizations that require an audit record of periodic calibration by a Root Time Authority, the TMC200 can also use this secure transport protocol to provide a certified record of synchronization to a recognized source of Coordinated Universal Time (UTC).

THE IMPORTANCE OF TIME

The validity of today's business systems and processes depends on their use of trustworthy and standardized time. In an increasingly connected world, network systems and tools must all reference a common and accurate time source in order to interoperate successfully. In the business world discrepancies between computer clocks may lead to transactions being recorded before the start of the trading day or money being credited to an account before it is withdrawn from another. Many leading edge technologies such as VoIP rely upon synchronized time and many security protocols, such as Kerberos (and therefore Active Directory), depend on accurate time synchronization between the computers that are participating in the authentication request.

Increasingly, legislation and compliance requirements mean that electronic data and documents must embody authoritative proof of time in order to establish when an event occurred. Audit requirements also highlight the need to verify the integrity of the data indefinitely. A time stamp can link a digital signature, used to prove the integrity of data, to the original digital certificate, allowing the signature to be verified, even if the certificate has expired or has been revoked. This allows the validity of documents to be checked long after the original digital signature was applied. However, this verification depends on the use of a common and trusted time framework that establishes the following:

- Accuracy of time – that clocks maintain accurate time values
- Reputable source of time - that time values can be synchronized to an internationally recognized source of Coordinated Universal Time (UTC)
- Integrity of time – reassurance that the time cannot have been manipulated
- Verification of time – an audit chain to a trusted underlying time source



Enterprise Time Infrastructure

TMC200 - A CENTRAL TIME RESOURCE

Time-stamping has emerged as one of the key components of public key infrastructure technology (PKI), delivering non-repudiation and ensuring the integrity of data is verifiable at a future point in time. TMC200 is fully compatible with nCipher's DSE200 time stamping appliance, providing a central, verifiable time source for inclusion within digital time-stamp signatures. At the heart of the system is a secure time delivery protocol, DS/NTP, which protects time values from network attack.

nCIPHER™

There are two distinct ways in which a DSE200 time stamping appliance can acquire time from a TMC200. Firstly, a Root Time Authority, such as National Measurement Institute, may deploy a TMC200 to provide a direct time calibration and audit service for any time stamping appliance connected via DS/NTP. Secondly, large organizations may choose to deploy a TMC200 as a central, internal time source for multiple DSE200 devices. Such enterprises may already have well established procedures for the acquisition of time and the TMC200 can be configured to use an existing organizational time source as its primary reference for secure time distribution. Alternatively, some organizations may require an audit record of periodic calibration to UTC time. In this instance a DS/NTP connection from an internal TMC200 to a Root Time Authority can provide a certified record of synchronization to a recognized source of UTC time.

ENSURING ACCURACY AND IN INTEGRITY

Given that local computer time is easy to change, standard NTP communications are insecure and even wireless transmissions are open to compromise, a secure and verifiable pathway to a trusted source of time is an essential prerequisite for business processes.

The TMC200 incorporates a number of controls to maintain the integrity of time values.

- The Rubidium atomic clock ensures accuracy, avoiding the need for regular re-calibration. This allows the TMC200 to be isolated within a secure environment, behind an internal firewall, protecting the time source from unauthorized manipulation
- The TMC200 uses a secure transport protocol, DS/NTP, incorporating mutual authentication, to establish a secure link to a DSE200 time stamping appliance or to a Secure Root Clock at a Root Time Authority. The cryptographic keys used in this authentication process are secured in a FIPS 140-2 Level 3 Hardware Security Module, ensuring that time values cannot be compromised in transit
- DS/NTP incorporates an automatic process of auditing and calibration to synchronize time. At the end of the process the TMC200 issues a signed certificate attesting to the calibration and traceability of the time. The signing keys used in this process are protected by a FIPS 140-2 Level 3 Hardware Security Module

SIMPLE MANAGEMENT AND DEPLOYMENT

The TMC200 is a networked appliance that is simple to setup and manage. Once the unit is connected and configured using standard built-in tools, management is achieved using a set of web based forms. Management functions may be carried out from any accessible point on the network. Access to the management interface requires user authentication and is secured using a standard HTTPS (SSL/TLS) connection.

TECHNICAL SPECIFICATIONS

- Form Factor: 1U (1.75") x 17" W x 18" D (4.5cm x 43.2cm x 45.7cm)
- Network: Dual 10/100 Base-Tx Ethernet
- Serial Port: DB-9
- Video Port: 15 pin VGA
- 2 USB 1.1 ports
- Input Voltage: 100-240 volts AC auto switching, 50-60Hz (nominal)
- Maximum Power Consumption: 240 watts (2.1 amps at 110 volts AC)
- Mounting Systems: 19" rack mount
- Temperature/Humidity (Operational): +10 to +35oC, 10 to 85% relative humidity, non condensing
- Acoustic Noise: <50dB at 1m in front of the system at full load

Front Panel

Connectors:

- Dual Ethernet port
- Serial Port for communications
- VGA connector for VDU
- Dual USB ports

LED Indicators:

- Power
- HDD Activity
- Ethernet Activity
- HSM status

Rear Panel

- Power: On/Off
- Modem port

Standards Certifications:

- FCC: CFR47, Part 15, Subpart B, Class A
- CE: EN55022, Class A; EN55024-1; EN60950
- FIPS 140-2 Level 3 certification

nCipher Inc.
500 Unicorn Park Drive
Woburn, MA 01801 USA
Tel: +1 (781) 994 4000
E-mail: ussales@ncipher.com

nCipher Corporation Ltd.
Jupiter House, Station Rd.
Cambridge, CBI 2JD UK
Tel: +44 (0) 1223 723600
E-mail: int-sales@ncipher.com

nCipher Corporation Ltd.
15th Floor, Cerulean Tower,
26-1 Sakuragaoka-cho, Shibuya-ku,
Tokyo 150 8512 Japan
Tel: +81 3 5456 5484
E-mail: int-sales@ncipher.com

Visit our Web site at www.ncipher.com – today!

Redefining cryptographic security

nCIPHER™