The SecureTime Server is a complete and easy-to-install solution that creates a trusted TimeStamp Authority at your location. The hardware is a stand-alone network appliance that provides auditable timestamps. The hardware uses a National Institute of Standards and Technology certified (NIST) tamper-detecting security module that contains the clock, clock audit trail, and PKIX timestamp creation software. For over 20 years, DigiStamp's Internet-based service (hardware, software, and processes) has been proven reliable, creating millions of timestamps for thousands of customers.

You can try a SecureTime server from your computer by using DigiStamp's Internet-based service and our desktop software.

SecureTime® Server Highlights

- Provides evidence that data existed at a particular time; as specified by IETF PKIX Time-Stamp Protocol RFC 3161 (and update RFC 5816 for ESSCertIDv2). Creates timestamps with RSA or Elliptic Curve bit signatures. TPS rates given below. Capacity can be expanded with additional HSMs.
- Built upon the IBM 4769 FIPS 140-2 Level 4 tamper-detecting Hardware Security Module (HSM) for performing all secure timestamp functions including Certificate Authority functions of creating signed OCSP and CSR responses.
- The HSM *internal* clock will not accept adjustments beyond these few, small calibration events per day. Clock value in the HSM persists after the Audit event across reboots or storage of the HSM. Competitor products do not secure the clock; the clock is external and implies the trust of your organization's administrative process.
- Enables secure, browser-based administration.
- Client integration toolkits from DigiStamp and other vendors support a variety of platforms: Linux, Window, Apple.
- Runs as a 2U, rack-mounted network appliance.

Trust Model Highlights

Your Operators nor DigiStamp can be compelled to create a backdated timestamp. The SecureTime *Robot* would detect tampering and wipeout all keys, never to be recreated.

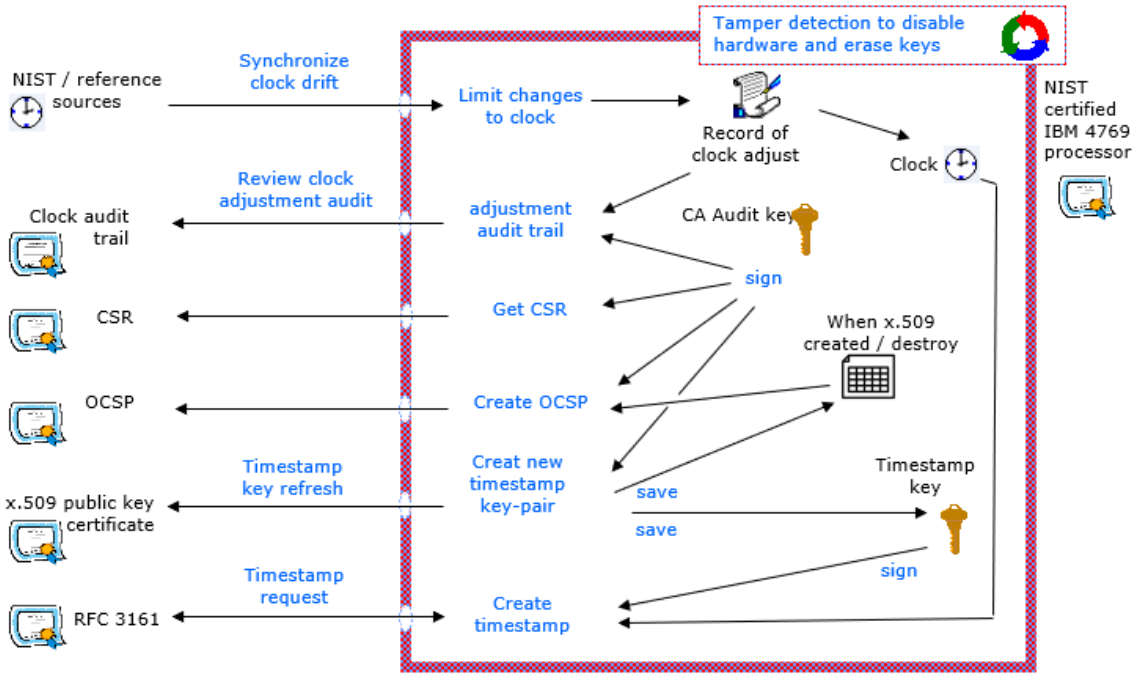
The value of a timestamp is determined by the trust of the timestamp provider. The SecureTime Server provides trust and evidence-quality timestamps with these features:

- No timestamp can be fraudulently created outside of the certified HSM.
- Every timestamp produced is traceable to two audited events, the source code compilation, and the lockdown of the SecureTime HSM.
- The SecureTime HSM's FIPS 140-2 Level 4 certification ensures keys cannot be extracted; only an unaltered SecureTime timestamp server can create trusted timestamps.
- The SecureTime HSM records a signed log of all clock adjustments. Clock cannot be backdated because technically not possible.

Hardware – HSM

The timestamp functions are performed within the HSM.

- Creates and stores the timestamp private signing key which cannot be extracted. Replacement timestamp keys can be generated, and the HSM issues the associated x.509 public key certificate. This includes Certificate Authority functions of creating the OCSP RFC 6960 response, CSR PKCS #10 for audit private keys.
- Contains the clock and an audit trail for all calibration events. This clock will not accept adjustments beyond these few, small calibration events. No adjustments are possible without it being included in the audit trail. The audit trail is digitally signed by the co-processor to detect any tampering.
- Creates the individual timestamps within its tamper-detecting environment.



Hardware – Server

The RHEL server hosts the HSM in a PCIe slot.

- 2U, rack-mounted Server Appliance
- RAID – 1
- Red Hat Enterprise Linux (customer supplies the license).
- Apache HTTPD manages the Internet connections and HTTP authentication or administrators
- Tomcat hosted Java application provides an administrator interface (described below) and automated time calibration to the HSM.

Secure browser-based administration

Your IT staff can manage and monitor the operations of the SecureTime Server using a browser-based interface. Actions include:

- Request change of timestamp key-pair and retrieve the public key x.509 certificate
- Configure the automatic error notification and status reports distribution.
- Retrieve signed clock adjust event log
- Retrieve CSR PKCS #10 for audit private keys.
- Retrieve OCSP RFC 6960 for x.509 timestamp certificate

Timestamp technical specifications

The server appliance provides time signing as specified by IETF PKIX Time-Stamp Protocol. The external interface accepts timestamp requests and responds as described in RFC 3161 with specific notes below:

The timestamp signature options: Note: TPS numbers are estimates and there will be variation.

- RSA 2048 or 4096 at 900/300 TPS (timestamp per second)
- NIST recommended Prime elliptic curves secp256r1 or secp521r1 at 2700/2500 TPS
- Brainpool defined elliptic curves brainpoolP256r1 or brainpoolP512r1 at 2400/2200 TPS

The timestamp request supports:

- Hash Algorithms SHA-2, SHA-3, RIPEMD-160
- User "*nonce*" value to size 128 bits.
- Time-Stamp Protocol via HTTP or HTTPS, user authentication is optional

The timestamp content information (*TSTInfo*) support:

- Each timestamp contains a serial number that is unique to the public key.
- Time is specified to the hundredths of a second, accuracy to +/- one second
- *Generalized* names and *extensions* are not used.

Server physical specifications

Form Factor: Height - 2U (3.5") X 17.3" W 25" D (4.37cm X 44cm X 63.5cm); 45lbs. (13.6kg)
Mounting Systems: 19" rack mount, adjustable rear support bracket included. Additional heavy-duty front support bracket supports relay rack mounting.
Input Voltage: 100-127/200 240 VAC (50/60 Hz)
Temperature/Humidity (operating): 10° to 34° C 8% - 80% RH, non-condensing
Pressure (operating/ship/storage) min/max mbar 768/1039, 550/1039, 700/1039
Altitude (operating): to 7,000 ft (2134m) maximum

Warranty, Support, and options

DigiStamp provides a limited warranty for the device for a period of 1 year. Telephone and email support is included. Optional use of DigiStamp's Internet-based servers is available by arrangement to be used as a backup to your in-house timestamp server.

The SecureTime Server and the DigiStamp software that it contains is licensed for use within a single organization and does not include distribution rights to the general public, reselling the timestamp service or reselling the device.

The IBM 4769 devices have an environmental check related to the tamper-detection mechanisms. Therefore, this hardware must be maintained within the specifications above. It must be shipped, stored and operated within these environmental conditions or the tamper sensors will render the system permanently inoperable and not replaceable by warranty.

DigiStamp can customize the solution based on individual client needs. Examples of additional requirements that we support are listed below. Please contact us with your specifics.

- Time calibration that includes GPS time.
- SecureTime Servers deployed in a High Availability mode for scaling and fault tolerance.
- Increasing capacity by adding HSMs to the server.

About DigiStamp

DigiStamp was founded in 1998 as a pioneer Timestamp Authority to protect your work and ideas. It provides a cloud-based service providing digital timestamps for intellectual property witnessing, records integrity, and e-commerce transaction verification. The timestamp can also be combined with digital signatures to offer a complete document authentication service.

Corporate offices are in Dallas, Texas. A second timestamping center in Chicago, Illinois provides fault tolerant reliability. DigiStamp is incorporated in Delaware and privately held.

DigiStamp was founded as a Timestamp Authority for biomedical researchers at Cornell University in 1998. The goal was to free the researcher's time to focus on their work of creating cures.

Two years later in October 2000 our API toolkits were developed for projects with the Mexican government and the State of Washington. We adopted the new timestamp protocol defined by the IETF. Our own C & Java toolkits allowed timestamps to be added to other software systems and are now supported with the work done by projects like BouncyCastle and OpenSSL. These institutions have already chosen SecureTime products and services:

○ Novartis	○ Bayer	○ Thales Group	○ EU Lotto Ltd
○ Sanofi	○ Abbott	○ U.S. DoD	○ Govt. of Quebec
○ Statoil	○ Infosys	○ Govt. of Australia	○ Lockheed Martin

DigiStamp, Inc.
3400 Oak Grove Ave Ste A120
Dallas, TX 75204 USA

Phone: 1-214-377-0378
www.digistamp.com
support@DigiStamp.com