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 ten 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 SecureTimeSM server from your computer by using DigiStamp’s Internet-based service and our desktop software.

**SecureTimeSM Server Highlights**

- Implements time signing as specified by IETF PKIX Time-Stamp Protocol RFC 3161
- Creates timestamps with RSA or Elliptic Curve bit signatures. TPS rates given below. Capacity can be expanded with additional cryptographic co-processors.
- Integrates NIST certified (FIPS 140-2 Level 4) tamper-detecting Hardware Security Module (HSM) for performing all secure timestamp functions, clock and audit trail
- Provides a secure, verifiable audit trail of time synchronizations by logging all clock adjustments and signing them inside the HSM
- 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 form and purpose of timestamps are defined by IETF technical standards. The value of a timestamp is determined by the trust of the timestamp provider. The role of a timestamp is to establish evidence indicating that data existed at particular time. 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’s clock is synchronized to official time sources via NTP or GPS.
- The SecureTime HSM records a signed log of all clock adjustments.
**Hardware – Cryptographic co-processor**

The timestamp functions are performed within the cryptographic co-processor.

- The co-processor hardware is IBM 4767 FIPS 140-2 Level 4.
- Software contained in the device is the DigiStamp SecureTime package supporting the IETF PKIX Time-Stamp Protocol and is traceable to its audited code signing.

This device is delivered pre-configured and performs all of the secure timestamp functions:

- Creates and stores the timestamp private signing key which cannot be extracted. Replacement timestamp keys can be generated and the device issues the associated x.509 public key certificate. This includes creating the OCSP responses.
- 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**

A standard Intel-based server contains a cryptographic co-processor and provides users with the network-based access for creating timestamps. This host server manages the Internet connections, provides an administrator interface and schedules time calibrations of the cryptographic co-processor. The server hardware is

- 2U, rack-mounted IBM System x Server
- RAID – 1
- Red Hat Enterprise Linux (customer supplies the license).
Secure browser-based administration

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

- Create and set your TSA Policy statement. Each timestamp token includes a policy identifier, indicating the unique security policy it was created under.
- Set your approved time sources for calibrating time values.
- Access the cryptographic module to internally create (non-retrievable) a RSA or ECC key pair used to create timestamps and issue the public key certificate (x.509).
- Configure the automatic error notification and status reports distribution.
- Utilize self-documenting interfaces for administration and configuration

Timestamp technical specifications

The server appliance provides time signing as specified by IETF PKIX Time-Stamp Protocol (TSP RFC 3161 version 1). The external interface accepts timestamp requests and responds as described in RFC 3161 with specific notes below:

The timestamp signature options:
- RSA 2048 or 4096 at 88/50 TPS
- NIST recommended Prime elliptic curves secp256r1 or secp521r1 at 100/95 TPS
- Brainpool defined elliptic curves brainpoolP256r1 or brainpoolP512r1 at 100/92 TPS

The timestamp request supports:
- Hash Algorithms SHA-1, SHA-256, SHA-384, SHA-512, 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 unique serial number.
- 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 768/1039 mbar
- min/max 550/1039 mbar
- min/max 700/1039 mbar
Altitude (operating): to 7,000 ft (2134m) maximum
FCC: Class A digital device, Part 15
UL: Listed IT Equip 1676
CSA: Canadian Standards Association - Certified
CE: Canada ICES - 003 Class A
EU: European Union EMC Directive 89/336/EEC
United Kingdom Telecommunications Requirement: NS/G/1234/J/100003
CISPR 22/European Standard EN

**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 4767 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 cluster for scaling and fault tolerance.
- Increasing capacity by adding cryptographic co-processors 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 we are now supported with the work done by projects like BouncyCastle. These institutions have already chosen SecureTime products and services:

U.S. DoD, Novartis, Sanofi, gov’t of Australia, gov’t of Quebec, Statoil, Infosys

DigiStamp, Inc.  Phone: 1-214-377-0378
2525 Turtle Creek Blvd Ste 403D  www.digistamp.com
Dallas TX  75219 USA