

The SecureTime<sup>SM</sup> Server is a complete and easy-to-install solution that creates a trusted Time Stamp Authority at your location. The hardware is a stand-alone network appliance that provides auditable time stamps. 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 time stamp creation software. For over five years, DigiStamp's Internet-based service (hardware, software, and processes) has been proven reliable creating millions of time stamps for thousands of customers.

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

### ***SecureTime<sup>SM</sup> Server Highlights***

- Implements time signing as specified by IETF PKIX Time-Stamp Protocol RFC 3161
- Creates time stamps with RSA 2048 bit signatures at a rate of 38 per second. Capacity can be expanded with additional cryptographic co-processors
- Integrates NIST certified (FIPS 140-1 Level 3) tamper-detecting hardware for performing all secure time stamp functions, clock and audit trail
- Provides a secure, verifiable audit trail of the time synchronization using regular time calibration periods and HSM signed audit trails
- Enables secure, browser-based administration
- Client integration toolkits from DigiStamp and other vendors support a variety of platforms: Linux, Window, Mac OS/X, AIX.
- Stores as a 2U, rack-mounted network appliance.

### ***Trust Model Highlights***

The form and purpose of time stamps are defined by IETF technical standards. The value of a time stamp is determined by the trust of the time stamp provider. The role of a time stamp is to establish evidence indicating that data existed at particular time. The SecureTime Server provides trust and evidence-quality time stamps with these features:

- No time stamp can be fraudulently created outside of the time stamp service.
- There is an audit capability to verify that the untampered time stamp server created each time stamp.
- The clock is calibrated through connection with an official time source. The clock maintains an audit log that cannot be altered by any human intervention.

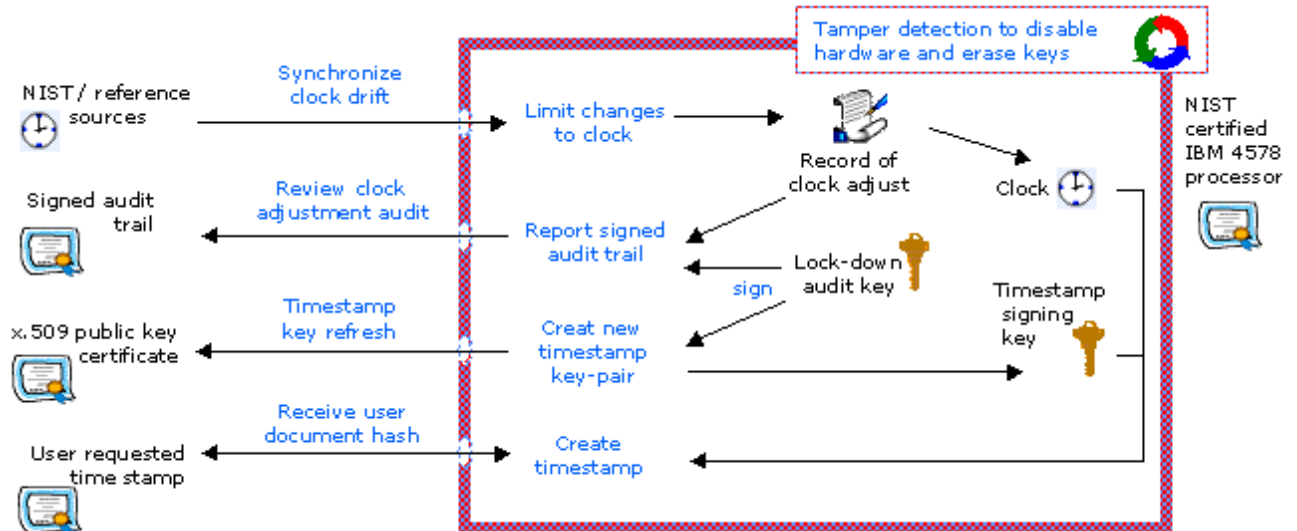
## Hardware – Cryptographic co-processor

The time stamp functions are performed within the cryptographic co-processor.

- The co-processor hardware is IBM 4758 FIPS 140-1 Level 3.
- Software contained in the device is the DigiStamp's SecureTime package that supports the IETF PKIX Time-Stamp Protocol and audit trail.

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

- Creates and stores the time stamp private signing key which cannot be extracted. Replacement time stamp keys can be generated and the device issues the associated x.509 public key certificate.
- 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 time stamps 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 time stamps. This host server manages the Internet connections, provides an administrator interface and schedules time calibrations of the cryptographic co-processor. The server hardware is

- Dell 2550 Intel Processor 1+ GHz
- 1 GB of memory
- 2 x 36GB RAID - 1
- 2U rack mount form factor
- Integrated dual 10/100/1000 Ethernet
- Windows 2000

### ***Secure browser-based administration***

The IT staff can monitor the operations of the SecureTime server using a browser-based interface. Benefits include:

- Create and set your TSA Policy statement. The policy identifier is included within each time-stamp token as an identifier to uniquely indicate the security policy under which the token was created.
- Set your approved time sources for calibrating time values. The audit trail is traceable to these sources. Options include NIST.gov Stratum-1, GPS, DigiStamp or others supporting NTP.
- Access the cryptographic module to internally create (non-exportable) a RSA key pair used to create time stamps and issue the public key certificate (x.509).
- Configure the automatic error notification and status reports distribution.
- Add/replace server administrator access security.

### ***Time Stamp 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 time stamp requests and responds as described in RFC 3161 with specific notes below:

The time stamp request supports:

- Hash Algorithms SHA-1, SHA-256, SHA-384, SHA-512, Ripemd-160
- No *extensions* are used.
- User "*nonce*" value to size 160 bits.
- Time-Stamp Protocol via HTTP, access to the time stamp interface is not restricted.

The time stamp content information (*TSTInfo*) support:

- Each time stamp contains a unique serial number.
- Time is specified to the hundredths of a second.
- The ordering of the time stamps created is maintained within the time stamp.
- *Generalized* names and *extensions* are used not used.

### ***Server physical specifications***

Form Factor: Height - 1U (1.75") X 17.3" W 25" D (4.37cm X 44cm X 63.5cm); 30lbs. (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 time stamp 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 time stamp service or reselling the device.

The IBM 4758 level 4 devices have an environmental check related to the tamper-detection mechanisms. Therefore, this hardware must be maintained within the specifications below. 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 Time Stamp Authority to protect your work and ideas. It operates Internet-based services providing digital time stamps for intellectual property witnessing, records integrity, and e-commerce transaction verification. The time stamp has now been combined with digital signatures to offer a complete document authentication service.

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

DigiStamp was founded as a Time Stamp 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 time stamp protocol defined by the IETF. The C & Java toolkits allow timestamps to be added to other software systems. International users led to the French translation and our distributors in Europe and Australia that focus on regional interests.

DigiStamp, Inc.  
4635 Travis St Ste 911  
Dallas TX 75205 USA

Phone: 1-214-377-0378  
Fax: 1-315-285-1788  
[www.digistamp.com](http://www.digistamp.com)