

# The Trusted Third-Party Time Authority



## SecureTime<sup>SM</sup> API Toolkit Overview

DigiStamp's *SecureTime API Toolkit* allows users to integrate their existing software with DigiStamp's *e-TimeStamp*<sup>®</sup> service, which provides a third-party witness of any digital file, attesting to a specific time that the file existed and verifying that its content has not been altered. As a Time Stamp Authority for trusted transactions, DigiStamp uses atomic clocks to provide global trusted time in the form of a digital time stamp returned to the client for use in their applications.

Examples of applications include digital signatures and receipts, data/time integrity of electronic records and e-commerce transactions, and protecting intellectual property (copyright material and inventor's rights as a precursor to patent filing).

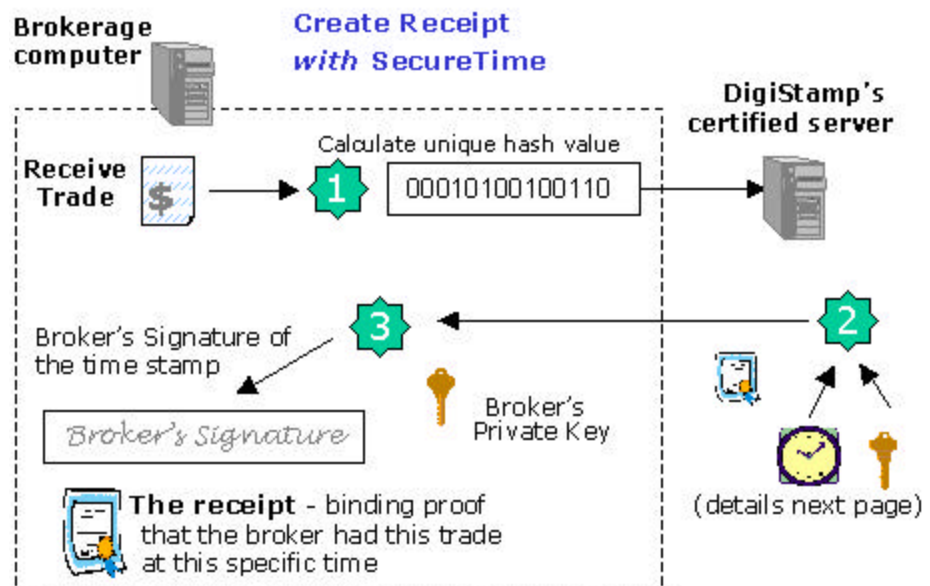
DigiStamp uses cryptographic techniques, digital signatures, your internal network, and the Internet to provide this low cost, easy-to-use time stamping solution.

### Client Software Services

DigiStamp provides the application programmer a toolkit of software services to create and manage the application interface including hash generation, server message formatting & reply parsing, time stamp server site selection & failure rollover, and Internet communications. Alternatively, the application programmer may write his own library calls formatted to the IETF protocol used by DigiStamp. A variety of transport protocols may be used to communicate with DigiStamp's servers to include HTTP or SSL.

Client services include creating and verifying time stamps, with the data files remaining in their original format. Only the data file's unique hash value is transmitted to DigiStamp; sensitive data is never transmitted outside the client. An example application is provided below in which time stamps are used in conjunction with PKI services to create receipts for transactions that can be stored alongside or within the data.

Time-stamping receipts between trading partners create binding proof of the specific point-in-time that a transaction was received. For example, as used by an on-line stock broker:



### APPLICATIONS:

#### E-Commerce Transactions:

- Binding receipts
- Electronic forms
- Financial transactions
- On-line auctions
- Legal filings

#### Protect Intellectual Property:

- Patent Protection
  - Researchers
  - Inventors
- Copyright Protection
  - Writers
  - Graphics Artists
  - Musicians
  - Architects

#### Records/Document Integrity:

- Doctors
- Lawyers
- Accountants
- Corporate
- Government

## SERVICE OPTIONS:

### SecureTime<sup>SM</sup> API Toolkit for Application Integration

- Transaction Time and Authentication
- Industry-based standard API based on IETF

### IP Protector<sup>SM</sup> for Individuals and Small Businesses

- Inventors
- Illustrators
- Writers
- Researchers
- Architects
- Business Documents
- Electronic Forms

### IP Vault<sup>SM</sup> for Work-Groups Large & Medium Businesses

- Intellectual Property First Use Protection
- Business Transactions Traceability

## SECURETIME<sup>TM</sup> API

### SYSTEM REQUIREMENTS:

- Internet access

### Java toolkit:

- Java VM 1.1.7+ platforms

### C and COM toolkit:

- Windows version for use with MS CryptoAPI.
- Other platform support for create and decoding time stamps

DigiStamp, Inc.  
105 West Mill Valley  
Colleyville, Texas 76034 USA

Phone: 1-817-428-8872  
Fax: 1-817-427-4584  
<http://www.DigiStamp.com>

Ver 5.3

Copyright © 2000 DigiStamp, Inc.  
All Rights Reserved

## DigiStamp's Secure Servers

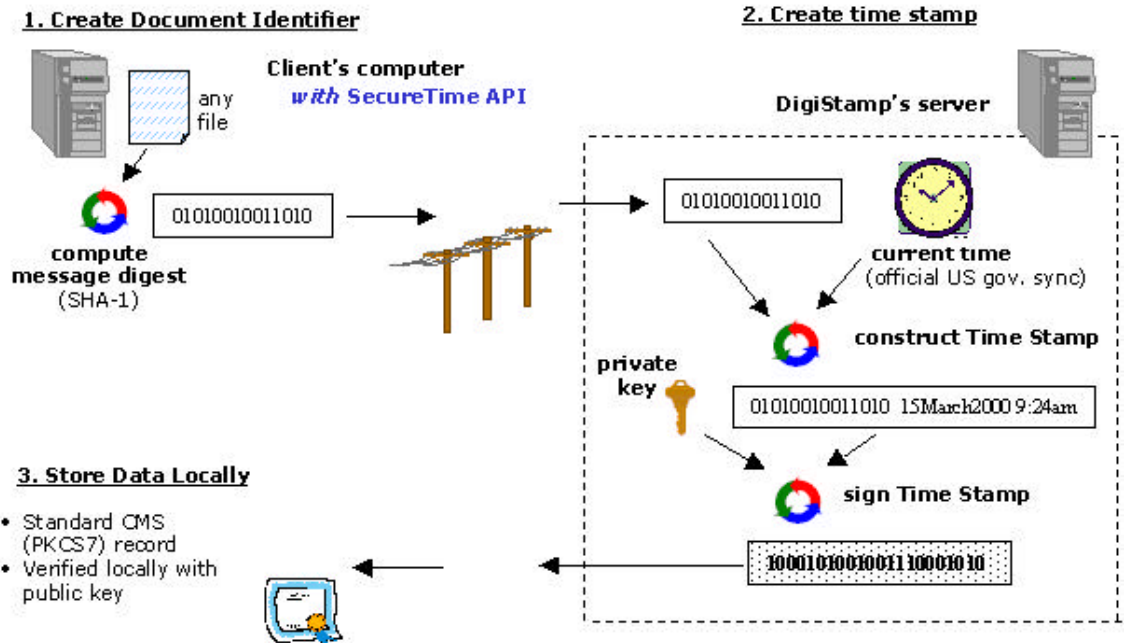
DigiStamp uses specialized encryption hardware that is certified by the National Institute of Science and Technology (NIST) and provides tamper detection against physical and electronic attacks, ensuring the integrity of the time stamps. The server's clock is secured in the certified hardware and synchronized with the U.S. Naval Observatory, the official standard of time in the U.S. Redundant, geographically-separated servers are used to ensure continual access to DigiStamp's service.

## Creating a Time Stamp

DigiStamp's software calculates a hash value for a data file of any size. This hash consists of a unique 160-bit message digest using the FIPS-standard SHA-1 algorithm.

DigiStamp's Internet-based server adds the current time to the hash value, signs that intermediate product (SHA-1 digest + current time) using RSA 2048-bit public key encryption, and generates a time stamp. The time stamp is delivered back to the client software for storage. See the figure below.

The data file itself never leaves the client's computer! The time stamp is an impregnable record of the information's existence at a specific time.



## Authenticating a Data File/Time Stamp

DigiStamp's service can also authenticate a data file by comparing its hash value with the hash in the original time stamp. The SecureTime API Toolkit generates the file's current hash value as described above. The toolkit compares the new hash value with the contents of the original time stamp. The software uses the public key to prove the time stamp is authentic. Any change to the original file or tampering with the time stamp will invalidate the file's authenticity.

Time stamps are created using industry-standard digital signature messages and can also be authenticated using third-party software and our public key.