

# 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. A time stamp is like a digital notary that 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 common, open standards and secure hardware to deliver a reliable Internet-based data authentication service.

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 or prior-use evidence).

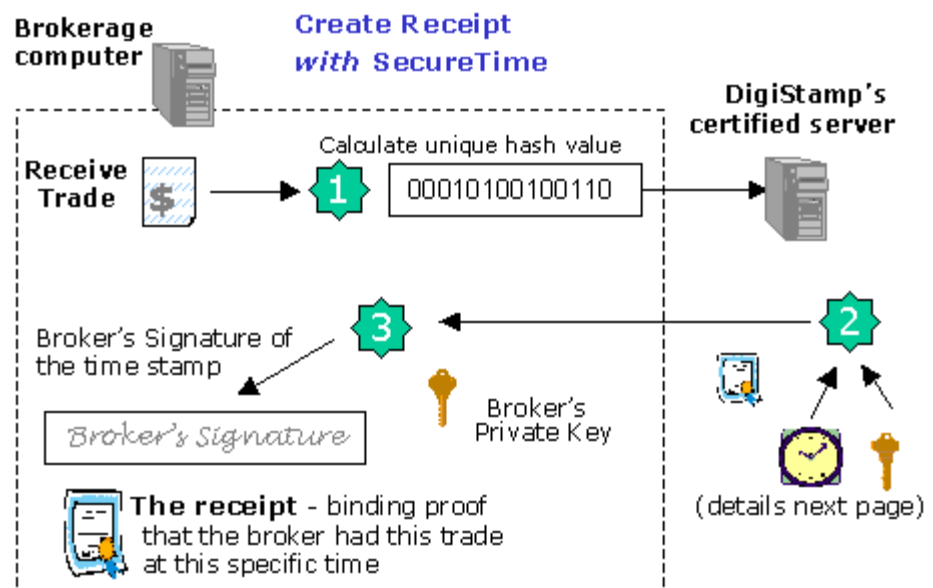
DigiStamp uses cryptographic techniques, digital signatures, your internal network, and the Internet to provide this low cost, easy-to-use time stamping solution.

### 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, you can use software like OpenSSL, BouncyCastle, S/MIME Library (SFL) and any software that supports standard time stamps (IETF RFC 3161).

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
  - Most businesses
- Copyright Protection
  - Writers
  - Graphics Artists
  - Musicians
  - Architects

#### Records/Document Integrity:

- Doctors
- Lawyers
- Accountants
- Corporate
- Government

### 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

### SecureTime<sup>SM</sup> Server on-site hardware solution

- Government Agencies
- High volume users

### SECURETIME<sup>TM</sup> API SYSTEM REQUIREMENTS:

- Internet access OR
- SecureTime Server

### API Language Options

- Java 2 on Windows and various UNIX platforms
- C#
- Libraries from [bounycastle.org](http://bounycastle.org)

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

Phone: 1-214-377-0378  
<http://www.DigiStamp.com>

Ver 7

Copyright © 2000-2011  
DigiStamp, Inc.  
All Rights Reserved

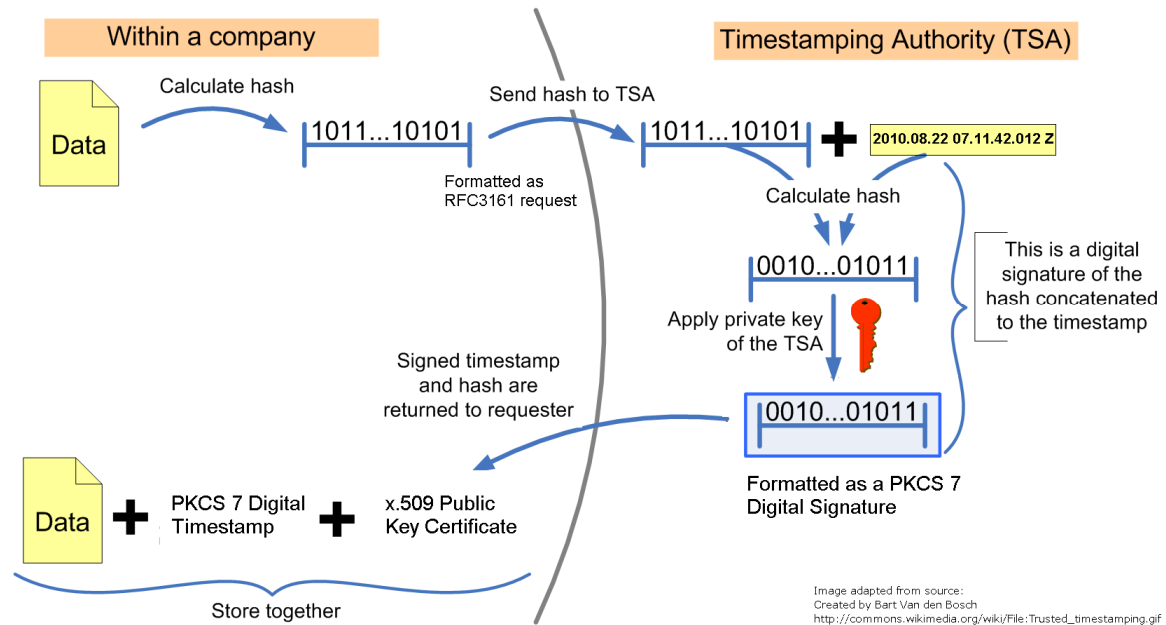
## DigiStamp's Secure Servers

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 its values are traceable to both US and EU official time sources. 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 virtually any size. This hash consists of a unique message digest using the FIPS-standard SHA-2 algorithms up to SHA-512.

DigiStamp's Internet-based server adds the current time to the hash value, signs that intermediate product (SHA-2 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 strong evidence of the information's existence at a specific time.

## Signing and Time-Stamping PDF Documents

DigiStamp's Java API toolkit now supports both signing and time-stamping of documents in the PDF format. The PDF signature toolkit is intended for use by software developers for integration in existing systems. Our first users are European Union businesses using time stamps for their e-Invoicing process.

## Authenticating a Data File/Time Stamp

DigiStamp's service authenticates 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 x.509 public key certificate.