

# The Trusted Third-Party Time Authority



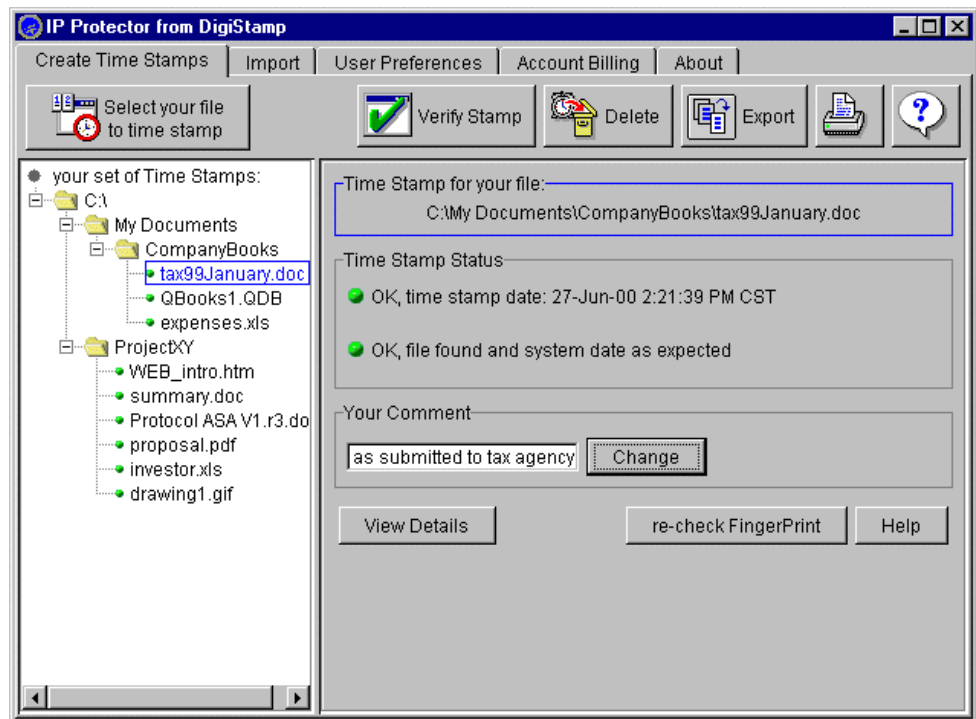
## IP Protector<sup>SM</sup> Service Overview

DigiStamp's *IP Protector* 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. A fingerprint (a short message digest) of your data is sent to DigiStamp's server and a time stamp is returned to your PC.

Applications of time stamping include protecting intellectual property (copyright material and inventor's rights as a precursor to patent filing), just like a modernized laboratory/engineering notebook, and data/time integrity of e-commerce transactions and electronic records.

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

## PC-Based Client Software



*IP Protector* protects valuable electronic records and intellectual property for companies and individuals. Free software, provided from our Internet web site, creates and stores the time stamps. The client downloads the application and then uses the Internet to contact DigiStamp whenever a time stamp is created or verified. Data files remain confidential because they are not sent over Internet. Time stamps are stored locally.

## User Interface

Using the point-n-click interface, the user selects files to timestamp or verify by navigating in a Windows Explorer format. Simple icons display the status of the time stamp while tabs and buttons execute functions. Accounting is through a simple pay-as-you-go account.

## Digistamp's Secure Server

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.

### APPLICATIONS:

#### Protect Intellectual Property:

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

#### Records/Document Integrity:

- Doctors
- Lawyers
- Accountants
- Corporate
- Government

#### E-Commerce Transactions:

- Electronic forms
- Financial transactions
- On-line auctions
- Legal filings
- Lotteries

### PC-BASED CLIENT SYSTEM

#### REQUIREMENTS:

- 16 MB RAM
- 8 MB Disk Space
- 80486 or equivalent
- Internet access
- Macintosh,  
WIN 95 / 98 / NT 4.0,  
Solaris operating systems

## FEATURE

## BENEFIT

Data file stays local to client's computer	Data remains secure
Takes only seconds to create a timestamp	Timestamp often in the creative process
Charged only when you access the server	Costs are known and controlled
Runs on most client platforms	Easy office network integration
Available in many languages	Global applications for e-commerce
NIST-certified hardware with tamper detect	Protects the server's encryption keys
Clients can verify timestamps directly	Authenticates a file's content in seconds

### SERVICE OPTIONS:

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

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

The software is provided Free of charge from our web site at:

[www.e-TimeStamp.com](http://www.e-TimeStamp.com)

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 5.2

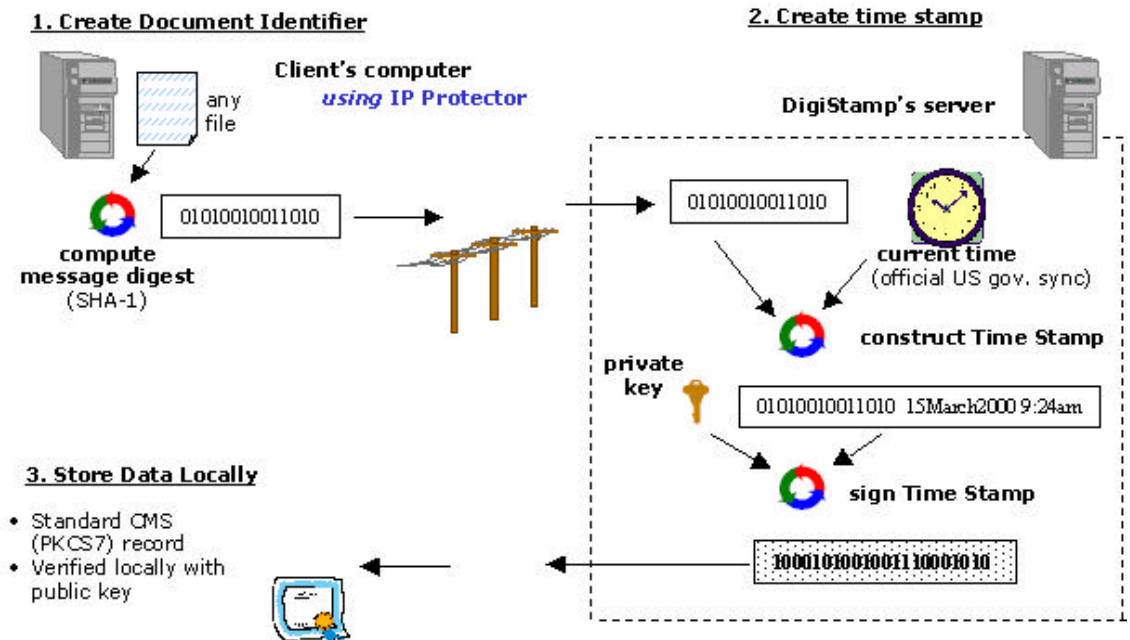
Copyright © 2000 DigiStamp, Inc.  
All Rights Reserved

### Creating a Time Stamp

DigiStamp's software calculates a hash or fingerprint for a data file of any size. This hash consists of a unique 160-bit message digest using the FIPS-standard SHA-1 algorithm. The fingerprint is a unique value that is based on the exact content of the data file.

DigiStamp's internet-based server adds the current time to the fingerprint, signs that intermediate product (SHA-1 digest + current time) using RSA 2048-bit public key encryption, generating 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 IP Protector generates the file's current hash value as described above. The software compares the new hash value with the contents of the original time stamp. The DigiStamp server 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.