



TRUSTED TIME STAMPING

Trusted time stamping is the process of securely tracking the creation and modification of an electronic document or transaction to prove its authenticity.

Time stamping is an important measure of protection used within many industries to protect, for example, intellectual property rights, documents or communications relating to patents, medical records, or legal proceedings, e.g. annual reports. Time stamps provide an important measure of protection as electronic documents are easier to forge and back-date than traditional paper-based ones. In several European countries some applications are required by law require to use time stamping.

An equally important application is the time stamping of digital signatures. One of the reasons for attaching a digital signature to a document or transaction is to achieve non-repudiation. The digital signature fixes the contents of a transaction or document and links it uniquely to the signer. The validity of a digital signature requires two things: 1) that the signature must match the signed data, and 2) the signer's certificate must be valid. Certificates can expire or be revoked, but this does not, of course, change the validity of signatures made prior to the expiration or revocation. Without a trusted time stamp it may not be possible to prove that the signature was actually made before the certificate lost its validity.

Time Stamps

A time stamp is issued by a neutral and trusted third party acting as a Time Stamping Authority (TSA). Cryptomathic's Time Stamping Authority issues a unique and irrefutable time stamp upon request from an external time stamp client or web service client. The time stamp can be assigned to any piece of electronic data to provide proof that it existed at a certain point in time without the owner being able to backdate the transaction. For added reliability multiple TSAs can be used.



Cryptomathic Time Stamping Authority

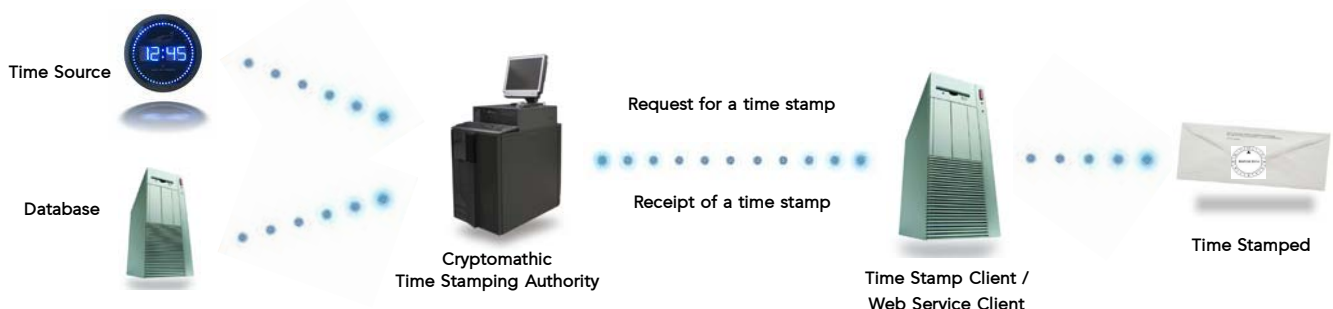
For providers of TSA services the Cryptomathic Time Stamping Authority has a number of benefits:

Remote Administration Client – allows everyday application management from outside the secure room where the server is kept.

SDK Available – for creating time stamp requests and validating time stamp responses.

Scale-out Clustering – assures high availability and performance and allows servers to be added or removed from a running system.

Hardware Security Modules – support for a number of hardware security modules. A single Time Stamping Authority can employ several HSMs, and several servers can run in a cluster for high availability and improved throughput.



TECHNICAL SPECIFICATIONS

Time Stamps

- RFC 3161
- Socket based Transport (also known as 'direct TCP') or SOAP over HTTP

Cryptographic Standards

- RSA 1024-4096 bit TSA keys – limit set by HSM

Certificates

- X.509 v3
- Certificate requests: PKCS #10 or self-signed X.509 v3

Key Management

- All TSA keys are hardware protected
- All auxiliary keys are hardware protected

Administrator Authentication

- Smart card authentication for all administrators
- Dual access control for sensitive operations

Operational Features

- All events are securely logged
- Scale-out clustering for high availability and performance
- Support for multiple HSMs in one server

SDK

- Available in ANSI C and Java

Operating Environment

- Microsoft Windows

Supported Time Sources

- True Time NTS-200 and NTS-150 GPS synchronised time servers
- Any other NTP-compliant time source

Hardware Security Modules

- Thales / nCipher
- IBM
- SafeNet

Supported Databases

- Microsoft SQL

System Architecture

The Cryptomathic TSA server resides in a secure room and handles all commands sent from the administration clients as well as from the time stamping clients. Administrators must log on to the administration client using smart cards under dual control access. The Cryptomathic TSA complies with the RFC 3161 timestamp protocol.

The administration clients initialise and administer the Cryptomathic TSA via a graphical user interface. There are two kinds of administration client: a secure client and a remote client. The secure client offers full functionality for setting up and administering the system, including performing security related operations, whilst the remote client allows for day-to-day administrative tasks to be performed away from the secure room.

The Cryptomathic TSA is designed to easily integrate into an existing infrastructure. The system is easy to set up which means it is both time- and cost-efficient.

All keys are generated and managed by Hardware Security Modules (HSMs), which means they are never exposed and cannot be tampered with. A single TSA server can employ multiple HSMs, and several servers can run in a cluster for high availability and performance.



ABOUT CRYPTOMATHIC

Cryptomathic is one of the world's leading providers of security solutions to businesses across a wide range of industry sectors, including finance, smart card, digital rights management and government. With over 20 years' experience, Cryptomathic provides customers with systems for e-banking, PKI initiatives, card personalization, ePassport, card issuing

and advanced key management utilizing best-of-breed security software and services. Cryptomathic prides itself on its strong technical expertise and unique market knowledge. Together with an established network of partners, Cryptomathic assists companies around the world with building security from requirement specification to implementation and delivery.

Learn more at cryptomathic.com