

## Cryptomathic Time Stamping Authority

### Time Stamps for Non-Repudiation

With Cryptomathic Time Stamping Authority a unique and unforgeable time stamp can be assigned to any piece of digital data. The time stamp provides proof that this particular data existed at a certain point in time. Time stamps are an important measure for protection of intellectual property rights. An equally important application is to time stamp digital signatures. One of the reasons for applying digital signatures to documents and transactions is to achieve non-repudiation. The digital signature fixes the contents of the transaction or document and links it uniquely to the signer. To achieve true non-repudiation, however, the recipient of a digital signature should also secure a proof of the signature's existence at that point in time. This proof is provided by a time stamp, issued by a trusted third party known as a TSA – a Time Stamping Authority.

### Benefits

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

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

**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 FIPS-certified hardware security modules.



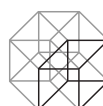
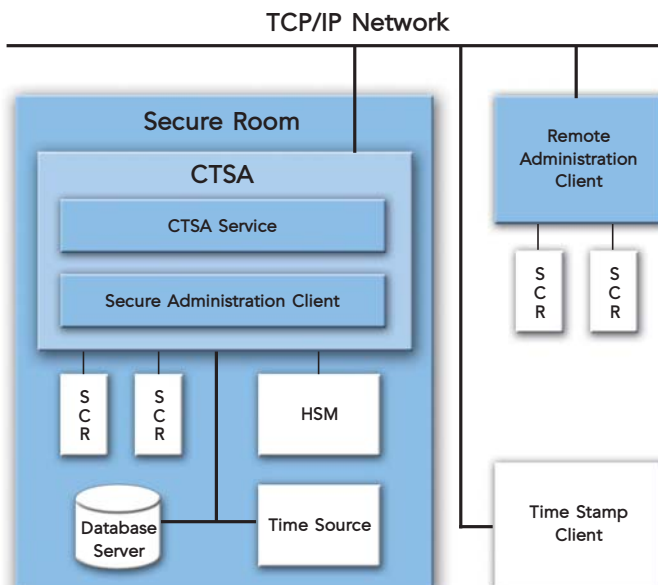
### Architecture

The Cryptomathic TSA server issues a time stamp token upon receipt of a request from an external time stamp client. Administration of the Cryptomathic TSA is handled from the administration clients. The database, hardware security module (HSM), and external time source are accessible to the TSA server, while the administration clients cannot directly access either of them.

The Cryptomathic TSA administration clients have a graphical user interface and are used to initialise and administer the Cryptomathic TSA server. There are two kinds of administration clients: a secure client and a remote client. The remote client allows administrators to perform day-to-day tasks from outside the secure server room. From the secure client the more critical tasks can be administered, and in addition the secure client has all the functionality of the remote client. The secure client must run inside the secure room on the same host as the server.

The administrators identify themselves with smart cards, and hence two smart card readers (SCR) must be connected to each administration client. All keys are securely generated and managed by a hardware security module (HSM). This way the keys are never exposed in clear 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 improved throughput.



## Technical Specifications

### Time Stamps

- RFC 3161
- Transport mechanism: Socket-based (also known as "direct TCP")

### Cryptographic Specification

- RSA 1024-4096 bit TSA keys, limit set by hardware security module

### Certificates

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

### Key Management

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

### Administrator Authentication

- Administrators are authenticated with smart cards
- Dual access control for the most sensitive operations

### Operational Features

- All events are MAC protected and securely logged in the database
- Scale-out clustering for high availability and performance
- Support for multiple hardware security modules in one server

### Operating Environment

- Server runs as Windows NT/2000 service
- Administration clients – Windows NT/2000 applications

### Supported Time Sources

- True Time NTS-200 and NTS-150
- Meinberg LANTIME (SHS)
- Any other NTP-compliant time source

### Supported Hardware Security Modules

- nCipher nShield F2 and F3
- IBM 4758
- Other PKCS #11 compliant hardware<sup>1</sup>

### Supported Databases

- Oracle 8 and 9
- Microsoft SQL Server 7 and 2000

<sup>1</sup>Upon request and subject to test

## Cryptomathic's Trust Products

Cryptomathic's family of trust products includes all the applications needed to set up and maintain a trust community, also known as a Public Key Infrastructure (PKI). Cryptomathic's trust products range from the central Certification Authority (CA), with supporting applications for registration of users and distribution of certificates, to components for time stamping and remote signature generation, which may be added as required. With Cryptomathic's trust products you can include the benefits of digital signatures and reliable authentication in a business application for internal or external use, offer trust services as a service provider, or even set up a public Certification or Time Stamping Authority. The simple, yet flexible, license forms and pricing models make Cryptomathic's trust products an attractive choice for solutions of any scope or size.

**Interoperable** – The trust products comply with business standards and are tested for interoperability. This ensures that the applications fit into existing infrastructures.

**Scalable and stable** – Designed with scalability and stability in mind, the trust products fit both current and future requirements.

**Proven** – Large enterprises and banks as well as financial and government institutions rely on Cryptomathic's trust products to protect their business.

**Flexible** – The trust products are designed for easy integration with existing business systems. In addition, our e-Security tools allow you to enable new and legacy applications to handle digital signatures.

**Secure** – Built by world-class security experts, Cryptomathic's trust products offer premium security.

**Hardware Crypto Enabled** – For physical security and even better performance all the trust products support hardware security modules.

## About Cryptomathic

With more than 15 years of experience, Cryptomathic is one of the world's leading providers of e-Security. We can assist you in securing your business by providing best-of-breed e-Security software products and services as well as consultancy and education.

Our range of software products covers e-Security tools for professional application development, trust products as well as data preparation for smart cards.

Cryptomathic's world-class experts offer e-Security consultancy at strategic level, for solution architecture, and integration.

We offer a complete modular education program, where you can learn what you need to know about e-Security – both on a general and product specific level.

We serve our customers through our head office in Denmark and our European subsidiaries. For more information, please fill in the interest card on our web site:

[www.cryptomathic.com](http://www.cryptomathic.com)



**CRYPTOMATHIC**  
e-Security for Better Business