

# CryptosecTSA

---

Digital Signature is becoming a routine process in the relationship with government, business-customer operations and, in general, is being provided to the software infrastructure of many many entities.

But digital signatures, which ensures who has made a particular action is not valid for ensure that action has occurred at a given time..

CryptosecTSA is an authority of time stamp that has the functionality to add the date and time to a particular action. An electronic signature together with the time stamp is the irrefutable Prof. That responds who and when Duch action took place within any electronic operating enviroment (banking environment, physical access, etc.)..

Moreover,

- Keep their keys in an extremely safe manner.
- Storage the generated stamps.
- Friendly administration system.

## Functional Description

Time stamp Authority CryptosecTSA CryptosecCA is an appliance composed of cryptographic hardware that aims to produce time stamps safely and quickly

To make this operational, before being put into production state it must be configured, this action is allowed through a user-friendly interface using HTTPS against the device. This configuration, among other things, consist of generate some asymmetric keys into the secure cryptographic device (HSM) integrated in CryptosecTSA in order to give the system a digital certificate and establish values under which generate the timestamps. In addition, has a system clock synchronization method with an external source through NTP protocol. However, it is possible to adapt other sincronization methods, depending on customer requirements (GPS, caesium clocks, etc).

Once system is configured and synchronized, CryptosecTSA is ready to work.

Access to authority CryptosecTSA by customers is done by HTTP following the standard rfc3161, the same way by which the generated stamp is released. Time stamps are signed into the HSM, embedded in CryptosecTSA.

Also are stored into an external to the system database.

Similarly CryptosecTSA supports a configuration in high availability or load balancing introducing a number of elements in the system, an external http balancer is required.



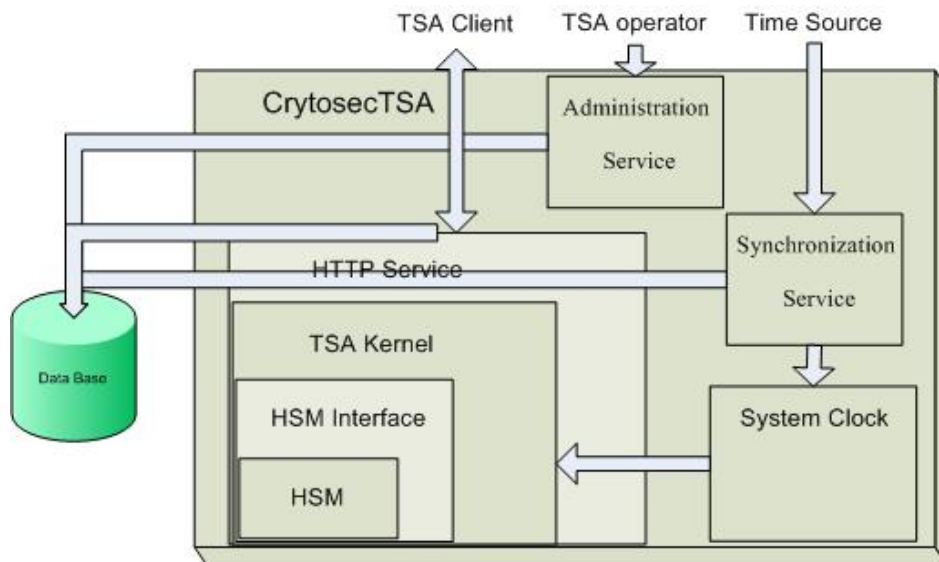
CryptosecTSA configuration

## Architecture

CryptosecTSA CryptosecCA is designed over a HSM (Hardware Security Module) engine. Both hardware and software are integrated into a single machine so the solution is offered in appliance format.

Service access is done through HTTP, following RFC3161, Time-Stamp Protocol (TSP).

Administration is made using HTTPS, requiring a valid administration operator certificate.



CryptosecTSA functional scheme

## Features

- Time stamp protocol http, following standard RFC3161.
- System administration using HTTPS with required operator certificate.

- RSA private keys generation, from 1024 to 4096 bits.
- Safely generation of certification requests from an accredited device.
- Time stamp service configuration, where is provided the safely creation of the TSA certificate private key, such as the import of the associated digital certificate in the cryptographic device.
- Total capacity in system configuration, network addresses cryptographic device initialization, etc.
- Capacity to configure multiple time distributed sources in different geographic areas.
- System clock Synchronization using NTP. (It is possible incorporate other sync systems: GPS, etc.).
- Cryptographic Hardware certified FIPS 140-2 Level 3.
- Access to external database Postgres and MySQL. ( Possible access to Oracle, MS SQL)
- Appliance format making easy its installation and set up to production state.



CryptosecTSA. Starting configuration screen

## Requirements

Because the product CryptosecTSA is delivered as an appliance format, all hardware and software is included with the device. It simply requires the following external systems:

- Database with Postgres or MySQL access, although it is possible to adapt any database according to customer requirements.
- VT100 terminal for safe administration of HSM.
- Access by TCP to a NTP Server using port 123.

## Details

**Family:**

Cryptosec OpenKey.

**Product:**

CryptosecRA.

**Clock Sync:**

NTP v3.0

**Time Reference:**

Preloaded external NTP Servers.

**Software Platform:**

Customized Operating System for operations of time stamping.

**Hardware Platform**

Cryptosec Secure Cryptographic Module.

**Device Administration:**

Web GUI using HTTPS and digital certificate required

**HSM Administration:**

VT100 Terminal.

**TSA Service Access:**

TSP protocol ( RFC3161 ) using HTTP

**Size:**

1U 19" Rack Mount

**Operacional Temperature**

10°C to 35°C

**Storage Temperature**

- 20°C to 60°C

**Operacional Humidity:**

10% to 85%

**Storage Humidity:**

0% to 95%

**Interfaces:**

Ethernet 10/100/1000, Serial Port: DB-9, 2 USB ports

**IP Protocols:**

IPv4

**Input Voltage:**

100-240 Volts AC

**Standard Certifications:**

FEDERAL COMMUNICATION COMMISSION PART 15 (radio frequency devices)

NATIONAL INSTITUTE OF STANDART AND TECHNOLOGY. FIPS 140-2 LEVEL 3

**Used standards:**

NTP v3.0, PKCS#1, PKCS#8, PKCS#10, PKCS#12, SHA, X.509v3 CRLv2 rfc3280, http, https.

---

**European Headquarters**

C/ Orense, nº 68 Pl. 11 28020 Madrid Tel: +(34) 91 449 03 30 Fax: + (34) 91 579 56 06

Email: [info@realsec.com](mailto:info@realsec.com)

**North America Headquarters**

710 Marshview Close, Roswell - Georgia 30076, USA Tel: +1.817-898-0153 Fax: +1.480-247-5501

Email: [infoatlanta@realsec.com](mailto:infoatlanta@realsec.com)

**Regional Offices**

Dallas

304 Eagles Court, Trophy Club Texas 76262 Tel: +1.817-898-0153 Fax: +1.480-247-5501

Email: [infodallas@realsec.com](mailto:infodallas@realsec.com)

Mexico, Central America and Caribbean

Av. Insurgentes Sur 800 Piso 21-A Col Del Valle México DF Tel: (+5255) 55 74 3205

Email: [infomexico@realsec.com](mailto:infomexico@realsec.com)