

CryptosecTSA

La firma digital está pasando a ser un proceso habitual en la relación con las administraciones públicas, en las operaciones empresa – proveedor, y en general se está dotando a las infraestructuras software de muchas entidades, de esta tecnología.

Pero la firma digital, que asegura quién ha realizado una determinada acción, no es válida para fijar que la acción se ha producido en un determinado instante de tiempo.

CryptosecTSA es una autoridad de sellado de tiempo que tiene la funcionalidad de agregar la fecha y la hora a una determinada acción. La firma electrónica junto con el sello de tiempo forman una prueba irrefutable que responde al quién y al cuándo se desarrolló tal acción electrónica dentro de cualquier entorno de operación (entorno bancario, accesos físicos, etc.).

Además,

- Custodia sus claves de una forma extremadamente segura.
- Mantiene almacenados los sellos generados.
- Esta dotada de un sistema de administración amigable.

Descripción Funcional

La autoridad de sellado de tiempo CryptosecTSA es un appliance compuesto por hardware criptográfico que tiene como finalidad la producción de sellos de tiempo de una manera segura y rápida. Para realizar esta operativa, antes de su puesta en producción debe ser configurada, acción que se posibilita mediante una interfaz amigable vía HTTPS contra el propio dispositivo. Esta configuración, entre otras cosas, consiste en generar unas claves asimétricas en el dispositivo criptográfico seguro (HSM en adelante) integrado en CryptosecTSA con el fin de poder más adelante dotar al sistema de un certificado digital y de establecer unos valores bajo los que se generarán los sellos de tiempo. Además el sistema posee un sincronizador de su propio reloj con una fuente externa mediante protocolo NTP. No obstante, es posible adaptar, según los requerimientos del cliente, cualquier dispositivo de sincronización del reloj del sistema (GPS, relojes de cesio, etc).

Una vez configurado y sincronizado el sistema, CryptosecTSA ya está preparada para iniciar su actividad.

El acceso por parte de los clientes a la autoridad CryptosecTSA se hace mediante HTTP y siguiendo el estándar rfc3161, mismo medio por el que se devolverá el sello generado. Los sellos de tiempo son firmados en el HSM embebido en CryptosecTSA.

Éstos mismos son almacenados en una base de datos externa al sistema.

De igual manera CryptosecTSA admite una configuración en alta disponibilidad o balanceo de carga introduciendo un número indeterminado de elementos en el sistema, siendo requerido un balanceador externo de protocolo HTTP.



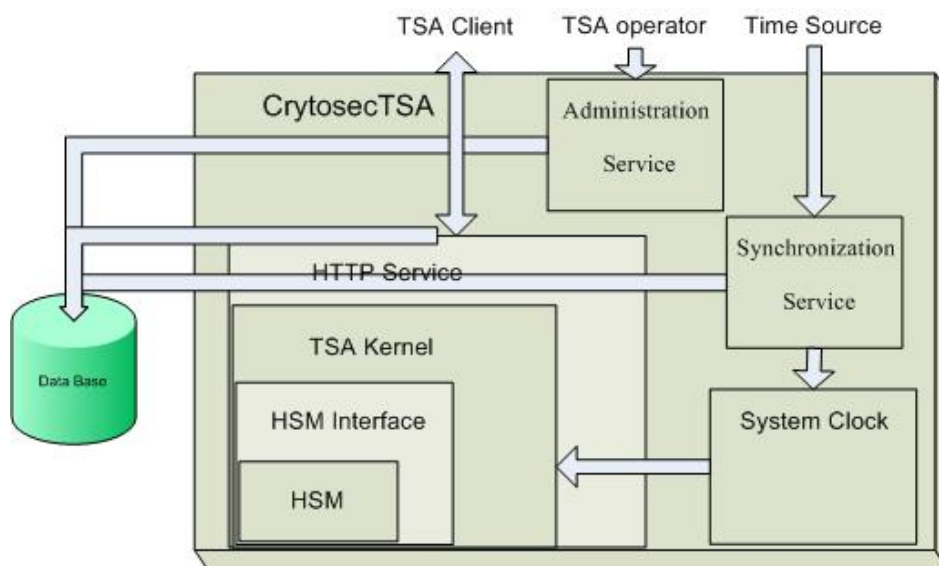
Pantalla de configuración de TSA

Arquitectura

CryptosecTSA está diseñado sobre un motor criptográfico hardware (HSM). Tanto el hardware como el software están integrados en una misma máquina, por lo que la solución se ofrece en formato appliance.

El acceso al servicio se hace a través de protocolo HTTP, siguiendo la RFC3161, Time-Stamp Protocol (TSP).

La administración se realiza a través de HTTPS, requiriendo la presentación de un certificado válido de operador.



Esquema funcional de CryptosecTSA

Características

CryptosecTSA está dotada de las siguientes características:

- Protocolo de sellado de tiempo HTTP siguiendo estándar RFC3161.
- Administración del sistema vía HTTPS con requerimiento de certificado de operador.
- Generación de claves privadas RSA, desde 1024 hasta 2048 bits.
- Generación de peticiones de certificados desde un dispositivo acreditado de forma segura.
- Configuración del servicio de sellado de tiempo, donde se provee la creación de la clave privada del certificado TSA de forma segura, así como la importación del certificado digital asociado dentro del dispositivo criptográfico.
- Capacidad total de configuración del sistema: dirección de red, inicialización de dispositivo criptográfico, etc.
- Capacidad de configurar múltiples repositorios de fuentes de tiempo distribuidos en distintas zonas geográficas.
- Sincronización del reloj del sistema vía NTP. (Posibilidad de incorporación de otros sistemas de sincronismo: GPS, etc.)
- Hardware criptográfico Cryptosec certificado FIPS 140-2 Level 3.
- Acceso a base de datos externa Postgress y MySQL. (Posibilidad de acceso a Oracle, MS SQL)
- Formato appliance facilitando la instalación y puesta en producción.



Pantalla de inicio de configuración de CryptosecTSA

Requerimientos

Debido a que el producto CryptosecTSA es entregado en formato appliance todo el hardware y software está incluido en el dispositivo. Simplemente se requieren los siguientes sistemas externos:

- Base de datos accesible Postgress o MySQL aunque es posible adaptar cualquier base de datos según requerimientos del cliente.
- Terminal VT100 para administración segura del HSM.
- Acceso por TCP a un servidor NTP a través de puerto 123.

Detalle

Familia:

Cryptosec OpenKey.

Producto:

CryptosecTSA.

Sincronismo del Reloj:

Protocolo NTP v3.0

Hora de Referencia:

Servidores NTP externos precargados.

Plataforma software:

Sistema operativo personalizado para operaciones de estampado de tiempo.

Plataforma hardware

Modulo criptográfico seguro Cryptosec.

Administración del dispositivo:

Web GUI a través de HTTPS y certificado digital requerido

Administración HSM:

Terminal VT100.

Acceso servicio TSA:

Protocolo TSP (RFC3161) a través de HTTP

Dimensiones:

1U 19" Rack Mount

Temperatura de operación

10°C to 35°C

Temperatura de almacenamiento

- 20°C to 60°C

Condiciones de humedad de operación:

10% to 85%

Condiciones de humedad de operación:

0% to 95%

Interfaces:

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

Protocolos IP:

IPv4

Voltaje de entrada:

100-240 Volts AC

Certificaciones estandares:

FEDERAL COMMUNICATION COMMISSION PART 15 (radio frequency devices)

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

Estándares utilizados:

NTP v3.0, TSP rfc3161, PKCS#1, PKCS#8, PKCS#10, PKCS#12, SHA, X.509v3, 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

North America Headquarters

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

Email: 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

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