Cryptosec Openkey TSA

Time Stamping Authority

A digital signature and a time stamp can be used as irrefutable evidence of who performed an electronic operation and when it took place.

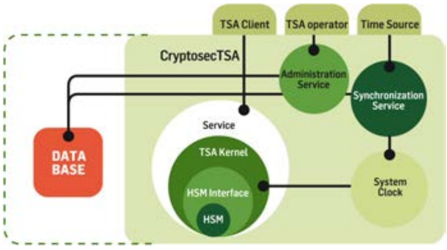
Cryptosec TSA is an appliance equipped with Cryptographic Software and Hardware (HSM) integrated into a single device, which considerably reduces the cost of the product and the time needed to install it.

"Cryptosec TSA allows for a high-availability configuration through an external load balancer." The system can synchronize its own clock with an external time source via the NTP protocol, though it can be adapted to use any synchronization device (GPS, cesium clocks, etc.).

It is configured by means of an HTTPS interface through which a series of symmetric keys are generated in the HSM. This allows the system to be equipped with a digital certificate and to set the values based on which the time stamps will be generated.

Client access to the system is performed according to the RFC 3161 standard (Time Stamp Protocol [TSP]) and the stamp thus generated will be returned by the same means.

Time stamps are signed in the HSM, which is embedded in the **Cryptosec TSA** appliance.



The **Cryptosec Openkey TSA Time Stamping Authority** is aimed at generating time stamps to quickly and securely certify the exact time a signature process has taken place.

“Digital Signature ensures who performed a certain action, but are not valid for certifying that the action actually took place at a specific time. That's where a Time Stamping Authority like Cryptosec OpenKey TSA is required.”

Features

- Time stamping protocol according to the RFC 3161 standard.
- Easy system administration via HTTPS requiring a digital operator certificate.
- RSA private key generation, from 1024 to 4096 bits.
- Time stamping service configuration, which provides for the secure creation of the private key for the TSA certificate, and also enables importing the corresponding digital certificate into the cryptographic device.
- Full system configuration capability: network address, cryptographic device initialization, etc.
- Capability of configuring multiple time source repositories across different geographic areas.
- Synchronization of the system's clock via NTP (Possibility of including other synchronization systems: GPS, cesium clocks, etc.).
- Access to the internal/external PostgreSQL database to store audit logs.
- Appliance format for enhanced installation and deployment.

Requirements

- Accessible Postgre or MySQL database, although any database may be adapted depending on customer requirements.
- VT100 terminal for secure HSM administration.
- TCP access to an NTP server through port 123.

realsec
The key to protecting your bussines

AEP

Ultra ELECTRONICS

Details

Family: Cryptosec OpenKey

Product: Cryptosec TSA

Clock Synchronisation: NTP Protocol v3.0 and SNTP

Time Source: Configurable external NTP servers

Software platform: Operating system tailored for time stamping operations

Hardware platform: Secure cryptographic module

Device administration: Web GUI through HTTPS, digital certificate required

HSM administration: VT100 terminal

TSA service access: TSP Protocol (RFC 3161)

Formats:
- 1U Rack Mount
- 2U Rack Mount with double power feed, 2 network interfaces and double RAID disk (high availability)

Operating temperature: 10°C to 35°C

Storage temperature: -20°C to 60°C

Operating humidity conditions: 10% to 85%

Non-operating humidity conditions: 0% to 95%

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

IP protocols: 1Pv4

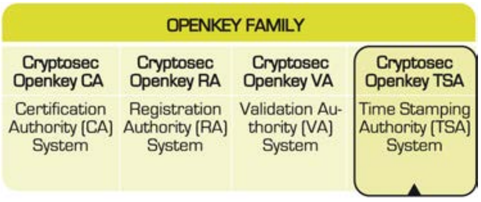
Input voltage: 100-240 volts AC. Standards used: NTP v3.0, PKCS#1, PKCS#8, PKCS#10, PKCS#12, SHA, certificates X.509 v3 and CRL X.509 v2 RFC 5280, HTTP, HTTPS

Standards used: NTPv3.0, TSP RFC 3161, PKCS#1, PKCS#8, PKCS#10, PKCS#12, SHA, certificates X.509 v3 RFC 5280, HTTP, HTTPS HTTP, HTTPS

Certifications

The **Cryptosec OpenKey TSA** solution integrates a Cryptosec PCI HSM, which can **optionally** be **certified for FIPS 140 Level 3** or for **Common Criteria EAL 4+** (with ALC_FLR.1 augmentation).

Ultra Electronics
AEP
Knaves Beech Business Centre
Loudwater
High Wycombe
Buckinghamshire, HP10 9UT
Main Switchboard: +44 (0)1628 642 600
Email: info@ultra-aep.com
www.ultra-aep.com
www.ultra-electronics.com



OPENKEY FAMILY

Cryptosec Openkey CA
Certification Authority (CA) System

Cryptosec Openkey RA
Registration Authority (RA) System

Cryptosec Openkey VA
Validation Authority (VA) System

Cryptosec Openkey TSA
Time Stamping Authority (TSA) System