Features

- Generation of certificates X.509 v3 and CRLS X.509 v2 according to the RFC 5280 standard.
- Administration of the system via HTTPS, requiring a digital operator certificate.
- Configuration as a Root or Subordinate Certification Authority.
- RSA private key generation, from 1024 to 4096 bits.
- Certificate generation according to configured policies.
- Capability of accepting requests from several Registration Authorities (RAs) simultaneously.
- Synchronization of the system's clock via NTP (Possibility of including other synchronization systems: GPS, cesium clocks, rubidium clocks, etc.).
- Access to PostgreSQL database, which enables storage of any audit logs, certificates and CRLs generated.
- Appliance format to facilitate installation and deployment.

Requirements

- Accessible PostgreSQL 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.

Cryptosec Openkey CA

Certification Authority

Cryptosec CA is an appliance equipped with Cryptographic Software and Hardware (HSM) integrated into a single device, which considerably reduces the product's costs and installation time.

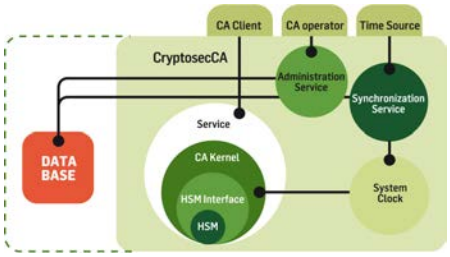
"Cryptosec CA allows for active - passive configuration with Database replication."

It is easily configured through an HTTPS interface requiring an operator certificate. This authenticated connection is totally secure.

The safekeeping of the authority's certificate keys as well as the certificate signature operation and the revoked certificate list (CRL) are performed in the HSM, which is integrated into the appliance. In addition to protecting the keys, this contributes to speeding up the generation processes.

The certificates generated and the CRLs can be posted on different RAs on a regular basis. The system includes a service for synchronising its clock via NTP.

It should be highlighted that all the data generated (Certificates and CRLs) are stored in the appliance's database.



The **Certification Authority** is the most important element of a public key infrastructure (PKI).
Cryptosec CA can perform two roles:

- Root Certification Authority
- Subordinate Certification Authority Its mission consists of generating Digital Certificates in a single-key structure (PKI).

"As a general rule, a Root CA does not generate end-entity certificates, but instead certifies other CAs known as Subordinates, which in turn are responsible for generating Digital Certificates for the end user. And this is precisely where Cryptosec OpenKey CA plays an important role as an essential element of the public key infrastructure (PKI)."

realsec The key to protecting your bussines

AEP

Ultra ELECTRONICS

Details

Family: Cryptosec OpenKey

Product: Cryptosec CA

Clock Synchronisation: NTP Protocol v3.0

Time Source: Configurable external NTP servers

Software platform: Operating system tailored for digital certificate generation and revocation operations

Hardware platform: Secure cryptographic module Cryptosec (HSM)

Device administration: GUI Web through HTTPS and digital certificate required

HSM administration: VT100 terminal

CA service access: Access via secure authenticated socket through configurable port

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

Certifications

The **Cryptosec OpenKey CA** 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