Cryptosec Openkey RA

Registration Authority

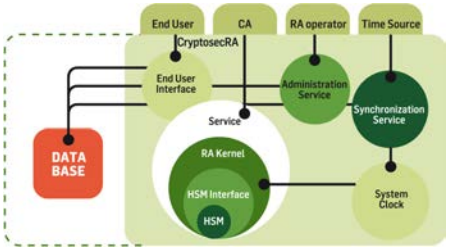
Cryptosec Openkey RA is the Registration Authority that serves as the Certification Authority's (Cryptosec CA) point of entry. It also offers users all the functionalities of generating certificate and revocation requests, in addition to allowing the RA operators to access certification usage policies.

Cryptosec Openkey RA allows for active - passive configuration with Database replication. This solution consists of an appliance whose Cryptographic Software and Hardware (HSM) are housed a single device, considerably reducing the cost of the product and the time needed to install it. It is designed to generate digital certification requests in a PKI structure.

Cryptosec Openkey RA allows for multiple certificate generation procedures, for instance: End users connect through an HTTPS-protected Web interface to make their certification requests and these requests are stored until an operator verifies them before then being sent to the CA. All this is performed in a protected and authenticated way, and once Cryptosec Openkey RA receives the certificate, it is sent to the end user.

The system is configured through an HTTPS interface which requires an operator certificate via a fully secure authenticated connection.

The certificates generated and the CRLs can be posted on different systems on a periodic basis. Each of these systems includes a service for clock synchronization via NTP. The data generated (Certificates and CRLs) are stored in the appliance's database.



The Registration Authority Cryptosec Openkey RA is the end users' point of access to the Certification Authority.
It is also the tool where certification and revocation requests are generated.

" Cryptosec Openkey RA can either send a certification request without being reviewed by an operator or require a review of the certification, depending on the certification policy, and it can even require the physical presence of the user who generated the certification request."

Features

- Easy administration of the system via HTTPS, requiring a digital operator certificate.
- Access to end users through HTTPS.
- Certification request generation functionality.
- Use of certification and registration policies.
- RSA private key generation from 1024 to 4096 bits.
- Secure generation of keys from an approved device.
- Posting of certificates and CRLs on LDAP, WEB and SAMBA.
- Synchronisation of the system's clock via NTP (Possibility of including other synchronisation systems: GPS, cesium clocks, rubidium clocks, etc.).
- Access to PostgreSQL databases to store audit logs and certificate requests.
- Appliance format which facilitates installation and deployment.

Requirements

- Accessible PostgreSQL database, although any database can be adapted depending on customer requirements.
- VT100 terminal for secure HSM administration.
- TCP access to an NTP server through port 123.
- Access to the CA (Certification Authority).

realsec
The key to protecting your bussines

AEP

Ultra ELECTRONICS

Details

Family: Cryptosec OpenKey

Product: Cryptosec RA

Clock Synchronization: NTP Protocol v3.0

Time Source: Configurable external NTP servers

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

Hardware platform: Secure cryptographic module Cryptosec (HSM)

Device administration: Web GUI through HTTPS, 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 RA** 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	**Cryptosec Openkey RA**	**Cryptosec Openkey VA**	**Cryptosec Openkey TSA**
Certification Authority (CA) System	Registration Authority (RA) System	Validation Authority (VA) System	Time Stamping Authority (TSA) System