

# CryptosecRA

---

Registration Authority (RA) is the access point for end-users to the certifying authority. RA is where certification and revocation requests are generated.

Depending on the certification policy, a RA may send a certification request to a CA without being endorsed by an operator, either requiring the visa, or furthermore requiring the physical presence of the user who generated the certification request.

CryptosecRA is registration authority of Cryptosec OpenKey family that makes the access point to the certification authority CryptosecCA. It provides all the features of creating certification requests to users and create the certification policies to the RA operators.

Moreover,

- Custody their keys in a extremely safer manner.
- It is equipped with a certificated cryptographic hardware.

## Functional Description

Registration authority CryptosecRA is an appliance composed of cryptographic hardware that aims to check users certification requests.

End users connect and make their certification requests through a secured HTTPS web interface. These requests are stored in the RA and the operator will check them to be sent to the CA. This is produced in a protected and authenticated mode and once the RA receives the certificate it is sent to the end user.

RA signature and authentication keys are kept into the cryptographic hardware integrated in the system.

CryptosecRA configuration is done through the friendly user interface HTTPS which can generate different certification and registration policies.

Generated certificates and CRLs can be published periodically in different manners.

There is a system clock synchronization service using NTP.

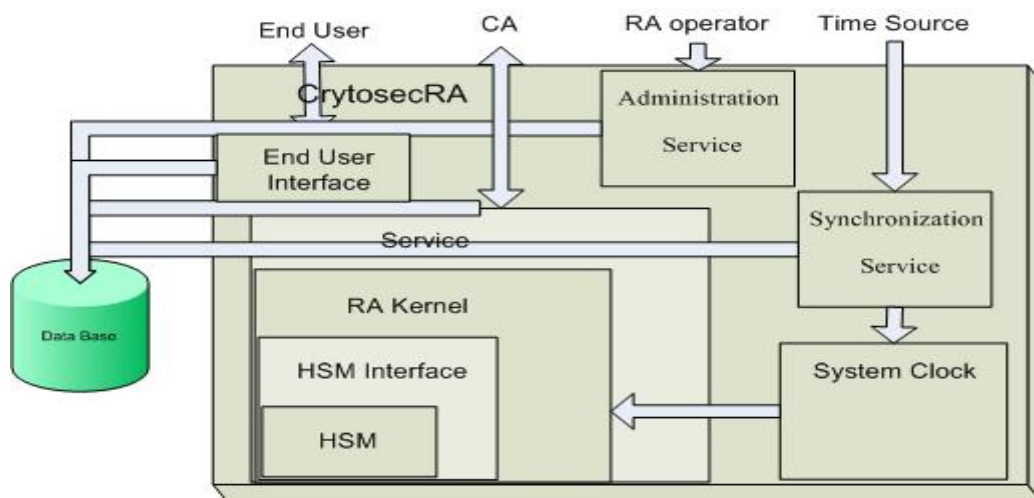
Both configuration as all generated data (certificates and CRL) are stored in a external database.



CryptosecRA. Certificate generation screen

## Architecture

CryptosecRA 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. Certification requests are sent using a secure and authenticated connection with the CA. Administration is done using HTTPS, requiring a valid administration operator certificate.



Esquema funcional de CryptosecCA

## Features

- System administration using HTTPS with required operator certificate.
- End user access through HTTPS.
- Functionality of certification request generation.
- Generation RSA private keys, from 1024 to 4096 bits.
- Safely generation of keys from an accredited device.
- Publication of certificates and CRL using LDAP, Web, SAMBA.
- System clock Synchronization using NTP. (It is possible incorporate other sync systems: GPS, etc.).
- Generation of certification and registration policies.
- CryptographicHardware 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.

## Requirements

Because the product CryptosecRA 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 acces, although it is posible 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.
- Access to the CA.

## 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 digital certificates generation.

**Hardware Platform**

Cryptosec Secure Cryptographic Module.

**Device Administration:**

Web GUI using HTTPS and digital certificate required

**HSM Administration:**

VT100 Terminal.

**RA Access:**

Web GUI using HTTPS.

**CA service access:**

Acceso por socket autenticado y seguro a través de puerto preconfigurado.

**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)