

# CryptosecCA

---

Certification Authority (CA) is the most important element in a public key infrastructure and has to be protected ensuring security measures. From this element a certification chain will be generated and the CA is the trusted third party of this chain.

Certification Authority may take two different roles:

- CA root.
- CA subordinate.

A CA root is that one which is at the top of the certification chain. Normally it does not generate end-user certificates, but certifies other certification authorities. Those authorities are called subordinate CA and that they finally do is generate the end-user certificates.

You can create structures of certification authorities of any depth but the most usual is two or three depth levels..

CryptosecCA is the Certification Authority of the family Cryptosec OpenKey that conforms the stricter requirements of a certification authority. CryptosecCA admits any configuration on depth of certification chain or making role, ie can work as CA root or subordinate.

Moreover,

- Keep their keys in an extremely safe manner.
- It is equipped with a certificated cryptographic hardware device.
- Accepts multiple registration authorities simultaneously.

## Functional Description

Certification authority CryptosecCA is an appliance composed of cryptographic hardware that aims to generate digital certificates covered by a structure of public key (PKI) totally reliable. The configuration is done through the friendly user interface HTTPS using a trusted administration operator certificate.

Once role of CryptosecCA device is set, CA root or CA subordinate, you can access into a menu where you can generate the certificate of the authority and configure the system.

Service allows online access to a preconfigured authority to make requests for end-users certificates. This connection is authenticated and secure.

Both the custody of the authority certificate keys as the operations of signing certification requests and certification list of revoked certificates (CRL), takes place into the HSM integrated with the appliance CryptosecCA. This is, in addition to ensure the protection of these keys, makes the generation processes considerably faster.

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.

**realsec** **CryptosecCA**

Inicio Operaciones Consulta Gestión Acceso Sistema

Operación > Generación de Petición de Certificado

**Atributos de Petición de Certificado Digital**

Petición de Certificado: 1024, 2048, 4096

Dirección de correo electrónico (emailaddress):

Nombre del País(c): ANDORRA

Localidad(l):

Nombre de la Organización(o):

Nombre de la Unidad de la Organización(ou):

Nombres Comunes(cn):

**Extensiones**

Restricciones Básicas  critica

Longitud del path CA: 1

Políticas de certificados  critica

CPS:  Si  No

OID:

URL:

Comentario:

Uso de la claves

**Uso mejorado de la clave**  critica

- Firma Electronica
- No repudio
- Clave de firma de certificado
- Cifrado de datos
- Clave de cifrado
- Solo cifrado
- Clave de negociacion
- Solo decifrado
- Clave de firma de CRL

**Uso extendido de la clave**  critica

- SSL/TLS Autenticacion para servicio web
- Firma Electronica
- SSL/TLS Autenticacion de cliente web
- Proteccion de correo electronico.
- Firma de codigo comercial para Microsoft
- Firma de codigo personal para Microsoft
- Sellado de tiempo seguro
- Firma de listas de revocacion de confianza
- Firma para encriptar el sistema de archivos
- Firma para servidor de puerta en enlace

Puntos de acceso de la información sobre la Autoridad de Certificación

Protocolo de acceso:  HTTP  FILE  LDAP  HTTPS

Dirección del repositorio de información:  Enviar

Repositorios:

Generar

Realsec Technologies S.L. Copyright © 2008

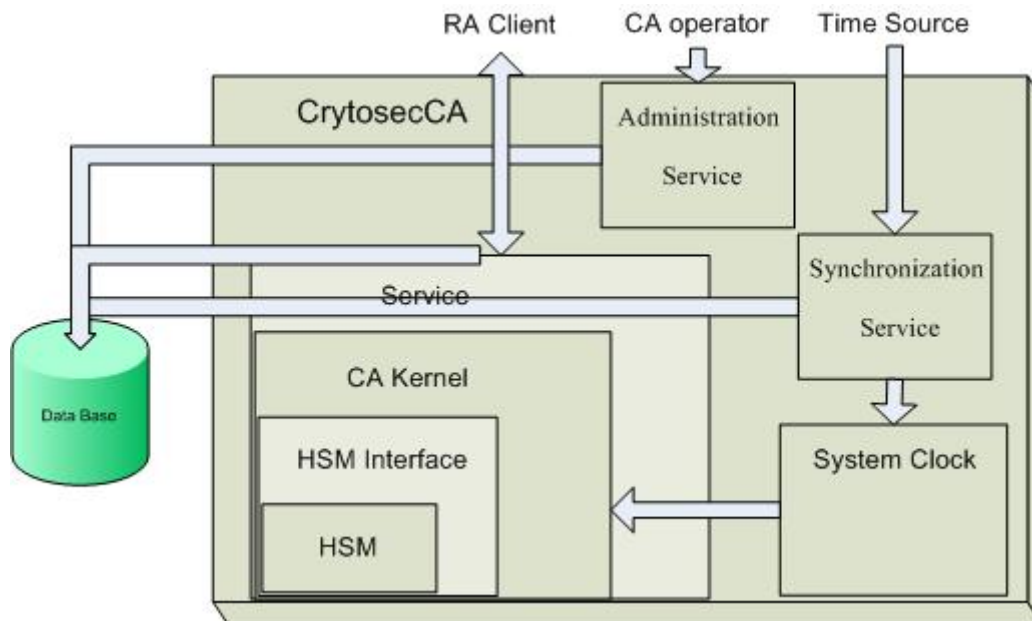
CryptosecCA. CA root certificate generation screen.

## Architecture

CryptosecCA 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.

The generation of end-users certificates is done through a secure and authenticated connection with a preconfigured registration authority.

Administration is done using HTTPS, requiring a valid administration operator certificate.



CryptosecCA functional scheme

## Features

- Generation of standard X.509v3 certificates rfc3280.
- System administration using HTTPS with required operator certificate.
- Configuration as CA root or CA subordinate.
- Generation RSA private keys, from 1024 to 4096 bits.
- Safely generation of certificates 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.).
- Ability to accept request from several Registration Authorities simultaneously.
- Generation of certificates using preconfigured 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 CryptosecCA is delivered as an appliance format, all hardware and software is included with the device. It simply requires the following external systems:

- Database with Postgress 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.

## Details

**Family:**

Cryptosec OpenKey.

**Product:**

CryptosecCA.

**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.

**CA Service Access:**

Access by an authenticated socket and safely through a preconfigured port.

**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)