

CryptosecCA

La autoridad de certificación es el elemento más importante y al que más hay que proteger en una infraestructura de clave pública. A partir de este elemento se generará la cadena de certificación y será la autoridad de certificación la tercera parte confiable de esta cadena.

La autoridad de certificación puede tomar dos roles:

- Autoridad de certificación raíz.
- Autoridad de certificación subordinada.

Una autoridad de certificación raíz es aquella que está en la cúspide de la cadena de certificación. Por regla general este ente no genera certificados de usuario final, sino que certifica a otras autoridades de certificación. Estas últimas autoridades son a las que se llama autoridades de certificación subordinadas y son éstas las que finalmente generarán los certificados digitales para los usuarios finales.

Se pueden crear estructuras de autoridades de certificación de cualquier profundidad pero lo habitual es que sean de dos o tres niveles.

CryptosecCA es la Autoridad de Certificación de la familia Cryptosec OpenKey que cumple los requisitos más estrictos de una autoridad de certificación. CryptosecCA admite cualquier tipo de configuración en cuanto a profundidad de cadena de certificación o de toma de rol, es decir puede funcionar como CA raíz o CA subordinada.

Además,

- Custodia sus claves de una forma extremadamente segura.
- Está dotada de un hardware criptográfico certificado.
- Admite varias autoridades de registro simultáneamente.

Descripción Funcional

La autoridad de certificación CryptosecCA es un appliance compuesto por hardware criptográfico que tiene como finalidad la generación de certificados digitales englobados en una estructura de clave pública PKI totalmente confiable. La configuración se hace a través de un interfaz amigable via HTTPS con requerimiento de certificado de operador.

Configurado el rol de dispositivo CryptosecCA, CA raíz o CA subordinada, se accede a un menú en el que se genera el certificado de la autoridad y se puede configurar el sistema.

El servicio de acceso permite conectarse a una autoridad preconfigurada para realizar las peticiones de certificados de usuario final. Esta conexión está autenticada y es segura.

Tanto la custodia de las claves del certificado de la autoridad como la operación de firma de peticiones de certificación y lista de certificados revocados o CRL, se realiza en el HSM

integrado en el appliance CryptosecCA. Esto además de asegurar la protección de estas claves hace que los procesos de generación se aceleren.

Los certificados generados y las CRLs pueden ser publicadas en diferentes sistemas periódicamente.

Existe un servicio de sincronización del reloj del sistema por medio de NTP.

Tanto la configuración como todos los datos generados (certificados y CRL) son almacenados en una base de datos externa al dispositivo.

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 crítica

Longitud del path CA: 1

Políticas de certificados crítica

CPS: Sí No

OID:

URL:

Comentario:

Uso de la claves

Uso mejorado de la clave crítica

- 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 crítica

- 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

Realia Technologies S.L. Copyright © 2008

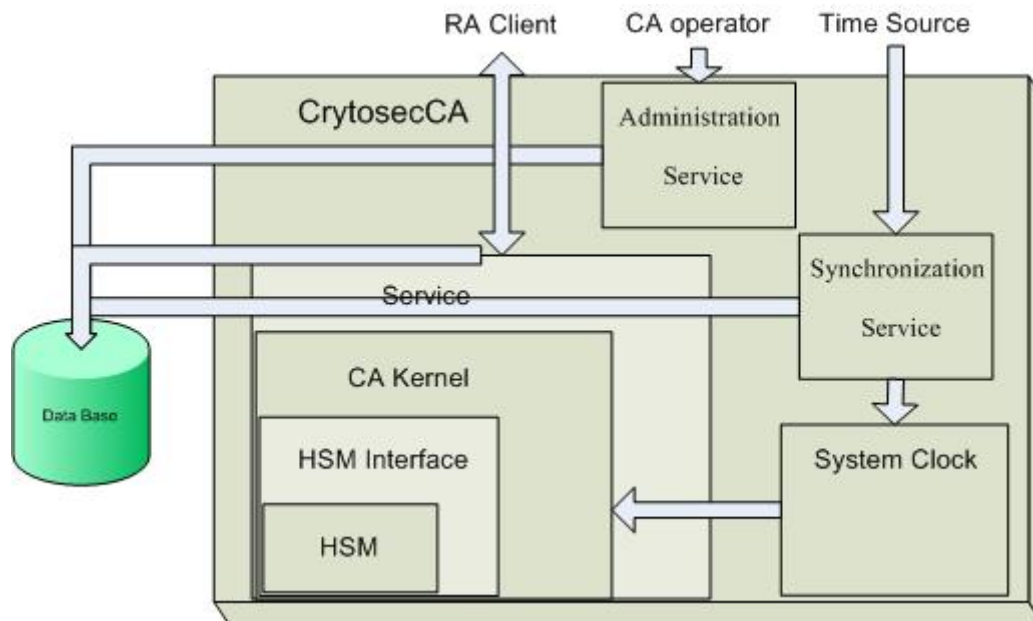
Pantalla de generación de certificado raíz CryptosecCA

Arquitectura

CryptosecCA está diseñado sobre un motor criptográfico hardware (HSM). Tanto el hardware como el software están integrados en una misma máquina, por lo que la solución se ofrece en formato appliance.

La generación de certificados de usuarios finales se hace a través de una conexión segura y autenticada con una autoridad de registro preconfigurada.

La administración se realiza a través de HTTPS, requiriendo la presentación de un certificado válido de operador.



Esquema funcional de CryptosecCA

Características

- Estándar de generación de certificados X.509v3 rfc3280.
- Administración del sistema vía HTTPS con requerimiento de certificado de operador.
- Configuración como autoridad de registro raíz o subordinada.
- Generación de claves privadas RSA, desde 1024 hasta 4096 bits.
- Generación de certificados desde un dispositivo acreditado de forma segura.
- Publicación de certificados y CRL en LDAP, Web, SAMBA.
- Sincronización del reloj del sistema vía NTP. (Posibilidad de incorporación de otros sistemas de sincronismo: GPS, etc.).
- Capacidad de aceptar peticiones de varias autoridades de registro de forma simultánea.
- Generación de certificados por políticas preconfiguradas.
- Hardware criptográfico Cryptosec certificado FIPS 140-2 Level 3.
- Acceso a base de datos externa Postgress y MySQL. (Posibilidad de acceso a Oracle, MS SQL)

- Formato appliance facilitando la instalación y puesta en producción.

Requerimientos

Debido a que el producto CryptosecCA es entregado en formato appliance todo el hardware y software está incluido en el dispositivo. Simplemente se requieren los siguientes sistemas externos:

- Base de datos accesible Postgress o MySQL aunque es posible adaptar cualquier base de datos según requerimientos del cliente.
- Terminal VT100 para administración segura del HSM.
- Acceso por TCP a un servidor NTP a través de puerto 123.

Detalle

Familia:

Cryptosec OpenKey.

Producto:

CryptosecCA.

Sincronismo del Reloj:

Protocolo NTP v3.0

Hora de Referencia:

Servidores NTP externos precargados.

Plataforma software:

Sistema operativo personalizado para operaciones de generación de certificados digitales.

Plataforma hardware

Modulo criptográfico seguro Cryptosec.

Administración del dispositivo:

Web GUI a través de HTTPS y certificado digital requerido

Administración HSM:

Terminal VT100.

Acceso servicio CA:

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

Dimensiones:

1U 19" Rack Mount

Temperatura de operación

10°C to 35°C

Temperatura de almacenamiento

- 20°C to 60°C

Condiciones de humedad de operación:

10% to 85%

Condiciones de humedad de operación:

0% to 95%

Interfases:

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

Protocolos IP:

IPv4

Voltaje de entrada:

100-240 Volts AC

Certificaciones estandares:

FEDERAL COMMUNICATION COMMISSION PART 15 (radio frequency devices)

NATIONAL INSTITUTE OF STANDART AND TECHNOLOGY. FIPS 140-2 LEVEL 3

Estándares utilizados:

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

North America Headquarters

710 Marshview Close, Roswell - Georgia 30076, USA Tel: +1.817-898-0153 Fax: +1.480-247-5501

Email: 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

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