

CryptosecRA

La autoridad de registro es el punto de acceso de los usuarios finales a la autoridad de certificación. Es a través de la autoridad de registro donde se generan tanto las solicitudes de certificación y las solicitudes de revocación.

Dependiendo de la política de certificación, una autoridad de registro puede enviar una solicitud de certificación a una autoridad de certificación sin ser visada por un operador, o bien requerir del visado, o más aún requerir la presencia física del usuario que generó la petición de certificación.

CryptosecRA es la autoridad de registro de la familia Cryptosec OpenKey que hace de punto de entrada a la autoridad de certificación CryptosecCA. Ofrece todas las funcionalidades de creación de peticiones de certificación a los usuarios y de creación de políticas de certificación a los operadores de la RA.

Además,

- Custodia sus claves de una forma extremadamente segura.
- Está dotada de un hardware criptográfico certificado.

Descripción Funcional

La autoridad de registro CryptosecRA es un appliance compuesto por hardware criptográfico que tiene como finalidad el registro de entrada de peticiones de certificación por parte de los usuarios.

A través de un interfaz Web protegido por HTTPS los usuarios finales se conectan y realizan sus peticiones de certificación. En la autoridad de registro quedan almacenadas y un operador las verificará para su envío a la CA. Éste se produce de forma protegida y autenticada y una vez que la autoridad de registro recibe el certificado es enviado al usuario final.

Las claves de firma y autenticación de la autoridad de registro están custodiadas en el hardware criptográfico integrado en el sistema.

CryptosecRA es configurable a través de un interfaz Web seguro HTTPS con el que se pueden generar diferentes políticas de certificación y diferentes políticas de registro.

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.

Características

- Administración del sistema vía HTTPS con requerimiento de certificado de operador.
- Acceso usuarios finales a través de HTTPS.
- Funcionalidad de generación de peticiones de certificación.
- Generación de claves privadas RSA, desde 1024 hasta 2048 bits.
- Generación de claves 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.).
- Generación de políticas de certificación y políticas de registro.
- 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 CryptosecRA 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.
- Acceso a la autoridad de certificación.

Detalle

Familia:

Cryptosec OpenKey.

Producto:

CryptosecRA.

Sincronismo del Reloj:

Protocolo NTP v3.0

Hora de Referencia:

Servidores NTP externos precargados.

Plataforma software:

Sistema operativo personalizado.

Plataforma hardware

Modulo criptográfico seguro Cryptosec.

Administración del dispositivo:

Web GUI a través de HTTPS y certificado digital requerido

Administración HSM:

Terminal VT100.

Acceso a RA:

Web GUI a través de HTTPS.

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