

CryptosecVA

El crecimiento en número de los certificados emitidos bajo una cadena de confianza tiene como consecuencia que las operaciones hechas con los mismos también se incrementen. El proceso de verificación de un certificado tiene como sub-operación la descarga de una lista de certificados revocados. Estas listas pueden ser de un tamaño considerable cuando los certificados emitidos por una autoridad de certificación son muchos. Además, estas listas de certificados revocados son válidas durante un periodo determinado, pudiéndola utilizar una aplicación para validar un determinado certificado durante dicho periodo. Esto provoca que un certificado pueda ser revocado durante este periodo de validez de la lista de certificados revocados y no sea reflejada esta revocación.

Las autoridades de validación nacen con dos metas bien identificadas:

- Reflejar en todo momento el estado de revocación de un certificado.
- Aligerar el tráfico de red consecuencia de descargas repetitivas de listas de certificados revocados.

Las autoridades de validación se alimentan de información tomando las propias listas de revocación o mejor aún accediendo directamente a la información que la CA contiene en su base de datos.

CryptosecVA es la autoridad de validación de la familia Cryptosec OpenKey que realiza la función de dar el estado de revocación de los certificados digitales emitidos bajo una determinada infraestructura. Debido al hardware criptográfico embebido dentro del sistema es capaz de responder a miles de peticiones por hora.

Además,

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

Descripción Funcional

La autoridad de validación CryptosecVA es un appliance compuesto por hardware criptográfico que tiene como finalidad generar respuestas a peticiones de clientes sobre el estado de revocación de un determinado certificado.

Al igual que todos los productos de la familia CryptosecOpenKey, se configura a través de un interfaz Web protegido por HTTPS. Se le dota de un certificado digital cuyas claves residen custodiadas en el hardware criptográfico alojado en su interior y el sistema está preparado para responder a peticiones de recuperación de estado de validación de certificados.

La información de revocación de los certificados es recuperado de la base de datos que crea el sistema CryptosecCA o bien de las listas de certificados revocados que publica dicho sistema.

Además es capaz de contestar a peticiones de estado de revocación de certificados emitidos bajo diferentes CAs.

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.



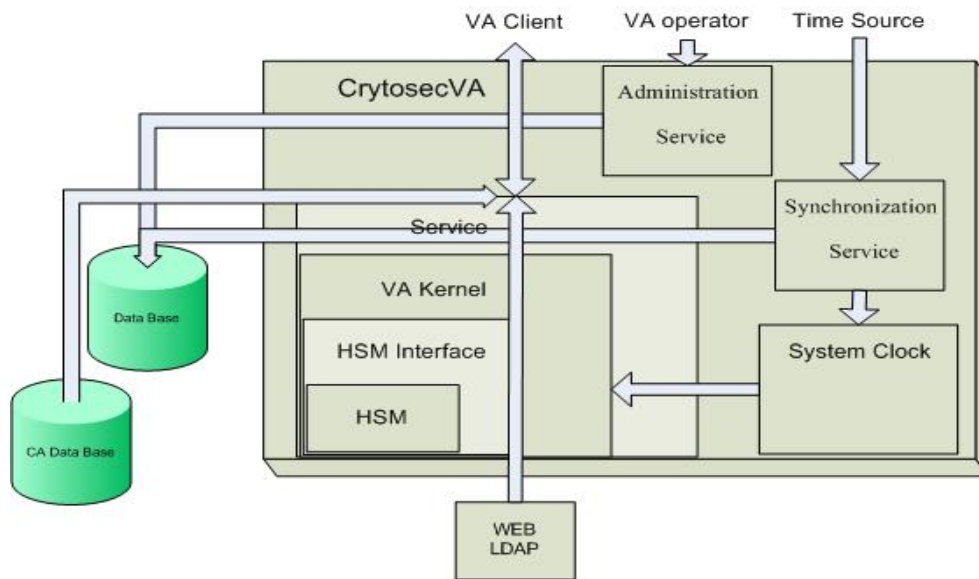
Pantalla de configuración de sistema de CryptosecVA

Arquitectura

CryptosecVA 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.

Las peticiones de consulta de estado de revocación son admitidas a través de protocolos HTTP y HTTPS.

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



Esquema funcional de CryptosecVA

Características

- Protocolo estándar OCSP (Online Certificate Status Protocol) rfc2560.
- Administración del sistema vía HTTPS con requerimiento de certificado de operador.
- Acceso usuarios finales a través de HTTP/HTTPS.
- Funcionalidad de generación de peticiones de certificación.
- Generación de claves privadas RSA, desde 1024 hasta 2048 bits.
- Generación de claves y firma de respuestas desde un dispositivo acreditado de forma segura.
- Acceso a información de revocación de base de datos de CryptosecCA y CRL en LDAP, Web, SAMBA.
- Sincronización del reloj del sistema vía NTP. (Posibilidad de incorporación de otros sistemas de sincronismo: GPS, etc.).
- 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 CryptosecVA 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 base de datos de CryptosecCA y repositorios con listas de certificados revocados configurados..

Detalle

Familia:

Cryptosec OpenKey.

Producto:

CryptosecVA.

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:

Protocolo OCSP (Online Certificate Status Protocol) sobre HTTP/HTTPS .

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:

OCSP rfc2560, NTP v3.0, PKCS#1, PKCS#8, PKCS#10, , 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