

CryptosecVA

The growth in number of certificates issued under a trusted chain has the consequence that transactions made by them also increased. The process of certificate verification has a sub-process of downloading a list of revoked certificates. These lists can be huge size when there are many certificates issued by a certification authority. In addition, these list of revoked certificates are valid for a specified period, an application could be used to validate a certificate during this period. This causes that a certificate might be revoked during the list period of validity, but this one could not be updated in a given time.

Validation Authorities are born with two well defined goals:

- Reflect in every moment the state of revocation of a certificate.
- Make the network traffic lighter, resulting from repetitive downloads of revoked certificate list.

Validation authorities are fed with information by taking their own revocation list or better accessing information contained in the CA database.

CryptosecVA authority is the validation of the family Cryptosec OpenKey that performs the function of giving the state revocation of digital certificates issued under a certain infrastructure. Due to cryptographic hardware embedded within the system is capable of responding to thousands of requests per hour.

Moreover,

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

Functional Description

validation authority is an appliance integrated with hardware cryptographic module that has the capabilities to generate VA responses from the clients (applications, services or proprietary application), delivered the electronic certificate status in this moment.

All the products that the CryptosecOpenKey, has the capability to configure all the functionalities in a web interfaces protected via HTTPS protocol. The appliance has the functionality to generate electronic certificate (mini-ca) with the Web Authentication Use, this process is supported with the entire task that has a PKIs Plataforms (electronic certificate generation and revocation).

The certificate revocation info is integrated with the process that are doing in the CryptosecCA and use all the Information that has in your repositories (physical (DataBases) and logical

repositories (class)), also has the capability to use a certificate revocation list that generate the CryptosecCA. These operations guarantee the interoperability with different Certification Authority.

There several Network time synchronize method to guarantee the time source trusted, the Validation Authority are prepared to use the Network Time Protocol via a NTP secure repositories.

Certificates revocation information is recovered from the database system created by CryptosecCA or lists of revoked certificates published that system. It is also capable of answering request for revocation state of certificates issued Ander different CAs.

There is a system clock synchronization service using NTP.

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



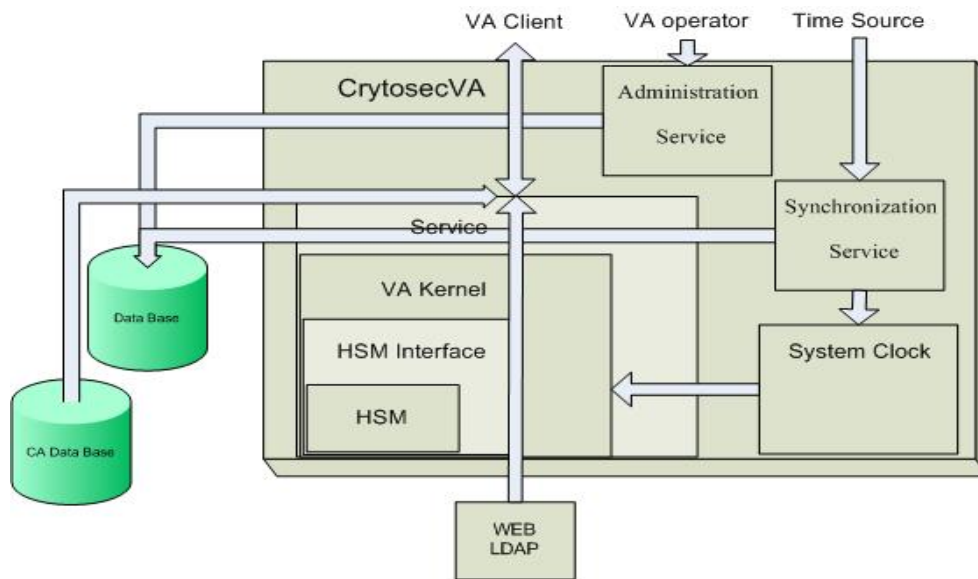
CryptosecVA configuration screen.

Architecture

CryptosecVA 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

- OCSP (Online Certificate Status Protocol) rfc2560
- 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.

Hardware Platform

Cryptosec Secure Cryptographic Module.

Device Administration:

Web GUI using HTTPS and digital certificate required

HSM Administration:

VT100 Terminal..

Access VA:

Web GUI via HTTPS.

VA service Access:

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

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

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