

INFORMACIÓN TÉCNICA

CryptosecMail

Características Funcionales

Cryptosecmail es un servidor de mensajería, que proporciona funcionalidades de firmado y cifrado digital de correos electrónicos de forma centralizada, incorporando igualmente la capacidad de almacenar y administrar, de forma segura, las claves de los certificados que se utilicen para confeccionar las operaciones criptográficas en los correos.

Funcionalidades

La arquitectura del Cryptosecmail integra procesos criptográficos y una biblioteca que incluyen interfaces nativas de cualquier servidor de correo electrónico, configurado para gestionar estructuras MIME y convertirlas a S/MIME. La estructura MIME esta diseñada para realizar firmas electrónicas y operaciones de cifrado sobre correos ensamblados en distintos formatos (texto, HTML, texto enriquecido) independientemente de que estos dispongan de cualquier archivo anexo.

Todos los procesos criptográficos (generación de claves, procesos de almacenamiento y exponenciación con clave privada) se realizan en el HSM, de forma que no pueden ser interceptadas por terceros, y dota al sistema de protección física y lógica.

El dispositivo de gestión de correos electrónicos dispone de las siguientes funcionalidades:

- Almacenamiento de correos electrónicos sobre esquemas relacionales y cifrados bajo demanda
- Interfaz Web de configuración securizada mediante certificados digitales.
- Capacidad de realizar gestión y administración de correos electrónicos sobre atributos de interés para el cliente.
- Creación, administración, asignación de capacidades criptográficas y configuración de buzones de mail,
- Estructura de logs orientada a eventos, basados en las operaciones de configuración, captura y envío de correo electrónico.

Arquitecturas propuestas.

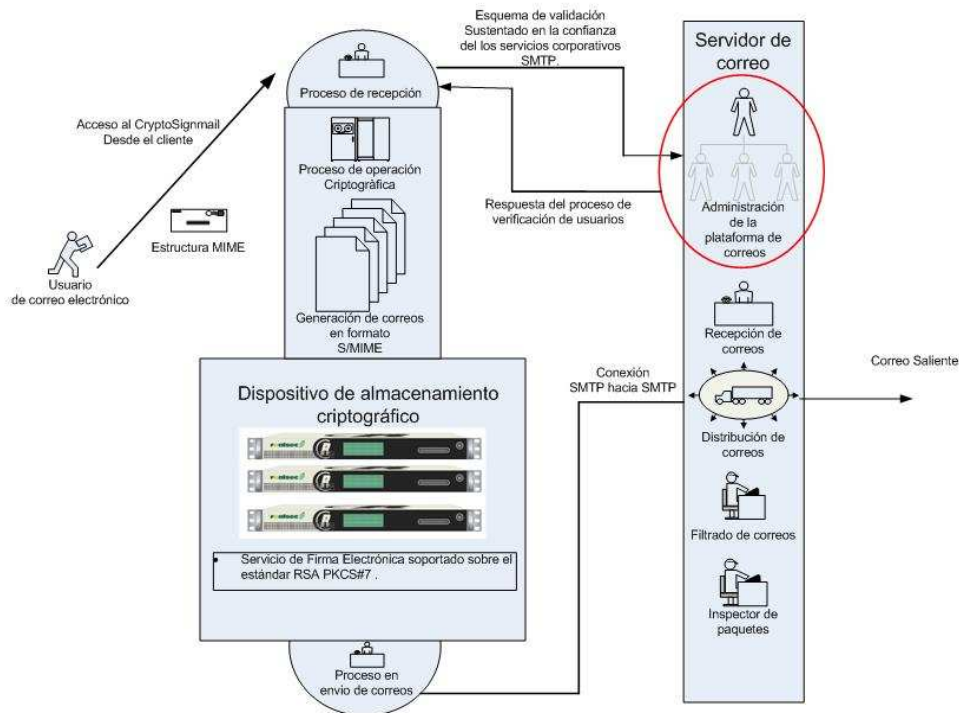
Dentro de las distintas arquitecturas de conectividad disponibles, para implementar de forma robusta el producto Cryptosecmail, se proponen las siguientes:

a) Arquitectura orientada a infraestructuras externalizadas.

Esta implementación es ideal cuando el servicio de correo electrónico está externalizado. Mediante la utilización del dispositivo, se logra de forma segura la firma de correo centralizada en la organización. Garantiza que todos los correos emitidos son correctamente firmados y sustentados sobre la jerarquía de la infraestructura PKI que emitió los certificados digitales de firma.

La implantación de Cryptosecmail, es completamente transparente al servicio externo de correo, no se requiere ningún cambio en los parámetros de configuración de dicho servicio. Las claves igualmente están centralizadas proporcionando de esta forma la seguridad y la capacidad de poder realizar despliegues en periodos cortos de tiempo.

La implementación del dispositivo puede apreciarse en el siguiente esquema:



Detallaremos cada uno de los elementos que integran este esquema:

- El Cliente de correo electrónico.

Es el software de correo electrónico cliente, dispone de la capacidad de dialogar en un protocolo afín al servicio centralizado de correos electrónicos (Servidor Cryptosecmail) y dispone de la capacidad de realizar una autenticación frente a un tercero (Servidor Remoto de Correo) convirtiendo el servidor de correo corporativo en un proveedor de identidades hacia la plataforma de operaciones criptográficas centralizada.

- Proceso de firma y cifrado digital en correos electrónicos.

Consiste en integrar las comunicaciones que intercambian servicios de firma y cifrado digital centralizado y el servicio externo de correo, todas las operaciones criptográficas se realizan, tomando como punto de partida la interrelación con el sistema preexistente de correo electrónico. El objeto de dicho proceso es disponer de un correo electrónico firmado con un certificado digital.

Cryptosecmail dispone de soporte para conectarse con cualquier correo que estructure los mensajes bajo el estándar MIME.

Las modalidades de autenticación constituyen un diálogo pregunta-respuesta, que, mediante un componente conmutador de tráfico SMTP y su integración con un tercero de confianza, robustece el proceso de envío de correos dejando las claves de los usuarios intactas y sin requerir ningún cambio en el momento de la implementación.

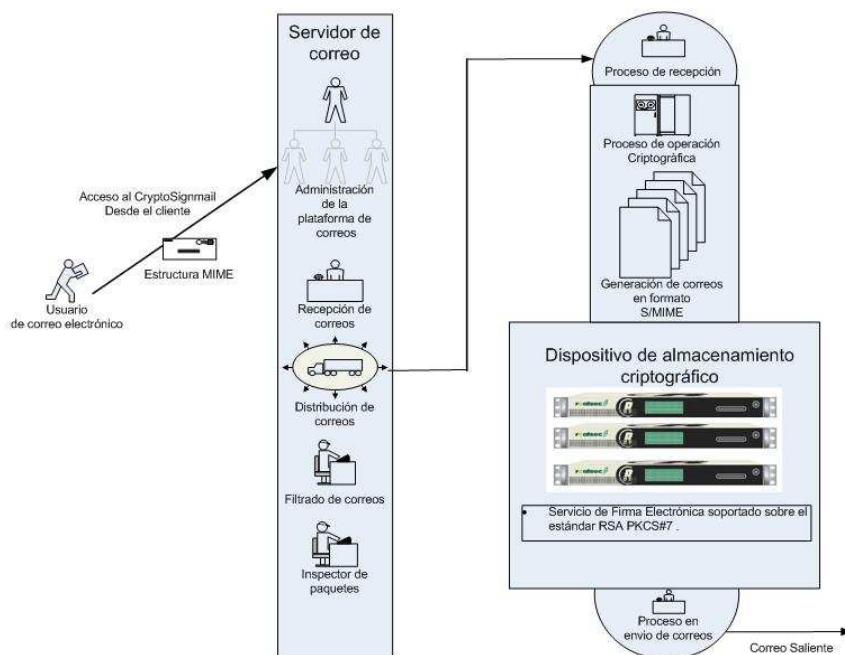
La arquitectura antes definida presenta el siguiente impacto sobre el entorno en donde se requiere implementar:

- Variaciones a nivel de arquitectura de conectividad, DNS.
- Ninguna modificación a nivel del cliente de correo.
- Ninguna modificación en la configuración del conector SMTP.
- Pruebas de disponibilidad sobre el esquema de autenticación de los clientes y el servicio de firma digital de correos electrónicos.

b) Arquitectura orientada a infraestructuras locales.

Este modelo de arquitectura se adapta a las infraestructuras corporativas, donde la responsabilidad de la administración del servicio de correo electrónico recae en la propia organización interna de la empresa.

La implementación de esta instalación conlleva cambios de las condiciones de operación del correo electrónico, ya que se debe configurar la plataforma local (servidor de correo existente) como un Proxy SMTP, y dejar el envío hacia el exterior al dispositivo criptográfico. Se mantiene el esquema en el que todos los clientes de correo electrónico interactúan directamente con el servidor preexistente.



En la arquitectura antes definida se observan las siguientes características:

- a) Pocas modificaciones a nivel de arquitectura.
- b) Ninguna modificación a nivel del cliente de correo.
- c) Modificaciones en la configuración del conector SMTP.
- d) Ninguna modificación respecto al esquema de autenticación de los clientes y el servicio de firma digital de correos electrónicos.

Especificaciones Técnicas

Sistema HSM

- El HSM cumple con la certificación del estándar FIPS 140-2 nivel 3.
- Generación de claves a través de un generador de números aleatorios, según lo especificado en FIPS 186-2 con nota de modificación y aprobado por FIPS 140-2.

Sistema Servidor

- Procesador con arquitectura Intel a 2.8 GHz de cuatro núcleos.
- 2048 MB de memoria interna.
- Dos conexiones ETHERNET 10/100/1000 Mbps con capacidades de configuración en tolerancia a fallas.

Capacidades Criptográficas

- Cifrado de clave simétrica:
 - Soporte para el cifrado de correos electrónicos con los siguientes algoritmos:
AES128_CBC, AES_192_CBC, AES256_CBC, CAST5_CBC, DES_EDE3_CBC, IDEA_CBC, RC2_CBC.
- Funciones Hash:
 - MD5.
 - SHA-1 SHA-2 hasta 512.
 - RIPEMD en 128 y 160 bit.
- Realización de firma electrónica bajo el estándar de clave pública RSA, con longitud de clave de hasta 4.096 bit.