

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 realizar estas operaciones criptográficas en los correos.

Funcionalidades

La arquitectura del Cryptosecmail integra procesos criptográficos y una biblioteca que incluye 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.

Los procesos de firmado y cifrado se realizan en el Hardware Criptográfico (HSM) lo que proporciona un gran incremento en la velocidad de los procesos.

La gestión de correos electrónicos seguros ofrece Utilidades de Administración como:

- Interfaz Web de Administración remota, securizada mediante la autenticación por certificado digital.
- Estructura de logs de Auditoria, separándose Logs de Administración, Logs de Procesos, y Logs de Errores.
- Envío automático, por correo electrónico al Administrador, de los Logs de Errores con frecuencia parametrizable (día, semana, etc)
- Generación automática de claves y "request" de certificación estándar a la PKI que se desee.

Además, se puede integrar con ERPs como SAP, People Soft, etc; Tomando la salida automática de correos confidenciales desde los ERPs para ser cifrados por Cryptosec Mail antes de su envío definitivo.

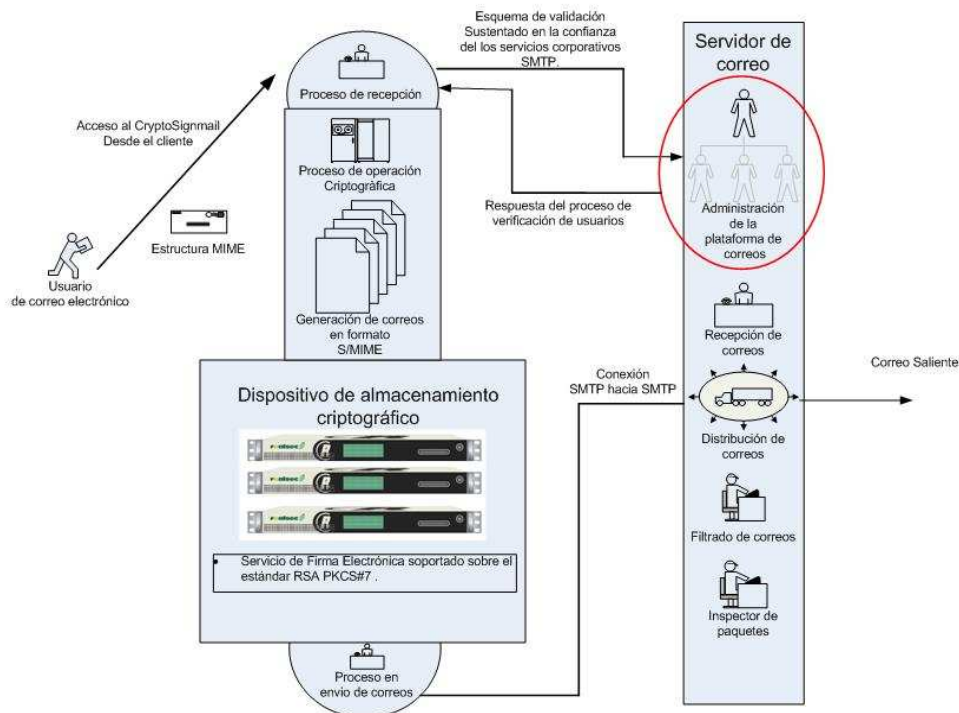
Esquema de Instalación.

Mediante Cryptosec Mail, se logra de forma segura la firma electrónica y/o cifrado de correo centralizada en la organización. Garantiza que 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 existente de correo.
- No se requiere ningún cambio en los parámetros de configuración de dicho servicio.
- Ninguna modificación a nivel del cliente de correo (Outlook o similar).
- Las claves están centralizadas, proporcionando la seguridad y la capacidad de poder realizar despliegues en periodos cortos de tiempo.

La implementación del dispositivo puede apreciarse en el siguiente esquema:



El esquema anterior integra los siguientes elementos::

- Cliente de correo electrónico.

Software de correo electrónico cliente (Microsoft Outlook, Lotus, etc.), que 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.

Integra 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.

Operativa de Firma de Correos

- Facilita la firma digital masiva de correos salientes, con un Certificado Corporativo de Entidad Jurídica, de manera que garantice su procedencia a los destinatarios.
- Las claves del certificado pueden ser generadas en el propio HSM, con la consiguiente construcción de “request” de certificación a la Autoridad de Certificación que se elija.
- En el caso de ya existir el certificado, éste puede ser instalado en el HSM por procedimientos seguros.
- Cryptosec Mail firma, tanto el cuerpo del mensaje, como los archivos adjuntos que se anexasen.
- Transforma la estructura MIME del mensaje en un S/MIME o MIME Seguro.
- Un servicio SMTP se encarga de dialogar con el/los clientes de correo (Outlook) y una interfaz de autenticación dialoga con el Servidor de Correo existente, para su envío.

Operativa de Cifrado de Correos

- Facilita el cifrado selectivo de correos salientes, de manera que su contenido sólo pueda ser visto por el destinatario.
- Es necesario que todos los destinatarios de correos cifrados dispongan de un certificado digital.
- El cifrado se realizará mediante la clave pública del destinatario, de forma que sólo él, con su clave privada, pueda descifrarlo.
- Cryptosec Mail accede al LDAP, Active Directory o similar, donde residan las claves públicas de los destinatarios, asociadas a su dirección de correo.
- El criterio de selección para cifrado o no-cifrado deberá venir marcado por alguna palabra clave en el campo “Asunto” del correo (por ejemplo, “Confidencial”)
- Cryptosec Mail cifra, tanto el cuerpo del mensaje, como los archivos adjuntos que se anexasen.
- Transforma la estructura MIME del mensaje en un S/MIME o MIME Seguro.
- Un servicio SMTP se encarga de dialogar con el/los clientes de correo (Outlook), una interfaz accede al Directorio, y otra interfaz de autenticación dialoga con el Servidor de Correo existente, para su envío.

Especificaciones Técnicas

Sistema Servidor

- Servidor instalable en rack de 2U, con 4Gb de RAM base ampliable
- 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 fallos.

- Doble fuente de alimentación (host swap) y dos discos en estructura redundante RAID-0 (en espejo)

Sistema HSM

- El HSM cumple con la certificación de seguridad del estándar FIPS 140-2 nivel 3, otorgada por el National Institute of Standards and Technology (NIST)..
- 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.

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.