FICHA DE DATOS

Certificados según el protocolo S/MIME para Seguridad de Correo Electrónico

Encripte comunicaciones internas y valide las fuentes de correo electrónico para evitar ataques de phishing

Las partes malintencionadas aplican métodos cada vez más sofisticados para atacar a las organizaciones a través del correo electrónico, incluso optan por interceptar mensajes para acceder a información sensible y/o suplantar identidades a través del correo electrónico con el fin de dirigir a los visitantes a sitios web de *phishing* o iniciar descargas de *malware*. El uso de certificados según el protocolo S/MIME para firmar y cifrar digitalmente correos electrónicos ayuda a las organizaciones a protegerse frente a estas amenazas y garantiza que únicamente los destinatarios legítimos pueden acceder al contenido del correo electrónico. Además, permite verificar la procedencia del mensaje para distinguir entre correos legítimos y/o maliciosos.

¿Qué es S/MIME?

S/MIME, o Extensiones de Correo de Internet de Propósitos Múltiples/Seguro (Secure/Multipurpose Internet Mail Extensions), es el estándar del sector para el cifrado de claves públicas de datos basados en MIME (basados en mensaje). Los certificados S/MIME proporcionan dos funciones clave de protección de correos electrónicos:

- **Firma Digital:** demuestra la autoría y evita la manipulación de correos electrónicos, garantizando al receptor que la comunicación procede de usted y no de un suplantador, y que el contenido del mensaje no ha sido modificado durante el tránsito.
- **Cifrado**: garantiza que el mensaje solo puede ser abierto por el destinatario legítimo y evita que la información sensible caiga en manos equivocadas.

Principales Características

- COMPROBACIÓN DEL ORIGEN DEL MENSAJE
  La firma digital de correos electrónicos verifica el origen del mensaje y garantiza a los receptores que la comunicación es legítima y no se trata de un mensaje fraudulento.
- CIFRADO DE MENSAJES DURANTE EL TRÁNSITO Y UNA VEZ RECIBIDOS
  El cifrado de correos electrónicos garantiza que solo los receptores legítimos pueden acceder al contenido, independientemente de la ubicación del correo electrónico.
- INTEGRIDAD DEL CONTENIDO
  La firma digital y/o el cifrado de correos electrónicos genera un sello antimanipulación para el contenido del mensaje que garantiza su integridad.
- COMPATIBILIDAD NATIVA
  Sin necesidad de contar con software adicional y compatible con los principales clientes de correo electrónico para empresas (Outlook, Thunderbird, Apple Mail, Lotus Notes, etc.).
- FACILIDAD PARA LOS USUARIOS FINALES
  Requiere una mínima formación por parte del usuario. Para la mayoría de los clientes, la firma digital y/o el cifrado de correos electrónicos es tan sencillo como hacer clic sobre un botón. Muchos clientes también ofrecen la opción de aplicar estas medidas de seguridad de forma automática para todos los mensajes salientes.
- ELECCIÓN DEL ALGORITMO DE FIRMA
  Elija entre SHA256RSA o RSASSA-PSS (disponible solamente para usuarios de PKI Gestionada).

GlobalSign
GMO INTERNET GROUP

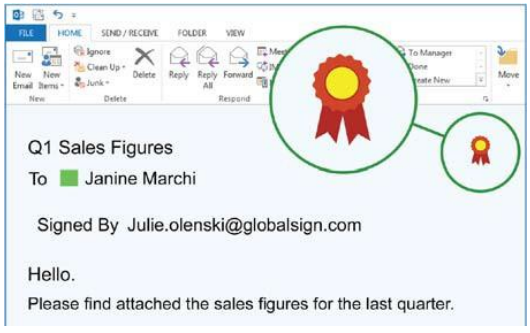
Certificados según el protocolo S/MIME para Seguridad de Correo Electrónico

Mitigación de los ataques de *phishing* y correos electrónicos fraudulentos

Verifique la procedencia de los correos electrónicos y la identidad del remitente

El envío de correos electrónicos desde una dirección falsa, lo que se denomina suplantación de identidad en correos electrónicos o *spoofing*, es uno de los métodos más populares para perpetrar un ataque de *phishing*.

La firma digital de correos electrónicos hace frente a esta amenaza presentando de forma inequívoca la información de identidad verificada del remitente del correo electrónico. De esta manera, los receptores de los correos pueden confiar en que el mensaje procede de una fuente legítima y verificada, y no de una dirección fraudulenta.



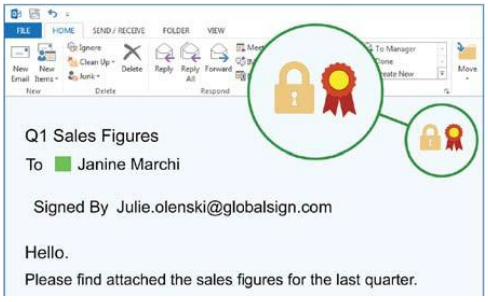
Ejemplo: Correo electrónico firmado digitalmente en Microsoft Outlook

Prevención de pérdidas y filtraciones de datos

Proteja las comunicaciones a través de correos electrónicos tanto durante el tránsito como una vez almacenados en los servidores de correo

Los correos electrónicos cifrados solo pueden ser descifrados por el receptor legítimo. Esto se debe al proceso criptográfico que tiene lugar en el momento del cifrado. El correo electrónico se cifra con la clave pública del receptor y solo puede descifrarse con la correspondiente clave privada.

Gracias a ello, nadie, salvo el receptor legítimo, puede descifrar el correo electrónico y leer el contenido, incluso si un intruso logra acceder al servidor de correo de la empresa o si el mensaje se intercepta durante el tránsito.



Ejemplo: Correo electrónico cifrado en Microsoft Outlook

Provisión y gestión de certificados

Los certificados S/MIME de GlobalSign son escalables para adaptarse a empresas de todos los tamaños, desde individuos hasta pequeñas y medianas empresas e incluso grandes organizaciones. Además, incorporan tecnologías de automatización y gestión del ciclo de vida de los certificados para simplificar las implantaciones de gran volumen.

- **PLATAFORMA PKI GESTIONADA**
  Las organizaciones que necesitan más de cinco certificados pueden aprovechar la plataforma PKI GESTIONADA (MPKI) de GlobalSign, que ofrece importantes descuentos por volumen frente a la compra de certificados individuales, y además centraliza la información de facturación y permite a los administradores emitir, renovar y revocar certificados eficazmente según las necesidades.

- **INTEGRACIÓN CON ACTIVE DIRECTORY**
  Automatice las implantaciones aprovechando la arquitectura existente de Active Directory y Group Policy para emitir e instalar de forma silente los certificados para terminales Windows y Apple OSX vinculados a dominios.

- **CERTIFICADOS INDIVIDUALES**
  Perfectos para aquellas organizaciones que necesitan un pequeño número de certificados (< 5). Los pedidos pueden realizarse directamente a través del sitio web de GlobalSign. Se envían correos electrónicos con recordatorios de renovación conforme se aproximan las fechas de vencimiento de cada uno de los certificados.

Acerca de GlobalSign

GlobalSign es el proveedor líder de soluciones confiables de identidad y seguridad digital que permiten que pequeñas y grandes empresas en todo el mundo, además, proveedores de servicios en la nube y empresas innovadoras en el área de la Internet de las Cosas (IoT), aseguren las comunicaciones en línea, administren millones de identidades digitales verificadas y automaticen la autenticación y el cifrado. Su infraestructura de clave pública (PKI) escalable y sus soluciones de identidad respaldan los miles de millones de servicios, dispositivos, personas y cosas que componen la Internet de Todo (Internet of Everything – IoE).

EE.UU.: +1 877 775 4562
Reino Unido: +44 1622766766
UE: +32 16 89 19 00

contacto@globalsign.com
www.globalsign.com

GlobalSign
GMO INTERNET GROUP