Authentication. Security. Trust.

GlobalSign®

GlobalSign - Productos

Ing. Víctor Alvarado
InterHAND S. A.
Costa Rica's GlobalSign CRP Partner

GlobalSign es una de las Autoridades Certificadores *(CA)* originales de todo el mundo. Hace parte del Grupo GMO Internet Group, el cual contiene más de 50 empresas concentradas en la industria del Internet, GlobalSign es el único representante del sector de la Seguridad Digital, lo que demuestra el compromiso y responsabilidad con el tema.

CA acreditada con el sello WebTrust hace más 24 años, 3 años seguidos en el cuadro de honor del Online Trust Alliance, es la CA con mayor y más rápido crecimiento en América Latina, GlobalSign se estableció en Agosto de 2013 como la segunda mayor **CA** en el Mercado Brasileiro y en el 2015 inicia operaciones en Costa Rica con la alianza estratégica a través de InterHAND S.A., el cual se convierte rápidamente en Socio Regional Certificado (CR) por el nivel de ventas, conocimiento del tema, certificación y alcance (sólo hay 4 en América Latina con este nivel de acreditación exclusivo).

El compromiso y preocupación de GlobalSign con la Seguridad Digital son comprobados a través de la acreditación en el mercado.

Autoridad de Seguridad Digital
Soluciones de IAM & PKI

Marca SSL
#1 en Japón,
UK, #2 Brasil,

US mercado de
mayor
crecimiento

300 empleados	5000 Socios	30,000 clientes	10m de identidades emitidas

Rentable. Pronóstico de Ganancias para 2016: $67m

CAB CA/BROWSER FORUM · OTA Online Trust Alliance · NIESB · kantara INITIATIVE · OpenSSL

Servicios

GlobalSign posee un portafolio completo de soluciones en seguridad digital, incluyendo certificados para:

- Permitir la autenticación en la red de un ordenador, evitando que dispositivos no identificados puedan acceder a la red.
- Autenticación de usuarios/Clientes
- Autenticación vía SmartCard
- Protección de correos electrónicos.
- Autenticación de servidores
- Identidades de Servidores Web (internos y externos)
- Firma digital de documentos con validación internacional

Certificados SSL/TLS

- Los certificados SSL/TLS antiguamente eran usados apenas para la protección del intercambio de información a través de los sitios web, siendo instalados en su mayoría en servidores Web.

- Hoy en día con el Internet de Todas las Cosas (*IoT*) los certificados SSL/TLS son usados en diferentes aplicativos, dispositivos y máquinas, realizando una criptografía de toda la información intercambiada entre dos ó más dispositivos.

Target (Usuarios)

- Los Certificados SSL son utilizados de manera obligatoria por:
  - Bancos y Entidades Financieras
  - Websites que contienen página de Pago Online (PCI)
  - Diferentes módulos como Oracle que posee instancias que funcionan únicamente con criptografía de información
- Usuarios Potenciales
  - Websites en general (Cualquier página con envió de datos como un formulario de contacto).
  - Ambiente externo e interno de las empresas (protección de información intercambiada)
  - Fábricas de Hardware/dispositivos/aparatos que poseen un intercambio de información (recibo y/o envío)
  - Dispositivos que necesiten un identificador para autenticación.

Certificados SSL

Características de los Certificados SSL:
Tres Niveles de Validación:

- Dominio – AlphaSSL & DomainSSL (DV)
  Realiza solamente la verificación del control del dominio, de manera Automática. Presenta solamente el nombre del dominio en sus detalles.

- Organización – OrganizationSSL (OV)
  Realiza la verificación del control del dominio y de la identidad de la empresa.
  Presenta el nombre del dominio y de la organización en sus detalles.

- Validación Extendida - Extended SSL (EV)
  Realiza la verificación del control del dominio y de la identidad de la empresa
  Presenta el nombre del dominio, de la organización y sus detalles.
  Activa la barra de navegación Verde conteniendo la razón social de la organización de manera visible.

Certificados SSL (características):

- Estándar : Protege un nombre de dominio completo. GlobalSign protege de manera gratuita y opcional la versión www y no –www del dominio y UCC (mail, owa y autodiscover) Ejemplo:

  `www.dominio.com`
  `dominio.com`
  `mail.dominio.com`
  `owa.dominio.com`
  `autodiscover.dominio.com`

- Wildcard: protege una cantidad ilimitada de subdominios de primer nivel.
  Disponible en: AlphaSSL/DomainSSL/OrganizationSSL, ejemplo:
  `*.dominio.com` (donde el asterisco es una variable, cada sub-dominio extra tiene un costo)

- SANs: protege hasta 100 nombres de dominios (FQDN)/subdominios/IPs/Local hosts de manera específica. Disponible para:
  DomainSSL: Subdominios
  OrganizationSSL: Dominios/Subdomínios/Ips
  ExtendedSSL: Dominios/Subdomínios

Los SANs están disponibles en el formato estándar o Wildcard, ejemplo de SANs de Wildcard:
Nombre Común: `*.dominio.com`
SANs: `*.mail.dominio.com`
`*.ftp.dominio.com`

Certificados SSL (características)

1. Nivel de criptografía mínimo de 256 bits;
2. Algoritmo de firma SHA-256
3. Llave Pública: RSA ó ECC (2048 bits en adelante);
4. Cumple con los requerimientos de WebTrust;
5. Raíz internacional y reconocimiento mundial
6. La mayor compatibilidad del Mercado (Interoperabilidad global);
7. Compatibilidad Universal con Navegadores
8. Compatibilidad Universal con dispositivos móviles
9. Sello de Seguridad Dinámico
10. Reemisión gratuita durante el período de validez del certificado.
11. Licencia para servidores ilimitada (otras CA's le cobran por cada servidor)
12. Cumple con la normativa # 049-MICITT, art. 06, 23 de mayo del 2013, La Gaceta 98, donde establece que el 30 de junio del 2015 es la fecha límite para la transición a IPv6 en los servicios). Link 01 y 02

Certificados ePKI –SMIME/Firma/Autenticación

Funciones de los certificados PersonalSign de GlobalSign

- Seguridad de Correo electrónico

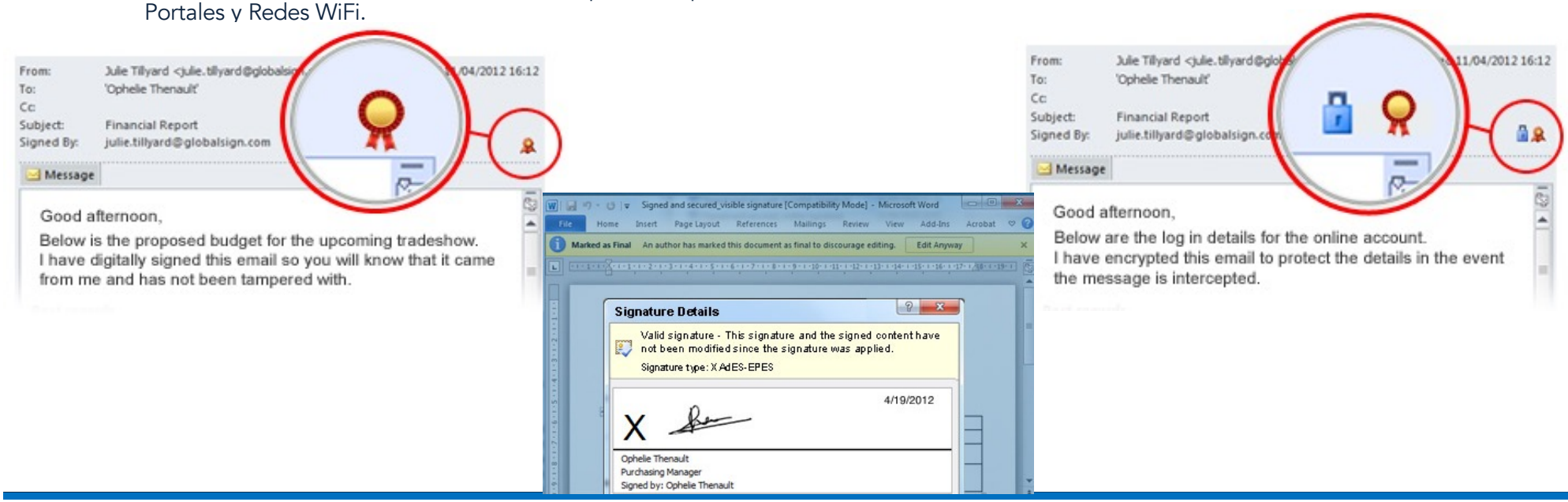
  Protege la identidad y el contenido de sus correos electrónicos contra invasiones o ataques de Phishing a sus direcciones de correo electrónico. Firma digitalmente sus correos electrónicos para garantizar su origen y cifra los mismos para aumentar la confidencialidad.

- Firme Documentos de Microsoft Office

  Agregue una firma digital a los documentos Microsoft Office como Word, Excel ó PowerPoint. La firma digital de un documento garantiza su autoría y el origen y alerta a los destinatarios en caso de que haya cualquier modificación no autorizada.

- Autenticación Online

  La solución de autenticación avanzada de GlobalSign utiliza los certificados digitales para un acceso conveniente y seguro basado en certificados y *tokens* para la autenticación de dos factores, realizando la protección de redes corporativas, datos y aplicativos, incluidos: Controladores de Dominio, Servidores, Máquinas, Dispositivos Móviles, Tarjetas Inteligentes, Tokens USB, Servicios en la Nube, VPNs, Portales y Redes WiFi.



Certificados ePKI – SMIME en detalle

Seguridad de Correo Electrónico

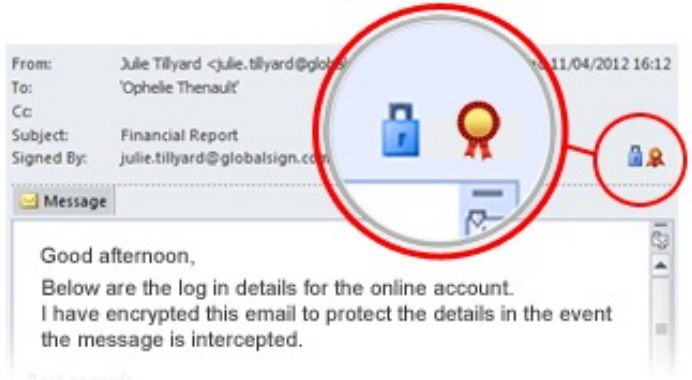
Toda empresa tiene un intercambio de millones de *e-mails* por día. Los ataques a través de *e-mails* son cada vez más frecuentes:

- Phishing: e-mails son enviados con links forjados enviándolos a una descarga de contenido malicioso o a paginas falsas.
- Email spoofing: uso de un alias como dirección de e-mail interno de la empresa de manera falsa. Por ejemplo, el hacker utiliza una dirección de e-mail de un director de un banco para solicitar informaciones. El destinatario visualiza un correo de un Director, pero es en si una copia falsa, que será direccionada a Hacker.
- Intercepción de informaciones: existe un intercambio diario de miles de informaciones confidenciales a través de e-mails, la pérdida de la información por intercepción es algo persistente y frecuente en el mercado.

¿Cómo ***S-MIME*** ayuda a la empresa a proteger sus e-mails?

Firmado los correos electrónicos el remitente pasa al destinatario la seguridad de su identidad, un e-mail pose la cinta roja, y haciendo clic en ella, el destinatario puede visualizar la información de la identidad del remitente. Evitando caer en ataques de *Phishing* o en *Spoofing* de correo electrónico.

- Al cifrar el contenido de un e-mail, el remitente o destinario(s) tienen la seguridad de que apenas ellos tienen acceso al contenido. En caso de que el mensaje sea interceptado o caiga en las manos equivocadas, el contenido estará completamente en blanco. Las informaciones estarán protegidas, así como la privacidad de las personas envueltas en el intercambio de información.



Certificados ePKI – Autenticación en detalles

Hoy en día las empresas posen diversos sistemas internos accedidos por el nombre de usuario y contraseña. Así como muchas utilizan el webmail de la misma manera. ¿Cuáles son los riesgos?

- Reutilización de la contraseña – usuarios utilizando la misma contraseña internamente que las de sus redes sociales. Una vez esta contraseña sea vulnerable, también estarán las informaciones internas de la empresa.
- Webmail- están siempre en riesgos de ataques. En 2014 por ejemplo, diversas entidades tuvieron informaciones de sus usuarios comprometidas, como Google y Yahoo, si la empresa utiliza una de sus plataformas, al sufrir un ataque, esas empresas colocan en riesgo la información de la empresa.

Utilizando el certificado para la autenticación de múltiples factores, las empresas estarán reforzando la Seguridad de sus accesos. Evitando la pérdida de información e invasiones.

Certificados ePKI – Firma de PDF

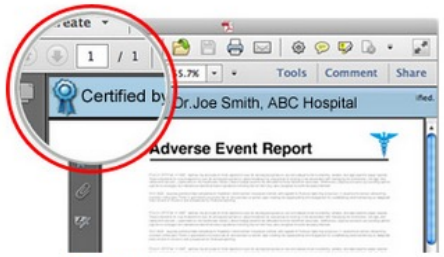
Características de la firma de PDF

- Ningún plug-in o software adicional es necesario.
- Cantidades limitadas de firmas de acuerdo con las necesidades del cliente.
- El certificado debe ser almacenado en un Token Criptográfico o HSM
- Solución escalables, opciones para desktop o servidor dedicado disponible.
- Sello de tiempo, imposibilitando la manipulación de los datos y hora.
- En conformidad con las normativas de firma digital.
- Economiza tiempo y recursos, elimina las transacciones en papel.
- Asegura la autenticidad e integridad del contenido del documento desde su firma.
- Las firmas pueden ser personalizadas con diferentes tipos de letras, tamaños e imágenes.
- Los documentos firmados son 100% aptos para pasar a través de auditorías debido a la imposibilidad de la manipulación de la información, hora y contenido.

Certificados ePKI – AATL Firma para PDF / Microsoft / Email

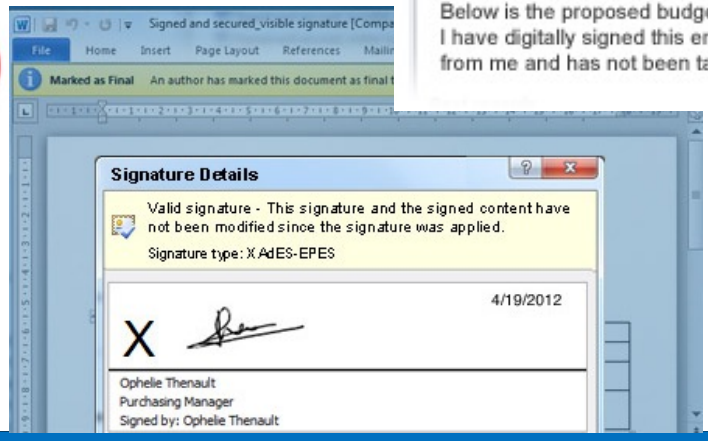
Características de Firma AATL

- Certificado pose autenticación inmediata en documentos PDF, Microsoft y firmas de Correos electrónicos.
- Cantidad ilimitada de firmas.
- Certificado debe ser almacenado en un token criptográfico o en HSM.
- No necesita de Plug-ins o software adicionales.
- Solución escalable, opciones para desktop o servidor dedicado disponible.
- No pose Sellado de Tiempo (Posibilidad de adicionar el sellado de tiempo a un costo adicional).
- En conformidad con las normativas de firma digital.
- Economiza tiempo y recursos, elimina las transacciones en papel.
- Asegura la autenticidad e integridad del contenido del documento desde su firma.
- Las firmas pueden ser personalizadas con diferentes tipos de letras, tamaños e imágenes.
- Documentos firmados pueden pasar por procesos de auditoría.
- Los documentos firmados son aptos para pasar a través de auditorías.



Certify:
Certifique: Prove a integridade dos documentos

Aprove:
Suporte para vários aprovadores



Certificados ePKI – Firma de Código Estándar

Características y ventajas

- Elimina la alerta de **"Unknown Publisher"** (Desarrollador Desconocido) en los navegadores y sistemas operativos.
- La firma no expira – servicio de Sello de Tiempo.
- Compatibilidad con todas las plataformas de desarrollo.
- Programa de Responsabilidad con garantía de $100.000.
- Asistencia Técnica Multilingüe.
- Acreditado con la Autoridad de Certificación WebTrust desde 2002.

Microsoft Authenticode Firma digitalmente controles ActiveX de Windows a través de software Authenticode (.exe, .ocx, .dll y otras extensiones de 32 y 64 bits) y Kernel para Windows. **Compatible con Windows 7.**	**Adobe AIR** Firma digitalmente aplicaciones de Adobe AIR. AIR sólo permite ejecutar aplicaciones firmadas digitalmente.
Java Firma digitalmente archivos applet JAR	**Microsoft Office y VBA** Firma digitalmente macros de Microsoft Office y Visual Basic for Applications (VBA).
Apple Firma digitalmente aplicaciones Mac de Apple. Apple introdujo la firma de código a partir del MacOS.	**Objetos de Mozilla y Netscape** Firma digitalmente archivos de objeto de Mozilla y archivos objeto heredados de Netscape.

Certificados ePKI – Firma de Código de Validación Extendida (EV)

Características y Ventajas

- Certificado debe de ser almacenado en un token criptográfico
- Elimina la alerta de "Unknown Publisher" (Desarrollador Desconocido) en los navegadores y sistemas operativos.
- Posee reputación automática inmediata en Microsoft Smartscreen
- La firma no expira – servicio de Sello de Tiempo.
- Además del Smartscreen, tiene compatibilidades con todas las plataformas de desarrollo.
- Programa de Responsabilidad con Garantía de $100.000
- Asistencia técnica multilingüe
- Acreditación de la autoridad de certificación Web Trust desde 2002.

Microsoft Authenticode Firma digitalmente controles ActiveX de Windows a través de software Authenticode (.exe, .ocx, .dll y otras extensiones de 32 y 64 bits) y Kernel para Windows. **Compatible con Windows 7.**	**Adobe AIR** Firma digitalmente aplicaciones de Adobe AIR. AIR sólo permite ejecutar aplicaciones firmadas digitalmente.
Java Firma digitalmente archivos applet JAR	**Microsoft Office y VBA** Firma digitalmente macros de Microsoft Office y Visual Basic for Applications (VBA).
Apple Firma digitalmente aplicaciones Mac de Apple. Apple introdujo la firma de código a partir del MacOS.	**Objetos de Mozilla y Netscape** Firma digitalmente archivos de objeto de Mozilla y archivos objeto heredados de Netscape.

Cuentas Gestionadas MSSL & ePKI

Los certificados previamente discutidos pueden ser emitidos y gestionadas uno por uno por el socio, o directamente a través de Cuentas Gestionadas. Las cuentas Gestionadas MSSL & ePKI son ofrecidas de manera estratégica por InterHAND. Ellas permiten que nosotros como socio de negocios Oro, le configuremos una cuenta propia para usted como cliente, en la cual se establecerá los valores y productos a los cuales el cliente tendrá acceso. El cliente tendrá control total y administrara de sus propios certificados a través de las cuentas gestionadas.

Clientes con potencial para 5+ certificados son indicados para las Cuentas Gestionada.

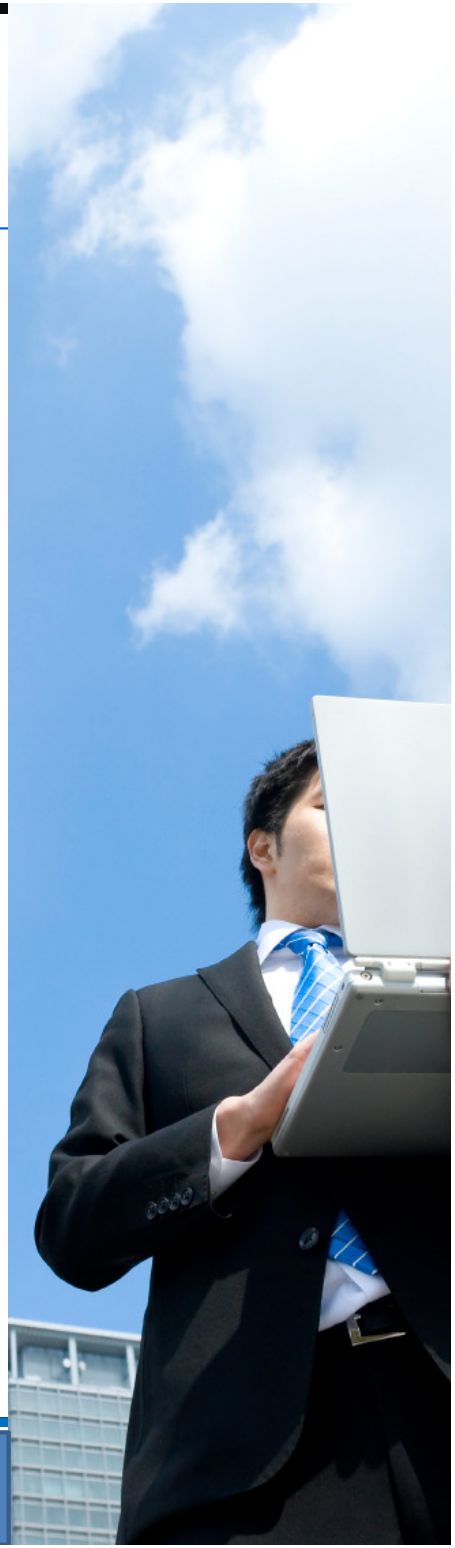
Certificados Disponibles :

- OrganizationSSL / ExtendedSSL
- SMIME/Autenticacion/Firma Digital (PersonalSign/CDS/AATL)
- Firma de Código

Características de las Cuenta Gestionada :

- Plataforma basada en la web.
- Una cuenta única puede centralizar todos los tipos de certificados en diferentes secciones.
- Controle el clico de vida completo del Certificado
- Registro de Usuarios
- Controle los privilegios de los usuarios
- Funciones completas de informes, facturas y contabilidad.
- SSL G Pro – Soporte para múltiples perfiles en una misma cuenta
- Eficiencia en la emisión (24x7 inmediato)
- Economía (mayores descuentos por volumen)
- APIs de integración
- Página de solicitud pública
- Automatización en la solicitud de identidades digitales.

Ejemplo de Clientes



Ing. Víctor Alvarado / IT Security
InterHAND S. A.

Phone: +506 2441-2411 / 8398-8445
E-mail: info@ssl.cr

www.SSL.cr