STN
SERTECNET VALENCIA

EMPRESA CONSULTORA DE SERVICIOS DE COMUNICACIONES Y REDES

Servicios de criptografía en la empresa

NOTAS ACERCA DE STN

Nuestra clave primaria se encuentra en PGP.REDIRIS.ES.

Se puede acceder a esta clave consultándola como contacte@sertecnet.com

```
--search-key
contacte@sertecnet.com
```

Su identificador es **538A41F0**

Para comprobar su validez, la huella digital es:

```
BEBE 4DBD 5738 3B14 3199  615A
     9DCA DD9C 538A 41F0
```

Si no confía en las características de la firma, debe contactar directamente con nuestras instalaciones y **ponerse en contacto con el responsable de sistemas**, de esta forma le aseguraremos la validez de los resultados que está obteniendo.

En caso de que desee obtener certificados digitales de alguien de esta institución antes tiene que dar un nivel alto de confianza a la clave antes mencionada e importarla directamente del servidor de REDIRIS.

Para obtener una validez plena de la clave STN tiene que haberle enviado por correo corriente tanto la validez de la huella que STN reconoce como la firma de los responsables de seguridad y de gerencia de la institución.

La firma caducará en un año.

Se pondrá a disposición nuevas firmas certificadas por este certificado primario.

Desconfíe de la recepción con el distintivo @sertecnet.com que no esté firmado. En caso de recibir un mensaje sospechoso desde esta dirección comuníquelo.

El uso primario que STN desea dar a las claves es el de firma por parte de nuestro personal, y permitir el envío cifrado de claves de acceso a sistemas únicamente al personal seleccionado.

Email: contacte@sertecnet.com

Tel.: 963160089

Fax: 963633064

Servicios de firma criptografía: Uso empresarial

Un sistema criptográfico es un medio capaz de transformar la información de forma que al ser interceptada únicamente el receptor reconozca el mensaje original.

Desde el punto de vista de la empresa, un sistema de este tipo permite mantener conversaciones seguras a través de medios inseguros y proteger la información de miradas indiscretas. Dentro de los usos de la criptografía están las llamadas **firmas digitales**. Una firma digital es un mecanismo que está destinado a verificar el origen del mensaje.

Firmas digitales y criptografías son mecanismos complementarios. La firma digital se basa en algoritmos criptográficos, la criptografía no se preocupa directamente de quien es el emisor si no de verificar que en el proceso transmisión/almacén no es interceptada.

Firma digital

La firma digital trata de obtener mediante medios criptográficos la identidad del emisor del mensaje. Dentro de la empresa un sistema de este tipo permite:

- **Validar la integridad de los datos**:

  Cualquier cambio la mensaje tendría como resultado que el destinatario registraría como inválida la firma con el documento.

- **Autenticación**:

  El destinatario puede asegurar que el mensaje ha sido enviado por quien alega haberlo enviado, ya que únicamente quien lo envió tiene la llave secreta.

- **Ausencia de rechazo**:

  Quien alega que envió el mensaje no puede después negar que generó y envió el mensaje.

- **Protección de reenvío**:

  Si integramos en el mensaje una secuencia o marta de tiempo para hacerlo único, estos datos pueden ser posteriormente verificados por el destinatario para asegurar que el mensaje no fue interceptado y reenviado. Esto puede ser importante si el mensaje fuera una instrucción de pago.

Esto permite estar reconocido como medio de trasmisión de facturas via internet, y su almacenamiento digital.

Uno de los puntos que trataremos es la autenticación. En efecto, uno de los grandes retos que aporta internet, es que el correo electrónico no fue diseñado para obtener de forma unívoca el remitente del mensaje.

Esta característica permite a empresas de **SPAM** y a software malicioso (virus, gusanos, ...) realizar operaciones de ***spoofing*** suplantación de identidad. Esto es reenviarse como un usuario que no es (generalmente utilizando información del equipo en compromiso) para ocultar la procedencia y permitir la propagación del software a terceros.

Aproximaciones al problema de la autenticación

En la actualidad existen dos medios ampliamente difundidos para conocer la identidad del emisor y permitir el empleo de la criptografía.

Hay que recordar que la firma digital identifica de forma plena al emisor, dentro del marco legal Español, esto permitiría emplear estos medios para validar cualquier tipo de documento electrónico. En realidad si los procesos se llevan adecuadamente y de forma rigurosa estos medios electrónicos son más eficientes en cuanto a identificación que cualquier otro.

Sistema de validación PKCS

En este sistema se emplea criptografía asimétrica y una ***entidad certificadora*** externa que hace las veces de notario. Esto es, un usuario genera un certificado digital posteriormente este certificado se emplea con un fin concreto, correo, WEB,... la entidad certificadora reconoce este certificado, y se encarga de reconocer por otros medios al usuario.

Usando estas técnicas están los protocolos SSL, o los sistemas de pago SET. Estos sistemas permiten validar tanto un servidor WEB como un usuario que accede a un sistema de forma efectiva. Por lo general son los medios que se acepta como más seguros para realizar cualquier tipo de transacción o comercio electrónico.

La ventaja es que la entidad certificadora es universal, lo que hace que sea idóneo para implantar medios de pagos con bancos, o acceso a información de Hacienda.Se mantiene el inconveniente de que desplegar este tipo de certificados a una empresa requiere contar con

Consideraciones de uso

una entidad que valide a todos los usuarios y servicios. Esto introduce un enorme coste.

Sistemas de validación por PGP

El sistema PGP o en su versión libre GPG, es otro sistema de criptografía asimétrica con conceptos similares a los que intervienen al PKCS.

Distingue un uso más personal, permitiendo mantener relaciones confidenciales o sistemas de firmas en entornos donde desplegar PKCS es caro o no está justificado.

Toda la infraestructura necesaria para generar dicha confianza en la indentidad es lo que comprende el sistema PGP.

La ventaja que tiene este sistema es el bajo coste de implantación, además de poder ofrecer una estructura común al cliente para que pueda obtener información acerca de los auténticos emisores de la información.

Consideraciones acerca de criptografía

Si bien trasmitir la información encriptada por la red nos protege de ataques e intrusiones externas, tenemos que plantearnos la utilidad de **almacenar información criptografiada** como forma de trabajo habitual.

Así si pensamos en la necesidad de almacenamiento tenemos que valorar su necesidad y riesgo en el uso empresarial y restringirlo a aquellos aspectos donde sean realmente requeridos.

Implantar el almacenamiento requiere pensar en:

- **Plan de continuidad**:

  En efecto, la criptografía hoy día tiene unas capacidades de resistencia a recuperación de información fuera del alcance de los medios informáticos de la mayoría de las empresas.

  Únicamente los Estados disponen de herramientas capaces de romper dichas barreras.

  El empleo de la criptografía nos impediría por ejemplo continuar el trabajo de un empleado que falleciera, o en caso de pérdida de las claves, perder toda la información que protegían dichas claves.

  La criptografía empleada en empresas tiene siempre que permitir la recuperación de los datos por medios ajenos a los empleados. Cualquier sistema no diseñado en esta línea pone en peligro trazar un plan de continuidad.

- **Accesibilidad de la información**:

  En efecto un gestor de correo que no permita realizar búsquedas en los documentos que se tienen producen ineficiencias.

  Si se emplea para almacenear información sensibles como números de cuentas en este caso su uso está más que justificado.

  La criptografía no tiene que impedir el normal funcionamiento de la empresa, en otro caso se fracasará en la implantación.

- **Costes de implantación**:

  La criptografía se basa en los mismos sistemas que tenemos las personas para reconocernos. Sin embargo requiere de un entendimiento a la hora de realizar su uso.

  Tenemos que plantearnos que en una empresa únicamente dos o tres personas van a alcanzar a disponer del conocimiento para evaluar todos los riesgos que supone estas técnicas.

  Creer que la criptografía resuelve todos los problemas de seguridad es un error, por tanto mantener una política de mínimos en su uso puede ser un gran avance.

  Pondremos en marcha únicamente aquellos elementos de los que estemos seguros que nuestro personal puede responder.

Además la criptografía puede ser recomendable para evitar accesos indeseados empleando aplicaciones como visores de documentos. Estas aplicaciones tienen que estar diseñadas teniendo en cuenta los criterios mencionados, y nos acercan a cumplir la legislación vigente (LOPD, LSSI,...).

Firma digital?

La firma digital es como se ha mencionado un mecanismo de autenticación de usuarios.

Evitar la suplantación del correo dentro de una institución permite regular su uso y evitar el fraude.

Acostumbrar a terceros acerca de que formatos digitales adquieren los documentos enviados por una empresa permite asimismo reducir el riesgo a que nos someten sistemas de spoofing etcétera.

Disponer durante la implantación de un mecanismo que nos permita dar a conocer a nuestros clientes y proveedores de que estamos sensibilizados con el problema que tiene no disponer de estos recursos es también un buen medio de trasmitir buenas prácticas de trabajo.

Conseguir el objetivo es la mejor forma de hacer que estas buenas prácticas sean evidentes.

Otros usos de la firma digital es el de permitir enviar de forma automática ficheros y validarlos en el sitio remoto.

De esta forma se facilitan los procesos de envío y se evitan errores informáticos o alteraciones debidas a problemas con la línea o de no finalización de la transmisión.

Cualquier sistema que permita la transmisión automática de información así como detectar la alteración maliciosa o no de los datos, ha de contar con un protocolo de firma digital que impida el error.

Recomendaciones

Si cree que su empresa requiere una implantación de criptografía para resolver problemas de seguridad y confidencialidad con sus clientes, así como mantener un grado mayor de satisfacción en su entorno, no dude en consultarnos.

STN pondrá a su disposición los mejores medios para implantar un sistema de criptografía en los siguientes entornos:

- WINDOWS
- UNIX
- MAC

Asimismo podemos ofertarle formación que cubra el alcance que desee ofrecer a sus clientes.

Si dispone de personal informático, una auditoría previa le permitirá conocer el grado de eficacia y de implantación que dispone su empresa.

Tenga en cuenta que a pesar de que los conceptos que abarca la criptografía no están al alcance de personal no formado, STN tiene experiencia en la formación adecuada atendiendo a los niveles de cada persona.

Por último si desea incorporar estas soluciones a sistemas cerrados ya existentes (Aplicaciones a medida, Outlook,...) disponemos de herramientas para facilitar y llevar a cabo una implantación con éxito.

Referencias

PKCS y SSL: www.openssl.org

Protección de Datos: www.agpd.es

GNUPG/GPG: www.gpg.org