Xarxa Punt TIC

MÓDULO 2 NIVEL AVANZADO
Las fuentes de información institucional
Unidad didáctica 5: La seguridad en las operaciones telemáticas

BY NC ND

plan avanza2
GOBIERNO DE ESPAÑA
Plan E
MINISTERIO DE INDUSTRIA, TURISMO Y COMERCIO
SECRETARÍA DE ESTADO DE TELECOMUNICACIONES Y PARA LA SOCIEDAD DE LA INFORMACIÓN
Generalitat de Catalunya

E. La seguridad en las operaciones telemáticas

La firma digital

La firma electrónica es un sistema electrónico de acreditación que permite verificar la identidad de las personas con el mismo valor que la firma tradicional manuscrita, autentificando las comunicaciones generadas por la persona que ha firmado y que se aplicará sobre documentos electrónicos.

La firma electrónica se genera con una clave privada de la persona que firma el documento. El receptor de este documento podrá, a la vez, garantizar la identidad del emisor, comprobando la firma electrónica con la clave pública de la persona que firma que, esta sí, es de dominio público.

Hay dos tipos de firma electrónica:

Firma electrónica simple (FES)

La firma electrónica simple es aquella firma que no cumple los requisitos para ser una firma electrónica avanzada.

Firma electrónica avanzada (FEA)

La firma electrónica avanzada está certificada mediante un emisor acreditado y ha sido creada utilizando los medios pertinentes para garantizar que la firma vincula únicamente al usuario con los datos que se facilitan. Permite la detección posterior de cualquier modificación y verifica en todo momento la identidad del titular.

La firma electrónica en tres pasos:

1. Generación del documento firmado: la persona emite un documento y, una vez finalizado, lo firma con su certificado digital con clave privada.
2. Envío del documento de forma telemática.
3. Recepción del documento y comprobación: la persona que recibe el documento, para certificar su autenticidad, debe acceder a la clave pública del emisor y comprobar sus datos.

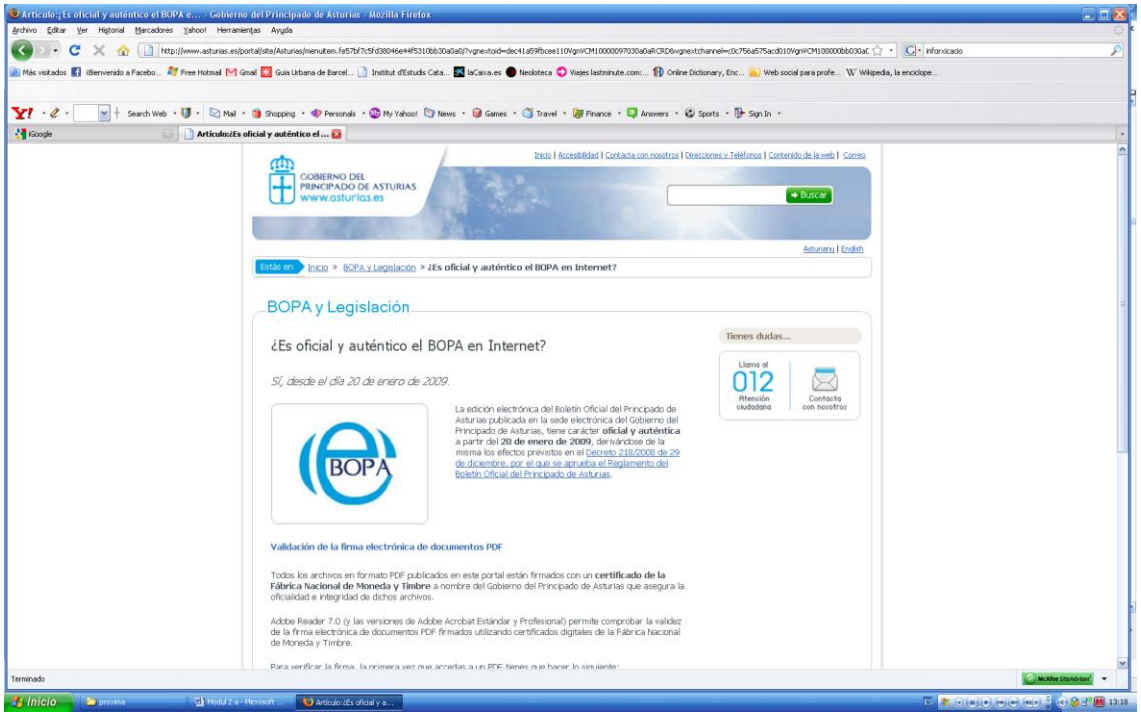

Imagen 1. Página del BOPA donde se habla de la firma electrónica.

La criptografía

Es la ciencia que estudia los métodos y procedimientos para modificar los datos con el objetivo de conseguir las características de seguridad. Las principales características que quiere obtener un sistema de seguridad son:

- Confidencialidad: consiste en garantizar que sólo las personas autorizadas tienen acceso a la información.
- Integridad: consiste en garantizar que el documento original no ha sido modificado. El documento puede ser tanto público como confidencial.
- Autenticación: permite garantizar la identidad del autor de la información.

Existen varios algoritmos matemáticos que intentan cubrir una o varias de estas características básicas de seguridad. El nivel de cumplimiento de sus objetivos es difícil de evaluar, puesto que varios algoritmos pueden ser vulnerables ante técnicas de ataque diferentes. Además, la mayoría de los algoritmos pueden trabajar con claves de diferente longitud, lo cual afecta directamente a la

robustez. Por otra parte, existen otras características aparte de la robustez del algoritmo, que también influyen en el proceso de selección del algoritmo más apropiado para una determinada aplicación. Algunas de estas características son: el tiempo de cálculo del proceso de cifrado, la relación de la medida entre el documento original y el documento cifrado, etc.

Existen infinidad de algoritmos criptográficos que, partiendo de un documento original, obtienen otro documento o conjunto de información. Los algoritmos más conocidos son los que obtienen un documento a partir de un documento original al aplicar un algoritmo que utiliza una llave secreta como argumento.

En líneas generales, los algoritmos criptográficos se pueden clasificar en tres grandes familias:

Criptografía de clave secreta o criptografía simétrica

Se incluyen en esta familia el conjunto de algoritmos diseñados para cifrar un mensaje utilizando una única clave conocida por los dos interlocutores, de forma que el documento cifrado solamente pueda descifrarse si se conoce la mencionada clave secreta. Algunas de las características más destacadas de este tipo de algoritmos son las siguientes:

- A partir del mensaje cifrado no se puede obtener el mensaje original ni la clave que se ha utilizado, aunque se conozcan todos los detalles del algoritmo criptográfico utilizado.
- Se utiliza la misma clave para cifrar el mensaje original que para descifrar el mensaje codificado.
- Emisor y receptor tienen que haber acordado una clave común mediante un canal de comunicación confidencial antes de poder intercambiar información confidencial por un canal de comunicación inseguro. A partir de un documento original se obtiene un documento cifrado al aplicar una llave secreta; esta misma llave secreta se utiliza posteriormente para volver a obtener el documento original.

Los algoritmos simétricos más conocidos son: DES, 3DES, RC2, RC4, RC5, IDEA, Blowfish y AES.

Criptografía de clave pública o criptografía asimétrica

Esta categoría incluye un conjunto de algoritmos criptográficos que utilizan dos claves diferentes para cifrar y descifrar el mensaje. Ambas claves tienen una relación matemática entre ellas, pero la seguridad de esta técnica se basa en que el conocimiento de una de las claves no permite descubrir cuál es la otra clave. En realidad haría falta conocer todos los números primos grandes para ser capaz de deducir una clave a partir de la otra, pero se ha demostrado que en la práctica se tardaría demasiados años solamente en el proceso de obtención de los números primos grandes.

Cada usuario cuenta con una pareja de claves, una la mantiene en secreto y se denomina clave privada y la otra la distribuye libremente y se denomina clave pública. Para enviar un mensaje confidencial sólo hace falta conocer la clave pública del destinatario y cifrar el mensaje utilizando esta clave. En este caso, los algoritmos asimétricos garantizan que el mensaje original sólo puede recuperarse utilizando la clave privada del destinatario. Como la clave privada se mantiene en secreto, sólo el destinatario podrá descifrar el mensaje.

Estos algoritmos pueden trabajar indistintamente en cualquiera de las claves, de forma que un mensaje cifrado con la clave pública solamente puede descifrarse con la clave privada, pero cualquier mensaje cifrado con la clave privada solamente puede ser descifrado con la clave pública. Esta característica permite utilizar este método para otras aplicaciones, además de las que sólo requieren confidencialidad, como es el caso de la firma electrónica.

Algunas de las características más destacadas de este tipo de algoritmos son las siguientes:

- Se utilizan una pareja de claves denominadas clave pública y clave privada, pero a partir de la clave pública no es posible descubrir la clave privada.
- A partir del mensaje cifrado no se puede obtener el mensaje original, aunque se conozcan todos los detalles del algoritmo criptográfico utilizado y aunque se conozca la clave pública utilizada para cifrarlo.
- Emisor y receptor no requieren establecer ninguna atención sobre la clave a emplear. El emisor se limita a obtener una copia de la clave pública del receptor, lo cual se puede realizar, en principio, por cualquier medio de comunicación aunque sea inseguro.

Algoritmos HASH o de resumen

Los algoritmos HASH parten de una información de entrada de longitud indeterminada y obtienen como salida un código, que en cierta medida se puede considerar único para cada entrada. La función de estos algoritmos es determinista, es decir, que partiendo de una misma entrada siempre se obtiene la misma salida. Aun así, el interés de estos algoritmos reside en que partiendo de entradas diferentes se obtienen salidas diferentes. Unos ejemplos muy sencillos, aunque muy vulnerables, son los dígitos de control y los CRC (*Cyclic Redundancy Code*), que se utilizan para detectar errores de transcripción o de comunicación.

Instituciones que otorgan firmas electrónicas

Agència Catalana de Certificació

Ceres

Las transferencias seguras

Los protocolos de transferencia segura: HTTPS/SSL

Hypertext Transfer Protocol Secure (en castellano: Protocolo seguro de transferencia de hipertexto), más conocido por sus siglas **HTTPS**, es un protocolo de Red basado en el protocolo HTTP, destinado a la transferencia segura de datos de hipertexto, es decir, es la versión segura del HTTP.

El sistema HTTPS utiliza un cifrado basado en las *Secure Socket Layers* (SSL) para crear un canal cifrado más apropiado para el tráfico de información sensible que el protocolo HTTP. De esta manera, se consigue que la información sensible (usuario y contraseñas, normalmente) no pueda ser empleada por un atacante que haya conseguido interceptar la transferencia de datos de la conexión, puesto que la única cosa que obtendrá será un flujo de datos cifrados que no podrá descifrar

Las pasarelas de pago seguro

Es un sistema proporcionado por una entidad financiera a una tienda virtual para gestionarle los cobros en línea con tarjetas de crédito.