Xarxa Punt TIC

MÒDUL 2 NIVELL AVANÇAT
Les fonts d'informació institucional
Unitat didàctica 5: La seguretat en les operacions telemàtiques

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

F. La seguretat en les operacions telemàtiques

La signatura digital

La signatura electrònica és un sistema electrònic d'acreditació que permet verificar la identitat de les persones amb el mateix valor que la firma tradicional manuscrita, autentificant les comunicacions generades per la persona que l'ha signat i que s'aplicarà sobre documents electrònics.

La signatura electrònica es genera amb una clau privada de la persona que signa el document. El receptor d'aquest document podrà, alhora, garantir la identitat de l'emissor, comprovant la signatura electrònica amb la clau pública de la persona que signa que, aquesta si, és de domini públic.

Hi ha dues classes de signatura electrònica:

Signatura electrònica simple (FES)

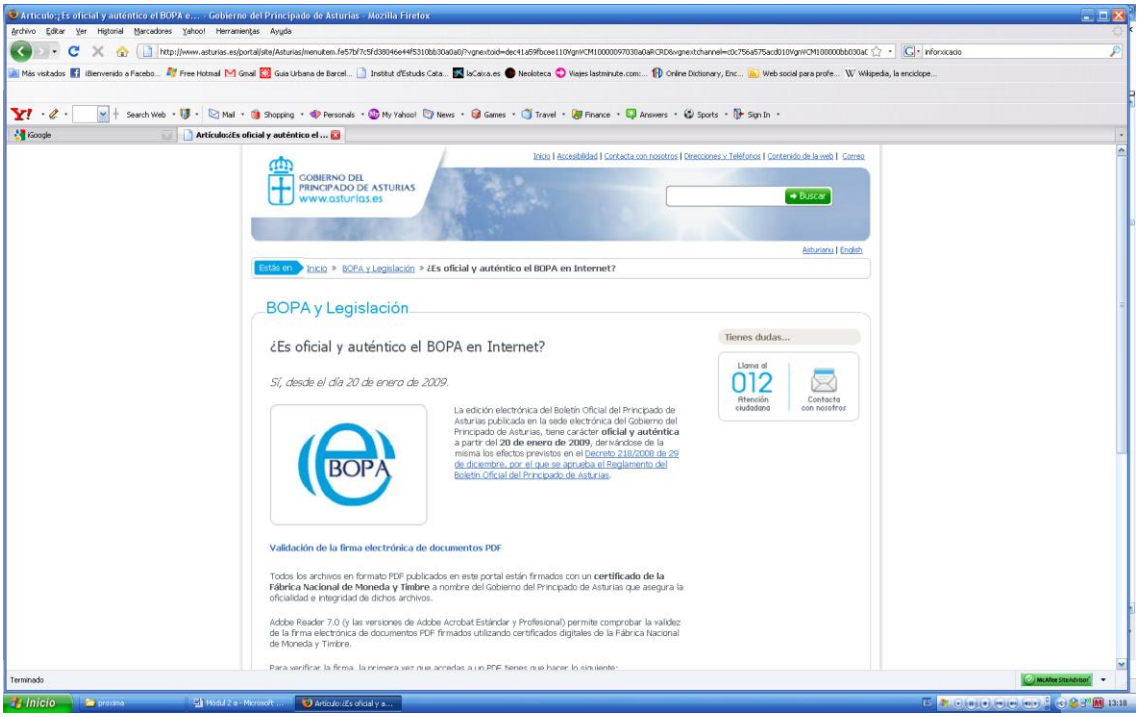
La signatura electrònica simple és aquella signatura que no compleix els requisits per ser una signatura electrònica avançada.

Signatura electrònica avançada (FEA)

La signatura electrònica avançada està certificada por un emissor acreditat i ha estat creada utilitzant els mitjans pertinents per a garantir que la signatura vincula únicament l'usuari amb les dades que es faciliten. Permet la detecció posterior de qualsevol modificació i verifica en tot moment la identitat del titular.

La signatura electrònica en tres passos:

1. Generació del document signat: la persona emet un document i, una vegada finalitzat, el signa amb els seu certificat digital amb clau privada.
2. Enviament del document de forma telemàtica.
3. Recepció del document i comprovació: la persona que rep el document, per tal de certificar la seva autenticitat, ha d'accedir a la clau pública de l'emissor i comprovar les seves dades.



Imatge 1. Pàgina del BOPA on es parla de la signatura electrònica.

La criptografia

És la ciència que estudia els mètodes i procediments per modificar les dades amb l'objectiu d'aconseguir las característiques de seguretat. Les principals característiques que vol obtenir un sistema de seguretat són:

- ➔ Confidencialitat: consisteix en garantir que només les persones autoritzades tenen accés a la informació.
- ➔ Integritat: consisteix en garantir que el document original no ha estat modificat. El document pot ser tant públic com confidencial.
- ➔ Autenticació: permet garantir la identitat de l'autor de la informació.

Existeixen diversos algoritmes matemàtics que intenten cobrir una o vàries d'aquestes característiques bàsiques de seguretat. El nivell de compliment dels seus objectius és difícil d'avaluar, ja que diversos algoritmes poden ser vulnerables davant tècniques d'atac diferents. A més, la majoria dels algoritmes poden treballar amb claus de diferent longitud, la qual cosa afecta directament la robustesa. Per altra banda, existeixen altres característiques a part de la robustesa de l'algoritme, les quals també influeixen en el procés de selecció de

l'algoritme més apropiat per a una determinada aplicació. Algunes d'aquestes característiques són: el temps de càlcul del procés de xifrat, la relació de la mida entre el document original i el document xifrat, etc.

Existeixen infinitat d'algoritmes criptogràfics que, partint d'un document original, obtenen un altre document o conjunt d'informació. Els algoritmes més coneguts són els que obtenen un document a partir d'un document original en aplicar un algoritme que utilitza una clau secreta com a argument.

En línies general, els algoritmes criptogràfics es poden classificar en tres grans famílies:

➔ Criptografia de clau secreta o criptografia simètrica

S'inclouen en aquesta família el conjunt d'algoritmes dissenyats per xifrar un missatge utilitzant una única clau coneguda pels dos interlocutors, de manera que el document xifrat solament pugui desxifrar-se si es coneix l'esmentada clau secreta. Algunes de les característiques més destacades d'aquest tipus d'algoritmes són les següents :

- A partir del missatge xifrat no es pot obtenir el missatge original ni la clau que s'ha utilitzat, encara que es coneguin tots els detalls de l'algoritme criptogràfic utilitzat.
- S'utilitza la mateixa clau per xifrar el missatge original que per desxifrar el missatge codificat.
- Emissor i receptor han d'haver acordat una clau comú mitjançant un canal de comunicació confidencial abans de poder intercanviar informació confidencial per un canal de comunicació insegur. A partir d'un document original s'obté un document xifrat en aplicar una clau secreta; aquesta mateixa clau secreta s'utilitza posteriorment per tornar a obtenir el document original.
- Els algoritmes simètrics més coneguts son: DES, 3DES, RC2, RC4, RC5, IDEA, Blowfish i AES.

➔ Criptografia de clau pública o criptografia asimètrica

Aquesta categoria inclou un conjunt d'algoritmes criptogràfics que utilitzen dues claus diferents per xifrar i desxifrar el missatge. Ambdues claus tenen una relació matemàtica entre elles, però la seguretat d'aquesta tècnica es basa en que el coneixement d'una de les claus no permet descobrir quina és l'altra clau. En realitat caldria conèixer tots els nombres primers grans per ser capaç de deduir una clau a partir de l'altre, però s'ha demostrat que en la pràctica es tardaria massa anys solament en el procés d'obtenció dels nombres primers grans.

Cada usuari compta amb una parella de claus, una la manté en secret i s'anomena clau privada i l'altra la distribueix lliurement i s'anomena clau pública. Per enviar un missatge confidencial només cal conèixer la clau pública del destinatari i xifrar el missatge utilitzant aquesta clau. En aquest cas, els algoritmes asimètrics garanteixen que el missatge original només pot recuperar-se utilitzant la clau privada del destinatari. Com que la clau privada es manté en secret, només el destinatari podrà desxifrar el missatge.

Aquests algoritmes poden treballar indistintament en qualsevol de les claus, de manera que un missatge xifrat amb la clau pública solament pot desxifrar-se amb la clau privada, però qualsevol missatge xifrat amb la clau privada solament pot ser desxifrat amb la clau pública. Aquesta característica permet utilitzar aquest mètode per a altres aplicacions, a més de les que només requereixen confidencialitat, com és el cas de la signatura electrònica.

Algunes de las característiques més destacades d'aquest tipus d'algoritmes son les següents:

- S'utilitzen una parella de claus anomenades clau pública i clau privada, però a partir de la clau pública no és possible descobrir la clau privada.
- A partir del missatge xifrat no es pot obtenir el missatge original, encara que es coneguin tots els detalls de l'algoritme criptogràfic utilitzat i encara que es conegui la clau pública utilitzada per xifrar-lo.
- Emissor i receptor no requereixen establir cap esguard sobre la clau a emprar. L' emissor es limita a obtenir una còpia de la clau pública del receptor, la qual cosa es pot realitzar, en principi, per qualsevol mitjà de comunicació encara que sigui insegur.

➔ Algoritmes HASH o de resum

Els algoritmes HASH parteixen d'una informació d'entrada de longitud indeterminada i obtenen com a sortida un codi, que en certa mesura es pot considerar únic per a cada entrada. La funció d'aquests algoritmes és determinista, és a dir, que partint d'una mateixa entrada sempre s'obté la mateixa sortida. Tanmateix, l'interès d'aquests algoritmes resideix en que partint d'entrades diferents s'obtenen sortides diferents. Uns exemples molt senzills, encara que molt vulnerables, són els dígits de control i els CRC (Cyclic Redundancy Code), que s'utilitzen per detectar errades de transcripció o de comunicació.

Institucions que atorguen signatures electròniques

Agència Catalana de Certificació

Ceres

Les transferències segures

Els protocols de transferència segura: HTTPS/SSL

Hypertext Transfer Protocol Secure (en català: *Protocol segur de transferència d'hipertext*), més conegut per les seves sigles **HTTPS**, es un protocol de xarxa basat en el protocol HTTP, destinat a la transferència segura de dades d'hipertext, és a dir, és la versió segura de l'HTTP.

El sistema HTTPS utilitza un xifrat basat en les *Secure Socket Layers* (SSL) per tal de crear un canal xifrat més apropiat per al tràfic d'informació sensible que el protocol HTTP. D'aquesta manera, s'aconsegueix que la informació sensible (usuari i contrasenyes, normalment) no pugui ser emprada per un atacant que hagi aconseguit interceptar la transferència de dades de la connexió, ja que l'única cosa que obtindrà serà un flux de dades xifrades que no podrà desxifrar.

Las passarel·les de pagament segur

És un sistema proporcionat per una entitat financera a una botiga virtual per gestionar-li els cobraments en línia amb targetes de crèdit.