2.9.SIGNATURA DIGITAL. CERTIFICAT DIGITAL DE L´EMPRESA.

SIGNATURA DIGITAL.

La **signatura digital** és un mecanisme de xifrat per autentificar informació digital. El mecanisme utilitzat és la criptografia de clau pública per això aquest tipus de signatura també rep el nom de signatura digital de clau pública.

> S'utilitza també el terme signatura electrònica com a sinònim de signatura digital, tot i que la signatura electrònica inclouria també altres mecanismes per identificar l'autor d'un missatge electrònic que no són purament criptogràfics.

Usos

Hi ha tres motius per utilitzar signatures digitals en les comunicacions:

- **Autenticitat**: Un sistema criptogràfic de clau pública permet a qualsevol enviar missatges utilitzant una clau pública. La signatura permet al receptor d'un missatge estar segur que el remitent és qui diu ser. Tot i així, el receptor no pot estar completament segur que el remitent és qui diu ser ja que el sistema criptogràfic es pot haver trencat.
- **Integritat**: Emissor i receptor voldran estar segurs que el missatge no s'ha alterat durant la transmissió.
- **No repudiació**: En un context criptogràfic, la paraula *repudiació* fa referència a l'acció de negar la relació amb un missatge (per exemple dient que ha estat enviat per un tercer). El receptor d'un missatge pot insistir que l'emissor adjunti una signatura per prevenir que més endavant l'emissor pugui repudiar el missatge, així, el receptor pot mostrar el missatge a un tercer i provar el seu origen.

Implementació

La signatura digital es basa en criptografia de clau pública. En aquest tipus de criptografia cada usuari té un parell de claus: una pública i una privada. La clau pública és distribueix lliurement, però la clau privada és secreta i no és deduïble a partir de la clau pública. Normalment un mecanisme de signatura digital defineix tres algorismes: un per generar la clau, un per signar i l'altre per verificar la signatura.

Quan un usuari A vol enviar un missatge a un usuari B i vol que l'usuari B estigui segur que el missatge prové d'ell se segueixen els següents passos: L'usuari A envia el seu missatge a l'usuari B i adjunta una signatura digital. Aquesta signatura es genera usant la clau privada de l'usuari A i pren la forma d'un valor numèric. En rebre el missatge, l'usuari B pot confirmar la procedència del missatge utilitzant la clau pública de l'usuari B, la signatura i el missatge. Si la verificació és correcta l'usuari B pot estar segur que el missatge procedeix de l'usuari A ja que l'algorisme de signat està dissenyat per a que sigui molt difícil crear una signatura que encaixi amb un missatge concret(sinó es coneix la clau privada).

Normalment, per raons d'eficiència, s'utilitza una funció de hash criptogràfica amb el missatge abans de signar-lo. D'aquesta manera s'aconsegueix una signatura més curta i s'estalvia temps ja que generar un hash és molt més ràpid que signar digitalment.

CRIPTOGRAFIA.

La **criptografia** (o **criptologia**, del grec κρυπτός, *kryptos*, "amagat, secret"; i γράφειν, *gráphin*, "escriptura", o -λογία, *-logia*, , "estudi", respectivament)[1] és, tradicionalment, l'estudi de formes de convertir informació des de la seva forma original cap a un codi incomprensible, de forma que sigui incomprensible pels que no coneguin aquesta tècnica. La criptografia moderna utilitza les disciplines de les matemàtiques, informàtica i electrotècnia. Algunes aplicacions de la criptografia inclouen caixers automàtics, contrasenyes i comerç electrònic.

La **criptologia** és l'estudi dels criptosistemes: sistemes que ofereixen mitjans segurs de comunicació amb els que l'emissor oculta o xifra el missatge abans de transmitir-ho perquè només un receptor autoritzat (o ningú) pugui desxifrar-ho. Les seves àrees principals d'interès són la **criptografia** i la criptoanàlisi, però també inclou l'esteganografia com part d'aquesta ciència aplicada. En temps recents, l'interès per la criptologia s'ha estès també a altres aplicacions, per part de la comunicació segura de informació i, actualment, una de les aplicacions més esteses de les tècniques i mètodes estudiats per la criptologia és l'autenticitat de la informació digital (també anomenada signatura digital).

Terminologia

De la informació original en diem el text pla (encara que no necessàriament treballem amb textos). Llavors passa per un procés de xifrat que fent servir algorismes converteix la informació original en un codi il·legible per tothom que no tingui els mitjans per desxifrar (un altre algorisme), i la clau.

Actualment els algorismes, o tècniques criptogràfiques, consisteixen en programes d'ordinador que aprofiten propietats numèriques que fan que sense la clau sigui molt difícil d'obtenir la informació.

Per exemple estem fent servir la criptografia quan ens connectem al nostre banc a través d'Internet, de manera que encara que algú intercepti la informació que intercanviem amb aquest, no podrà descodificar la informació interceptada.

ALGORISME.

Un **algorisme** o **algoritme**[1] és un conjunt finit d'instruccions o passos que serveixen per a executar una tasca o resoldre un problema. En la vida quotidiana s'empren algorismes en multitud d'ocasions per resoldre diversos problemes com per exemple per posar una rentadora (conjunt d'instruccions enganxades a la tapa de la màquina), per tocar música (partitures), per construir un aeroplà a escala (expressats en les instruccions), per fer trucs de màgia (passos per a fer el truc) o, fins i tot, per a fer receptes de cuina (passos de la recepta).

CERTIFICAT DIGITAL.

Un **Certificat Digital** és un document digital mitjançant el qual un tercer confiable (una autoritat de certificació) garanteix la vinculació entre la identitat d'un subjecte o entitat i la seva clau pública.

> Si bé existeixen variats formats per a **certificats digitals**, els més comunament emprats es regeixen per l'estàndard UIT-T X.509. El **certificat** conté usualment el nom de l'entitat certificada, un nombre serial, data d'expiració, una còpia de la clau pública del titular del certificat (utilitzada per a la verificació de la seva signatura digital), i la signatura digital de l'autoritat emissora del certificat de manera que el receptor pugui verificar que aquesta última ha establert realment l'associació.

Format de certificat digital

Un certificat emès per una entitat de certificació autoritzada, a més d'estar signat digitalment per aquesta, ha de contenir almenys el següent:

- Nom, adreça i domicili del subscriptor.
- Identificació del subscriptor nomenat en el certificat.
- El nom, l'adreça i el lloc on realitza activitats l'entitat de certificació.
- La clau pública de l'usuari.
- La metodologia per a verificar la signatura digital del subscriptor imposada en el missatge de dades.
- El nombre de sèrie del certificat.
- Data d'emissió i expiració del certificat.

Emissors de certificats

Qualsevol individu o institució pot generar un **certificat digital** però si aquest *emissor* no és reconegut per qui interactuessin amb el propietari del certificat, és gairebé igual que si no hagués estat signat. Per això els emissors han d'acreditar-se per a així ser reconeguts per altres persones, comunitats, empreses o països i que el seu signatura tingui validesa.