Seguretat i criptografia

Criptografia

Josep Gutiérrez

Departament d'informàtica
Salesians de Sarrià

Criptografia

Definició de Criptografia

- La criptografia s'encarrega de l'estudi dels algoritmes, protocols i sistemes que s'utilitzen per dotar de seguretat a les comunicacions, la informació i les entitats que es comuniquen entre si.
- La criptografia comprèn tota una sèrie de tècniques associades al procés de convertir un text normal en un text inintel·ligible i viceversa. Això es fa per tal que el text sigui incomprensible pels que no disposin de la clau o l'algoritme apropiat.
- De la informació original en diem text pla (plaintext) encara que no necessàriament sigui un text. 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–lo (un altre algorisme), i la clau.
- La criptografia s'utilitza en moltes aplicacions, com ara transaccions bancàries, contrasenyes i transaccions de comerç electrònic.

Propietats de la criptografia

- **Confidencialitat**. Garanteix que la informació sigui accessible únicament al personal autoritzat, que disposarà de la clau de desxifrat
- **Integritat**. Garanteix que la informació no s'ha pogut modificar. Per aconseguir-ho pot fer servir per exemple funcions hash criptogràfiques MDC o protocols de compromís de bit.
  - Els Codis de detecció de manipulacions són també anomenats Codis de detecció de modificacions, MDC (Modification Detection) Un codi de detecció de modificacions és una funció hash criptogràfica sense clau secreta que pot ser usada per a detectar qualsevol modificació de la cadena a la qual s'apliqui, ja sigui aquesta modificació accidental o malintencionada. Per tant les MDC permeten protegir la integritat de la informació.

Propietats de la criptografia

- **Vinculació o No-Repudi**. Permet vincular un document o transacció a una persona o un sistema de gestió criptogràfic determinat. El remitent no pot negar haver realitzat la transmissió de la informació en una etapa posterior
- Normalment s'aconsegueix afegint un resum del mateix (CheckSum) amb la data i d'altres camps addicionals abans de xifrar el text.
  - Demostra que només nosaltres podem haver escrit un cert document.
  - Hi diu la data i l'hora, de forma que si es modifiqués, el resum del missatge no coincidiria (perquè és un xifrat de només un sentit, i només es pot verificar si és vàlid o no). Es pot demostrar que un cert document s'ha fet no després d'una certa data i hora.
  - Si en comptes de canviar la data es canvia el contingut, el resultat és el mateix. És a dir, la comprovació de consistència del missatge amb el reu resum xifrat no coincidiria.
  - Aquests principis són els que es fan servir per a construir la signatura digital.

Propietats de la criptografia

- **Autenticació**. Proporciona mecanismes que permeten verificar la identitat del comunicador i el receptor. Per aconseguir-ho s'utilitzen funcions hash criptogràfiques MAC o protocols de coneixement zero.
- Les funcions MAC (Message authentication code) són una porció d'informació utilitzada per autenticar un missatge. Els valors MAC es calculen mitjançant l'aplicació d'una funció hash criptogràfica amb clau secreta K, que només coneixen el remitent i destinatari, però no els atacants. Es diu que la funció hash ha de ser criptogràfica perquè ha de complir certes propietat de seguretat que les fan resistents davant atacs d'adversaris.

Propietats de la criptografia

- Un bon sistema de codificació posa tota la seguretat en la clau i cap en l'algoritme. En altres paraules, no hauria de ser de cap ajuda per a un atacant conèixer l'algorisme que s'està utilitzant. Només si l'atacant obtingués la clau, seria d'utilitat conèixer l'algoritme. Els algorismes d'encriptació àmpliament utilitzats tenen aquestes propietats
- Donat que tota la seguretat està en la clau, és important que sigui molt difícil d'endevinar el tipus de clau.
- Actualment, els ordinadors poden desxifrar claus amb extrema rapidesa, i aquesta és la raó per la qual la mida de la clau és important en els criptosistemes moderns. L'algoritme DES (ja obsolet) genera una clau de 56 bits, el que significa que hi ha 2^{56} claus possibles (72.057.594.037.927.936 claus). Tot i que això representa un nombre molt alt de claus, un ordinador genèric pot verificar el possible conjunt de claus en qüestió de dies i una màquina especialitzada pot fer-ho en hores.

Tècniques criptogràfiques

- Funcions Hash.
- Criptografia de clau simètrica
- Criptografia de clau pública

Funcions Hash

Definició de Hash

- Els hash o funcions de resum són algoritmes que aconsegueixen crear a partir d'una entrada (ja sigui un text, una contrasenya o un arxiu, per exemple) una sortida alfanumèrica de longitud normalment fixa que representa un resum de tota la informació que se li ha donat (és a dir, a partir de les dades de l'entrada crea una cadena que només pot tornar-se a crear amb aquestes mateixes dades)
- Les funcions hash s'encarreguen de representar de forma compacta un arxiu o conjunt de dades que normalment és més gran que el hash independentment del propòsit del seu ús.
- Aquest sistema de criptografia fa servir algoritmes que asseguren que amb la resposta (o hash) mai es podrà saber quines han estat les dades inserides, el que indica que és una funció unidireccional

Utilitats de les funcions Hash

Protegir la confidencialitat d'una contrasenya

- Les funcions hash són molt usades per protegir la confidencialitat d'una contrasenya emmagatzemada en format pla en una base de dades. En aquest cas, per saber si una contrasenya que està guardada és igual a la que hem introduït, li apliquem el hash a la guardada i a la introduïda i les comparem, de forma que en cap cas mostrem o utilitzem el text pla per la xarxa i sempre comparem el hash.

Asegurar la integridad de la información

- Un altre ús és la de garantir la integritat de les dades. Això ho haureu comprovat en algunes webs que proporcionen descàrregues d'arxius grans, per exemples de programari, que permeten descarregar també el resum de l'arxiu i la funció hash utilitzada.
- Això permet comprovar que l'arxiu s'ha descarregat correctament i que ningú ha modificat el seu contingut durant la transmissió.

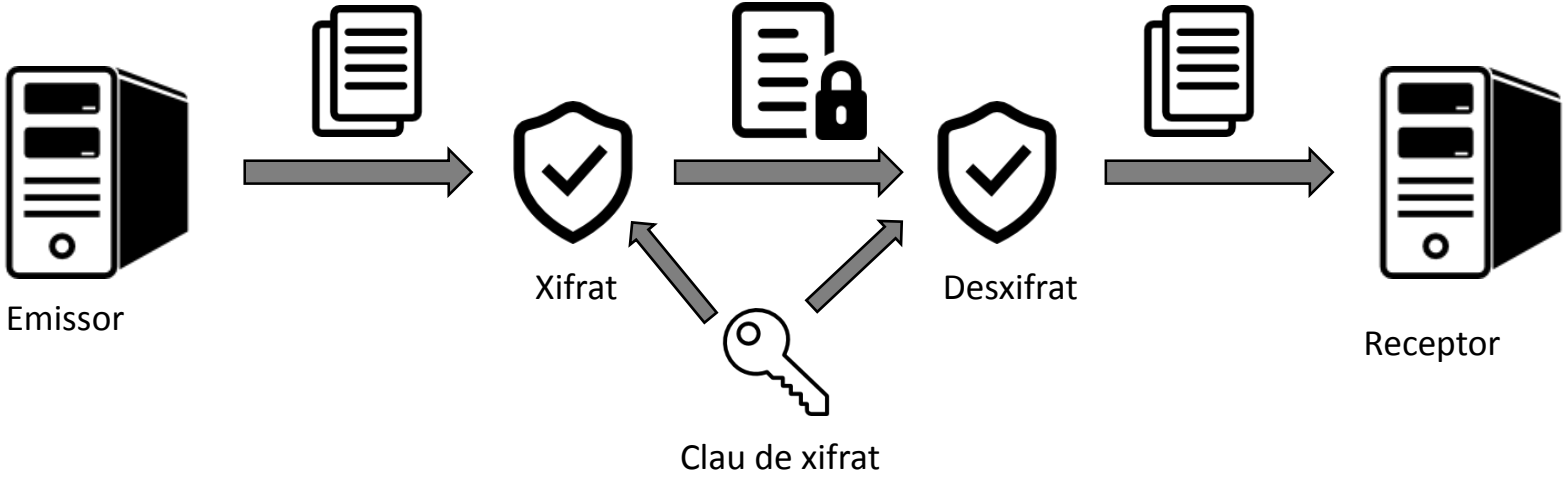
Utilitats de les funcions Hash

Firma digital

- Les funcions hash implementen el mètode més simple de signatura digital, que consisteix a crear un hash de la informació enviada i xifrar amb la nostra clau privada perquè qualsevol amb la nostra clau pública pugui veure el hash real i verificar que el contingut l'arxiu és el que hem enviat nosaltres.

Criptografia de clau simètrica

- La criptografia simètrica és un mètode criptogràfic en el qual tant el remitent com el destinatari comparteixen una clau que s'utilitza per realitzar el xifrat i desxifrat.
- La criptografia simètrica pot proporcionar integritat de dades quan s'utilitza juntament amb altres algorismes per crear codis d'autenticació de missatges (MAC).



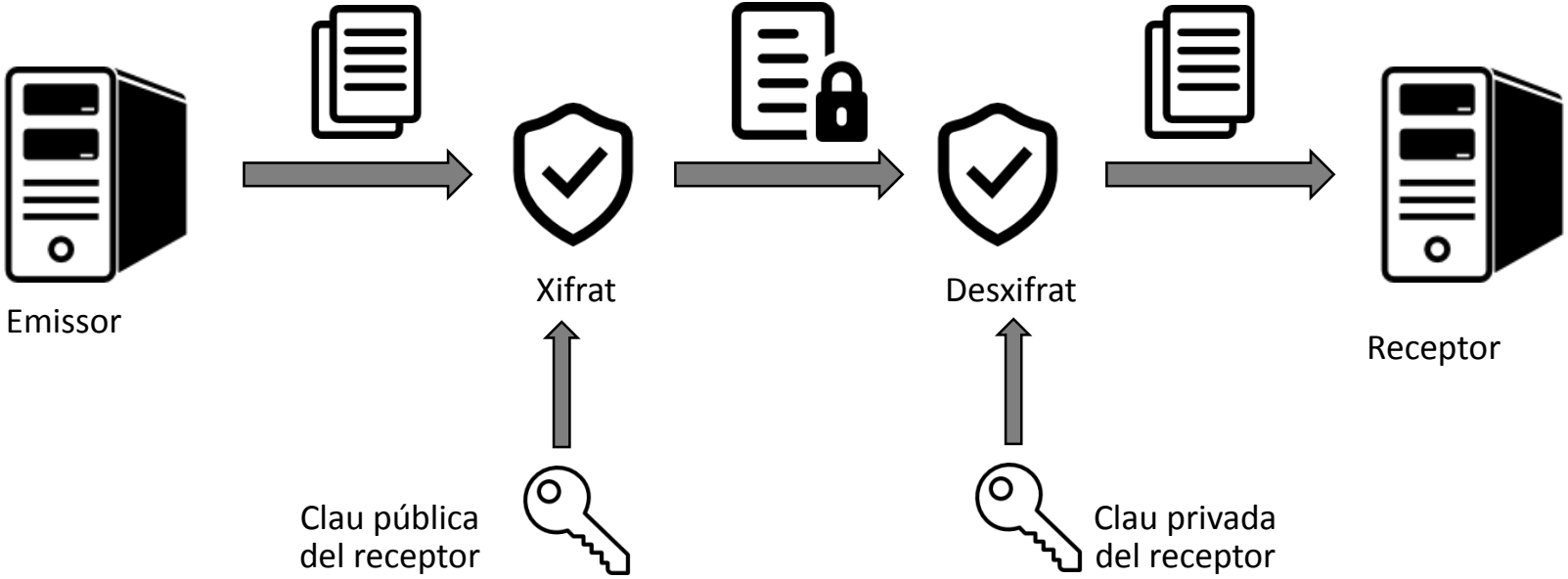
Criptografia de clau simètrica

- La criptografia simètrica és comparativament senzilla, ja que la clau secreta que s'utilitza tant per al xifratge com per al desxifratge es comparteix entre l'emissor i el destinatari.
- Actualment s'utilitzen nombrosos algorismes simètrics. Alguns dels algorismes més comuns inclouen Rijndael (AES) i Triple DES (3DES). Aquests algorismes estan dissenyats per funcionar de manera eficient en arquitectures de hardware comuns.
- El principal problema amb els sistemes de xifrat simètric no està lligat a la seva seguretat, sinó a l'intercanvi/distribució de claus. Una vegada que el remitent i el destinatari hagin intercanviat les claus poden usar-les per comunicar-se amb seguretat, però cal escollir acuradament un canal de comunicació segur per tal de transmetre les claus, ja que per a un possible atacant seria molt més fàcil intentar interceptar la clau que provar les possibles combinacions de l'espai de claus.
- En alguns casos (com ara SSL), la criptografia asimètrica es pot utilitzar per garantir que l'intercanvi de claus inicial es produeixi a través d'un canal segur.

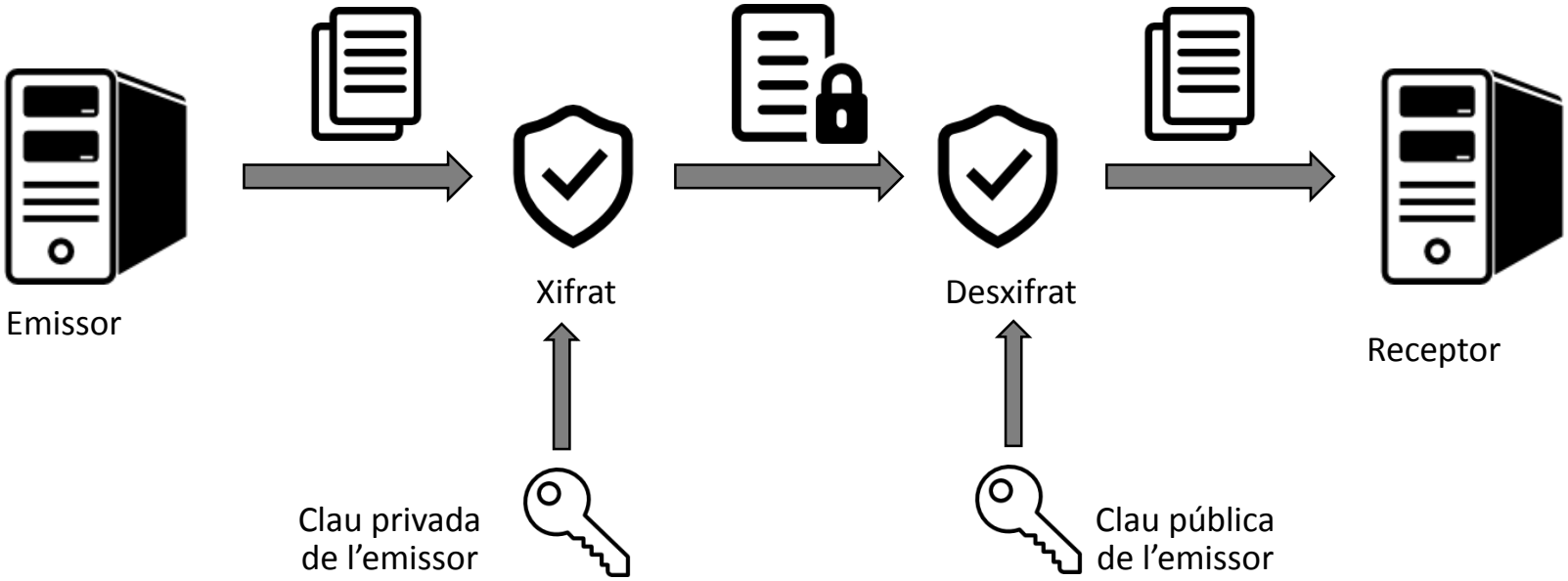
Criptografia de clau pública

- La criptografia de clau pública també anomenada criptografia asimètrica és el mètode criptogràfic que utilitza un parell de claus per a l'enviament de missatges. Les dues claus pertanyen a la mateixa entitat. Una clau és pública i es pot lliurar a qualsevol persona, l'altra clau és privada i el propietari ha de guardar-la de manera que ningú hi tingui accés.
- Els mètodes criptogràfics garanteixen que aquesta parella de claus només es pot generar una vegada, de manera que es pot assumir que no és possible que dues persones hagin obtingut casualment la mateixa parella de claus.
- Actualment, s'utilitzen pocs algoritmes asimètrics. L'algoritme asimètric més utilitzat és l'algoritme RSA.
- El xifratge asimètric requereix més recursos de processament que el xifrat simètric.

Criptografia de clau pública



Criptografia de clau pública



salesians SARRIÀ

Criptografia de clau pública

- Si una persona emet un missatge per a un destinatari, fa servir la clau pública d'aquest últim per xifrar-lo de forma que un cop xifrat, només la clau privada del destinatari podrà desxifrar el missatge, ja que és l'únic que hauria de conèixer-la. Per tant s'aconsegueix la confidencialitat de l'enviament del missatge, ja que ningú excepte el destinatari pot desxifrar-lo.
- Si el propietari del parell de claus utilitza la seva clau privada per xifrar un missatge, qualsevol pot desxifrar-lo utilitzant la clau pública del primer. En aquest cas s'aconsegueix la identificació i autenticació del remitent, ja que se sap que només va poder ser ell qui va emprar la seva clau privada.
- Aquesta idea és el fonament de la signatura electrònica, on jurídicament hi ha la presumpció que el signant és efectivament l'amo de la clau privada.

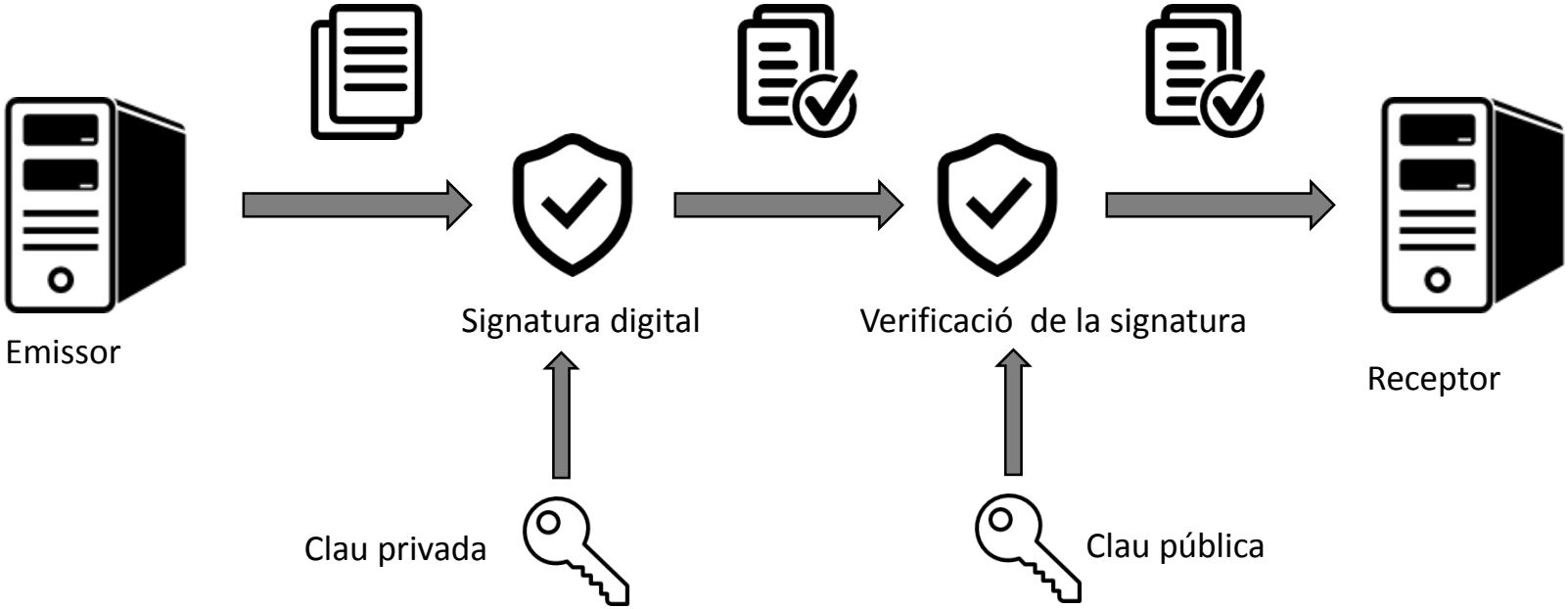
Criptografia de clau pública

- Un problema amb els criptosistemes de clau pública és que els usuaris han d'estar constantment vigilants per garantir que s'estan xifrant la clau de la persona correcta. En un entorn on s'intercanvien les claus a través de servidors públics, els atacs man-in-the-middle són una amenaça potencial.
- En aquest tipus d'atac, algú envia una clau falsa amb el nom i l'identificador d'usuari del destinatari destinat a l'usuari. Les dades encriptades per - i interceptades per - el veritable propietari d'aquesta clau falsa ara està en mans equivocades.
- En un entorn de clau pública, és vital que tingueu la seguretat que la clau pública a la qual esteu xifrant dades és, de fet, la clau pública del destinatari i no una falsificació. Només s'haurien de xifrar aquelles claus que s'han lliurat físicament. Però suposem que necessiteu intercanviar informació amb persones que mai no heu conegut; Com es pot assegurar que es té la clau correcta?
- Per solucionar aquest problema apareixen els certificats digitals.

Signatura digital

- Un gran avantatge de la criptografia de clau pública és que proporciona un mètode per emprar signatures digitals. Les signatures digitals permeten al destinatari d'informació verificar l'autenticitat de l'origen de la informació i verificar que la informació estigui intacta. D'aquesta manera, les signatures digitals de clau pública proporcionen autenticació i integritat de dades. Una signatura digital també proporciona no repudi
- Una signatura digital té el mateix propòsit que una signatura manuscrita. No obstant això, una signatura manuscrita és fàcil de falsificar mentre que una signatura digital presenta una seguretat superior a la d'una signatura manuscrita, ja que és gairebé impossible falsificar, i a més verifica la integritat del contingut de la informació i la identitat del signant.
- L'usuari que vol signar el text utilitza la seva clau privada per signar-lo, de forma que el receptor ha d'utilitzar la clau pública de l'emissor per verificar la signatura

Signatura digital



Certificats digital

- Els certificats digitals, o certs, simplifiquen la tasca d'establir si una clau pública pertany realment al suposat propietari.
- Un certificat és una forma de credencial. Són dades que funcionen de forma molt semblant a les d'un certificat físic. Un certificat digital és informació inclosa amb la clau pública d'una persona que ajuda els altres a verificar que una clau sigui autèntica o vàlida. Els certificats digitals s'utilitzen per frustrar els intents de substituir la clau d'una persona per un altre.
- Un certificat digital consta de tres coses:
  - Una clau pública.
  - Informació del certificat.
  - Una o més signatures digitals.
- El propòsit de la signatura digital d'un certificat és indicar que la informació del certificat ha estat verificada per alguna altra persona o entitat de prestigi.

Certificats digital

- Un certificat és bàsicament una clau pública amb una o dues formes d'identificació adjunta, a més d'un segell de l'aprovació d'un altre entitat de confiança.
- El format més utilitzat de certificat és el **X.509**
- El certificat X.509 és un estàndard que defineix el format dels certificats de clau pública i s'utilitzen en molts protocols d'Internet, incloent TLS/SSL. També s'utilitzen per a fer signatures electròniques.
- Un certificat X.509 conté una clau pública i una identitat (un nom d'entitat o de persona) i està signada per una autoritat certificadora.
- Quan un certificat està signat per una autoritat de certificació de confiança o validat per altres mitjans, algú que conté aquest certificat pot confiar en la clau pública que conté per establir comunicacions segures amb una altra part o validar documents signats digitalment per la clau privada corresponent.

Autoritats de certificació

- Una autoritat de certificació(CA per les seves sigles en anglès Certification Authority) és una entitat de confiança, responsable d'emetre i revocar els certificats digitals o certificats, utilitzats en la signatura electrònica, amb els quals s'empra la criptografia de clau pública.
- Jurídicament és un cas particular de prestador de serveis de certificació.
- En el cas d'Espanya la AC més utilitzada és la FNMT (Fábrica Nacional de Moneda y Timbre) a través de l'entitat CERES (CERtificación ESpañola)
- En el cas de Catalunya la Generalitat ha creat l' Agència Catalana de Certificació (CatCert)

Extensions dels certificats

Extensions més habituals d'arxiu de certificats X.509

- **.CER** - Certificat codificat en CER, algunes vegades és una seqüència de certificats
- **.PFX** - (Personal Information Exchange) i s'usa per intercanviar objectes públics i privats dins d'un arxiu.
- **.P12** - PKCS#12, pot contenir certificat (s) (públic) i claus privades (protegit amb clau), és una evolució del .PFX

Escenari Criptogràfic

- Crear un escenari criptogràfic no és una tasca trivial, i es sol fer combinant diferents tècniques per tal d'aprofitar la seguretat que aporta la criptografia de clau pública i la rapidesa de la criptografia simètrica.
- Un escenari habitual presenta els següents passos:
  - Cada part genera un parell de claus pública/privada utilitzant RSA.
  - Les parts s'intercanvien les seves claus públiques de manera segura
  - Cada part genera una clau secreta per al xifrat AES (simètric), i xifra la clau creada recentment (la clau simètrica) utilitzant la clau pública RSA de l'altre.
  - Cada part envia la clau AES encriptada amb la clau pública RSA de l'altre.
  - A partir d'aquí poden enviar i rebre dades de forma segura utilitzant criptografia simètrica.