Glossari de terminologia de certificació digital

Algorisme criptogràfic: Els algorismes que tenen per finalitat el tractament del secret de la informació s'anomenen criptogràfics i són essencials per a la signatura electrònica, ja que permeten l'ús de xifres segures per a la producció i comprovació de la signatura electrònica.

Arxiu amb extensió ".CSR": Són les sigles de "Certificate Signing Request", que vol dir "Sol·licitud de certificació". Un arxiu de sol·licitud de certificació indica quina és la clau pública a certificar i quines són les dades : nom, atributs, etc.

Arxiu amb extensió ".p12" o ".pfx": Aquests fitxers contenen un certificat digital, junt amb la clau privada corresponent i els certificats de totes les autoritats de certificació fins a la que és arrel (o, com sol dir-se, la cadena de certificació).

Autenticitat documental electrònica: L'autenticitat és una propietat del document electrònic que ens informa del fet que el document té unes determinades característiques.

Autoritat de certificació (AC): Una autoritat de certificació és un sistema informàtic dedicat a l'emissió i gestió posterior de certificats digitals, incloent-hi la renovació, l'expiració, la suspensió, l'habilitació i la revocació de certificats, a petició de l'autoritat de registre. L'emissió de certificats es fa d'una forma automatitzada i sempre amb la prèvia confirmació de l'autoritat local de registre. Són funcions bàsiques de les autoritats de certificació: 1) verificar la identitat dels sol·licitants de certificats i 2) publicar les llistes de revocació de certificats.

Cadena de certificats: Les cadenes de certificats permeten que els empleats públics de dues administracions públiques s'enviïn documents signats i verifiquin correctament les signatures.

Caducitat: Els certificats tenen un període de validesa determinat. Un cop aquest ha passat, si no ha estat renovat, el certificat deixa d'estar operatiu i per tant, deixar d'estar vigent.

Certificat digital: Un certificat digital és un document electrònic signat per una autoritat de certificació, que garanteix a les terceres persones que el rebin o l'utilitzin una sèrie de manifestacions que s'hi contenen, com per exemple, la identitat de la persona, les autoritzacions, la seva capacitat per realitzar un determinat acte, etc. El certificat digital permet a les parts tenir confiança en les transaccions a internet, doncs garanteix la identitat del seu posseïdor a internet mitjançant un sistema segur de claus administrat per una tercera part de confiança, l'autoritat de certificació. El certificat permet realitzar un conjunt d'accions de forma segura i amb validesa legal: signar documents, entrar a llocs restringits, identificar-se davant l'administració, etc.

Cicle de vida d'un certificat: Un certificat digital des del moment de la seva emissió pot passar per diversos estats: vàlid, suspès, caducat i revocat.

Clau criptogràfica: Les claus criptogràfiques són els elements numèrics que formen una xifra criptogràfica i que funcionen conjuntament amb els algorismes criptogràfics per generar signatures electròniques i les formes d'autenticació o per fer confidencial un document.

Clau pública: La clau pública és necessària per comprovar la identitat de l'emissor o l'autenticitat d'un document signat. Permet validar una signatura que hagi estat generada amb la clau privada complementària. La clau pública es l'únic element del certificat digital que es pot trobar a l'abast de tothom. Les claus públiques estan disponibles en directoris publicats a internet i en algun cas en bases de dades corporatives. Es relaciona, mitjançant procediments matemàtics, amb un altre element (clau privada) per garantir la seva confidencialitat i integritat. La clau pública serveix bàsicament per a xifrar, tot i que també es fa servir per a verificar signatures digitals. Qualsevol persona pot xifrar un missatge fent servir la clau pública, però tan sols el posseïdor de la clau privada podrà desxifrar-lo.

Clau privada: La clau privada serveix per signar documents electrònics. És l'element secret del certificat. Es troba relacionat, mitjançant procediments matemàtics, amb un altre element (clau pública). La clau privada es sol guardar en la targeta intel·ligent de la persona certificada i, per tant, té totes les garanties de seguretat, encara que es pot trobar en repositori o clau USB. Serveix, bàsicament, per desxifrar els missatges rebuts, tot i que també es fa servir per crear la firma digital.

CPS - Pràctiques de Certificació: Les Pràctiques de Certificació recullen els procediments i requeriments mínims per a l'emissió de certificats digitals als quals s'ajusta l'Agència Catalana de Certificació. En definitiva, la CPS detalla i concreta el procés complet de certificació.

Criptografia: La criptografia és la ciència que tracta la protecció de la informació mitjançant el desordre per transposició o substitució (cryptós) de les lletres (graphós) d'un document, amb l'objectiu de fer-lo confidencial.

Dispositiu de signatura electrònica: Un dispositiu de creació de signatura electrònica és un programa o sistema informàtic que serveix per aplicar les dades de creació de signatura electrònica.

Document electrònic: D'acord amb l'article 3.5 de la Llei 59/2003, de 19 de desembre, de signatura electrònica, és document electrònic el redactat en suport electrònic que incorpori dades signades electrònicament i que, segons l'article 3.6 de la llei 59/2003, serà suport de documents públics, documents expedits i signats electrònicament per funcionaris i documents previs.

Entitat de Certificació: Persona física o jurídica que emet certificats, d'acord amb la Llei de signatura electrònica. En ocasions es tracta com un sinònim d'autoritat de certificació, que és un component tècnic del servei.

Funcions *hash* o de resum: Una funció *hash* és una operació de resum que es realitza sobre un conjunt de dades. Amb aquesta operació s'obté un resum que està associat a les dades originals. Gràcies a aquest resum les comunicacions electròniques poden realitzar-se més ràpidament perquè la mida de les dades és menor i per tant pesen menys, la qual cosa agilitza la transmissió de les dades. Sempre que es disposi del conjunt de dades inicials es pot obtenir el resum, però des del resum no es pot obtenir les dades inicials.

Garantia de la signatura electrònica: La garantia de la signatura electrònica la dóna el prestador de serveis de certificació en relació amb la qualitat dels algorismes, de les claus i del seu funcionament conjunt i correcte amb la resta d'elements necessaris per produir signatures electròniques.

Habilitació: L'habilitació consisteix en tornar a activar un certificat que ha estat suspès. Aquesta habilitació sempre s'ha de sol·licitar expressament i en un termini màxim de 120 dies des de la data de la suspensió.

PKI – "Public Key Infrastructure": Expressió referent a tota la infraestructura necessària per poder posar en marxa i explotar sistemes i aplicacions que fan ús de tècniques de criptografia asimètrica. La criptografia asimètrica consisteix en assignar dues claus a diferents usuaris perquè en les seves comunicacions electròniques puguin desxifrar la clau de l'altre usuari i així certificar la seva identitat.

Prestador de serveis de segells de data i hora: Un prestador de serveis de certificació que emet segells de data i hora és una persona física o jurídica que produeix i signa en nom seu els segells de data i hora. Per tant, legalment és el responsable de la qualitat i seguretat del segell de temps i respon dels danys que qualsevol pugui patir en cas de confiar en els segells.

Prova de la signatura electrònica: La prova de la signatura electrònica és el suport on es troben les dades signades que seran admissibles com a prova documental en un judici.

Renovació: La renovació consisteix en sol·licitar un nou certificat mitjançant un certificat vigent però que està a punt de caducar. D'aquesta manera, durant el dos mesos anteriors a la caducitat d'un certificat es pot sol·licitar la renovació i això implica que s'emeti un nou certificat vàlid.

Revocació: Anul·lació definitiva d'un certificat digital, bé a demanda del subscriptor, o bé per pròpia iniciativa de l'autoritat de certificació en cas de dubte sobre la seguretat de les claus. La revocació és un estat irreversible. Es pot demanar la revocació d'un certificat després d'una situació de suspensió o per voluntat de les persones autoritzades a sol·licitar-la. De la mateixa manera, en el cas d'un certificat suspès, si ha passat el període de suspensió màxim, si el certificat no ha estat habilitat, passa a estar definitivament revocat. Un cop l'entitat de certificació revoca o suspèn un certificat, ha de fer-ho constar a les Llistes de Certificats Revocats (CRL), per fer públic aquest fet. Per tal de verificar l'estat d'un certificat cal consultar la CRL publicada més recentment de l'entitat de certificació que va emetre el certificat en el qual es desitja confiar. Aquestes llistes són públiques i han d'estar sempre disponibles.

Segellat de temps: Un segell de temps o segell de data i hora, concretament, és un document que ens indica la data i l'hora en què s'ha produït un acte, mitjançant una font de temps fiable de data i hora. El servei de segellat de temps permet associar un document a una data i hora, i d'aquesta manera obtenir evidències (tècniques i jurídiques) de que tal acte s'ha produït abans d'un determinat moment del temps.

Signatura digital: Una signatura digital es una transformació matemàtica d'un document, realitzada mitjançant una operació de xifratge asimètric amb la clau privada del signatari.

Signatura electrònica: La signatura electrònica és un concepte legal, neutral des d'una perspectiva tecnològica, que dóna cobertura a l'ús de qualsevol tecnologia que permeti obtenir les mateixes funcions, amb tècniques electròniques, informàtiques i telemàtiques, que la signatura de documents en suport paper. La Llei 59/2003 de signatura electrònica reconeix tres tipus de signatura electrònica, en funció del certificat digital que la genera: signatura electrònica ordinària, signatura electrònica avançada i signatura electrònica reconeguda, aquesta última equiparada a la signatura manuscrita.

Suspensió: Invalidació temporal d'un certificat digital, bé a demanda del subscriptor, o bé per pròpia iniciativa de l'autoritat de certificació en cas de dubte sobre la seguretat de les claus.

Xifrat: És el procés que s'aplica a unes dades per tal de fer-les incomprensibles i evitar que siguin espiades. D'aquesta manera és possible assegurar la confidencialitat de les dades. Només les podrà fer comprensibles un receptor que tingui una clau per desxifrar-les. Només aplicant el procés contrari, denominat desxifrat, a les dades xifrades serà possible regenerar les dades originals (i, per tant, fer-les de nou intel·ligibles).