CENTRE DE SERVEIS CIENTÍFICS
I ACADÈMICS DE CATALUNYA

Com funciona la certificació digital?

Font: CATCert

La certificació digital funciona amb la criptografia asimètrica. La criptografia asimètrica consisteix bàsicament en dues claus, una privada i una pública. Allò que està codificat amb una clau privada necessita la seva corresponent clau pública per ser descodificat, i a l'inrevés.

La clau privada és secreta i només la posseeix l'usuari. Amb ella pot signar documents electrònics.

La clau pública està a disposició de qualsevol usuari. Permet validar una signatura digital que hagi estat generada amb la clau privada complementària.

Si l'emissor desitja enviar un missatge en format electrònic i que el receptor del mateix estigui segur que ha estat ell qui li ha enviat, pot signar-lo digitalment, usant la tecnologia de certificació digital.

Aquest és el procés que es duu a terme per enviar informació a través d'internet mitjançant signatura electrònica, tant des del punt de vista de l'emissor com del receptor d'aquesta informació.

Com procedeix l'emissor?

Tal i com podeu veure a la fig. 1, s'aplica al missatge o document original una funció de resum (*hash*), que és una operació que dóna com a resultat un conjunt fix de dades, una espècie de resum del missatge original. Aquest resum, està unívocament relacionat amb el missatge original, i per tant, qualsevol petit canvi en el missatge original donaria com a resultat un resum diferent. La llargada del resum normalment és de 160 bits, tot i que n'hi ha de més llargs o més curts. Com més llarg menys risc de col·lisió, però més consum de memòria i temps de càlcul.

Una vegada obtenim aquest resum, el xifrem amb la clau privada de l'emissor i dóna com a resultat la signatura digital del document o missatge. D'aquesta manera, l'emissor envia el missatge vinculat a una signatura digital.

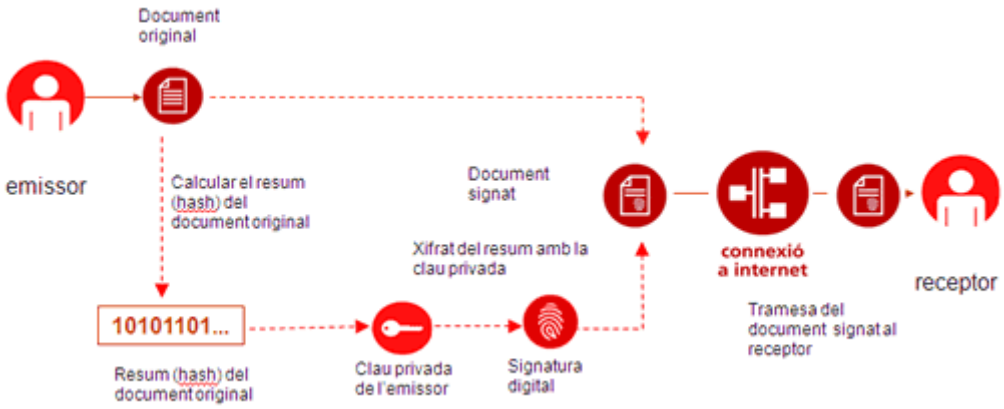

Figura 1. Procés de signatura electrònica.

Com procedeix el receptor?

Quan el receptor del missatge el rebi, podrà comprovar l'autoria del missatge i estar segur que qui li envia és qui diu ser, realitzant el següent procés, que podeu visualitzar a la fig. 2.

Primer de tot, s'ha d'extreure la signatura electrònica del document original, separant doncs, documentació i signatura electrònica. Posteriorment, per una banda, cal desxifrar la signatura electrònica (resum del missatge que ha estat xifrat per l'emissor amb la seva clau privada), amb la clau pública de l'emissor, obtenint el resum original.

D'altra banda, cal d'aplicar la funció resum (*hash*) al document o missatge rebut, tot obtenint un nou resum. Si el resum enviat per l'emissor (un cop desxifrat) coincideix amb el resum obtingut del document, la signatura digital és vàlida i per tant, el missatge no ha estat modificat, és l'original i pertany a l'emissor.

Si els dos resums no coincideixen significa que és possible que el contingut del missatge o document hagi estat modificat, o bé, que l'emissor no és qui diu ser, doncs la seva clau privada no és complementària de la clau pública que disposem.

Actualment els propis sistemes informàtics gestionen les claus públiques d'una manera transparent a l'usuari.

Tot aquest procediment és el que es realitza automàticament per part de les aplicacions que utilitzen signatura electrònica (portals, aplicacions, gestors de correu electrònic, programes informàtics, etc.) i és transparent a l'usuari. D'aquesta manera, no cal realitzar els passos de realitzar el resum, comparar-lo, etc. Només signant un correu electrònic o rebent-lo signat, les aplicacions realitzen tot el procediment i ens tornen la resposta si la signatura és vàlida o no.

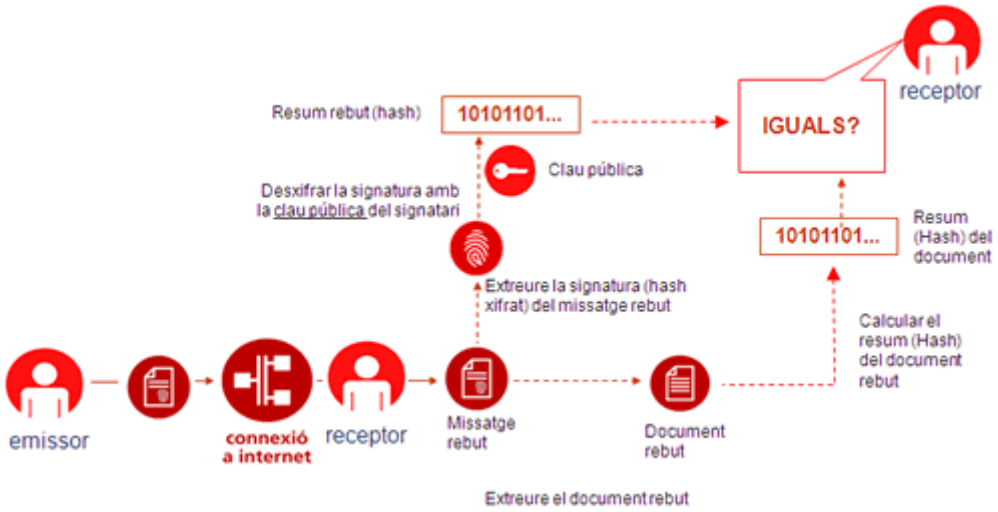

Figura 2. Procés de verificació.

Com se xifra un document?

El xifrat és el procés que s'aplica a unes dades per tal de fer-les incomprensibles.

D'aquesta manera ens assegurem la confidencialitat d'aquestes dades. Per poder xifrar un document és necessari que tant l'emissor com el destinatari disposin d'un certificat digital (clau pública i privada).

A continuació, només heu de xifrar el document fent servir la clau pública de la persona que desitgeu que pugui llegir-lo. Aquest document sols podrà ser desxifrat per la persona que posseeix la clau privada complementària.

D'aquesta manera, el xifratge de la informació, pròpiament dita, implica que paral·lelament a l'obtenció de la signatura electrònica mostrat a la fig.3, xifrem el document original amb la clau pública del nostre receptor, enviant d'aquesta manera el document xifrat i signat, garantint que només ell podrà llegir-lo.

Quan el receptor rebi el document, prèviament a poder fer la comparació dels dos resums, haurà de desxifrar el document rebut amb la seva clau privada i obtenir així el document original. Una vegada obtingut el document original i extreta la signatura, podrem procedir a la verificació de la signatura digital que s'explica a la fig. 4.

Podem veure detalladament el procés de xifratge i desxifratge a les fig. 3 i 4 respectivament. Com podem observar, la única diferència entre el procés de signatura i el procés de signatura i xifratge és que no s'adjunta directament la signatura al document, sinó que aquest es xifra prèviament amb la clau pública del receptor. D'aquesta manera, enviem un document xifrat amb la signatura adjunta.

De la mateixa manera, en el procés de verificació, la única diferència és que en comptes de rebre un document signat (document + signatura) rebem un document xifrat i signat (document xifrat + signatura). Per tal de verificar la signatura, hem de separar el document de la signatura i en comptes d'obtenir el resum directament, prèviament hem de desxifrar el document amb la clau privada del receptor, obtenint el document original. La resta del procés és la mateixa.

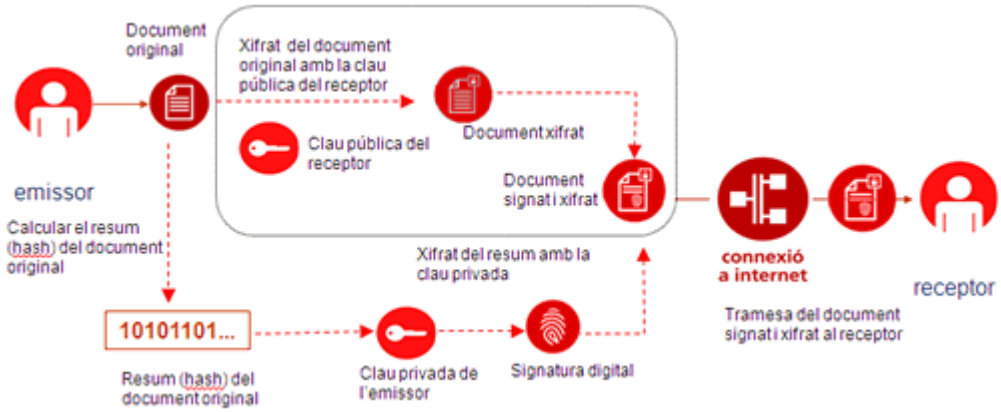

Figura 3. Procés de signatura i xifratge.

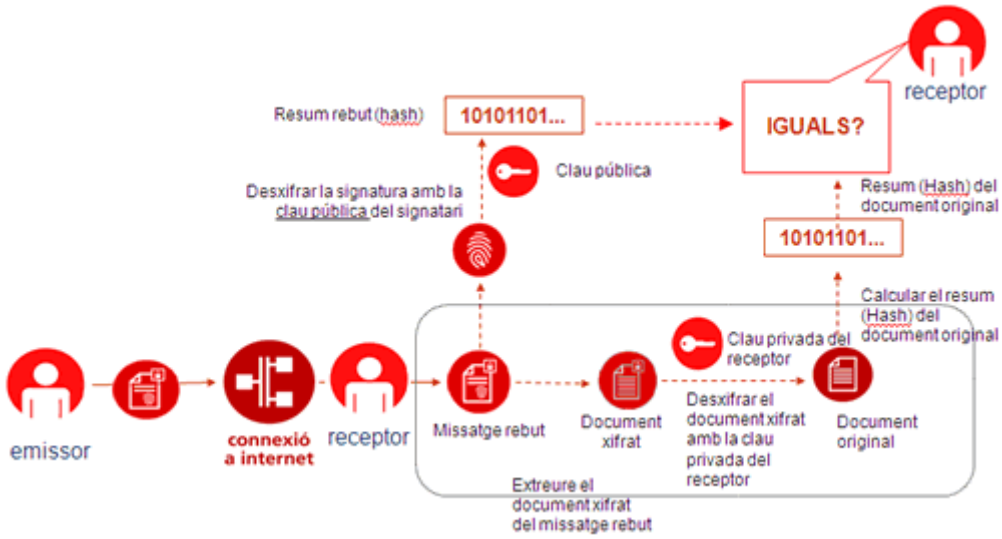

Figura 4. Procés de verificació signatura.