printemps des sciences

Avec le soutien de la Ministre de l'Enseignement supérieur et de la Recherche scientifique

Terre à terres

10 - 16 mars 2008

PRINCIPES ET APPLICATIONS DE LA SIGNATURE DIGITALE

Nguyen Thanh Yên
Département d'informatique

La **signature digitale** permet de "signer" un document électronique; elle garantit que rien n'a été modifié au contenu du document et que l'expéditeur est effectivement la personne qu'il prétend être. Une fois que la personne a signé, elle ne peut nier sa responsabilité sur le document. Une différence par rapport à la signature conventionnelle est qu'une signature digitale n'est pas attachée *physiquement* au message signé.

Fonction de hachage:

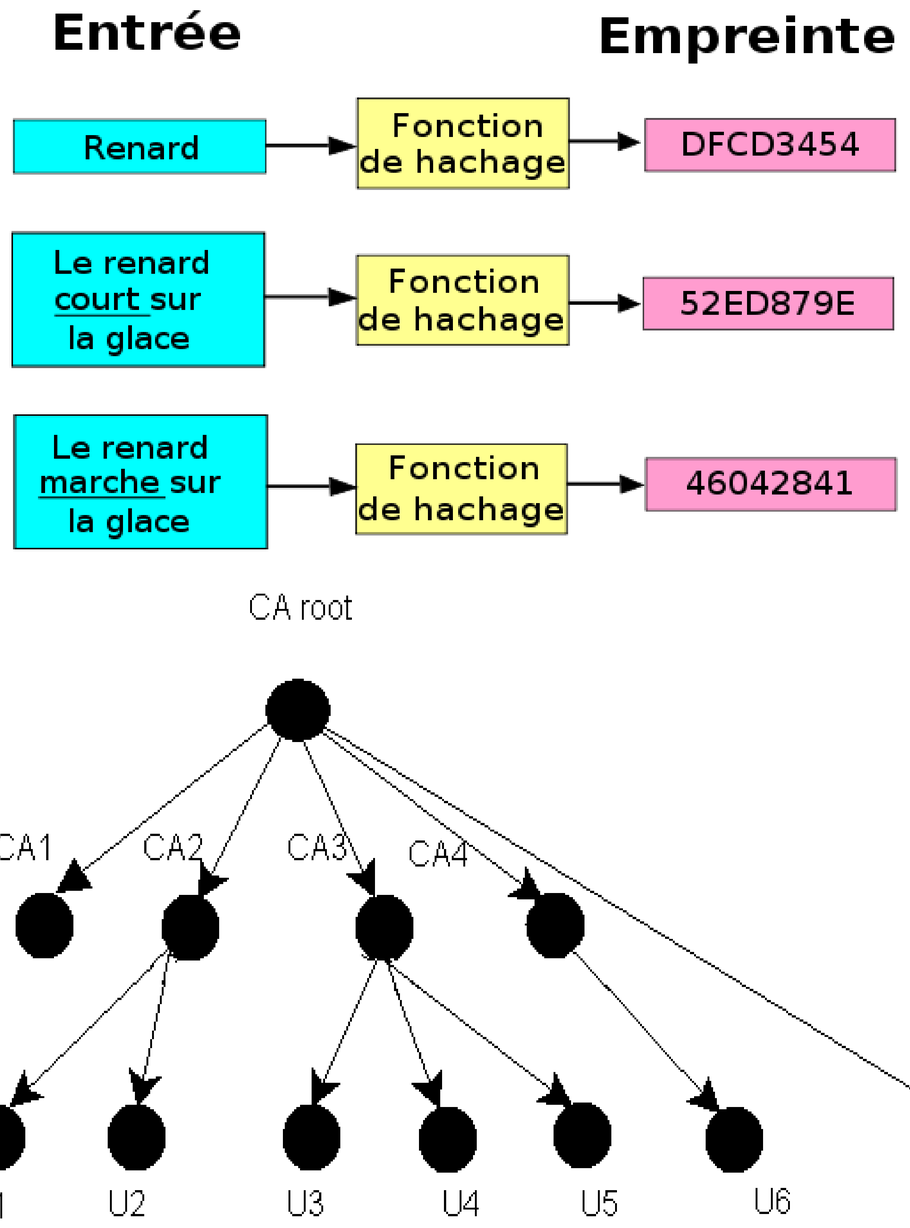
En prenant en entrée une donnée de longueur variable, elle la convertit en une donnée de longueur fixe (généralement de taille plus petite), appelée une *empreinte*. Les schémas de signature sont presque toujours utilisés avec une fonction de hachage publique très rapide afin de renforcer l'intégrité des données et de prévenir les falsifications.

Le certificat

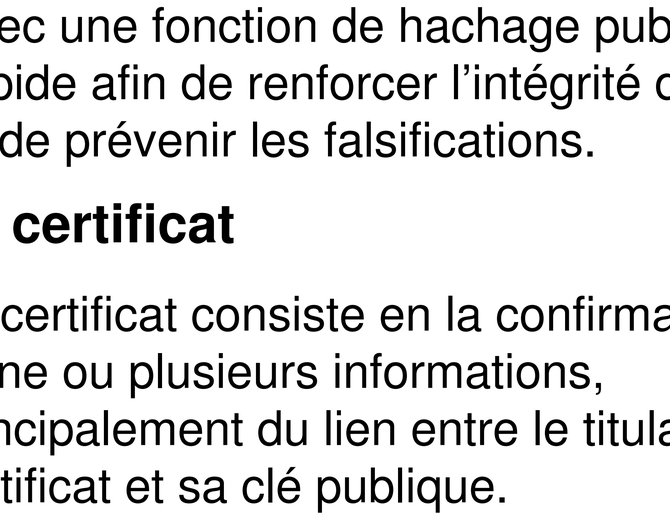
Le certificat consiste en la confirmation d'une ou plusieurs informations, principalement du lien entre le titulaire du certificat et sa clé publique.

Chaque certificat est signé par la clé privée d'une autorité de certification CA se trouvant au-dessus dans un chemin de certificats remontant jusqu'à la racine qui est auto-signée.

La **signature digitale** est fondée sur la cryptographie asymétrique, dite "à clé publique". Dans un système à clé publique, une personne dispose de deux clés mathématiques complémentaires: une clé privée, dont le caractère secret doit effectivement être préservé, et une clé publique, qui peut être librement distribuée. On désire évidemment qu'il soit impossible de déduire de la clé publique la clé privée correspondante.



Applications dans la vie quotidienne?



Paiement par Internet

S'identifier sur eBay avec sa carte d'identité