La signature numérique

Il s'agit d'un sceau numérique permettant d'établir un lien univoque et non manipulable entre une personne physique et un document électronique (p. ex. un courriel). Une empreinte numérique (ou « hash ») est obtenue à partir du document signé suite à une transformation mathématique. Cette valeur de hash est ensuite chiffrée avec la clé de signature secrète de l'expéditeur et envoyée au destinataire en même temps que le document original. Celui-ci utilise ensuite le même procédé de calcul mathématique pour obtenir une valeur de hash à partir du document. Avec la clé publique de l'expéditeur, il va également déchiffrer la valeur de hash qu'il a reçue de la part de l'expéditeur. Si ces deux valeurs sont identiques, il peut être certain de l'intégrité du document et que l'expéditeur est bien qui il prétend être.