La signature numérique est un mécanisme permettant d'[authentifier](https://fr.wikipedia.org/wiki/Authentification) l'auteur d'un document électronique et d'en garantir la [non-répudiation](https://fr.wikipedia.org/wiki/Non-r%C3%A9pudiation), par analogie avec la [signature](https://fr.wikipedia.org/wiki/Signature) manuscrite d'un document papier.

**Les différentes fonctions de la signature numérique :**

* Identifier la personne ou l’organisme qui a apposé sa signature
* Garantir document pas été altéré entre instant où auteur signé et moment lecteur consulte.

**Pour cela, les conditions suivantes doivent être réunies:**

* authentique : l'identité du signataire doit pouvoir être retrouvée de manière certaine ;
* infalsifiable : la signature ne peut pas être falsifiée. Quelqu'un ne peut se faire passer pour un autre ;
* non réutilisable : la signature n'est pas réutilisable. Elle fait partie du document signé et ne peut être déplacée sur un autre document ;
* inaltérable : un document signé est inaltérable. Une fois qu'il est signé, on ne peut plus le modifier ;
* irrévocable : la personne qui a signé ne peut le nier.

**Chiffrement asymétrique :**

Clé publique = chiffrer

Clé privée = déchiffrer

**Fonctionnement algorithme signature :**

Pour la signature, les données du fichier sont hachés, ce qui nous donne une empreinte. Celle-ci sera chiffrer avec la clé privée de la signature. Ainsi, il nous reste à faire la liaison aux données entre le certificat et la signature pour donner au final les données signées numériquement.

Pour la vérification, on doit prendre d’un côté les données que l’on doit haché pour donner une empreinte, de l’autre la signature où l’on doit le déchiffre avec la clé publique du signataire pour donner une empreinte.On doit comparer les 2 empreintes que nous avons obtenu et si elles sont identiques, alors cela veut dire que la signature est valide.