# Introduction

Une signature numérique, *digital signature* en anglais, est un mécanisme informatique basé sur le chiffrement d’une donnée numérique, donc sur les mathématiques. Une signature numérique peut être utilisée pour signer une donnée numérique, telle qu’un message, un document, un site internet, un logiciel, etc.

La signature numérique d’un document, par exemple, permet de garantir la non-répudiation de ce dernier. Autrement-dit, le document ne peut pas être remis en cause par son signataire. La non-répudiation d’un document signé numériquement est assurée par les garanties offertes par une signature numérique :

* **Authenticité**: Le signataire est bien celui qu’il prétend être.
* **Intégrité** : Le document n’a pas été altéré entre sa signature et sa consultation.

Contrairement à une signature manuscrite utilisée pour signer un document papier, une signature numérique n’est pas visible, c’est pourquoi des éléments graphiques peuvent être ajoutés pour rendre l’utilisation des signatures numériques plus intuitive. Par exemple, un document numérique tel qu’un contrat, signé numériquement, inclut souvent une image de la signature manuscrite du signataire, mais ce sont bien les métadonnées sauvegardées avec le document qui apportent les garanties propres aux signatures numériques et non l’image de la signature manuscrite.



De plus, une signature numérique ne doit pas être confondue avec une signature électronique, qui est une signature faite à la main et scannée ou capturée par un appareil électronique. Une signature électronique est moins sécurisée qu’une signature numérique, car elle peut être facilement contrefaite.

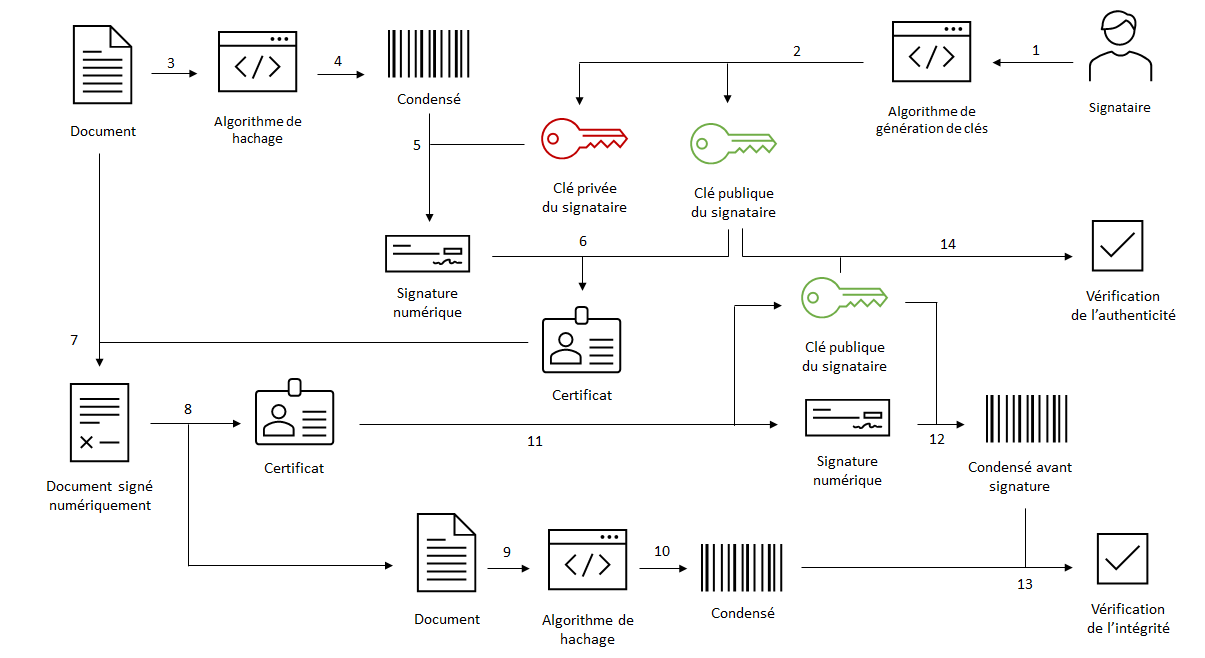
# Fonctionnement

Une signature numérique est créée à l’aide d’une paire de clés de chiffrement, en suivant les étapes suivantes :

* **Création du condensé** : Un algorithme de hachage transforme le message en un condensé, *hash* en anglais, une suite de charactères de taille définie.
* **Création de la signature numérique** : Le condensé est chiffré avec la clé privée du signataire afin qu’il ne puisse être déchiffré qu’avec la clé publique du signataire.
* **Création du document signé numériquement :** La signature numérique et le certificat du signataire contenant, entre autres, sa clé publique sont ajoutés au document d’origine.

La vérification d’un document numériquement signé se fait en suivant les étapes suivantes :

* **Déchiffrement de la signature** **numérique** : La signature numérique est déchiffrée avec la clé publique du signataire afin d’obtenir le condensé du document.
* **Recréation du condensé** : Le condensé du document est recréé afin d’être comparé avec celui obtenu dans l’étape précédente.
* **Comparaison des condensés** : Le condensé recréé est comparé avec celui obtenu par le déchiffrement de la signature numérique. Si les condensés sont identiques, alors le contenu du document n’a pas été altéré entre sa signature et sa consultation.



Documentation :

* https://www.francenum.gouv.fr/guides-et-conseils/pilotage-de-lentreprise/dematerialisation-des-documents/la-signature
* https://learn.microsoft.com/fr-fr/windows/win32/seccrypto/digital-signatures