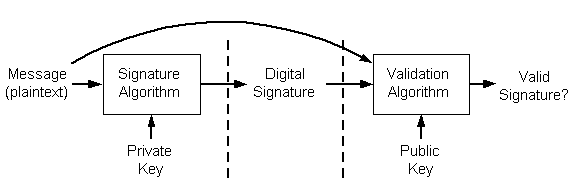
Une signature numérique est un tampon d’authentification électronique chiffré sur des informations numériques comme des messages électroniques, des macros ou des documents électroniques. La signature confirme que les informations proviennent du signataire et n’ont pas été modifiées.

L’utilisation de signature numérique peut permettre certaines garanties :

* **Authenticité :** Le signataire est confirmé en tant que tel.
* **Intégrité :** Le contenu d’un document n’a pas été modifié ou falsifié depuis sa signature numérique.
* **Non-répudiation :** Prouve à toutes les parties l’origine du contenu signé. Le terme répudiation fait référence à l’acte d’un signataire rejetant tout lien avec le contenu signé.
* **Notarisation :** Dans certains cas, les signatures confirmées par un serveur d’horodatage sécurisé dans les fichiers Microsoft Word, Microsoft Excel ou Microsoft PowerPoint ont la validité d’une notarisation.

Les signatures numériques sont générées à l’aide d’algorithmes de signature à clé publique. Une clé privée génère la signature, et la clé publique correspondante doit être utilisée pour valider la signature.



La création d’une signature numérique à partir d’un message se fait en deux étapes. La première étape consiste à créer une valeur de hachage (également appelée synthèse de message) à partir du message. Cette valeur de hachage est ensuite signée à l’aide de la clé privée du signataire.

Pour vérifier une signature, le message et la signature sont requis. Tout d’abord, une valeur de hachage doit être créée à partir du message de la même façon que la signature a été créée. Cette valeur de hachage est ensuite vérifiée par rapport à la signature à l’aide de la clé publique du signataire. Si la valeur de hachage et la signature correspondent, vous pouvez être sûr que le message est bien celui que le signataire a signé à l’origine et qu’il n’a pas été falsifié. Le diagramme suivant illustre le processus impliqué dans la vérification d’une signature numérique.

Documentation :

* <https://learn.microsoft.com/fr-fr/windows/win32/seccrypto/digital-signatures>