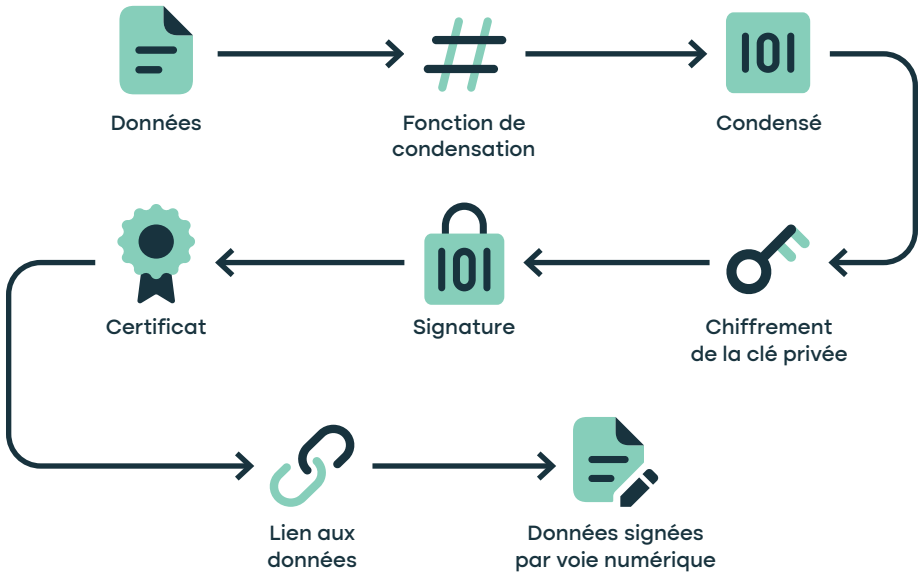
Signatures numériques 101

PORTAGE cybertech

Un individu disposant d'une signature numérique se voit assigner un certificat contenant ses informations publiques ainsi qu'un binôme de clé privée et de clé publique unique.

Lors de la signature numérique d'un document :

- Le contenu du fichier est résumé à l'aide d'une fonction mathématique standardisée en une chaîne de caractères de longueur définie.
- La chaîne est chiffrée avec la clé privée assignée au signataire dont l'accès est protégé par différents facteurs, dont un mot de passe.
- La chaîne chiffrée, le certificat, la clé publique du signataire, les preuves de vérification de révocation et un jeton temporel certifié constituent la signature du document et sont ajoutés à celui-ci.



Lors de la vérification de la signature :

- Le contenu du fichier (excluant la signature) est résumé à l'aide de la même fonction mathématique en une chaîne de caractères de longueur définie.
- La chaîne chiffrée incluse dans la signature est déchiffrée à l'aide de la clé publique pour retrouver la valeur incluse lors de l'étape de signature.
- Si les deux chaînes sont identiques, on peut alors conclure que le document n'a pas été modifié (intégrité préservée), qu'il peut être lié à l'identité définie dans le certificat et aux clés privée/publique et que les autres éléments de la signature sont valides.