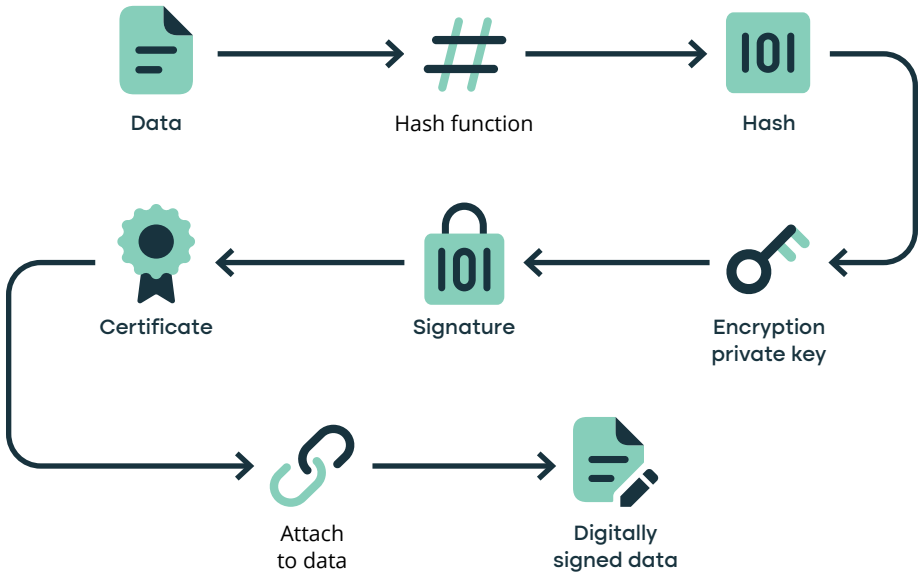
Digital Signatures 101

PORTAGE cybertech

An individual with a digital signature is assigned a certificate containing their public information and a unique public/private key pair.

When a document is digitally signed:

- The contents of the file are summarized by a standard mathematical function into a string of characters with a defined length.
- The string is encrypted with the private key assigned to the signer, whose access is protected in different ways, including by a password.
- The encrypted chain, certificate, signer's public key, proof of revocation verification and a certified time token are all part of the document's signature and are added to the document.



When a signature is verified:

- The contents of the file (excluding the signature) are summarized by the same standard mathematical function into a string of characters with a defined length.
- The encrypted string included in the signature is decrypted using the public key to recover the value included during the signature stage.
- If the two strings are identical, we can conclude that the document has not been modified (integrity preserved), that it can be linked to the identity specified in the certificate and to the private/public keys, and that the other elements of the signature are valid.