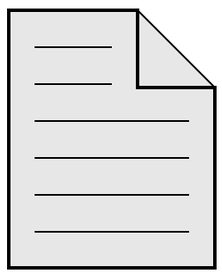
Signing



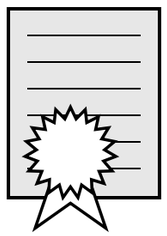
Data

Hash function

101100110101

Hash

Encrypt hash using signer's private key

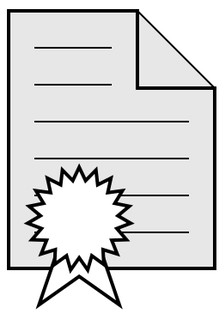


Certificate

111101101110

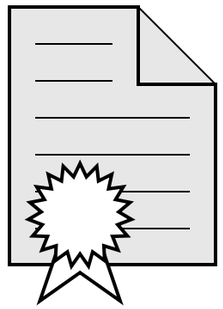
Signature

Attach to data

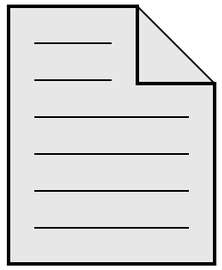


Digitally signed data

Verification



Digitally signed data



Data

Hash function

101100110101

Hash

?

111101101110

Signature

Decrypt using signer's public key

101100110101

Hash

If the hashes are equal, the signature is valid.