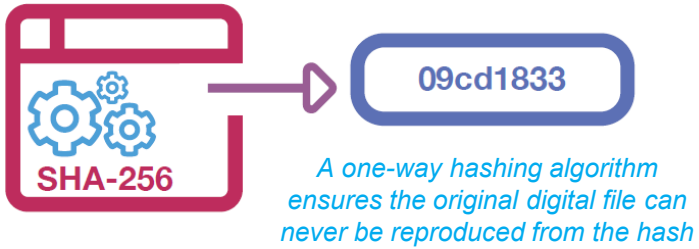
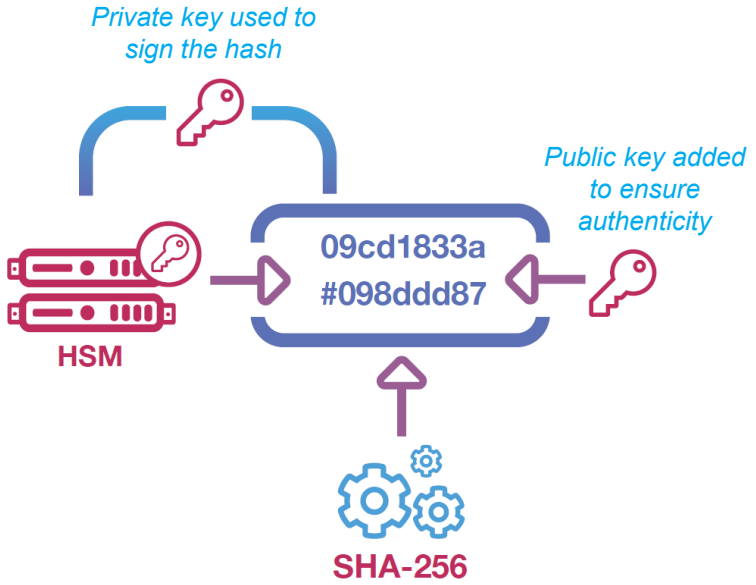
What is a WIPO PROOF token and how is it verified ?

WIPO | PROOF
Trusted Digital Evidence

What is a WIPO PROOF token?





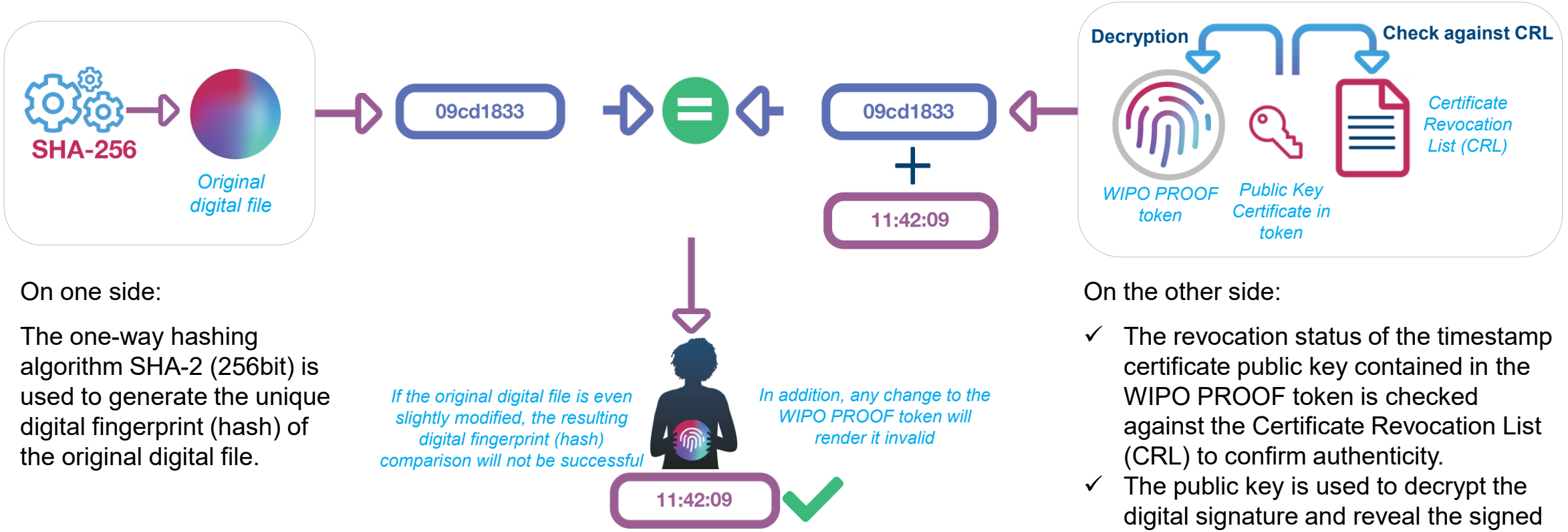
The client-side browser generates a unique digital fingerprint (hash) of the original digital file using the strong one-way hashing algorithm SHA-2 (256bit). The original digital file always remains on the client side and only its hash is uploaded to WIPO PROOF.

WIPO PROOF's audited and high-integrity backend system timestamps the hash of the original digital file.
The hardware-based time source used to timestamp the hash is synchronized to the Coordinated Universal Time (UTC).

The hash is signed with the private key stored in a locked-down Hardware Security Module (HSM) certified to FIPS-140 level 3 standard, creating a digital signature. A public key is added to the digital signature to ensure authenticity.
All this information is encrypted in a .TSR file which represents the trusted proof of existence that the file existed at the moment it was processed in WIPO PROOF.

How is a WIPO PROOF token verified?

WIPO PROOF complies with standard PKI-based timestamp verification



On one side:

The one-way hashing algorithm SHA-2 (256bit) is used to generate the unique digital fingerprint (hash) of the original digital file.

The verification succeeds when the unique hash of the original digital file matches the hash contained in the WIPO PROOF token, which confirms that the original digital file effectively existed at the date and time indicated in the WIPO PROOF token.

On the other side:

- ✓ The revocation status of the timestamp certificate public key contained in the WIPO PROOF token is checked against the Certificate Revocation List (CRL) to confirm authenticity.
- ✓ The public key is used to decrypt the digital signature and reveal the signed hash of the original digital file.

WIPO | PROOF

WIPO

WIPO | PROOF

Trusted Digital Evidence