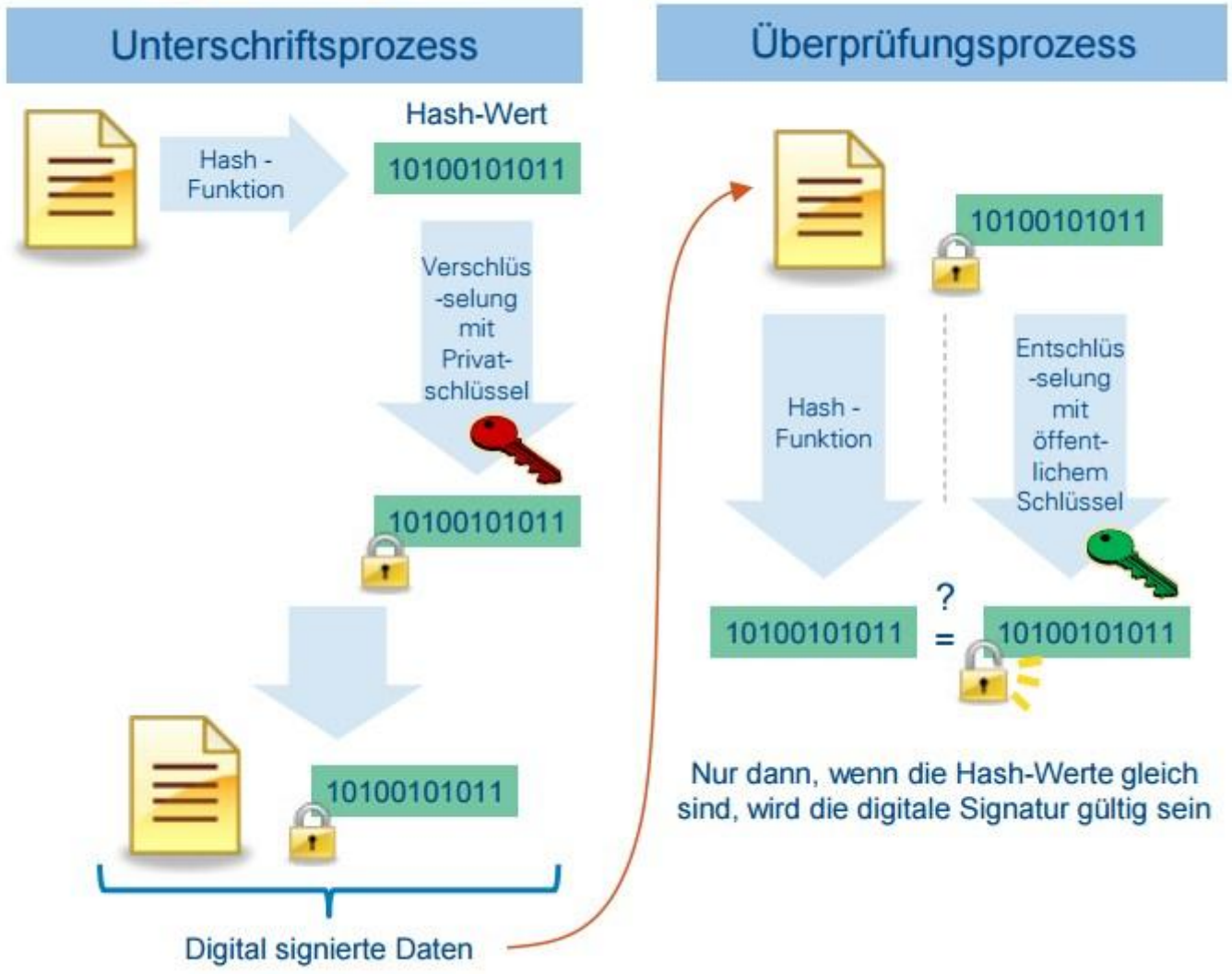
Digitale Signatur

Durch eine Digitale / Elektronische Signatur können zwei der vier Anforderungen an die Kryptografie erfüllt werden.
Dazu wird sich die asymmetrische Kryptografie zu Nutze gemacht.
Die Digitale Signatur erfüllt die:

- Integrität
- Verbindlichkeit

Bild 1: Der Unterschrifts- und Verifikationsprozess der Digitalen Signatur



Quelle: Arthur D. Little

Für digitale Signatur braucht, muss man ein Schlüsselpärchen generieren.

Das Signieren passiert in 3 schritten

1. Hashen der Datei
2. Verschlüsseln des Hashes mit Private Key
3. Versenden der Datei mit dem verschlüsselten Hash

Zum Prüfen der Signatur braucht der Empfänger deinen Public Key. Die Authentität dieses muss durch manuellen Abgleich des Fingerabdrucks (Hash) geprüft werden.

Zum Prüfen wird die Signatur mit dem Public Key entschlüsselt, dadurch erhalt man den Hash. Dann wird die ursprüngliche Datei gehashed und die beiden Hashes verglichen.
Wenn beide gleich sind, ist die Signatur korrekt.

Revision #2
Created 24 October 2025 20:48:13 by Felix
Updated 24 October 2025 21:05:52 by Felix