

### Digitale Signatur:

Kryptografisches Verfahren, bei dem zu einer "Nachricht" (d.h. zu beliebigen Daten) eine Zahl (die "digitale Signatur") berechnet wird, deren Urheberschaft und Zugehörigkeit zur Nachricht durch jeden geprüft werden können.

**Digitale Signaturen** basieren auf **asymmetrischen Kryptosystemen** und verwenden folglich ein Schlüsselpaar, das aus einem **privaten** und einem **öffentlichen Signaturschlüssel** besteht.

### Sicherheit

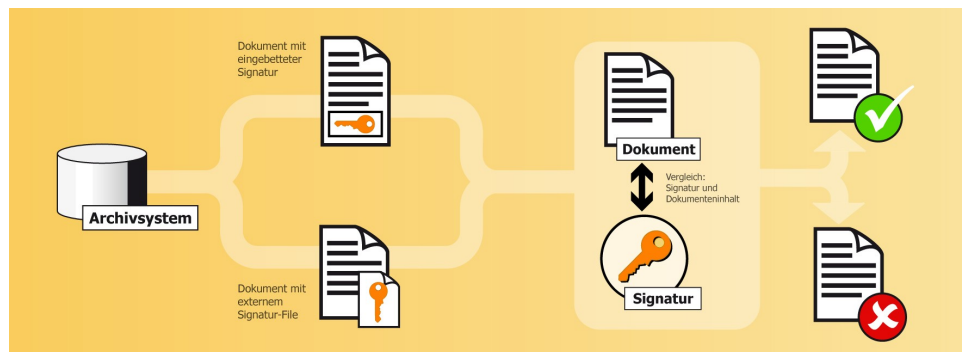
- Auswahl der Parameter
- Kollisionssichere Hash-Funktion
- Geschützte persönliche Sicherheitsumgebung

### Signatur elektronischer Dokumente:

## Prüfung durch jadice

**Digital vorliegende Dokumente müssen mit einer digitalen Signatur versehen werden, um die Originalität des Dokuments zu belegen. Bei Dokumenten, die im Original in Papierform vorliegen und erst nach Eingang digitalisiert werden, bestätigt die digitale Signatur die völlige Übereinstimmung mit dem Original und garantiert den unveränderten Inhalt.**

Das Signieren eines Dokuments besteht aus zwei Arbeitsschritten: Der eigentlichen Signatur und der Verifikation dieser Signatur. Im ersten Schritt überprüft eine Person mit Signierrecht das digitale Dokument. Stimmt das vorliegende Dokument mit dem Original vollständig überein, erhält es eine Signatur. Ein externes, unabhängiges Trust-Center verifiziert die Plausibilität der Signaturdaten (Zeitpunkt der Signatur, signierberechtigte Person etc.). Danach wird das Dokument mit der entsprechenden Signatur im Unternehmensarchiv abgelegt.



Verifizieren, Prüfen, Bearbeiten, .....

Wird das Dokument dann aus dem Archiv abgerufen und würde es an dieser Stelle verändert werden, dann würde die entsprechende Signatur nicht mehr mit dem Dokument übereinstimmen. Eine offensichtliche Warnung oder genauere Hinweise dazu gäbe es aber nicht!

levigo bietet hierfür mit **jadice** einen Revisor-Arbeitsplatz an, welcher für unterschiedliche Einsatzmöglichkeiten konfiguriert werden kann und auf eine Abweichung hinweist.

Falls Dokumente nur im besonderen Einzelfall überprüft werden sollen, kann der **jadice signatur client** als externer Arbeitsplatz eingerichtet werden. Dabei schickt die jadice-Komponente das fragliche Dokument mit seiner Signatur zur Überprüfung an die ursprüngliche Signatursoftware. Das Ergebnis der Überprüfung wird an jadice übermittelt und **jadice** zeigt an, ob Dokument und Signatur übereinstimmen oder nicht.

Soll jedes zur Bearbeitung aufgerufene Dokument überprüft werden, wird der **jadice signatur client** so integriert, dass er automatisch jedes Dokument mit der entsprechenden Signatur zur Überprüfung an die jeweils eingesetzte Signatursoftware sendet. Das Prüfergebnis, das **jadice** von der Signatursoftware erhält, wird dem Sachbearbeiter als entsprechende Statusmeldung angezeigt.

Mit **jadice** wird hier ein für den Sachbearbeiter homogener Arbeitsplatz ermöglicht, der sowohl den Dokumentstatus als auch vollen Funktions- und Annotationsumfang anbietet.