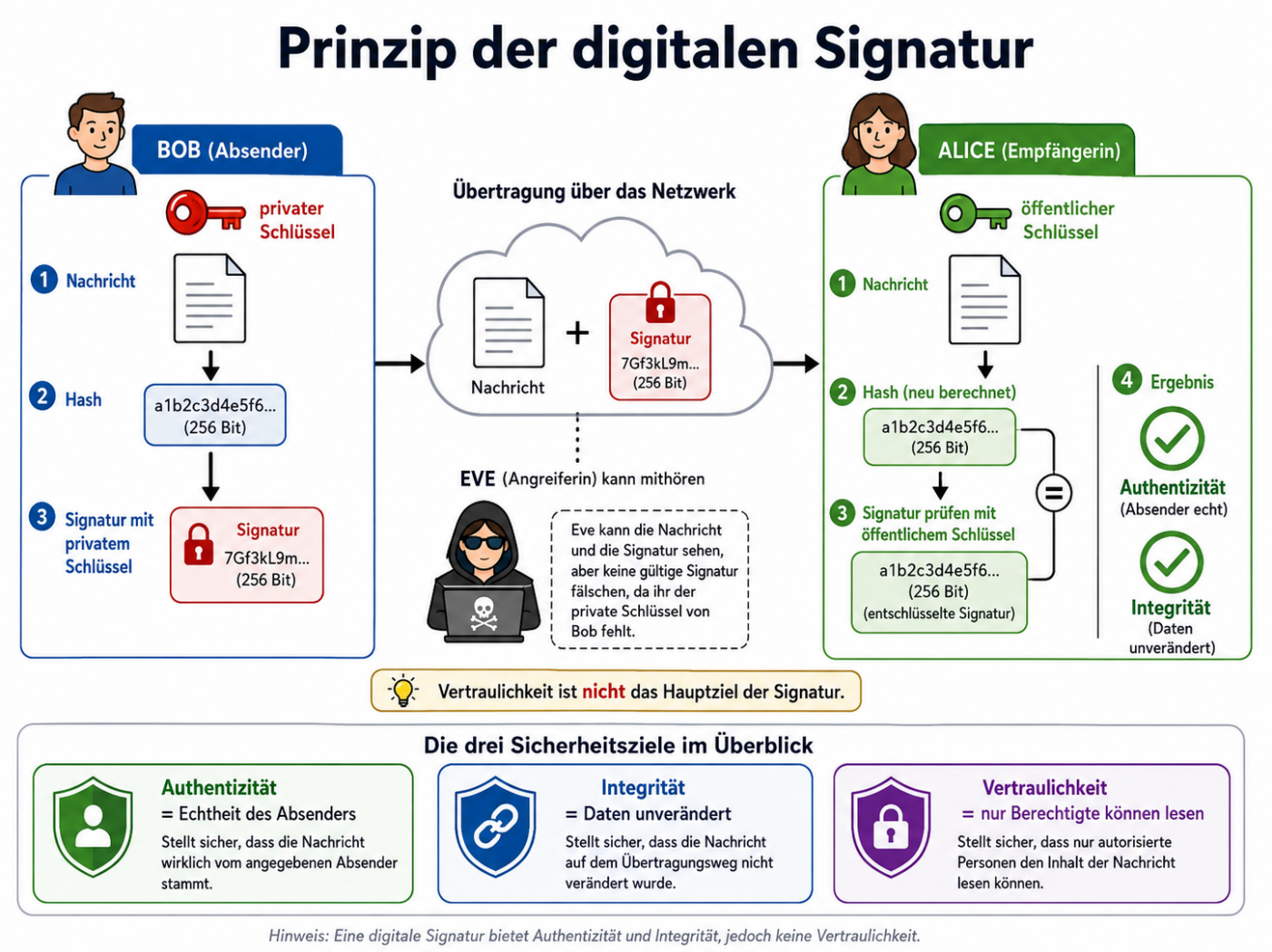
13.3 Digitale Signatur



Hinweis: Eine digitale Signatur bietet Authentizität und Integrität, jedoch keine Vertraulichkeit.

Kurzüberblick

Eine **digitale Signatur** ist kein Verfahren, um eine Nachricht geheim zu machen.

Eine digitale Signatur dient vor allem dazu zu prüfen:

- Stammt die Nachricht wirklich vom angegebenen Absender?
- Wurde die Nachricht unterwegs verändert?

> **IHK-Merksatz:**
> Digitale Signatur = **Authentizität + Integrität**
> Nicht das Hauptziel = **Vertraulichkeit**

Grundidee

Bei der digitalen Signatur wird das asymmetrische Prinzip anders genutzt als bei der Verschlüsselung.

Bei der Verschlüsselung gilt:

- Alice verschlüsselt mit Bobs öffentlichem Schlüssel.
- Bob entschlüsselt mit Bobs privatem Schlüssel.
- Ziel: Nur Bob soll lesen können.

Bei der Signatur gilt:

- Bob signiert mit seinem privaten Schlüssel.
- Alice prüft mit Bobs öffentlichem Schlüssel.
- Ziel: Alice soll prüfen können, ob es wirklich von Bob stammt.

Wichtigster Unterschied

Thema	Ziel
Verschlüsselung	Inhalt vor Mitlesen schützen
digitale Signatur	Absender-Echtheit und Unverändertheit prüfen

> **Kurz gesagt:**
> Verschlüsselung schützt den **Inhalt**.
> Signatur prüft **Echtheit und Unverändertheit**.

Welche Schlüssel werden benutzt?

Vorgang	Schlüssel
Signatur erstellen	privater Schlüssel des Absenders
Signatur prüfen	öffentlicher Schlüssel des Absenders

Wenn Bob eine Nachricht signiert:

- Bob benutzt seinen **privaten Schlüssel**.
- Alice prüft mit Bobs **öffentlichem Schlüssel**.
- Eve kann Bobs öffentlichen Schlüssel auch besitzen.
- Eve kann damit die Signatur prüfen, aber keine gültige Signatur von Bob erzeugen.

>

> **Merksatz:**
> Signieren = privater Schlüssel
> Prüfen = öffentlicher Schlüssel

Ablauf einer digitalen Signatur

Schritt	Erklärung
1	Bob erstellt eine Nachricht.
2	Aus der Nachricht wird ein Hashwert gebildet.
3	Bob signiert diesen Hash mit seinem privaten Schlüssel.
4	Bob sendet Nachricht und Signatur an Alice.
5	Alice berechnet selbst den Hash der empfangenen Nachricht.
6	Alice prüft die Signatur mit Bobs öffentlichem Schlüssel.
7	Wenn die Prüfung passt, sind Absender und Inhalt vertrauenswürdig.

Was prüft Alice dadurch?

Wenn die Signaturprüfung erfolgreich ist, weiß Alice:

Prüfung	Bedeutung
Authentizität	Die Nachricht stammt wirklich von Bob.
Integrität	Die Nachricht wurde unterwegs nicht verändert.

Wenn die Prüfung fehlschlägt, kann das bedeuten:

- Die Nachricht wurde verändert.
- Die Signatur passt nicht zur Nachricht.
- Die Signatur stammt nicht von Bob.
- Der falsche öffentliche Schlüssel wurde verwendet.
- Der private Schlüssel wurde möglicherweise missbraucht.

Warum wird ein Hash verwendet?

In der Praxis wird normalerweise nicht die komplette Nachricht direkt signiert.

Stattdessen wird zuerst ein **Hashwert** der Nachricht gebildet.

Ein Hash ist ein Prüfwert fester Länge.

Beispiel:

Eingabe	Hashwert
Nachricht A	a1b2c3d4...
Nachricht A mit kleiner Änderung	9f8e7d6c...

Schon eine kleine Änderung an der Nachricht verändert den Hashwert stark.

Darum eignet sich ein Hash gut, um Veränderungen an Daten zu erkennen.

> **Wichtig:**
> Ein Hash ist **keine Verschlüsselung**.
> Ein Hash wird normalerweise nicht entschlüsselt, sondern verglichen.

Signatur mit Hash – vereinfacht

Bob macht:

Schritt	Vorgang
1	Nachricht schreiben
2	Hash der Nachricht berechnen
3	Hash mit privatem Schlüssel signieren
4	Nachricht + Signatur senden

Alice macht:

Schritt	Vorgang
1	Nachricht empfangen
2	Hash der empfangenen Nachricht neu berechnen
3	Signatur mit Bobs öffentlichem Schlüssel prüfen
4	Ergebnis bewerten

Warum kann Eve die Signatur nicht einfach fälschen?

Eve kann die Nachricht und die Signatur möglicherweise sehen.

Aber Eve besitzt nicht Bobs privaten Schlüssel.

Deshalb kann Eve keine gültige Signatur erzeugen, die wie eine echte Signatur von Bob geprüft werden kann.

Person	Hat Bobs privaten Schlüssel?	Kann gültig als Bob signieren?
Bob	ja	ja
Alice	nein	nein
Eve	nein	nein

> **Achtung Prüfungsfalle:**
> Der öffentliche Schlüssel darf bekannt sein.
> Gefährlich wäre der Verlust des privaten Schlüssels.

Was passiert bei Manipulation?

Angenommen Bob sendet eine signierte Nachricht an Alice.

Eve verändert unterwegs den Inhalt.

Dann passiert bei Alice:

1. Alice berechnet den Hash der veränderten Nachricht.
2. Alice prüft die Signatur.
3. Der neu berechnete Hash passt nicht mehr zur Signatur.
4. Alice erkennt: Die Nachricht wurde verändert.

Damit ist die **Integrität** verletzt.

Was eine digitale Signatur leistet

Sicherheitsziel	Wird durch Signatur unterstützt?	Erklärung
Authentizität	ja	Absender kann geprüft werden
Integrität	ja	Veränderung der Daten kann erkannt werden
Vertraulichkeit	nein, nicht automatisch	Inhalt ist dadurch nicht geheim

---

Was eine digitale Signatur nicht automatisch leistet

Eine digitale Signatur macht den Inhalt nicht automatisch geheim.

Wenn Bob eine Nachricht nur signiert, aber nicht verschlüsselt, kann Eve den Inhalt eventuell mitlesen.

Eve kann die Nachricht zwar nicht unbemerkt verändern, aber sie kann den Inhalt sehen.

Darum gilt:

Ziel	Benötigte Technik
Inhalt geheim halten	Verschlüsselung
Absender prüfen	digitale Signatur
Veränderung erkennen	Hash / digitale Signatur

Kombination aus Verschlüsselung und Signatur

In der Praxis kann man Signatur und Verschlüsselung kombinieren.

Beispiel:

Bob möchte Alice eine Nachricht senden.

Dafür kann Bob:

1. die Nachricht signieren
2. die Nachricht für Alice verschlüsseln
3. beides an Alice senden

Alice kann dann:

1. die Nachricht entschlüsseln
2. die Signatur prüfen

Dadurch werden mehrere Sicherheitsziele kombiniert.

Ziel	Technik
Vertraulichkeit	Verschlüsselung
Authentizität	digitale Signatur
Integrität	digitale Signatur / Hash

Vergleich: Verschlüsselung und Signatur

Merkmal	Verschlüsselung	Digitale Signatur
Hauptziel	Vertraulichkeit	Authentizität und Integrität

Merkmal	Verschlüsselung	Digitale Signatur
schützt vor Mitlesen	ja	nein, nicht automatisch
erkennt Veränderung	nicht Hauptzweck	ja
beweist Absender	nicht Hauptzweck	ja
Sender nutzt	öffentlichen Schlüssel des Empfängers	privaten Schlüssel des Senders
Empfänger nutzt	privaten Schlüssel des Empfängers	öffentlichen Schlüssel des Senders

---

Beispiel aus dem Alltag

Eine digitale Signatur kann man sich ähnlich wie eine Unterschrift vorstellen.

Aber technisch ist sie stärker, weil sie nicht nur sagt:

„Das kommt von Bob."

Sondern auch:

„Der Inhalt wurde seit der Signatur nicht verändert."

Allerdings gilt:

Eine normale Unterschrift steht sichtbar auf einem Dokument.
Eine digitale Signatur ist ein technischer Prüfwert.

Typische Praxisbeispiele

Bereich	Rolle der digitalen Signatur
Software-Downloads	prüfen, ob Software vom echten Hersteller stammt
Zertifikate	Identität und öffentlicher Schlüssel werden abgesichert
E-Mail-Sicherheit	Absender und Unverändertheit prüfen
Dokumente	digitale Unterschrift
Updates	Schutz vor manipulierten Aktualisierungen
TLS / HTTPS	Zertifikatsprüfung und Vertrauensketten

Typische IHK-Fragen zur digitalen Signatur

Was ist eine digitale Signatur?

Eine digitale Signatur ist ein Verfahren, mit dem man die Echtheit des Absenders und die Unverändertheit der Daten prüfen kann.

Welche Sicherheitsziele erfüllt eine digitale Signatur hauptsächlich?

Authentizität und Integrität.

Bietet eine digitale Signatur automatisch Vertraulichkeit?

Nein. Eine digitale Signatur macht den Inhalt nicht automatisch geheim.

Welchen Schlüssel nutzt der Absender zum Signieren?

Der Absender nutzt seinen privaten Schlüssel.

Welchen Schlüssel nutzt der Empfänger zum Prüfen?

Der Empfänger nutzt den öffentlichen Schlüssel des Absenders.

Warum wird häufig ein Hash verwendet?

Weil ein Hash ein kompakter Prüfwert der Nachricht ist und Veränderungen an der Nachricht erkennbar macht.

Was passiert, wenn die Nachricht nachträglich verändert wird?

Die Signaturprüfung schlägt fehl, weil der Hash nicht mehr passt.

Prüfungsfalle: Signatur ist nicht Verschlüsselung

Eine digitale Signatur bedeutet nicht automatisch, dass niemand die Nachricht lesen kann.

Beispiel:

Bob sendet eine signierte, aber unverschlüsselte Nachricht.

Dann kann Alice prüfen:

- Nachricht stammt von Bob.
- Nachricht wurde nicht verändert.

Aber Eve könnte den Inhalt trotzdem lesen, wenn sie die Übertragung sieht.

> **Merksatz:**
> Signatur schützt nicht automatisch vor Mitlesen.
> Dafür braucht man Verschlüsselung.

Prüfungsfalle: Wer benutzt welchen Schlüssel?

Ziel	Schlüssel beim Sender	Schlüssel beim Empfänger
Verschlüsseln für Bob	Bobs öffentlicher Schlüssel	Bobs privater Schlüssel
Signatur von Bob	Bobs privater Schlüssel	Bobs öffentlicher Schlüssel

> **Kurzform:**
> Geheim an Bob senden: **Bobs öffentlicher Schlüssel**
> Bob unterschreibt digital: **Bobs privater Schlüssel**
> Alice prüft Bob: **Bobs öffentlicher Schlüssel**

Zusammenfassung

Die digitale Signatur nutzt asymmetrische Kryptografie.

Der Absender signiert mit seinem privaten Schlüssel.

Der Empfänger prüft mit dem öffentlichen Schlüssel des Absenders.

Dadurch kann geprüft werden:

- Ist der Absender echt?
- Wurde die Nachricht verändert?

Die digitale Signatur schützt aber nicht automatisch die Vertraulichkeit.

> **IHK-Spickzettel:**
> Digitale Signatur = Authentizität + Integrität
> Signieren = privater Schlüssel des Absenders
> Prüfen = öffentlicher Schlüssel des Absenders
> Hash = Prüfwert der Nachricht
> Vertraulichkeit = nur mit Verschlüsselung

Revision #3
Created 2 June 2026 23:31:15 by Admin
Updated 3 June 2026 06:18:12 by Admin