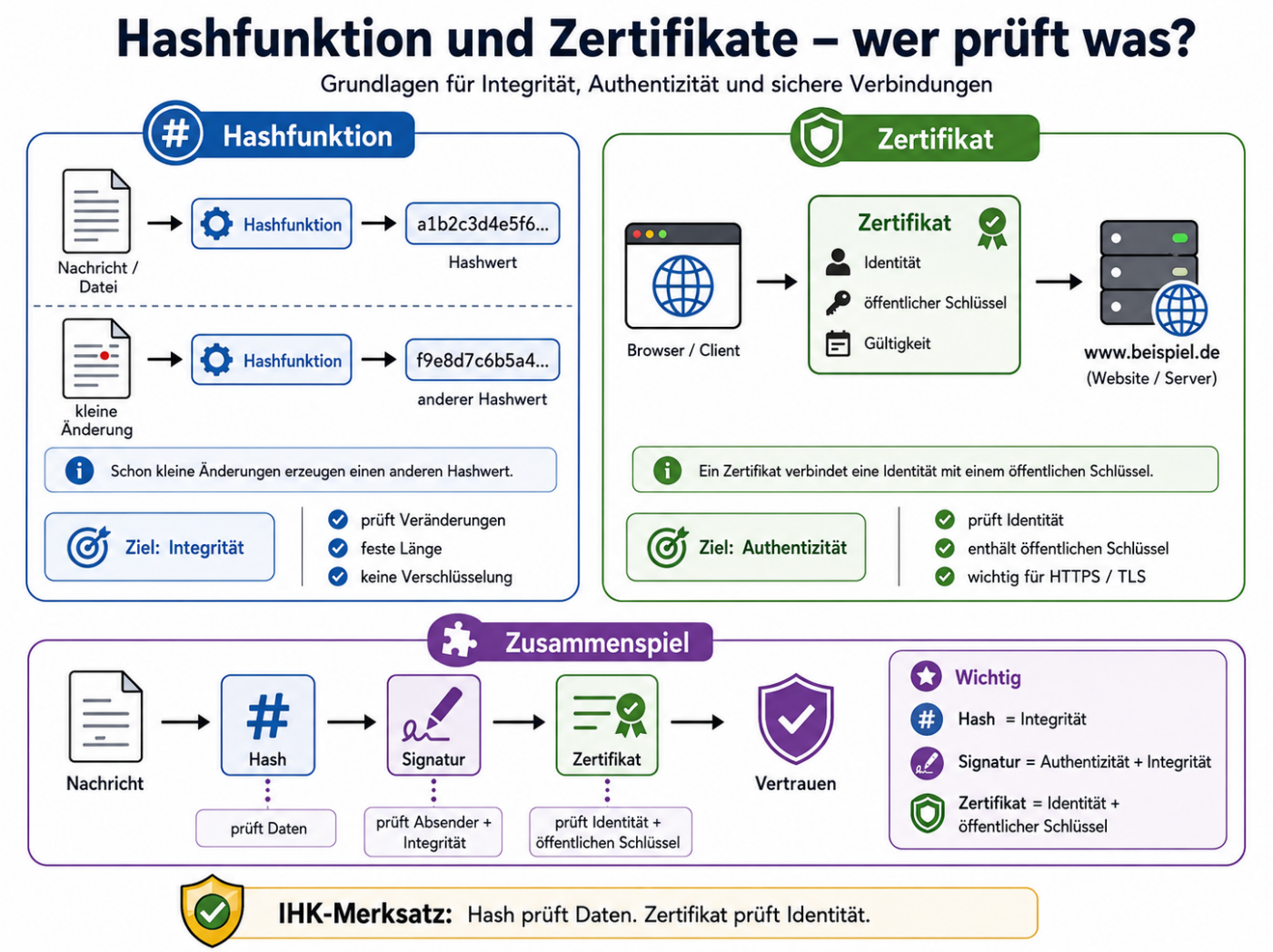
13.5 Hashfunktion und Zertifikate



Kurzüberblick

Hashfunktionen und Zertifikate gehören zu den wichtigsten Grundlagen der IT-Sicherheit.

Sie lösen unterschiedliche Aufgaben:

Thema	Hauptaufgabe
Hashfunktion	prüfen, ob Daten verändert wurden
Zertifikat	prüfen, ob ein öffentlicher Schlüssel zu einer bestimmten Identität gehört

> **IHK-Merksatz:**
> Hash = Integrität prüfen
> Zertifikat = Identität mit öffentlichem Schlüssel verbinden

Quelle 11.4 – Einordnung in die Sicherheitsziele

In der Quelle werden drei Sicherheitsziele besonders hervorgehoben:

Sicherheitsziel	Leitfrage	Typische Technik
Authentizität	Ist die Identität echt?	Zertifikat, digitale Signatur, Login
Integrität	Wurden Daten verändert?	Hashfunktion, digitale Signatur, Prüfsumme
Vertraulichkeit	Können Dritte mitlesen?	Verschlüsselung, VPN, HTTPS

Diese Seite konzentriert sich auf:

- Hashfunktion
- Zertifikate
- Zusammenhang mit Signatur und HTTPS

Hashfunktion

Eine Hashfunktion erzeugt aus Daten einen Prüfwert.

Dieser Prüfwert heißt:

- Hash
- Hashwert
- Fingerabdruck
- Prüfsumme im weiteren Sinn

Beispiel:

Eingabe	Hashwert
Hallo	a1b2c3d4...
Halla	9f8e7d6c...

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

> **Kurz gesagt:**
> Ein Hash ist wie ein digitaler Fingerabdruck von Daten.

Wofür braucht man Hashwerte?

Hashwerte werden genutzt, um Veränderungen zu erkennen.

Beispiele:

- Datei wurde verändert
- Download ist beschädigt
- Nachricht wurde manipuliert
- Passwort wird nicht direkt im Klartext gespeichert
- digitale Signatur prüft den Hash einer Nachricht

Einsatz	Erklärung
Dateiprüfung	Ist die Datei noch unverändert?
Downloadprüfung	Wurde die Datei korrekt übertragen?
digitale Signatur	Der Hash der Nachricht wird signiert
Passwortspeicherung	Es wird normalerweise nicht das Passwort selbst gespeichert
Integritätsprüfung	Veränderungen an Daten können erkannt werden

---

Eigenschaften einer Hashfunktion

Eigenschaft	Bedeutung
feste Länge	Der Hashwert hat immer eine feste Länge
empfindlich gegen Änderungen	kleine Änderung an Daten verändert den Hash stark
nicht sinnvoll rückrechenbar	aus dem Hash soll man den ursprünglichen Inhalt nicht berechnen können
schnell berechenbar	der Hash soll effizient erzeugt werden können
möglichst kollisionsarm	zwei verschiedene Eingaben sollen nicht denselben Hash ergeben

---

Hash ist keine Verschlüsselung

Ein häufiger Fehler ist:

Hash mit Verschlüsselung zu verwechseln.

Das ist falsch.

Thema	Verschlüsselung	Hashfunktion
Ziel	Inhalt geheim halten	Veränderung erkennen

Thema	Verschlüsselung	Hashfunktion
Rückweg möglich?	ja, mit Schlüssel entschlüsselbar	nein, normalerweise nicht rückrechenbar
Ergebnis	Geheimtext	Hashwert
braucht Schlüssel?	meistens ja	klassische Hashfunktion nicht
Sicherheitsziel	Vertraulichkeit	Integrität

> **Achtung Prüfungsfalle:**
> Ein Hash wird nicht entschlüsselt.
> Ein Hash wird neu berechnet und verglichen.

Beispiel: Datei mit Hash prüfen

Angenommen, Alice lädt eine Datei herunter.

Der Hersteller gibt zusätzlich einen Hashwert an.

Alice kann dann selbst den Hash der heruntergeladenen Datei berechnen.

Schritt	Erklärung
1	Hersteller veröffentlicht Datei und Hashwert.
2	Alice lädt die Datei herunter.
3	Alice berechnet den Hash der Datei selbst.
4	Alice vergleicht den berechneten Hash mit dem veröffentlichten Hash.
5	Stimmen beide überein, wurde die Datei wahrscheinlich nicht verändert.

Beispiel mit kleiner Änderung

Originaltext:

```
Hallo
```

Hashwert:

```
a1b2c3d4...
```

Geänderter Text:

```
Halla
```

Neuer Hashwert:

```
9f8e7d6c...
```

Obwohl nur ein Buchstabe anders ist, sieht der Hash komplett anders aus.

> **Merksatz:**
> Kleine Änderung an den Daten = großer Unterschied beim Hash.

Hash und Integrität

Hashfunktionen gehören zum Sicherheitsziel:

Integrität

Integrität bedeutet:

> Daten wurden nicht verändert.

Mit einem Hash kann man prüfen:

- Ist die Datei noch dieselbe?
- Wurde die Nachricht verändert?
- Ist der Download beschädigt?
- Passt die Signatur noch zur Nachricht?

Frage	Antwort durch Hash möglich?
Wurde etwas verändert?	ja
Wer hat die Daten gesendet?	nein, dafür braucht man Signatur oder Zertifikat
Können Dritte den Inhalt lesen?	nein, dafür braucht man Verschlüsselung
Ist der Inhalt geheim?	nein

Hash und digitale Signatur

Bei digitalen Signaturen wird häufig nicht die komplette Nachricht direkt signiert.

Stattdessen wird ein Hashwert der Nachricht gebildet.

Ablauf:

Schritt	Erklärung
1	Bob erstellt eine Nachricht.
2	Aus der Nachricht wird ein Hash gebildet.
3	Bob signiert diesen Hash mit seinem privaten Schlüssel.
4	Alice berechnet den Hash der empfangenen Nachricht neu.
5	Alice prüft die Signatur mit Bobs öffentlichem Schlüssel.
6	Wenn alles passt, sind Authentizität und Integrität erfüllt.

> **Kurz gesagt:**
> Der Hash prüft die Daten.
> Die Signatur prüft, ob der Hash wirklich vom Absender stammt.

Was ist ein Zertifikat?

Ein Zertifikat ist ein digitaler Nachweis.

Es verbindet:

- eine Identität
- mit einem öffentlichen Schlüssel

Beispiel:

Eine Webseite behauptet:

```
Ich bin www.beispiel.de
```

Das Zertifikat hilft dem Browser zu prüfen:

> Gehört dieser öffentliche Schlüssel wirklich zu dieser Webseite?

Warum braucht man Zertifikate?

Bei asymmetrischer Verschlüsselung ist der öffentliche Schlüssel frei verteilbar.

Das Problem ist aber:

> Woher weiß Alice, dass der öffentliche Schlüssel wirklich zu Bob gehört?

Genau hier helfen Zertifikate.

Problem	Lösung durch Zertifikat
öffentlicher Schlüssel ist sichtbar	ist grundsätzlich erlaubt
aber Identität muss geprüft werden	Zertifikat verbindet Identität und öffentlichen Schlüssel
Angreifer könnte falschen Schlüssel anbieten	Zertifikatsprüfung soll das erkennen
Browser muss Webseite prüfen	Zertifikat hilft bei HTTPS

Zertifikat als digitaler Ausweis

Ein Zertifikat kann man sich wie einen digitalen Ausweis vorstellen.

Es sagt vereinfacht:

Inhalt	Bedeutung
Name / Domain	Für wen gilt das Zertifikat?
öffentlicher Schlüssel	Welcher öffentliche Schlüssel gehört dazu?
Aussteller	Wer hat das Zertifikat bestätigt?
Gültigkeitszeitraum	Von wann bis wann gilt es?
Signatur des Ausstellers	Wurde das Zertifikat bestätigt und nicht verändert?

> **Merksatz:**
> Zertifikat = digitaler Ausweis für einen öffentlichen Schlüssel.

Zertifikate und Authentizität

Zertifikate gehören besonders zum Sicherheitsziel:

Authentizität

Authentizität bedeutet:

> Ist die Identität echt?

Bei HTTPS fragt der Browser zum Beispiel:

- Ist diese Webseite wirklich die angeforderte Webseite?
- Gehört der öffentliche Schlüssel wirklich zu dieser Domain?
- Ist das Zertifikat gültig?
- Ist das Zertifikat von einer vertrauenswürdigen Stelle ausgestellt?
- Ist das Zertifikat abgelaufen oder widerrufen?

Zertifikate bei HTTPS

Bei HTTPS nutzt der Browser Zertifikate, um die Identität des Servers zu prüfen.

Vereinfacht:

Schritt	Erklärung
1	Browser ruft eine HTTPS-Webseite auf.
2	Server sendet sein Zertifikat.
3	Browser prüft das Zertifikat.
4	Browser prüft, ob die Domain passt.
5	Browser prüft, ob das Zertifikat gültig ist.
6	Danach kann eine sichere Verbindung aufgebaut werden.

Was prüft der Browser beim Zertifikat?

Typische Prüfungen:

- Passt der Domainname?
- Ist das Zertifikat noch gültig?
- Ist das Zertifikat von einer vertrauenswürdigen Zertifizierungsstelle ausgestellt?
- Wurde das Zertifikat widerrufen?
- Passt der öffentliche Schlüssel zum Zertifikat?
- Ist die Zertifikatskette vertrauenswürdig?

>

> **Achtung Prüfungsfalle:**
> Ein Zertifikat verschlüsselt nicht selbst die Daten.
> Es hilft dabei, die Identität und den öffentlichen Schlüssel zu prüfen.

Public-Key-Zertifikat

Ein Public-Key-Zertifikat bestätigt, dass ein bestimmter öffentlicher Schlüssel zu einer bestimmten Identität gehört.

Das ist besonders wichtig bei:

- HTTPS
- TLS
- VPN
- digitalen Signaturen
- E-Mail-Sicherheit
- Serveridentifikation

Begriff	Bedeutung
Public Key	öffentlicher Schlüssel
Zertifikat	bestätigte Zuordnung zu einer Identität
Zertifizierungsstelle	Stelle, die Zertifikate ausstellt
Zertifikatskette	Vertrauenskette bis zu einer vertrauenswürdigen Stelle

---

Hash, Signatur und Zertifikat im Zusammenspiel

Diese Begriffe hängen eng zusammen.

Baustein	Aufgabe
Hash	prüft, ob Daten verändert wurden
Signatur	bestätigt Absender und Integrität
Zertifikat	bestätigt, wem ein öffentlicher Schlüssel gehört
öffentlicher Schlüssel	wird zum Prüfen oder Verschlüsseln genutzt
privater Schlüssel	wird zum Signieren oder Entschlüsseln genutzt

Beispiel HTTPS:

Bestandteil	Rolle
Zertifikat	Browser prüft Identität des Servers

Bestandteil	Rolle
öffentlicher Schlüssel	ist im Zertifikat enthalten
private Schlüssel	bleibt beim Server
Hash / Signatur	hilft bei Prüfung und Vertrauensaufbau
symmetrischer Sitzungsschlüssel	schützt später die Nutzdaten

Typische Praxisbeispiele

Bereich	Hashfunktion	Zertifikat
HTTPS	Integrität und Prüfmechanismen	Serveridentität prüfen
Software-Download	Datei-Hash prüfen	Herstellerzertifikat möglich
digitale Signatur	Hash der Nachricht wird signiert	öffentlicher Schlüssel wird zugeordnet
VPN	Integrität und Schlüsselmaterial	Identität von Gegenstellen prüfen
Passwortspeicherung	Passwort-Hash speichern	nicht Hauptaufgabe

---

Typische IHK-Fragen zu Hashfunktionen

Was ist eine Hashfunktion?

Eine Hashfunktion erzeugt aus Daten einen Hashwert fester Länge.

Wozu dient ein Hash?

Ein Hash dient vor allem zur Integritätsprüfung.

Ist ein Hash Verschlüsselung?

Nein. Ein Hash wird normalerweise nicht entschlüsselt, sondern neu berechnet und verglichen.

Was passiert, wenn Daten verändert werden?

Der Hashwert verändert sich deutlich.

Welches Sicherheitsziel passt zur Hashfunktion?

Integrität.

Typische IHK-Fragen zu Zertifikaten

Was ist ein Zertifikat?

Ein Zertifikat verbindet eine Identität mit einem öffentlichen Schlüssel.

Wozu braucht man Zertifikate?

Damit geprüft werden kann, ob ein öffentlicher Schlüssel wirklich zu einer bestimmten Person, Organisation oder Webseite gehört.

Welches Sicherheitsziel passt besonders zu Zertifikaten?

Authentizität.

Wo werden Zertifikate häufig verwendet?

Bei HTTPS, TLS, VPN, digitalen Signaturen und sicherer Serveridentifikation.

Verschlüsselt ein Zertifikat selbst die Daten?

Nein. Ein Zertifikat bestätigt vor allem Identität und öffentlichen Schlüssel.

Prüfungsfalle: Hash, Signatur und Zertifikat nicht verwechseln

Begriff	Nicht verwechseln mit	Richtige Bedeutung
Hash	Verschlüsselung	Prüfwert zur Integritätskontrolle
Signatur	reine Verschlüsselung	prüft Authentizität und Integrität
Zertifikat	Datenverschlüsselung selbst	verbindet Identität mit öffentlichem Schlüssel
öffentlicher Schlüssel	geheimer Schlüssel	darf verteilt werden
privater Schlüssel	öffentlicher Schlüssel	muss geheim bleiben

> **Kurzform:**
> Hash prüft Daten.
> Signatur prüft Absender und Daten.
> Zertifikat prüft Identität und öffentlichen Schlüssel.

Zusammenfassung

Hashfunktionen und Zertifikate sind wichtige Bausteine der Netzwerksicherheit.

Eine Hashfunktion erzeugt einen Prüfwert für Daten.

Damit kann man erkennen, ob Daten verändert wurden.

Ein Zertifikat verbindet eine Identität mit einem öffentlichen Schlüssel.

Damit kann man prüfen, ob ein öffentlicher Schlüssel wirklich zur angegebenen Person, Organisation oder Webseite gehört.

> **IHK-Spickzettel:**
> Hash = Prüfwert
> Hash ist keine Verschlüsselung
> Hash gehört zu Integrität
> Zertifikat = digitaler Ausweis
> Zertifikat verbindet Identität mit öffentlichem Schlüssel
> Zertifikat gehört zu Authentizität
> HTTPS nutzt Zertifikate zur Prüfung der Serveridentität

Revision #4
Created 2 June 2026 23:35:27 by Admin
Updated 3 June 2026 06:18:12 by Admin