Hashwerte, Fingerprints und digitale Signaturen

Hashwerte und Prüfsummen

Eine kryptografische Hashfunktion berechnet aus Daten einen Wert fester Länge. Kleine Änderungen der Eingabe führen üblicherweise zu einem stark veränderten Hashwert. SHA-256 ist ein verbreitetes Beispiel.

```
sha256sum beispiel.txt
```

Ein Hashwert allein beweist **nicht**, wer die Datei erstellt hat: Ein Angreifer könnte Datei und veröffentlichten Hashwert gemeinsam austauschen.

Fingerprints

Ein Fingerprint ist eine kompakte, aus dem öffentlichen Schlüssel oder Zertifikat abgeleitete Kennzeichnung. Er ist nicht geheim. Seine Sicherheitswirkung entsteht erst, wenn er über einen unabhängigen, vertrauenswürdigen Kanal abgeglichen wird.

SSH-Fingerprint eines öffentlichen Schlüssels anzeigen:

```
ssh-keygen -lf ~/.ssh/id_ed25519.pub
```

Fingerprint eines OpenPGP-Schlüssels anzeigen:

```
gpg --fingerprint <schluessel>
```

SHA-256-Fingerprint eines X.509-Zertifikats anzeigen:

```
openssl x509 -in zertifikat.pem -noout -fingerprint -sha256
```

Digitale Signaturen

Eine Signatur wird mit dem privaten Signaturschlüssel erstellt und mit dem öffentlichen Schlüssel geprüft. Sie schützt die Integrität der signierten Daten und belegt die Verwendung des zum Prüfschlüssel gehörenden privaten Schlüssels. **Sie verschlüsselt die Daten nicht.**

Beispiel für eine abgetrennte OpenPGP-Signatur:

```
gpg --armor --detach-sign beispiel.txt
```

```
gpg --verify beispiel.txt.asc beispiel.txt
```

Die Prüfung ist nur dann aussagekräftig für die Identität des Absenders, wenn der verwendete öffentliche Schlüssel vertrauenswürdig zugeordnet wurde.

Zertifikatssignaturen

Bei TLS signiert eine Zertifizierungsstelle (CA) ein Zertifikat. Browser prüfen unter anderem Zertifikatskette, Gültigkeit und Domainnamen. Ein Zertifikat ist kein geheimer Schlüssel; der zugehörige private Server-Schlüssel muss geheim bleiben.

Häufige Verwechslungen

Begriff	**Was er leistet**	**Was er nicht leistet**
Hashwert	Vergleich von Datenständen	Identitätsnachweis ohne vertrauenswürdige Quelle
Fingerprint	Identifizierung eines bestimmten Schlüssels	Automatische Bestätigung des Schlüsselinhabers
Signatur	Prüfung von Integrität und Schlüsselzugehörigkeit	Geheimhaltung des Inhalts
Verschlüsselung	Schutz der Vertraulichkeit	Automatisch Nachweis der Urheberschaft

---

Zurück zur Übersicht

From:
https://wiki.bluegnu.de/ - **wiki**

Permanent link:
https://wiki.bluegnu.de/doku.php/open:it:secure:fingerprint_signatur

Last update: **2026/11/15 20:18**