

# Digitale Signaturen

---

- Wie können wir für ein Dokument/eine Datei sicher sein, dass sie...
  - ...wirklich vom angenommenen Autor stammt?
  - ...nicht unbefugt verändert wurde?
- Problem relevant für wichtige Dokumente (Verträge etc.), aber bspw. auch für ausführbare Programme
- Lösung: Digitale Signatur

- Ziele:
  - Sicherstellen, dass ein bestimmter Inhalt von der korrekten Quelle stammt
  - Sicherstellen, dass der Inhalt nicht unerlaubt verändert wurde
- Verfügbare Werkzeuge:
  - Zertifikate
  - Kryptographische Hashfunktionen
- Überlege Dir, ob und wie sich mit diesen Werkzeugen die genannten Ziele erreichen lassen

Vorgehen zum Signieren eines Dokuments  $m$  mit einer digitalen Signatur:

1. Berechnung des Hashwert  $h(m)$  des Dokuments unter Verwendung einer kryptographischen Hashfunktion
2. Verschlüsseln des Hashwerts  $h(m)$  mit dem eigenen, privaten Schlüssel zur Signatur  $s$
3. Übermitteln des Tupels  $(m, s, z)$  an den/die Empfänger
  - Bei  $z$  handelt es sich um ein gültiges Zertifikat, das den eigenen, öffentlichen Schlüssel enthält (muss nicht mitgesendet werden, falls der korrekte öffentliche Schlüssel dem Empfänger aus anderen Quellen bekannt ist)

Prüfen der Signatur:

1. Berechnung des Hashwerts  $h(m)$  der empfangenen Nachricht
2. Anwenden des öffentlichen Schlüssels (enthalten in  $z$ ) auf  $s$ 
  - Stimmen  $h(m)$  und der so entschlüsselte Wert überein, ist die Signatur gültig

Zusammenfassend werden durch den Einsatz von kryptographischen Verfahren folgende Ziele angestrebt:

**Vertraulichkeit (Zugriffsschutz)** Nur berechtigte Personen sollen Zugriff auf bestimmte Daten erlangen

**Integrität (Änderungsschutz)** Die Daten dürfen sich nicht unbemerkt von Unbefugten verändern lassen

**Authentizität (Fälschungsschutz)** Die Urheberschaft der Daten ist nachweisbar/überprüfbar

**Verbindlichkeit (Nichtabstreitbarkeit)** Die Urheberschaft der Daten kann nicht abgestritten werden

- Welche der genannten Ziele werden mit einer digitalen Signatur erreicht?
- Welche der genannten Ziele werden mit einer reinen Verschlüsselung (bspw. AES) erreicht?