

# **Thema 9: Verfahren zur Gewährleistung der Integrität/Authentizität**

---

Oliver Lohrberg

Christian-Weise-Gymnasium Zittau

# Gliederung

---

- 1. Begriffserklärung elektronische und digitale Signatur
  - 2. Anwendungsbeispiele
  - 3.1 Vorteile
  - 3.2 Nachteile
  - 4. One-Way-Hash Funktion
  - 5. Quellen
-

# 1. Begriffserklärung elektronische und digitale Signatur

---

Elektronische  
Signatur:

- Daten elektronischer Form, die an andere Daten angefügt sind
  - sichern die Echtheit von Daten
  - rein rechtlicher Begriff
- 

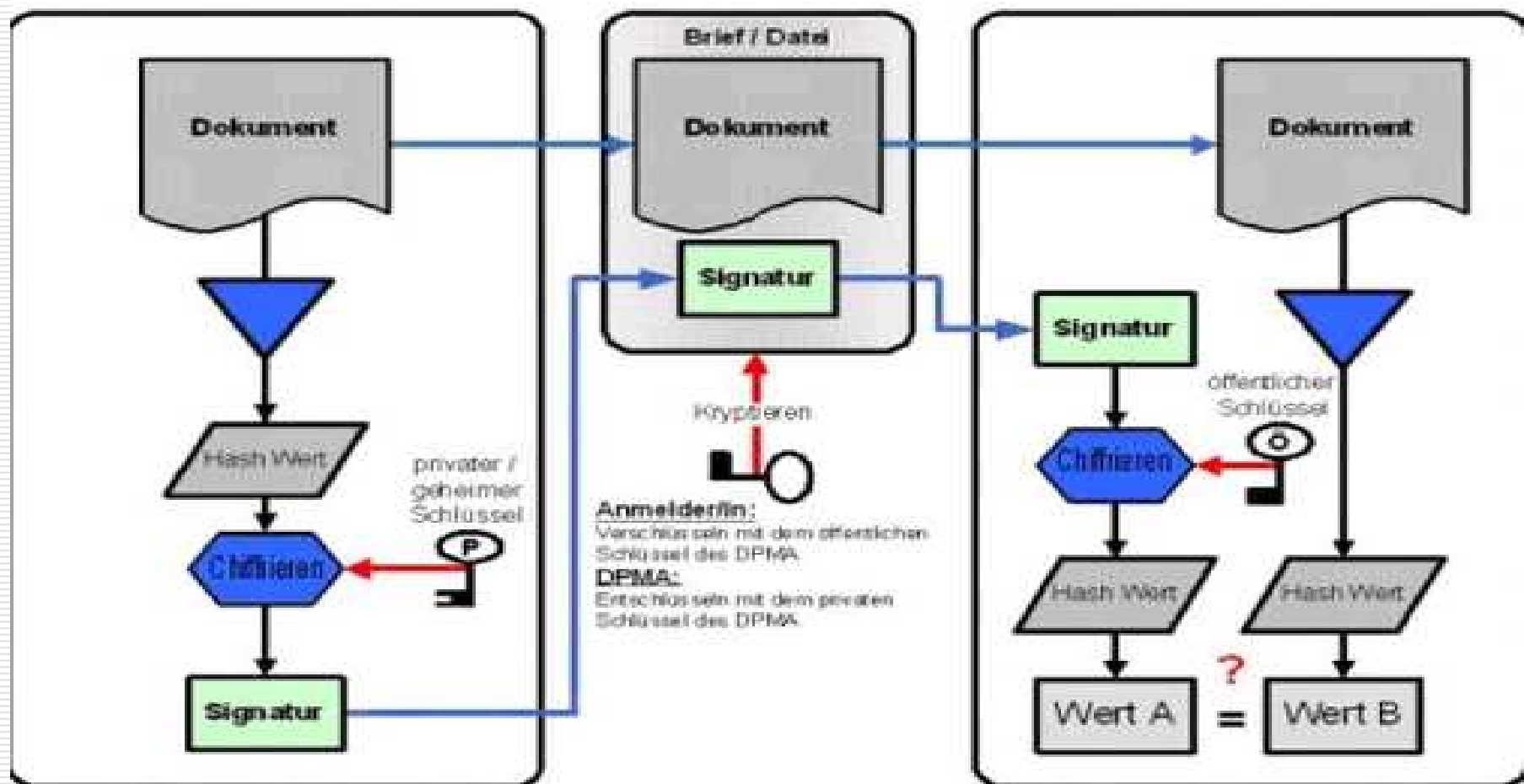
Digitale Signatur:

- kryptographisches Verfahren
- verschlüsselter Hashwert, der die Echtheit von Daten gewährleistet

Anmelder/In

versendete Datei

D P M A



## 2. Anwendungsbeispiele

---

- ❑ Übermittlung von Abrechnungen
  - ❑ elektronische Signaturen für eingescannte Dokumente, eingescannte Unterschriften sind nicht beweiskräftig
  - ❑ Zeitstempel
  - ❑ bei Willenerklärungen und Verträgen sind elektronische Signaturen nötig, z.B. in Onlineshops
-

## 3.1 Vorteile

---

- ❑ Entlastung, da Dokumente nicht ausgedruckt und eigenhändig unteschrieben werden müssen
  - ❑ die Echtheit von Dokumenten kann leicht überprüft werden
  - ❑ Absender sind schnell zu identifizieren
  - ❑ Anträge und Formulare können als E-Mail versendet werden → kopieren und sortieren nicht nötig
-

## 3.2 Nachteile

---

- Betrüger können Daten unter falschem Namen signieren
  - private Signaturschlüssel können entwendet werden
  - Signaturen können nur mit geeigneter Software überprüft werden
  - Prüfsoftware kann manipuliert sein
  - Fälschungen können zum Teil nicht erkannt werden
-

## 4. One-Way-Hash Funktion

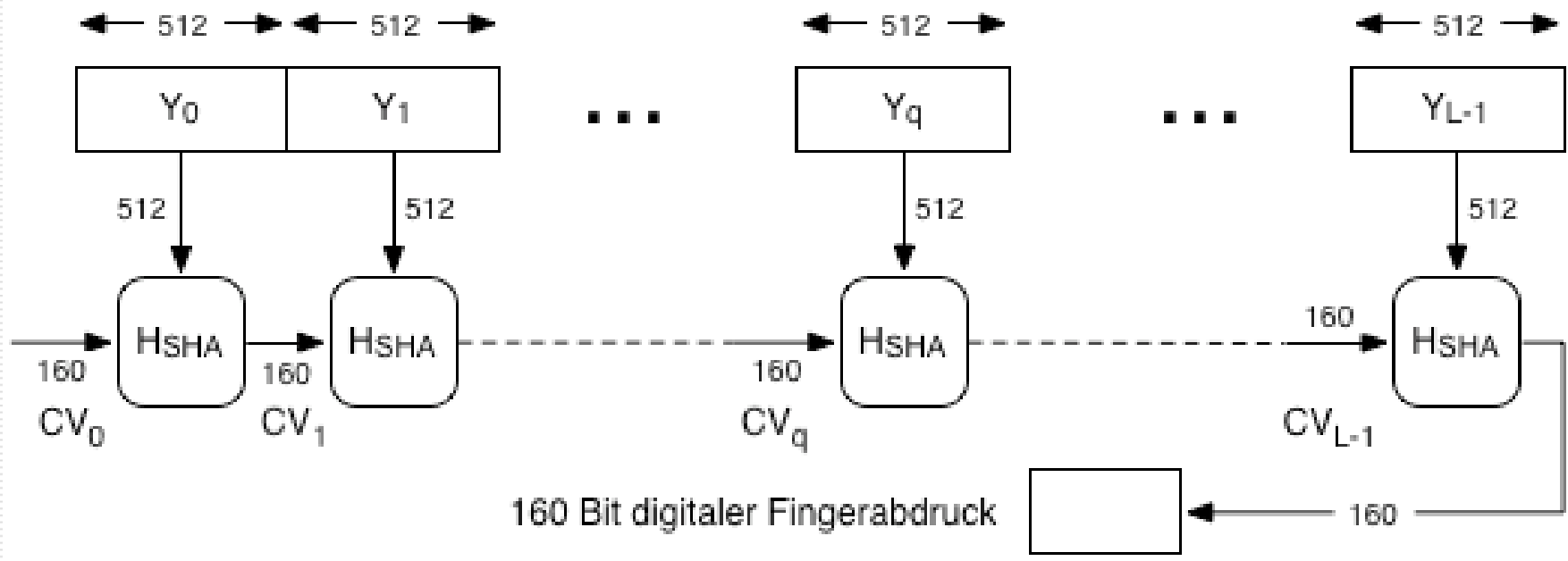
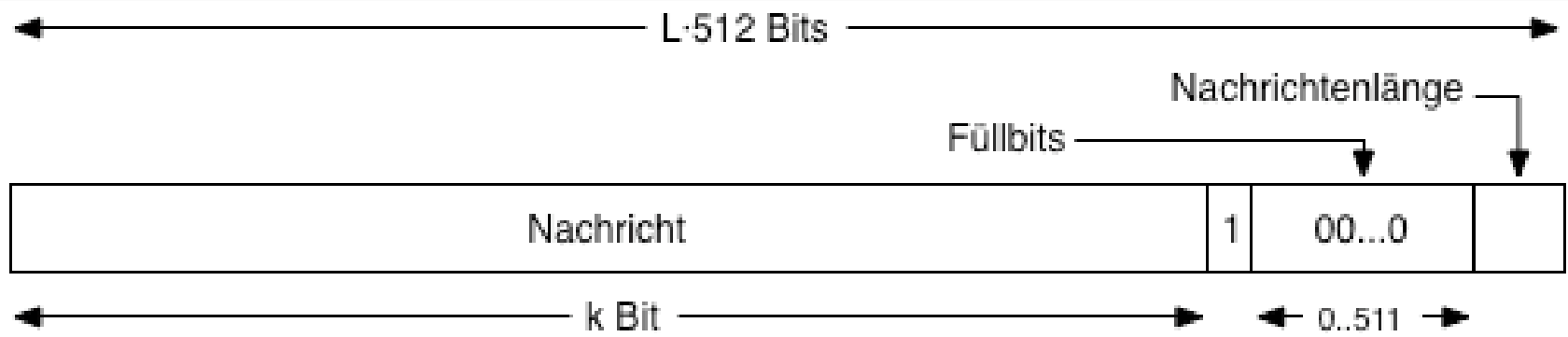
---

- ❑ Algorithmus, mit dem ein Text beliebiger Länge in einen Datenblock fester Länge umgewandelt wird
  - ❑ ein Rückschluss auf die Eingabe ist nicht möglich
  - ❑ arbeitet kollisionsfrei, zu jeder Eingabe wird genau eine Ausgabe erzeugt
-

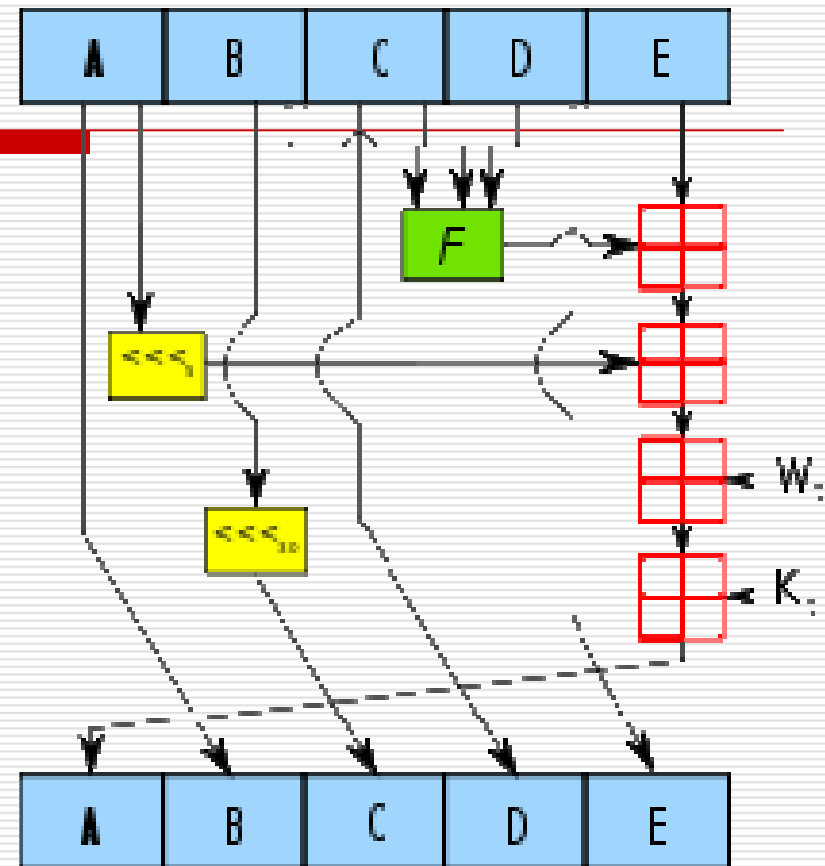
# Der Secure Hash-Algorithm

---

- ❑ Zerlegung der Nachricht in 512 Bit lange Blöcke
  - ❑ der letzte Block muss 448 Bit lang sein, wenn das nicht zutrifft werden Nullbits angehängt
  - ❑ die Nachrichtenlänge wird als 64-Bit-Zahl an den letzten Block gehängt
  - ❑ eine Funktion generiert nun aus jedem Block einen 160 Bit-Wert
  - ❑ aus vorherigem Block generierter 160 Bit-Wert wird als neue Eingabe verwendet
-



- Zerlegung der 512 in 16 32 Bit-Blöcke
- Erzeugung von weiteren 64 32 Bit-Blöcken
- Aufteilung der 160 Bit-Blöcke aus der Eingabe in 5 32 Bit-Blöcke und Verarbeitung mit den weiteren 32 Bit-Blöcken
- Die 160 Ausgabebits setzen sich aus Bits 5 verschiedener Blöcke zusammen → sehr sicher



# Quellen

---

- ❑ [http://www.dpma.de/images/service/e\\_dienstleistungen/dpmadirekt/grafik\\_signatur.jpg](http://www.dpma.de/images/service/e_dienstleistungen/dpmadirekt/grafik_signatur.jpg)
  - ❑ [http://de.wikipedia.org/wiki/Digitale\\_Signatur](http://de.wikipedia.org/wiki/Digitale_Signatur)
  - ❑ [http://de.wikipedia.org/wiki/Elektronische\\_Signatur](http://de.wikipedia.org/wiki/Elektronische_Signatur)
  - ❑ <http://signaturrecht.de/vorteilenachteile/vorteile/index.html>
  - ❑ <http://signaturrecht.de/vorteilenachteile/nachteile/index.html>
  - ❑ <http://www.signaturrecht.de/beispiele/index.html>
  - ❑ <http://ig.cs.tu-berlin.de/oldstatic/ap/rg/002/glossar/e-terms/einweghashfunktion.html>
  - ❑ <http://upload.wikimedia.org/wikipedia/commons/thumb/e/e2/SHA-1.svg/220px-SHA-1.svg.png>
  - ❑ <http://www.rwg-neuwied.net/informatik/sek2/krypt/digsign/sha1/page68.html>
-