

Thema 9:

Verfahren zur Gewährleistung der Integrität/Authentizität

Martin Völkel

Christian-Weise-Gymnasium Zittau



Gliederung

1. Elektronische und digitale Signatur
2. Vor- und Nachteile
3. Anwendung der Signaturen
4. Die One-Way-Hash Funktion
5. Quellen



1. Elektronische und digitale Signatur

elektronische Signatur:

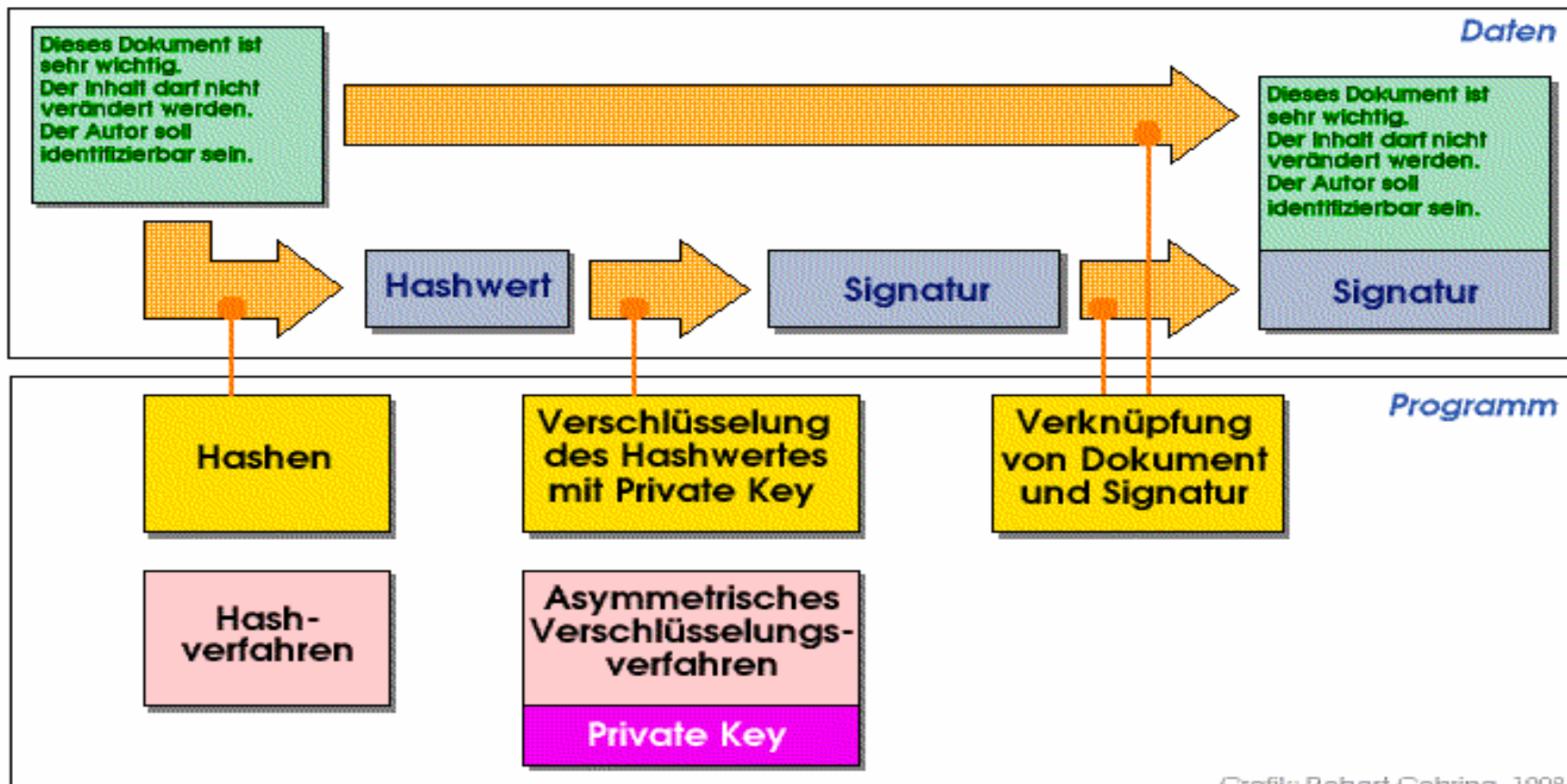
- Ist ein Rechtsbegriff, welcher im Signaturgesetz festgehalten wurde.
- elektronische Bestätigung oder Willenserklärung

digitale Signatur:

- technischer Begriff für elektronische Signatur
- ist ein verschlüsselter Hashwert für Daten
- man kann ablesen ob Veränderungen vorgenommen wurden

1. Elektronische und digitale Signatur

Signieren





2. Vor- und Nachteile

Vorteile:

- Anträge und Formulare müssen nicht eigenhändig Unterscriben werden
- wichtige Dokumente können leicht und sicher versendet werden
- bequeme Überprüfung des Absenders und der Echtheit des Dokuments
- Formulare und Anträge können schnell per E-Mail verschickt werden



2. Vor- und Nachteile

Nachteile:

- der Signaturschlüssel kann in falsche Hände geraten
- Signaturschlüssel können nur von speziellen Programmen überprüft werden
- Prüfprogramme können leicht umgangen werden
- Betrüger können unter falschen Namen Dokumente erstellen die als vertrauenswürdig erkannt werden



3. Anwendung der Signaturen

Personal <ul style="list-style-type: none">• Urlaubsantrag• Überstundenantrag• Dienstreisenabrechnung	IT-Infrastruktur <ul style="list-style-type: none">• Antrag auf Systemzugang• Änderung von E-Mail und Telefon• Bestellung von HW, SW, Services
Entwicklung und Produktion <ul style="list-style-type: none">• Freigabe Konstruktionszeichnungen• Prüfprotokolle• Qualitätssicherung• Produkthaftung	Einkauf <ul style="list-style-type: none">• Bestellungen• Dienstleistungsverträge• Einholen verbindlicher Angebote
Verkauf <ul style="list-style-type: none">• Abgabe verbindlicher Angebote• Vertragsabschlüsse	Finanzen <ul style="list-style-type: none">• Rechnungsstellung• Prüfung von Eingangsrechnungen• Umsatzsteuer (UStG)
Geschäftsleitung <ul style="list-style-type: none">• Geschäftsbriefe• Rundschreiben• Vertraulichkeitsvereinbarungen• Haftungsfragen	Formularwesen <ul style="list-style-type: none">• Antragsformulare• Formularprozesse



3. Anwendung der Signaturen

Öffentliche Verwaltung <ul style="list-style-type: none">• E-Government, E-Vergabe• ELSTER• EU-Dienstleistungsrichtlinie	Pharma & Medizintechnik <ul style="list-style-type: none">• Compliance 21 CFR Part 11• HIPAA
Energie <ul style="list-style-type: none">• Stromhandel• Emissionshandel	Gesundheitswesen <ul style="list-style-type: none">• Patientenakte• E-Rezept• Verwaltungsabläufe
Justiz <ul style="list-style-type: none">• Elektronischer Rechtsverkehr• Elektronisches Gerichts- und Verwaltungspostfach	Industrie <ul style="list-style-type: none">• Prozessautomatisierung• Compliance• Produkthaftung
Banken & Versicherungen <ul style="list-style-type: none">• Elektronischer Kontoauszug• Online-Banking	Telekommunikation <ul style="list-style-type: none">• Online Rechnungen• Behördenprozesse



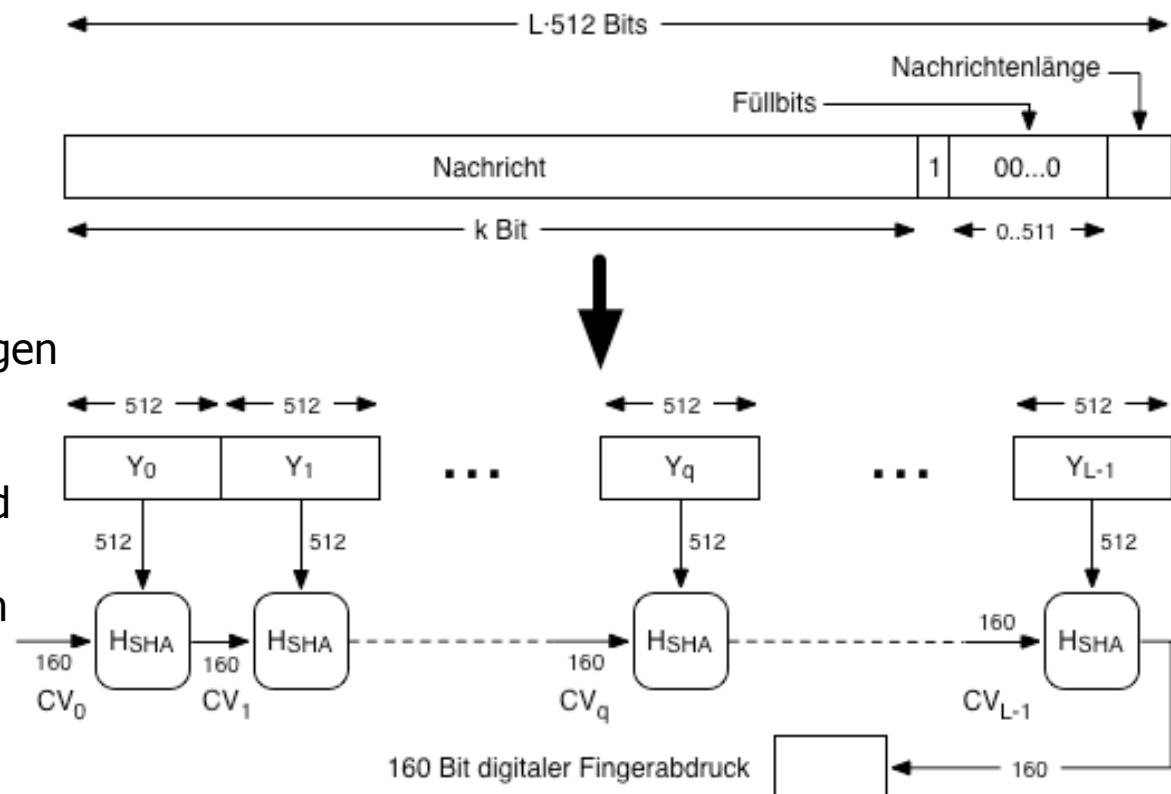
4. Die One-Way-Hash Funktion

- Hashfunktion aus dem engl. to hash (zerhacken)
- im deutschen Steuerwertfunktion
- ist ein kryptologisches Verfahren
- dienen zum Signieren von Dokumenten, oder als Prüfsumme um Veränderungen zu erkennen

4. Die One-Way-Hash Funktion

Der SHA -1 Algorithmus

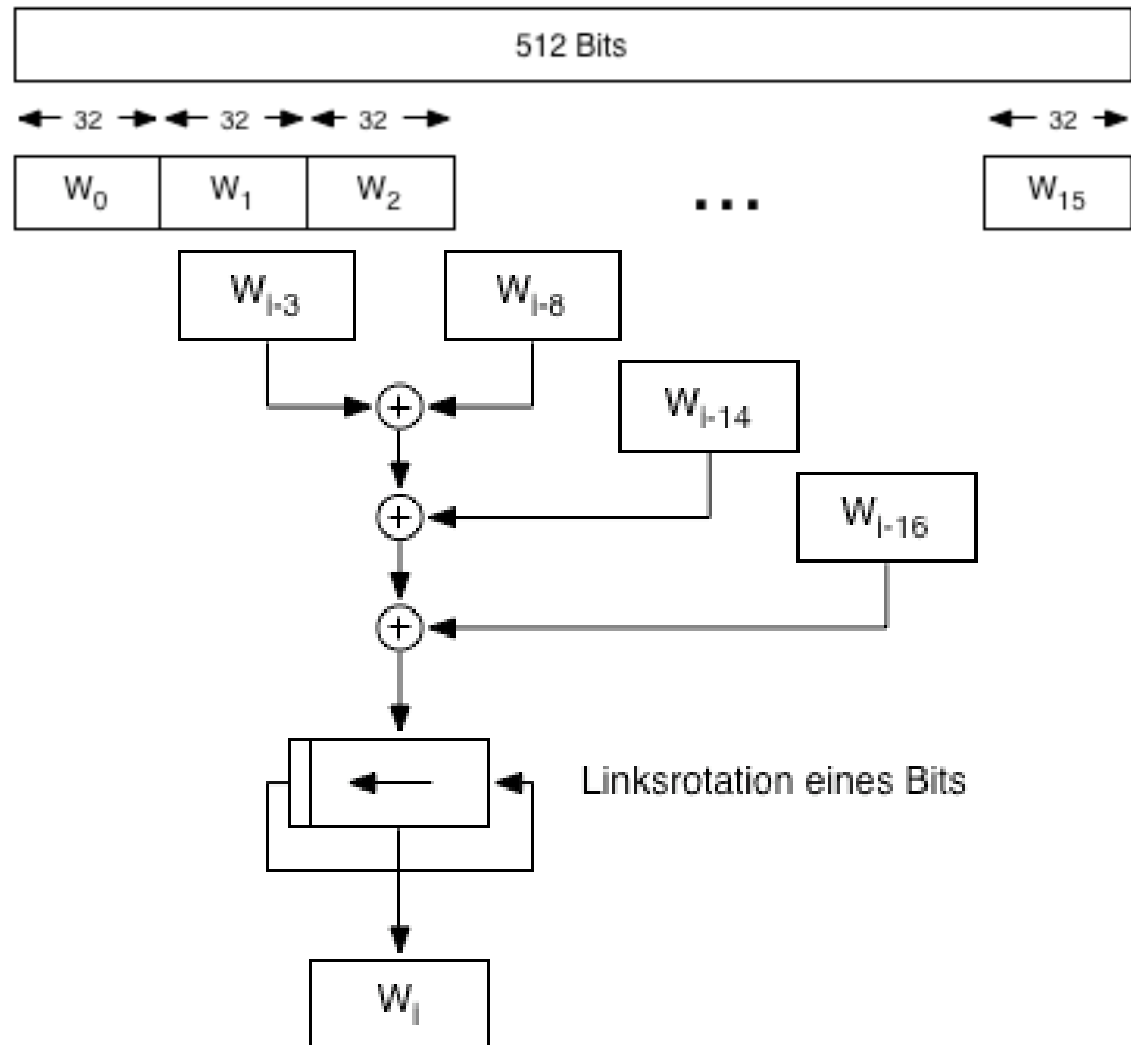
- Nachricht wird in 512-Bit-Blöcke zerlegt
- An diese Blöcke wird ein Bit mit dem Wert 1 drangehängt.
- Wenn letzter Block 448 Bit groß --> wird eine 64-Bit-Zahl angehängen
- Falls kleiner wird mit Nullbits
- Aufgefüllt bis 448 Bit erreicht sind
- Jeder Block wird an eine Funktion übergeben.
- 160-Bit-Wert wird generiert und dient später als Eingabe



4. Die One-Way-Hash Funktion

Die erzeugten 512-Bit-Blöcke werden weiter in 16 32-Bit-Blöcke zerlegt.

Anschließend werden 64 weitere 32-Bit-Blöcke erzeugt.





4. Die One-Way-Hash Funktion

Die Eingabe wird in 5 32-Bit-Blöcke geteilt.

Diese werden in 80 Durchgängen mit den Restlichen 32-Bit-Blöcken verarbeitet.

Die Ausgabe setzt sich aus den Bitblöcken a, b, c, d und e zusammen.

Durch mehrfache Teilung und Verarbeitung, kann man nicht mehr auf die Ausgangsnachricht schließen.

```
for i from 0 to 79
    if 0 ≤ i ≤ 19 then
        f := (b and c) or ((not b) and d)
        k := 0x5A827999
    else if 20 ≤ i ≤ 39
        f := a xor c xor d
        k := 0x6ED9EBA1
    else if 40 ≤ i ≤ 59
        f := (b and c) or (b and d) or (c and d)
        k := 0x8F1BBCDC
    else if 60 ≤ i ≤ 79
        f := a xor c xor d
        k := 0xCA62C1D6
    temp := (a leftrotate 5) + f + c + k + w(i)
    c := d
    d := c
```



5. Quellen

- https://docs.google.com/viewer?url=http://www.signature-perfect.de/docs/Leitfaden_Elektronische_Signatur.pdf&embedded=true&chrome=true
- <http://ig.cs.tu-berlin.de/oldstatic/ap/rg/1998-06/digitalesignatur-fol.gif>
- <http://www.digitalesignatur.org/digitale-signaturen-schutzen-vor-phishing/>
- <http://aktuell.de.selfhtml.org/artikel/internet/signatur/>
- <http://www.cryptoshop.com/index.php>
- <http://windows.microsoft.com/de-DE/windows-vista/What-is-a-digital-signature>
- <http://signaturrecht.de/vorteilenachteile/vorteile/index.html>
- <http://signaturrecht.de/vorteilenachteile/nachteile/index.html>
- https://docs.google.com/viewer?url=http://www.secardeo.de/Files/PDF-Files/SECARDEO-WP_Einsatz_Digitaler_Signaturen.pdf&embedded=true&chrome=true
- http://de.wikipedia.org/w/index.php?title=Datei:Hash_function_long.svg&filetimestamp=20051202013811
- <http://de.wikipedia.org/wiki/Hashfunktion>