Problemstellung digitale Signatur

Ziel(e) digitaler Signatur

- Nicht Bestreitbarkeit eines Rechtsvorgangs
- Vermeidung von Medienbrüchen
- weitesgehend automatisierte Abwicklung (Bestellungen, Sachbearbeitung, ...)
- Nachweisbarkeit der Durchführung einer Transaktion / Zustellung / Hinterlegung

Digitale Signatur ist ein Ausweis, der auch unterschriftstauglich ist

-

Technische Beschreibung

Schritt I: Hashverfahren

Schritt II: Personenbindung

Schritt III: Verifikation

Digitale Signatur ist nicht mit Verschlüsselung zu verwechseln!

-

Technik digitale Signatur

technischer Ablauf - Schritt I

Hashverfahren

Aus einem digitalen String (z.B. Vertragstext) wird ein Hashcode "Fingerprint" generiert

- Typische Techniken: SAH1, RIPEMD-160, MD5, ...)
- Typische Länge: 40 Byte und mehr
- kleine Änderungen im Text sollen starke Änderungen im Hashcode bewirken

Einsatzgebiete

- Sicherung der Authentizität eines Dokuments
- Änderungskontrolle

Einsatz nicht notwendigerweise personenbezogen!

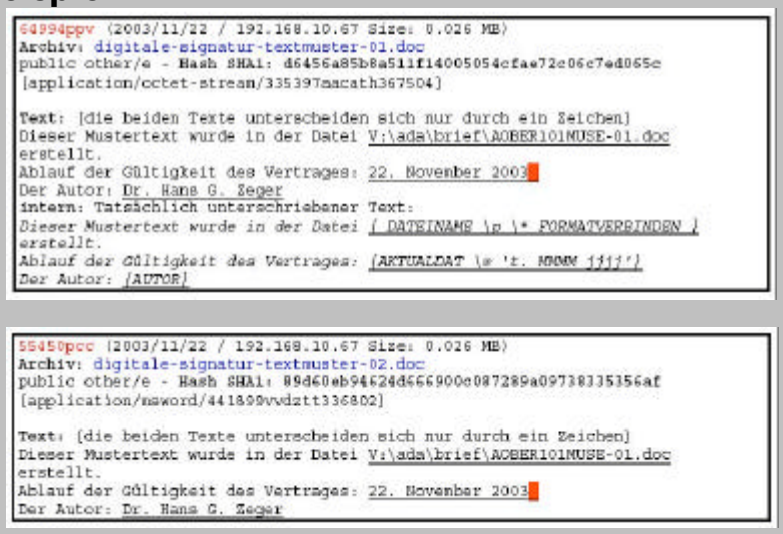
ARGE DATEN

Beispiel Hashanwendung:

11497vdd (2003/04/26 / 192.168.10.67 Size: 0.3 MB)
Original-Site: http://www.w3c.org/Consortium
Archiv: About the World Wide Web Consortium (W3C).pdf
public **legal/m** - **Hash SHA1: fa880f5e4eaf9e90756679bece43127f2a4eb8e0**
[application/pdf/707125hjhdnc651473]

Text: W3C Recommendations include:
(X)HTML: Several versions of HTML have stabilized the explosion in functionalities of the Web's primary markup language. HTML 3.2 was published January 1997, followed by HTML 4 (first published December 1997, revised Apr 1998, and revised again as HTML 4.01 in December 1999). XHTML 1.0, which features the semantics of HTML 4.01 using the syntax of XML, became a .....

Beispiel



Dokumente können mit beliebigen Programmen (sofern sie dieselben Hash-Techniken verwendeen) analysiert und der Hashcode verglichen werden (der eventuell über einen anderen Übertragungsweg übermittelt und verifiziert wird).

Probleme bei Hash-Erzeugung

- Sicherheit des Hash-Verfahrens
- Authentizität des Dokuments
- Beweisbarkeit des Zeitpunkts der Dokumentenprüfung
- Durchschaubarkeit des unterschriebenen digitalen Textes
- Empfindlich gegenüber Medienwechsel / Programmwechsel / Darstellungswechsel
- ein sicherer Hash-Code ist nicht merkbar (Länge und Aufbau)

- *Sicherheit des Hash-Verfahrens*

Wenn der Hash-Code fälschbar ist, sind alle Dokumente mit diesem Verfahren nicht mehr als fälschungssicher anzusehen.
MD5 wird nach heutigen stand der Technik als nicht sicher angesehen, SHA-1 und RIPEMD-160 werden gem. Signaturverordnung als sicher bis 31.12.2005 angesehen.

- *Authentizität des Dokuments*

Nachvollziehbarkeit, von wen ein Dokument tatsächlich stammt

- *Beweisbarkeit des Zeitpunkts der Dokumentenprüfung*

Meist wird nicht bestritten, dass überhaupt etwas unterschrieben wurde, sondern wann genau was angeboten, akzeptiert und unterschrieben wurde (etwa Sonderangebote, Auftragsbestätigungen, Einbringungsfristen, Kündigungstermine, ...).

- *Durchschaubarkeit des unterschriebenen digitalen Textes*

Bekannte Office-Produkte produzieren einen digitalen String, der sich bei Anzeige ändert. Daher besteht die Erfordernis eines "secure viewers".

- *Empfindlich gegenüber Medienwechsel / Programmwechsel / Darstellungswechsel*

Schon kleinste, für eine Vereinbarung irrelevante Beifügungen, etwa ein zusätzlicher Zeilenumbruch, ein Leerzeichen usw. verändern den Text. Dies passiert etwa sehr leicht bei der e-mail-Übertragung

- *ein sicherer Hash-Code ist nicht merkbar (Länge und Aufbau)*

Bei jeder Dokumentenverwendung müßte eine Prüfung durchgeführt werden, erfolgt jedoch nicht immer. Meist "Vertrauen" die Teilnehmer der Richtigkeit.

technischer Ablauf - Schritt II

Personenbindung

Hashcode wird mit persönlichem Code ("privater Schlüssel") verknüpft

- Methode: asymetrische Verschlüsselung
- Typische Techniken: RSA (eingesetzt in Programmen wie PGP, sMIME, ...), DSA

-

Beispiel

```
-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA1

Dies ist ein Kunsttext, der zu Demonstrationszwecke
mittels einer PGP-Signatur unterschrieben wurde.

-----BEGIN PGP SIGNATURE-----
Version: PGP Personal Edition 6.0.2

iQA/AwUBOcm/3yR73vxnG7lfEQKA6QCg4UWGogP3qR094fUQ+UrG1HeN7EAAnOEK
bgfJwTsqbVPool/7iK6zW8gy
=3Lc0
-----END PGP SIGNATURE-----
```


-

Probleme bei Personenbindung

- Sicherstellung der Identität des Unterzeichners
- Sicherstellung der Willenserklärung
- Keine Nachahmbarkeit/Verfälschbarkeit des Schlüssels

Personenbindung wird praktisch immer durch Kombination von Besitz und Wissen erreicht

- *Sicherstellung Identität des Unterzeichners*

Erfolgt in der Regel durch Ausweiskontrolle und Unterschrift bei Ausgabe/Verifizierung des Schlüssels durch eine Zertifizierungsstelle.
Rechtsgrundlage: Signaturgesetz + privatrechtliche Vereinbarung
Weiters wird der elektronische Schlüssel von der Zertifizierungsstelle unterzeichnet.

- *Sicherstellung der Willenserklärung*

Erfolgt in der Regel durch zwingende Eingabe einer Aktivierungscodes (Passphrase, PIN, Paßwort, ...)

- *Keine Nachahmbarkeit/Verfälschbarkeit des Schlüssels*

Erfolgt in der Regel durch hardwaretechnische Maßnahmen, wie Chipkarten, Sim-Karten, (USB-)Token oder vergleichbare Techniken
Private Schlüssel werden in System "eingeschlossen" und sind nicht mehr abrufbar

Dokumente werden auf Chipkarte geladen, unterfertigt und retourniert, nicht umgekehrt. Was im Detail auf der Karte passiert, weiß nur der Systemdesigner!

technischer Ablauf - Schritt III

Verifikation (Übermittlung / Prüfung)

Originaltext und Anhang werden gemeinsam (oder auch getrennt) übermittelt

- öffentliche Schlüssel zur Prüfung notwendig
- öffentliche (sekundenaktuell) geführte Vrezeichnisse notwendig
- vertrauenswürdige Bestätigungsstellen notwendig
- einheitlicher Zeitstandard notwendig

-

Beispiel Zertifikat

```
Zertifikatsprüfung [a-sign-Premium-Enc-01]
Titel Dipl-Ing. Dr. Techn.
Name Reinhard Posch
Seriennummer 1A00
CIN 859852035747
Gültig von 24.02.2003 11:06:24
Gültig bis 24.02.2006 11:06:24
Status OK
```

Beispiel öffentlicher Schlüssel

```
Type Bits/KeyID    Date       User ID
pub  1024/14CBB955 1997/09/25 Meldestelle SOKO Briefbomben <SOKO-Briefbomben>

-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: 2.6.3i

mQCNAzQqmqsAAAEEALjmeRsGP+y32j4rn39bdXnoKT0utYo42+ZZt8CGHjqXq8ea
y1+rlI74w8Yf2soCTAlhcLaHzdB1RND69nPjI998P1MxeMwY0DHj435UpG7+1Wzi
2Gw+rWJV9C1uUpm8yIkuCjV2uCOu/dew8eROyu7f9MLL7UXPJhcv1XgOy71VAAUZ
tC9NZNkkZXN0ZWxzIEBTTOtPIEJyaWVnYm0tYmVuIDxTT0tPLUJyaWVnYm9tYmVu
PokA1QMFEDQqmqwcb414FMu5VQEB+MkD+wf/X+4+UVBJDUdSrXkOrPaOwIqGFnK5
IRjJnj7marS12NNVu0qy+hExCeXPHLzsWQOVBdwC7wKYR/XO1zxal6C/34n88bnO
1edNA9zG4qPqvvDRbKngH2HvjNDh9pTdNFRIPiLL5LI7spPd5HOHgnwYnsDPHFDE
clRnsAzYA3GS
=nw7h
-----END PGP PUBLIC KEY BLOCK-----
```


-

Probleme bei Prüfung

- Durchschaubarkeit der Authentisierung
- Zuverlässigkeit des Betreibers öffentlicher Verzeichnisse

Authentisierungsstelle und Verzeichnisverwalter müssen nicht ident sein!

- *Durchschaubarkeit der Authentisierung*

Der Empfänger muß darauf vertrauen können, dass Zertifizierungsstelle korrekt gearbeitet hat. Wie zuverlässig erfolgte die Identitätsprüfung bei der Schlüsselvergabe?

- *Zuverlässigkeit des Betreibers öffentlicher Verzeichnisse*

Wie aktuell und sicher abrufbar sind die öffentlichen Verzeichnisse?

digitale Signatur - Grenzen

Grundsätzliche Unterschiede digitaler/natürlicher Signatur

- keine unmittelbare Einsichtigkeit des Vorgangs (technische Vermittlung)
- Ablaufdatum der Gültigkeit
- Abhängigkeit von technicher Infrastruktur Dritter

- **keine Synchronität** zwischen Ausweisleistung und Willenserklärung

digitale Unterschriften werden niemals persönlichen Unterschriften gleichzusetzen sein

ARGE DATEN

Auf Grund der grundsätzlichen Unterschiede wird es niemals zu einer Gleichsetzung kommen.

Es sind jedoch Szenarien vorstellbar, in denen eine digitale Unterschrift höhere Beweiskraft zukommt, als eine persönliche. Etwa dann, wenn die Ermittlung eines exaktenZeitpunkts einer verteilt abgegebenen Willenserklärung notwendig ist.