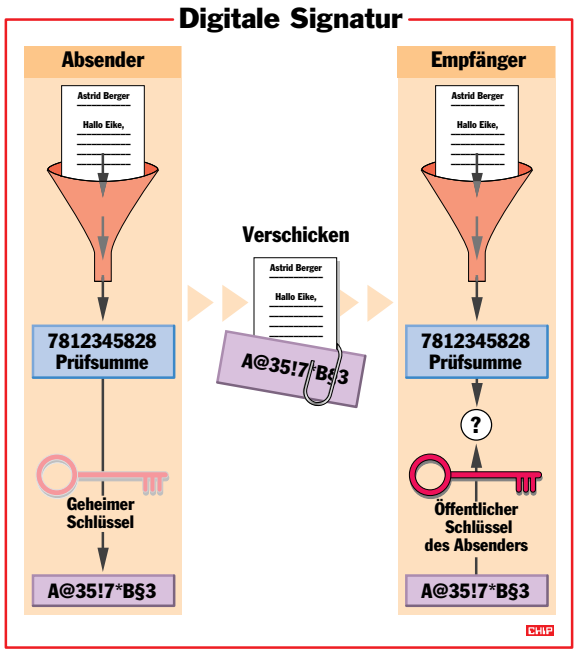
# Echter geht's nicht mehr

Dünnes Eis für Telebanker und Online-Shopper: Woher wissen sie, wer am anderen Ende der Leitung sitzt? Die digitale Unterschrift soll alle Zweifel beseitigen.




**Nicht zu fälschen: Die beigefügte digitale Unterschrift paßt nur zum Originaldokument und zum Geheimschlüssel des Absenders**

Es geht ums Ganze: Wenn Authentizität und Integrität digitaler Informationen nicht garantiert sind, ist jeder Online-Vertragsabschluß eine Farce. Die nötige Sicherheit könnten digitale Signaturverfahren bringen. Eine digitale Information – egal, ob Software, Bild- oder Textdatei – erhält dabei eine kurze verschlüsselte Zeichensequenz als Zugabe. Der Empfänger der Datei kann damit nicht nur wie bei der handschriftlichen Unterschrift überprüfen, wer die Nachricht verfaßt hat, sondern sogar, ob sie unverändert ist.

„Das verbreitetste und derzeit noch sicherste ist das RSA-Verfahren", meint Jutta Stolp, Pressesprecherin des auf Datensicherheit spezialisierten Unternehmens Utimaco Safeware aus Oberursel. Die nach ihren Erfindern Ronald L. Rivest, Adi Shamir und Leonard Adleman benannte Methode benutzt zwei unterschiedliche Schlüssel: Jeder Teilnehmer verfügt über einen öffentlich bekannten und einen geheimen Schlüssel.

## 0 Jede Unterschrift ist anders

Für die elektronische Unterschrift verschlüsselt der Absender nicht die komplette Nachricht, sondern eine für das Dokument berechnete charakteristische Prüfsumme (siehe Grafik). Im Gegensatz zu einer Unterschrift von Hand ist also keine elektronische Unterschrift gleich, sie verändert sich mit jeder Nachricht.

Der Empfänger entschlüsselt die Prüfsumme mit dem öffentlichen Schlüssel des Absenders und erhält so einen bestimmten Wert. Diesen Wert vergleicht er mit der aus dem Dokument selbst ermittelten Prüfsumme. Stimmen beide überein, so ist die Nachricht unversehrt und ihre Herkunft eindeutig.

Das Verfahren ist elegant und wirkungsvoll, doch die Probleme liegen an anderer Stelle: Welche vertrauenswürdige Instanz erzeugt das Schlüsselpaar? Wo wird der geheime Schlüssel unzugänglich gespeichert? Wer garantiert, daß der öffentliche Schlüssel von Herrn Maier tatsächlich der seine ist und nicht der von Herrn Schmidt?

Des Problems der Zertifizierung durch vertrauenswürdige Instanzen („Trust Center") ist sich der Gesetzgeber durchaus bewußt. Daher wird das derzeit diskutierte „Informations- und Kommunikationsdienstegesetz" (ehemals „Multimediagesetz" genannt) mit der Regelung der digitalen Signatur auch einen Vorschriftenkatalog für die Zulassung solcher Zertifizierungsinstanzen vorsehen. Diese Aufgabe sollen „privatrechtlich organisierte Instanzen übernehmen, etwa Banken oder Notare, wenn sie die Anforderungen an die Vertrauenswürdigkeit erfüllen", so Marit Blattner-Zimmermann vom Referat für Sicherheit in der Informationstechnik im Bundesinnenministerium.

Außerdem wollen die Beamten mit dem Gesetz eine „vergleichbare Rechtssicherheit wie bei herkömmlichen Dokumenten" schaffen. Dabei gehe es nicht um „technische Vorschriften", sondern darum, Fälschungen der Urheberschaft vorzubeugen, betont die Referatsleiterin. Ein digitales Dokument solle vor dem Gesetz behandelt werden wie eine Urkunde.

Dies halten manche Fachleute allerdings für bedenklich, wenn absolute Sicherheit für die Schlüssel nicht erreichbar ist. Eine gefälschte Handschrift kann wenigstens im Prinzip der Gerichtssachverständige entlarven; eine mit gestohlenem Geheimschlüssel erzeugte digitale Unterschrift ist dagegen nicht als Fälschung erkennbar.

*Jan Vollmuth*

Albrecht Beutelspacher: Kryptologie, Vieweg-Verlag, ISBN 3-528-28990-2

Friedrich L. Bauer: Kryptologie, Springer-Verlag, ISBN 3-540-57771-8