

Sicher Surfen V: Digitale Signaturen

Georg Wagner

25. Mai 2001

1 Wozu dienen Digitale Signaturen?

Digitale Signaturen haben zwei Aufgaben:

- Prüfen der Integrität einer Nachricht oder Datei, d.h. mithilfe einer *Digitalen Signatur* lässt sich feststellen, ob eine Nachricht/Datei absichtlich oder unabsichtlich verändert wurde.
- Prüfen der Authentizität einer Nachricht; der Urheber einer Nachricht lässt sich verifizieren.

2 Was ist eine Digitale Signatur?

Wenn Sie verstehen wollen, wie eine *Digitale Signatur* funktioniert, müssen Sie zuerst wissen, was sich hinter dem Begriff *Kryptographische Prüfsumme*¹ verbirgt.

2.1 Die Kryptographische Prüfsumme

Die *Kryptographische Prüfsumme*² ist nichts anderes als eine Zahl. Interessant ist, wie diese Zahl gebildet wird: Eine spezielle mathematische Funktion³ nimmt eine Eingabe variabler Länge entgegen und reduziert diese Eingabe zu einer kleinen Zahl fester Länge. Bei der gleichen Eingabe erhalten Sie immer die gleiche Zahl als Ergebnis. Diese Funktion hat zwei wichtige Eigenschaften:

1. Das Ergebnis der Funktion kann nicht verwendet werden, um die Eingabe zu bestimmen, die Funktion lässt sich also nicht umkehren⁴.
2. Die zweite Eigenschaft ist, dass eine kleine Änderung in der Eingabe zu grossen Änderungen im Ergebnis führen.

¹In der englischen Fachliteratur werden die Begriffe Message Digest, fingerprint, cryptographic checksum oder cryptographic hashcode synonym verwendet.

²Sie wird in der deutschen Fachliteratur auch als Komprimat oder Extrakt bezeichnet.

³Eine sogenannte Hash-Funktion

⁴Wie im realen Leben gibt es auch in der Mathematik Dinge, die schwer rückgängig zu machen sind. Sie können ganz leicht eine Porzellanvase aus 10 Metern Höhe auf einen Betonboden fallen lassen. Die Scherben wieder zu einer intakten Vase zuasammensetzen, dürfte nahezu unmöglich sein.

Sie können sich sicher bereits denken, wozu eine *Kryptographische Prüfsumme* verwendet werden kann. Sie können ein Dokument elektronisch publizieren, es also im Internet verteilen. Gleichzeitig verteilen Sie auch die *Kryptographische Prüfsumme*. So kann jeder der Ihr Dokument aus dem Internet bezieht, die gleich mathematische Funktion auf Ihr Dokument anwenden. Er erhält die *Kryptographische Prüfsumme* und vergleicht sie mit der von Ihnen publizierten. Sind beide Prüfsummen identisch, muss das bezogene Dokument dem Original entsprechen; ist also nicht verfälscht worden.

Aber niemand hindert einen Fälscher daran, Ihr Dokument aus dem Internet herunterzuladen, es zu verändern, eine neue *Kryptographische Prüfsumme* zu berechnen und beides wieder in Internet einzuspeisen. Die *Kryptographische Prüfsumme* allein reicht also nicht aus, da Ihre Urheberschaft noch nicht mit dem Dokument verknüpft ist.

2.2 Von der Kryptographischen Prüfsumme zur Digitalen Signatur

Erinnern Sie sich an die asymmetrische Kryptographie. Sie hängt von zwei Schlüsseln ab:

1. Dem öffentlichen Schlüssel: Er wird zum Verschlüsseln einer Nachricht verwendet. Wird normalerweise weit verteilt.
2. Der geheime/private Schlüssel: Er wird geheimgehalten und normalerweise zum Entschlüsseln einer Nachricht verwendet.

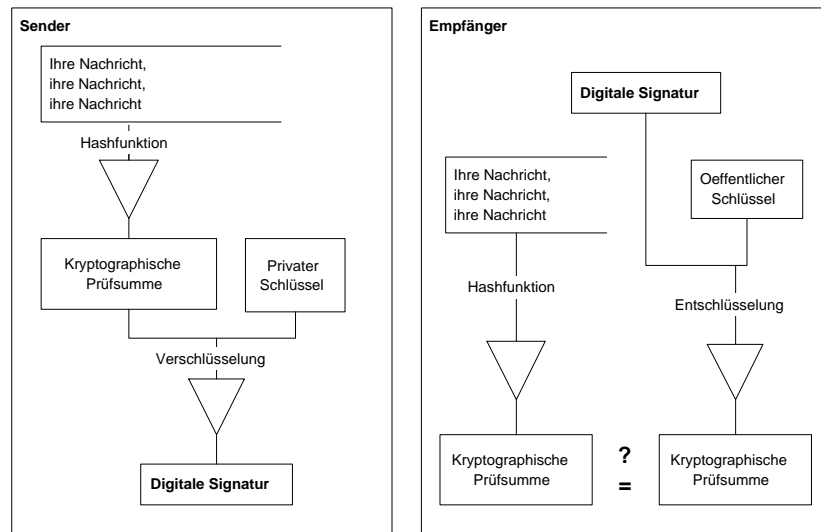
Nun erinnern Sie sich sicher, dass ich Sie gewarnt habe, nie eine Nachricht mit Ihrem geheimen Schlüssel zu verschlüsseln, da jeder, der Ihren öffentlichen Schlüssel hat, diese dann entschlüsseln kann. Genau diese Eigenschaft wird nun bei der *Digitalen Signatur* ausgenutzt. Denn es gibt zu jedem öffentlichen Schlüssel genau einen privaten Schlüssel. Wenn also eine Nachricht mit Ihrem öffentlichen Schlüssel entschlüsselt werden kann, dann muss sie mit Ihrem privaten Schlüssel verschlüsselt worden sein.

Das heisst, Sie haben Ihre Nachricht signiert. Warum wird aber dann die *Kryptographische Prüfsumme* verwendet? Das Verschlüsseln einer längeren Nachricht mit Ihrem geheimen Schlüssel würde sehr viel Zeit in Anspruch nehmen. Stattdessen wird zuerst die *Kryptographische Prüfsumme* gebildet, die Sie dann mit Ihrem geheimen Schlüssel verschlüsseln. Die mit Ihrem geheimen Schlüssel verschlüsselte *Kryptographische Prüfsumme* ist also Ihre *Digitale Signatur*.

3 Detaillierte Darstellung des Verfahrens

Die einzelnen Schritte beim Erstellen und Prüfen einer *Digitalen Signatur* werden im folgenden beschrieben:

1. Sie schreiben Ihre Nachricht.
2. Dann lassen Sie die *Kryptographische Prüfsumme* erstellen.
3. Diese verschlüsseln Sie mit Ihrem geheimen Schlüssel. Dies ist die *Digitale Signatur* Ihrer Nachricht.

Abbildung 1: Erstellen und Prüfen einer *Digitalen Signatur*

4. Sie hängen die Digitale Signatur an Ihre Nachricht an und versenden Sie an den Empfänger.
5. Der Empfänger zerlegt Ihre Email wieder in Ihre Nachricht und Ihre *Digitale Signatur*.
6. Dann bildet er die *Kryptographische Prüfsumme* Ihrer Nachricht.
7. Zum Schluss entschlüsselt er Ihre *Digitale Signatur* mit Ihrem öffentlichen Schlüssel und erhält so die von Ihnen gebildete *Kryptographische Prüfsumme*.
8. Er vergleicht die beiden *Kryptographischen Prüfsummen* miteinander. Sind sie identisch, dann muss die Nachricht von Ihnen stammen. Ausserdem kann er sicher sein, dass die Nachricht auf dem Weg durch das Internet nicht verändert wurde.

Im oben beschriebenen Verfahren wurde die Nachricht zwar mit einer *Digitalen Signatur* versehen, aber die Nachricht selber wurde offen versendet. Sie können natürlich die Nachricht mitsamt der *Digitalen Signatur* vor dem Versenden noch mit dem öffentlichen Schlüssel des Empfängers verschlüsseln. Dann kann nur der Empfänger Ihre Nachricht lesen.

4 Die Digitale Signatur in der Praxis

4.1 Vorteile der Digitalen Signatur

- In der *Digitalen Signatur* ist gegenüber einer Handunterschrift Information über das signierte Dokument enthalten. Nachträgliche Änderungen an dem Dokumenten werden also bemerkt.

- Die Echtheit⁵ des Absenders ist nachweisbar.
- Mit der *Digitalen Signatur* können auch geistiges Eigentum und Urheberrechte signiert werden.
- Die *Digitale Signatur* ist nicht nachahmbar.
- Die *Digitale Signatur* ist einfach zu leisten.

4.2 Geplante Einsatzgebiete

In Deutschland wurde mit dem Signaturgesetz bereits ein rechtlicher Rahmen für den Einsatz der *Digitalen Signatur* geschaffen, In folgenden Bereichen ist der Einsatz der *Digitalen Signatur* geplant:

- bei Banken
- in Grundbuchämtern
- im Gesundheitswesen, um die Integrität von Krankheitsgeschichten zu garantieren,
- Behörden, Handel, Wirtschaft, Versicherungswesen und Industrie.

Die Liste liesse sich beliebig erweitern.

4.3 Die Zertifizierungsinstanz

Es muss eine unabhängige und vertrauenswürdige Instanz geben, die beglaubigt, dass ein öffentlicher Schlüssel zu einer bestimmten Person gehört. Diese Instanz spielt für die Glaubwürdigkeit der *Digitalen Signatur* eine zentrale Rolle. In Deutschland müssen solche Stellen daher speziell genehmigt werden.

4.4 Im realen Einsatz

Der beschriebene Ablauf bei der *Digitalen Signatur* sieht sehr umständlich und arbeitsintensiv aus. In der Praxis sind aber alle Abläufe automatisiert. Das Signieren geschieht beim Senden einer Nachricht auf Knopfdruck, die Überprüfung beim Empfang ist sogar vollautomatisch.

Für den privaten Gebrauch hat sich das Paket *Pretty Good Privacy* (PGP) als Quasi-Standard etabliert.

⁵Authentizität