

Prof. Dr. Norbert Pohlmann, Malte Hesse

Kryptographie: Von der Geheimwissenschaft zur alltäglichen Nutzanwendung (V) – Prüfsummen, Zertifikate und die sichere elektronische Signatur

Die handschriftliche Unterschrift ist seit Jahrhunderten bewährt. Anders als in der elektronischen Welt sind bei einem Vertragsabschluss die Parteien zugegen und können den Vertragspartner persönlich einschätzen und überprüfen. Dies grenzt auf natürliche Weise den Aktionsradius für Betrüger erheblich ein. In der elektronischen Welt können wir nicht auf diese bewährten Mechanismen zurückgreifen, da wir z. B. über das Internet lediglich indirekt kommunizieren. Daher müssen grundlegende Sicherheitsbedürfnisse anders befriedigt werden als in der realen Welt.

Einem Bericht des Bundeskriminalamtes zur Entwicklung der Wirtschaftskriminalität 2005 lässt sich entnehmen, dass die Zahl der mit Hilfe des Internets begangenen Delikte gegenüber dem Vorjahr um 73,1 Prozent gestiegen ist. Der Bericht geht weiter davon aus, dass „diese Entwicklung sich im Zuge der weiteren Verbreitung und zunehmenden Nutzung des Internets fortsetzen dürfte.“ Elektronische Signaturen können helfen, diesen Prozess zu stoppen, werden aber beispielsweise bei den für Betrügereien besonders beliebten Onlineauktionen noch zu selten bzw. gar nicht eingesetzt.

Die elektronische Signatur soll zweierlei leisten, nämlich die Identität eines Benutzers, also etwa des Absenders einer E-Mail, bestätigen und nachweisen, dass eine Nachricht auf dem Weg zum Empfänger nicht verändert worden ist (Integritätsschutz). Dafür ist die mathematische Verknüpfung eines asymmetrischen Schlüsselpaar mit der Identität eines Benutzers sowie einer Nachricht mit dem bei einem Verschlüsselungsvorgang entstehenden Wert erforderlich. Wie dieser Prozess funktioniert, wollen wir in diesem Artikel erläutern.

Prüfsummenbildung und One-Way-Hashfunktionen

Auch wenn die elektronische Signatur sich im elektronischen Geschäftsverkehr nur sehr zögerlich durchsetzt, bietet sie gegenüber der eigenhändigen Unterschrift doch einige entscheidende Vorteile. Der wichtigste darunter ist, dass sie – anders als ihr „analoges“ Gegenstück – benutzt werden kann, um die Integrität, also die Unverletztheit des unterzeichneten Dokuments, zu prüfen und zu bestätigen. Mit anderen Worten: Manipulationen lassen sich schnell und mit verhältnismäßig geringem Aufwand feststellen. Leider sind die dabei verwendeten asymmetrischen Operationen sehr aufwändig und damit langsam in der Ausführung (vgl. dazu Teil IV dieser Reihe in Heft 9/2006). Außerdem wird noch einmal genau so viel Speicherplatz für die Signatur benötigt wie für den Klartext.

In der Praxis wird daher nicht die eigentliche Nachricht signiert, sondern lediglich eine charakteristische, kryptographische Prüfsumme (Hashwert), die gleichsam deren „Konzentrat“ bildet. Dazu wird die Nachricht an eine One-Way-Hashfunktion übergeben, welche die Prüfsumme bildet (vgl. Abb. 1).

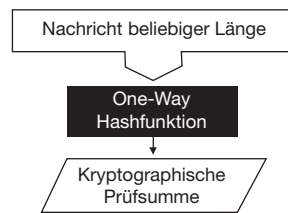


ABB. 1: Berechnung einer kryptographischen Prüfsumme

Die One-Way-Hashfunktion berechnet aus einer beliebig umfangreichen Nachricht eine kryptographische Prüfsumme (Hashwert) mit einer zuvor festgelegten Länge. Dabei gilt die Formel

$$h = H(M)$$

– wobei h die Prüfsumme (den Hashwert), H die One-Way-Hashfunktion und M die Nachricht bezeichnet.

Eine Hashfunktion muss also bestimmte Eigenschaften aufweisen, damit sie für den kryptographischen Einsatz taugt. So zählt sie immer zur Gruppe der kontrahierenden Einwegfunktionen, mit deren Hilfe sich der Umfang der Prüfsumme (Hashwert) auf eine definierte Länge reduzieren lässt. Gleichzeitig stellt sie sicher, dass nicht von der Prüfsumme auf den Klartext geschlossen werden kann. Es existiert also keine Funktion $f()$, mit der der Inhalt der Nachricht M aus dem Hashwert h wieder hergestellt werden kann:

$$M \neq f(h)$$

Weiterhin muss eine One-Way-Hashfunktion kollisionsresistent sein, d. h. es darf nicht möglich sein, systematisch eine bestimmte Prüfsumme $h = H(M')$ zu erzeugen, die derjenigen der ursprünglichen Nachricht entspricht. Anders ausgedrückt: Es muss praktisch unmöglich sein, zu einer gegebenen Nachricht M eine weitere Nachricht M' mit identischem Wert zu finden; die Gleichung $H(M) = H(M')$ darf nie zutreffen.

Die Kollisionsresistenz verhindert, dass Signaturen für beliebige Nachrichten gelten bzw. diese systematisch so gestalten werden, dass eine gewollte Prüfsumme entsteht. Andernfalls ließe sich eine vorhandene signierte Nachricht gezielt ersetzen oder manipulieren, ohne dass man dies nachweisen könnte. Ferner spielt hier die Prüfsummenlänge eine wichtige Rolle: Zwar sollte ein Hashwert kurz sein, allerdings darf es nicht zu leicht sein, Kollisionen zu finden. Aufgrund der ständig zunehmenden Rechenleistung moderner Computer ist jedoch abzusehen, dass solche Kollisionen für derzeit verwendete Prüfsummenlängen in einigen Jahren gezielt errechnet werden können. Das eröffnet erhebliche und bisher unzureichend gelöste Probleme im elektronischen Geschäftsverkehr, besonders bei Verträgen mit langer Laufzeit und bei der Langzeitarchivierung. Der MD5 mit einer Prüfsummenlänge von 128 Bit, der in vielen Standards noch angegeben ist, sollte jedenfalls nicht mehr verwendet werden.

Wie für jeden Verschlüsselungsalgorithmus gilt auch für One-Way-Hashfunktionen, dass sie öffentlich bekannt sein sollten: Das ist einerseits notwendig, da sie auf allen an einem Datenaustausch beteiligten Systemen verfügbar sein müssen, andererseits garantiert nur die öffentliche Bekanntheit ihre genaue Begutachtung durch Experten.

Wichtigster Vorteil einer One-Way-Hashfunktion ist, dass sie sehr viel schneller zu berechnen ist als eine asymmetrische Verschlüsselung und in der Regel auch schneller arbeitet als symmetrische Verfahren. Bekannte und gebräuchliche One-Way-Hashfunktionen sind z. B. SHA-1 und RIPEMD160. Beide haben derzeit Schlüssellängen von 160 Bit.

Zertifikate

Ein Problem mit öffentlichen Schlüsseln ist, dass sie zwar tatsächlich öffentlich bekannt sind, sich aber mit bloßem Auge nicht feststellen lässt, ob sie wirklich vom angegebenen Absender stammen. Bei der Überwindung dieser Unsicherheit helfen Zertifikate, mit deren genau dies überprüft werden kann. Bei Zertifikaten handelt es sich also um elektronische Dokumente, die den öffentlichen Schlüssel eines Nutzers sowie weitere Angaben wie Name, E-Mail-Adresse und andere Informationen enthalten. Ein Zertifikat ist demnach das Äquivalent zu einem Personalausweis oder Reisepass in der realen Welt.

Ausgestellt wird es durch eine Zertifizierungsinstanz, die zuvor die Angaben des Benutzers wirksam, beispielsweise durch Vorlage eines Ausweises, überprüft. Als Zertifizierungsinstanz kommen spezialisierte Anbieter für elektronische Signaturen in Frage, aber auch die Personal- und IT-Abteilungen von Unternehmen oder eine Behörde. Informationen über den Aussteller sind ebenfalls Teil des Zertifikats; außerdem signiert er alle Attribute des Zertifikats. Zweck ist, die Authentizität zu gewährleisten und das Zertifikat vor Manipulation zu schützen. Als allgemeinverbindlicher Standard hat sich der ITU-Standard X.509 für Zertifikate durchgesetzt.

Erstellung und Verifizierung von Zertifikaten

Der öffentliche Schlüssel eines jeden Nutzers wird in Form eines Zertifikats zur Verfügung gestellt. Dieses enthält mindestens die Kennung der Zertifizierungsinstanz, die Kennung des Nutzers, seinen öffentlichen Schlüssel und eine Angabe zur Gültigkeitsdauer des Zertifikats.

Das Zertifikat ist von der erstellenden Zertifizierungsinstanz digital signiert. Jeder, der den öffentlichen Schlüssel der Zertifizierungsinstanz besitzt, kann somit überprüfen, ob der öffentliche Schlüssel eines Nutzers wirklich von der Zertifizierungsinstanz stammt. Mit anderen Worten: Die Zertifizierungsinstanz bestätigt mit jedem einzelnen Nachweis, dass ein öffentlicher Schlüssel tatsächlich zu einem bestimmten Benutzer gehört.

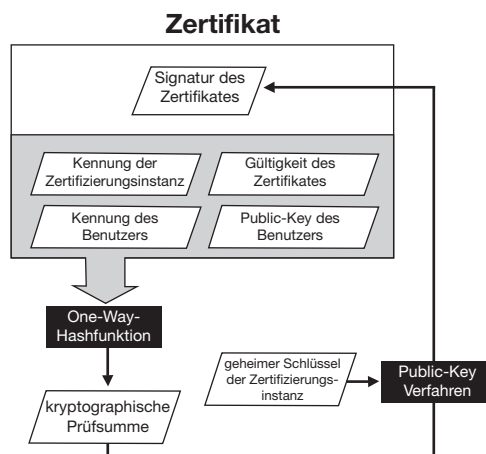


ABB. 2: Prüfsummencheck mit Hilfe eines Zertifikats

Ein System berechnet nach Erhalt eines Zertifikats die aktuelle kryptographische Prüfsumme über dessen Inhalt (vgl. Abb. 2). Außerdem wird aus der Signatur des Zertifikats und dem öffentlichen Schlüssel der Zertifizierungsinstanz unter Verwendung des Public-Key-Verfahrens die ursprüngliche kryptographische Prüfsumme berechnet. Stimmen beide Prüfsummen überein, sind die Unversehrtheit der übermittelten Nachricht und die Echtheit des öffentlichen Schlüssels des Nutzers bewiesen (vgl. Abb. 3).

Voraussetzung ist, dass alle Nutzer des Sicherheitssystems der Zertifizierungsinstanz vertrauen. Daher muss diese bestimmten Sicherheitsanforderungen genügen, die im Gesetz über Rahmenbedingungen für elektronische Signaturen (SigG) und der zugehörigen Verordnung zur elektronischen Signatur (SigV) beschrieben sind. Dazu zählen unter anderem vertrauenswürdige Personal, zertifizierte Sicherheitskomponenten und eine vertrauenswürdige Systemumgebung.

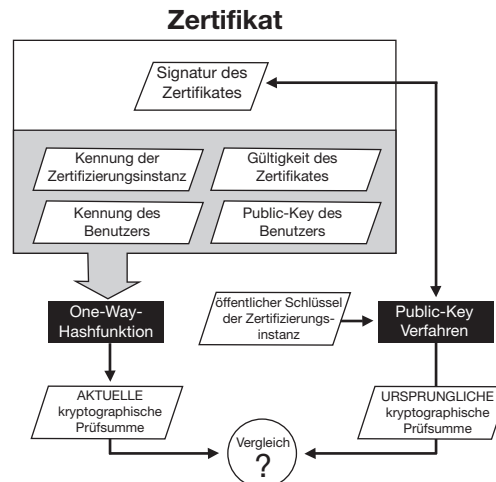


ABB. 3: Integritäts- und Echtheitsprüfung mit Hilfe eines Zertifikats

In der Praxis stellt die Beschaffung des öffentlichen Schlüssels der Zertifizierungsinstanz ein großes Problem dar. Eine Möglichkeit ist die Nutzung eines Wurzelzertifikats. Dabei handelt es sich um ein selbst signiertes Zertifikat, das den öffentlichen Schlüssel des Ausstellers, also der Zertifizierungsinstanz enthält. Wurzelzertifikate sind besonders sensibel und haben einen hohen Schutzbedarf. Gelänge es einem Angreifer, auf einem Rechner ein falsches Wurzelzertifikat unterzubringen, wären die Benutzer dieser Systeme Betrügnern, die sich dies zunutze machen, schutzlos ausgeliefert. Daher werden Betriebssysteme und Webbrowser bereits mit den gängigsten Wurzelzertifikaten ausgeliefert. Beim Erwerb dieser Produkte sollte man deshalb auf einen vertrauenswürdigen Bezugskanal achten.

Fazit

Elektronische Signaturen sollen im elektronischen Geschäftsverkehr die eigenhändige Unterschrift ersetzen. Dabei bieten sie zweierlei Vorteile: Sie bestätigen nicht nur die Identität eines Nutzers (z. B. des Absenders einer E-Mail), sondern schützen auch die Nachricht selbst gegen nachträgliche Manipulationen. Damit das funktioniert, müssen sie sich in der Praxis jederzeit auf ihre Echtheit kontrollieren lassen. Dabei helfen einerseits One-Way-Hashfunktionen, mit denen sich für jede Nachricht eine spezifische kryptographische Prüfsumme bilden lässt, und andererseits Zertifikate, die bestätigen, dass der mit der Signatur übermittelte Schlüssel auch tatsächlich zum Absender gehört. Hash-Algorithmen und Zertifikate sind daher zentrale Bestandteile moderner Sicherheitssysteme.

Zu den Autoren: Prof. Dr. Norbert Pohlmann ist Geschäftsführender Direktor des Instituts für Internet-Sicherheit der Fachhochschule Gelsenkirchen. E-Mail-Kontakt: norbert.pohlmann@informatik.fh-gelsenkirchen.de

Malte Hesse ist Mitarbeiter am Institut für Internet-Sicherheit der Fachhochschule Gelsenkirchen. E-Mail-Kontakt: hesse@internet-sicherheit.de