Neue Kryptoserie - Teil 1

Digitale Signaturen

von Robert Gehring

Im vergangenen Jahr wurde vom Deutschen Bundestag das Gesetz zur digitalen Signatur (Signaturgesetz, SigG) beschlossen. Damit hält zum einen die moderne Verschlüsselungstechnologie Einzug in die rechtsverbindliche Kommunikation. Zum anderen wird die Kultur der Unterschrift, wie sie jedem vertraut ist, einem Wandel unterworfen. Diese Artikelserie soll beide Aspekten vorstellen und die Entwicklung beleuchten.

Digitale Signaturen greifen auf die Idee der Unterschrift und die Methoden der Kryptographie zurück. Das angestrebte Ziel ist die Absicherung von Kommunikation jedweder Art. Dazu gehören z.B. Briefe, Verträge, Nachrichten, ... fast jede erdenkliche Information. Das menschliche Sicherheitsbedürfnis verlangt danach, über den Urheber und den Inhalt einer Information Gewißheit zu haben. Und dabei handelt es sich um ziemlich ein altes Bedürfnis, wie ein Blick in die Geschichte zeigt.

Beide, Unterschriften und Kryptographie, haben sich in ihren konzeptionellen Ansätzen bereits vor Jahrtausenden entwickelt. Ihre konkreten Erscheinungen unterscheiden sich regional und kulturell, an ihrem Einsatzzweck lassen sie sich jedoch wiedererkennen.

Unterschrift

Die Parallelität der Ereignisse läßt sich auf dem Papier nur schwer wiedergeben. Willkürlich soll zuerst auf die Entwicklung der Unterschrift eingegangen werden.

Es begann vor über 5000 Jahren, daß die Menschen sich selbst erkenntlich zeigen wollten. Im wahrsten Sinn des Wortes sollte die Person, die eine Nachricht sandte, für den Empfänger zu erkennen sein. Dazu brachte sie an der Nachricht ein Zeichen an.

In Mesopotamien wurden dazu Stempel oder Siegel benutzt, aus Ton geformt oder aus Knochen geschnitzt. Aus dem alten China sind derartige Siegel/Stempel ebenfalls überliefert, auch aus Japan. Sie erfüllten hier wie dort denselben Zweck.

Die Römer griffen die Technik der Stempel und Siegel auf und verfeinerten sie. Kostbare Materialien wurden zu Gemmen verarbeitet. Die Qualität einer solchen Gemme sagte viel über den Status ihres Besitzers aus.

Mit dem Übergang zum Mittelalter und dem damit verbundenen Verlust an Hochkultur büßten die Siegel und Stempel an Bedeutung ein. Größeren Bedarf an einem Einsatz hatten nur noch Könige und Kirchenobere.

Erstere siegelten ihre untereinander geschlossenen Verträge damit. Letztere benutzten sie, um Abschriften alter, antiker Originale zu autorisieren. Solche autorisierten Abschriften erhielten die Bezeichnung „Authentik". Daraus wurde unser Begriff vom „Authentischen" abgeleitet. Im Wort „Siegel" steckt übrigens das „signum", zu deutsch: Zeichen. Und „signieren" heißt eigentlich nichts weiter als „(ab-/unter-)zeichnen".

In der Renaissance erfolgte ein neuerlicher, kultureller Aufschwung. Davon getragen, erholte sich das Selbstbewußtsein der Menschen und ebenso ihr Bedürfnis, den Dingen den Stempel ihrer Persönlichkeit aufzudrücken. Nach und nach wandelte sich die (bild)symbolgetragene Kultur des Mittelalters in eine zeichengetragene.

Die Rede ist von der Schrift, die Einzug in den Alltag hielt. Anfangs profitierte insbesondere das erstarkende Bürgertum davon, seit ein-, zweihundert Jahren auch der Rest der Bevölkerung. Unterzeichnet wird seitdem nicht mehr mit dem Siegel oder Stempel, sondern mit der persönlichen Unterschrift (Im Amtsgebrauch sind Stempel noch heute groß in Mode.).

Zum 1. Januar 1900 trat das Bürgerliche Gesetzbuch in Kraft, das der persönlichen Unterschrift eine besondere Bedeutung verliehen hat. Durch eine eigenhändig voll-

zogene Unterschrift wird aus einem Dokument eine Urkunde. Kann im Streitfalle eine der beteiligten Parteien eine entsprechende Urkunde zum Beleg für ihre Behauptungen vorweisen, so wird diese als Beweis anerkannt. Der Partei, die unterzeichnet hat, wird in der Regel unterstellt, daß sie sowohl willentlich gehandelt hat, als auch vom Inhalt des Dokuments Kenntnis hatte.

In Konflikten, in denen es um Verträge geht, stellen unterschriebene Dokumente das wichtigste Beweismittel dar. Fälschungen von Inhalten oder Unterschriften lassen sich mit kriminaltechnischen Methoden in den meisten Fällen nachweisen. Darauf basiert auch das Vertrauen in die Unterschrift als Instrument zur Vertragsabsicherung.

Seitdem Computer bezahlbar geworden sind, werden sie immer stärker zum Dokumentenaustausch eingesetzt. Die weltweite Vernetzung liefert seit den siebziger Jahren in wachsendem Maße einen Beitrag zu dieser Entwicklung. Durch die dem Computer geschuldete Form der digitalen Speicherung und Übertragung von Daten, ist es nicht mehr möglich, elektronische Dokumente mit einer eigenhändigen Unterschrift zu versehen. Und eine wie auch immer digitalisierte Unterschrift ist kein Ersatz. Das unbemerkte Fälschen wäre doch zu einfach. Deshalb steht vor einem Problem, wer den Nachrichtenaustausch mittels Computer beweisbar machen will.

Soviel zu „Aufstieg und Untergang" der klassischen Unterschrift. Inwieweit digitale Unterschriften deren Funktion übernehmen könne und werden, soll später genauer untersucht werden. Das Signaturgesetz geht erst einmal davon aus - und auch nicht. Der Wirkungsbereich der digitalen Signatur wird darin nicht genauer beschrieben. Daß digital signierte Dokumente nicht den Stellenwert einer Urkunde erhalten setzt in der Praxis enge Grenzen.

Wir wenden uns erst einmal der Kryptographie zu, ohne die es digitale Signaturen nicht geben würde.

Kryptographie

Aus antiken Zeiten stammen die ersten Berichte über den Einsatz von Verschlüsselungstechniken. Die erste Verschlüsselung, die Berühmtheit erlangte, war die Cäsar-Chiffrierung. Der römische Kaiser ersetzte in seinen geheimen Nachrichten jeden Buchstaben durch dessen dritten Nachfolger im Alphabet. Heraus kam ein für damalige Zeit vielleicht irritierender Buchstabensalat. Diesen wieder lesbar zu machen, blieb denjenigen vorbehalten die über den Schlüssel, sprich die Stellenanzahl der Verschiebung, Bescheid wußten.

Im Laufe der Jahrhunderte gab es viele Abwandlungen dieser Methode, die unter dem Namen „Substitution" in den Lehrbüchern beschrieben wird. Später ersetzte man die Zeichen nicht nur, sondern vertauschte zusätzlich die Zeilen und Spalten der Nachrichten (Transposition). Darauf folgten die Verfahren, die Zeichengruppen durch Zeichen oder andere Zeichengruppen ersetzen. Die Regeln für die Ersetzungen wurden in Codebüchern festgehalten. So ein Codebuch stellte mithin den Schlüssel dar, mit dessen Hilfe entziffert wurde.

Zum Einsatz kamen diese geheimen Methoden in den Geheimkabinetten der Königshäuser und Kirchenpolitiker. Nicht von ungefähr hatten diese Personengruppen ein besonderes Interesse an sicherer Kommunikation. Es ging um Politik.

Anfang des zwanzigsten Jahrhunderts, die Industrialisierung der Wirtschaft stand in voller Blüte, wurde dann auch die Verschlüsselung automatisiert. Für mehrere Jahrzehnte blieben Rotormaschinen unterschiedlichster Bauart das vorherrschende Instrument der Chiffreure. In direkter Linie stammen von diesen die symmetrischen Verschlüsselungsverfahren ab.

Die Ablösung der mechanischen Rotormaschinen durch die Computertechnik vollzog sich bis in die siebziger Jahre nahezu im Verborgenen. Die Ursachen dafür sind in der symbiotischen Beziehung von Verschlüsselungsverfahren und Schlüssel zu sehen, durch die klassische Kryptographie bestimmt wurde. Oft genug war eine Trennung von Verschlüsselungsverfahren und Schlüssel nicht gegeben. Wer Kenntnis vom Verfahren hatte, konnte die Verschlüsselung brechen. [Im Falle der Cäsar-Chiffrierung hätte einfaches Ausprobieren genügt, um herauszufinden, daß jedes Zeichen durch seinen dritten Nachfolger ersetzt wurde.! Geheimhaltung des Nachrichteninhalts war praktisch immer gleichbedeutend mit der Geheimhaltung des Verfahrens.

Der Wechsel in den Paradigmen der Kryptologen vollzog sich mit der Entwicklung der Informationstheorie seit Claude Shannon und dem zunehmenden Einsatz von Computern. Das Ziel der Entwicklung von Verschlüsselungsverfahren war, ohne Geheimhaltung des Verfahrens auszukommen. Der potentielle Gegenspieler sollte das Verfahren ruhig kennen. Solange er nicht über den passenden Schlüssel verfügte, würden seine Entschlüsselungsbemühungen ins Leere laufen.

Diese neue Auffassung von Ver-

schlüsselung entsprach eher den Bedingungen der Praxis, als die bis dato bestehende Forderung nach absoluter Geheimhaltung der Verfahren und Schlüssel. Die vorangegangenen Weltkriege hatten gezeigt, daß absolute Geheimhaltung Illusion bleiben muß, solange das Geheimnis an mehr als einem Ort verwahrt werden muß. Den Kulminationspunkt dieser Entwicklung stellte die Veröffentlichung des DES-Verfahrens Mitte der siebziger Jahre dar.

Nahezu zeitgleich wurde eine neue Art von Verschlüsselung entwickelt. Ihr wurde anfangs nur wenig Aufmerksamkeit zuteil. Die Rede ist von der asymmetrischen Verschlüsselung, die Whitfield Diffie und Martin Hellman zu verdanken ist. Der herausragende Vertreter dieses Typs ist das RSA-Verfahren, auf das wir später zurückkommen werden. Im Unterschied zur symmetrischen Verschlüsselung, gibt es nur einen geheimen Schlüssel. Zum Vergleich: Symmetrische Verfahren setzen zwei Kopien eines Schlüssels ein, eine Kopie für die Verschlüsselung, die andere für die Entschlüsselung.

Mit asymmetrischer Verschlüsselung wird das Problem der Schlüsselgeheimhaltung gegenüber der symmetrischen Verschlüsselung halbiert. Es gibt nur noch einen geheimen, den privaten Schlüssel. Zu ihm gehört ein zweiter Schlüssel, der öffentlich gemacht werden kann. Die paarweise Verwendung von ungleichen Schlüsseln eröffnet den asymmetrischen Verfahren große Einsatzmöglichkeiten.

Leider werden diese Möglichkeiten durch den immensen Rechenaufwand, den asymmetrische Verschlüsselung erfordert, wieder stark eingeschränkt. Zur Verschlüsselung großer Datenmengen, wie etwa ganzer Festplatten oder Videofilme, sind asymmetrische Verfahren denkbar ungeeignet. Die benötigte Rechenleistung ist um einen Faktor 1.000-10.000 höher, als bei vergleichbar sicheren symmetrischen Verfahren, eine nicht zu vernachlässigende Größenordnung. Den Königsweg stellt die geeignete Kombination aus symmetrischem und asymmetrischem Verfahren dar, hybride Verschlüsselung genannt. Moderne Verfahren für verschlüsselten Dokumentenaustausch greifen darauf zurück. PGP sei als Beispiel genannt.

Bevor sich asymmetrische und hybride Verfahren zum authentischen Dokumentenaustausch etablieren konnten, wurden symmetrische Verfahren eingesetzt. Einige der dabei entwickelten Ideen wurden von den modernen Konzeptionen aufgegriffen, andere verworfen. Das wohl wichtigste Überbleibsel ist die „Trusted Third Party" (TTP), die als „Certification Authority" (CA) oder auch „Trust Center" (TC) eine Schlüsselrolle inne hat, auch nach dem Signaturgesetz, wo sie als *Zertifizierungsstelle* firmiert.

Ein Beispiel zur Illustration

In den letzten Monaten ist häufig von E-Kommerz die Rede, d.h. dem Handel, der über elektronische Medien, z.B. über das Internet, abgewickelt wird: Ein Anbieter veröffentlicht im Internet einen Katalog von Waren oder Dienstleistungen und bietet sie zu einem bestimmten Preis an. Das ganze auf seiner Homepage, die von einem Provider betrieben und gepflegt wird. Die angebotenen Waren beispielsweise lassen sich über ein Formular online bestellen. Dazu wählt Knut Kunde sie per Mausklick aus und schickt die Bestellung gegen Rechnung ab. Nachdem die Waren bei ihm eingetroffen sind, flattert ein paar Tage später die Rechnung ins Haus. Nun hat der Knut jedoch nicht das erhalten, was er bestellt hat. Statt einer AGP-Grafikkarte lag eine PCI-Karte im Paket und statt SDRAMs fanden sich EDO-RAMs. Die Rechnung weist zudem einen deutlich höheren Betrag auf, als bei der Bestellung am Monitor angezeigt worden war. Das liegt an der Mehrwertsteuer. Diese war nicht kurzfristig erhöht worden. Nein, der Anbieter hatte sie bei den Preisangaben schlicht und einfach vergessen. Soll ja vorkommen ;-) Knut beschwert sich beim Anbieter. Der verspricht, die korrekten Bauteile zu liefern und die falschen zurückzunehmen. Aus Kulanz. Dazu solle Knut jedoch erst einmal die Rechnung bezahlen. Der Fehler mit der Mehrwertsteuer läge im übrigen beim Provider, der sich nicht an die Vorgaben des Anbieters gehalten hätte. Dort möge Knut seine Forderungen geltend machen.

Und wenn sie nicht gestorben sind, so sind sie noch lange auf dem Rechtswege.

Authentischer Dokumentenaustausch mit symmetrischer Verschlüsselung

Es sollte noch einmal klargestellt werden, worum es bei einem authentischen Dokumentenaustausch geht: Um Rechtssicherheit. Vorbedingung für die Rechtssicherheit ist die technische Sicherheit, d.h. die Unverfälschtheit des Ablaufs

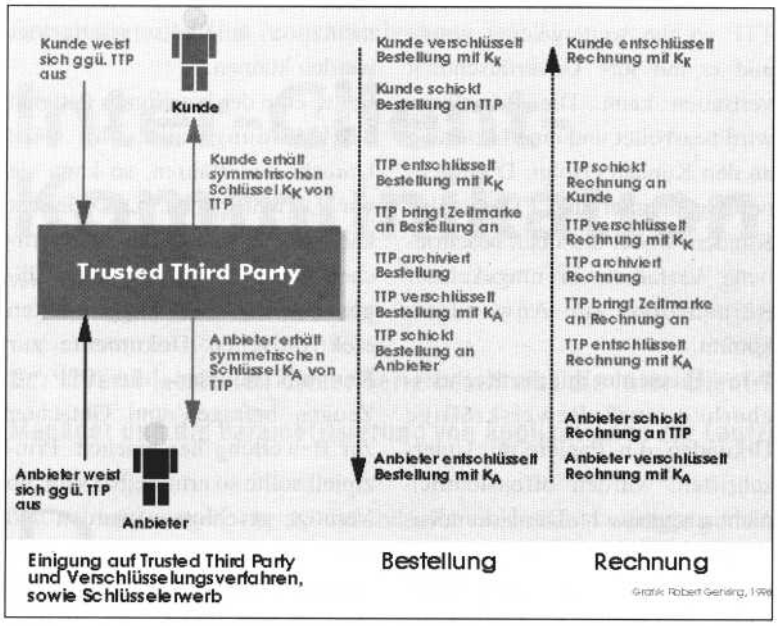

Abbildung 1: Dokumentenaustausch mit symmetrischer Verschlüsselung

und der Daten. Weder dürfen gefälschte Dokumente als authentische gelten können, noch darf die Reihenfolge des Austauschs manipulierbar sein. Man denke an Bieteverfahren oder Wahlen auf elektronischem Wege, wenn man sich die Bedeutung der Forderungen anschaulich machen will. Die Rechtssicherheit wird nach der technischen Sicherheit hergestellt sein, wenn die technische Sicherheit *beweisbar* ist. Wenn die an der Kommunikation beteiligten Parteien einem Außenstehenden beweisen können, welche Dokumente zu welchem Zeitpunkt ausgetauscht wurden, so können Rechte, die aus dem Kommunikationsinhalt abgeleitet werden, geltend gemacht werden.

Das Beispiel zeigt -an den Haaren herbeigezogen natürlich- einige Probleme auf, mit denen man sich konfrontiert sehen kann, wenn man vertrauensselig handelt. Hätten Knut, Anbieter und Provider sich besser abgesichert, so wären die Fehlerquellen schnell zu finden gewesen und der Streit aus der Welt geschafft. Wie hätte diese Absicherung ausgesehen, wenn sie auf symmetrischer Verschlüsselung aufgebaut worden wäre?

Wir lassen den Provider aus dem Beispiel weg, da das vorgestellte Konzept auf fast beliebig viele Parteien ausgedehnt werden kann.

Die folgende Abbildung zeigt ein Anbieter-Kunde-Verhältnis unter Einbeziehung einer Trusted Third Party. Das Ziel der beteiligten Parteien besteht darin, eine Bestellung und Rechnung online abzuwickeln.

Bevor der Handel zustandekommen kann, müssen sich Anbieter und Kunde über den Ablauf einig sein. Dazu gehört, sich auf eine Trusted Third Party als Vermittler festzulegen. Ohne solch einen Vermittler funktioniert das Verfahren nicht. Im Aufgabenbereich des Vermittlers liegt es, die Identitäten von Kunde und Anbieter zu überprüfen, ihnen ein Verschlüsselungsverfahren zur Auswahl zu stellen, passende Schlüssel zu vergeben, die Verfälschung der auszutauschenden Dokumente zu verhindern und die Dokumente für den Streitfall zu archivieren. Es ist offensichtlich, daß Kunde und Anbieter dem Vermittler volles

Vertrauen entgegenbringen müssen, um sich auf dessen Regeln einzulassen.

Ebenso einsichtig ist die Forderung nach Unabhängigkeit des Vermittlers. Diese bezieht sich primär auf die Interessen der Anbieter und Kunden. Im Interesse eines weitergehenden Datenschutzes sollte sie auch gegenüber staatlichen Stellen und anderen Außenstehenden garantiert sein.

Wurde ein geeigneter Vermittler gefunden, sind die Verschlüsselungsverfahren festgelegt und die Schlüssel vergeben, so kann der Handel beginnen. Der Kunde wählt auf der Webseite des Anbieters aus, was er erwerben möchte, und macht daraus eine Bestellung. Diese verschlüsselt er mit seiner Kopie des symmetrischen Schlüssels K K. Die solcherart verschlüsselte Bestellung schickt er an die Trusted Third Party (TTP), die über die zweite Kopie des Kundenschlüssels verfügt. Mit dieser entschlüsselt sie die Bestellung. Bei erfolgreicher Entschlüsselung weiß die TTP, daß die Bestellung vom Inhaber des Schlüssels KK stammen muß, dessen Identität sie kennt. **(Anmerkung:** Die kritische Ausnahme bildet der Fall, daß der Schlüssel kompromittiert wurde. Daß dies nicht geschieht, fällt in die Verantwortung von TTP und Kunde. Gleiches gilt z.B. für die PINs der EC-Karten.) Die entschlüsselte Bestellung wird mit einer Zeitmarke versehen und archiviert. Damit kann später festgestellt werden, wann die Bestellung eingegangen ist.

Im nächsten Schritt wird die Bestellung mit der Kopie des Schlüssels KA des Anbieters verschlüsselt und an diesen gesandt. Der Anbieter nimmt die Bestellung entgegen und entschlüsselt sie mit seiner Kopie von KA. Bei Erfolg weiß er, daß die Bestellung von der TTP an ihn weitergeleitet wurde und er auf ihre Unverfälschtheit vertrauen kann. Die Bestellung wird bearbeitet und eine Lieferung an den Kunden erfolgt. Die Rechnung geht über die TTP an den Kunden, wobei das oben beschriebene Verfahren in umgekehrter Reihenfolge zur Anwendung kommt.

Wie sieht es nun mit der Rechtssicherheit aus? Beweiskräftige Urkunden, d.h. Papiere mit Unterschriften, wurden offensichtlich nicht ausgetauscht. Der Urkundenbeweis entfällt. Beweise müssen demnach anders gesichert werden.

Kunde und Anbieter müssen in die Qualität der Arbeit der TTP und deren Unabhängigkeit Vertrauen haben. Die TTP muß sichere Verschlüsselungsverfahren einsetzen, gute Schlüssel erzeugen und für deren sichere Weiterleitung an Kunden und Anbieter Sorge tragen. Im Streitfalle lassen sich die Inhalte der ausgetauschten Bestellungen und Rechnungen aus dem Archiv der TTP holen. Durch die Zeitmarken läßt sich der zeitliche Ablauf rekonstruieren. Die Unabhängigkeit der TTP macht diese zu einem geeigneten Zeugen. Damit Gutachter über die Sicherheit der eingesetzten Verfahren und Schlüssel urteilen können, müssen deren Spezifikation und Implementation möglichst offengelegt werden können.

Sollte eine der beteiligten Parteien der Meinung sein, ihr wäre Unrecht widerfahren, so kann sie vor Gericht gehen. Das Gericht kann im Prozeß durch „richterlichen Augenschein" die vom Kläger bei der TTP angeforderten elektronischen Dokumente zur Kenntnis nehmen, die TTP als Zeugen befragen und Gutachter zur Bewertung heranziehen. Prinzipiell sollte so ermittelbar sein, ob Verträge geschlossen wurden und wenn ja, welche Inhalte sie hatten. Damit ist in gewissem Rahmen ein Pendant zum schriftlichen Vertrag mit eigenhändiger Unterschrift gegeben. Den Umfang der Beweiswürdigung zu bestimmen, liegt allein im Ermessen des Richters. Für viele Verträge fordert das BGB jedoch ausdrücklich die Schriftform, d.h. Schrift auf Papier. Elektronische Dokumente erfüllen diese Forderung nicht, da helfen keine Zeugen und keine Gutachter.

Und noch etwas schränkt den Wert solcherart geschlossener Verträge ein. Die Trusted Third Party mag unabhängig sein. Ob jeder einzelne Mitarbeiter auch unabhängig ist, läßt sich von außen schwer feststellen. Und da bei der TTP Kopien sowohl vom Kundenschlüssel, als auch vom Anbieterschlüssel vorliegen, könnten Mitarbeiter die Inhalte von Bestellungen und Rechnungen manipulieren. Oder schlimmer noch, sie könnten Schlüsselkopien an Konkurrenten weitergeben. Niemand wäre so einfach in der Lage, das zu beweisen. Man sieht, symmetrische Verschlüsselungsverfahren als Unterschriftenersatz sind mit Vorsicht zu genießen. Aus diesem Grunde wird den asymmetrischen Verfahren in der Regel der Vorzug gegeben. Denen werden wir uns in der nächsten Folge zuwenden.

DER AUTOR

Robert Gehring ist Student der Informatik und Philosophie an der TU Berlin. Seit der Linux-Version 0.9.12 ist er mit dabei, entwickelte diverse Software und setzt dieses Betriebssystem auch ausgiebig für seine Studien/Diplomarbeit ein. Zu erreichen ist er unter *rag@zblmath.FIZ-Karlsruhe.DE*.