

E-Commerce-Sicherheit, Kryptografie und Digitale Signatur

Beitrag zum 3. Freiburger Wirtschaftssymposium „Wissens Wert – Ökonomische Perspektiven der Wissensgesellschaft“, Okt 1999. Tagungsband Nomos-Verlag, Nov 2000.

Rüdiger Grimm <grimm@ darmstadt.gmd.de>

August 2000

Zusammenfassung

E-Commerce verlangt Sicherheit. In erster Linie muss die Technik zuverlässig funktionieren. Aber das reicht nicht aus. Man muss auch wissen, dass der Kommunikationspartner im Internet wirklich der ist, der er behauptet zu sein (Authentizität), dass seine Versprechen nicht abstreitbar sind (Verbindlichkeit), dass nicht jeder einfach mithören kann, was da geschäftlich ausgehandelt wird (Vertraulichkeit). Darüber hinaus soll die Kommunikation nicht zweckentfremdet werden können, etwa zum Ausforschen persönlichen Verhaltens (Datenschutz). Es wird hier gezeigt, wie die digitale Signatur funktioniert und wie sie zur Sicherung von E-Commerce beitragen kann.

1 Verbindliche Telekooperation im offenen Internet

Das Internet mit seinem multimedialen „World-Wide Web“ ist uns in den vergangenen Jahren als schnelles und billiges Kommunikationsmedium, das die ganze Welt umspannt, vertraut geworden. Es ist offen. Es ist jedermann zugänglich. Es gehört niemandem. Jeder, der es möchte, kann das Netz mit wenig Soft- und Hardware vergrößern, indem er eine Mailbox, einen Netzknoten oder einen Informationsserver an das Netz anschließt und dadurch zum Mitbetreiber wird. Das Internet wächst unaufhaltsam.

Es liegt auf der Hand, das Internet nicht nur für unverbindliche Mitteilungen, sondern auch „im Ernst“ für geschäftliche Anwendungen, Verwaltungsaufgaben und private Kommunikation zu benutzen. Warenangebote und Bestellungen, Zeugnisse, Verträge, Willenserklärungen, urheberrechtlich geschützte Texte und Dokumente aller Art, ja sogar digitales Geld können über das Internet viel schneller, direkter und billiger kommuniziert werden. Unter Electronic Commerce (oder kurz E-Commerce) versteht man alle Geschäftsabwicklungen in elektronischer Form, vor allem über das Internet.

Aber der verbindlichen Kommunikationsform steht die gegenwärtige Technik des Internets im Wege: seine Technik ist so einfach, dass sie nicht nur leicht zu *gebrauchen*, sondern auch leicht zu *missbrauchen* ist. Das Internetprotokoll (IP) ist nach dem Postkartenprinzip aufgebaut. Mit einfachen Mitteln kann man sich mit fremden Namen maskieren, Adressen fälschen, Durchgangspost verändern und mitlesen. Und weil das *möglich* ist, kann man gegebene Versprechen einfach abstreiten und behaupten, da habe irgend jemand anderes einen Namen oder einen Inhalt gefälscht. Auf dieser Basis kann man elektronisch keine verbindlichen Erklärungen abgeben, Verträge schließen oder Geld übertragen.

2 Authentizität, Integrität und Korrektheit

Verbindliche Kommunikation erfordert in erster Linie Authentizität. Texte, die als verbindlich anerkannt werden wollen, müssen unabstreitbar sein, und zwar sowohl in Bezug auf ihre Herkunft, als auch auf ihren Wortlaut. Für elektronische Dokumente ist dafür die digitale Signatur entwickelt worden, welche sich gut für Telekooperationen eignet. In

Deutschland legt seit 1997 das Signaturgesetz [IUK_97] einen Sicherheitsstandard fest, unter dem eine digitale Signatur als sicher anzusehen ist. Die europäische Richtlinie für die „elektronische Signatur“ (wie es dort heißt) verlangt die Gleichstellung der Rechtswirksamkeit elektronisch signierter Dokumente mit der handschriftlicher Dokumente (allerdings ohne die Beweiskraft zu regeln) [ESig_99]. Wie die digitale Signatur funktioniert und wie man mit ihrer Hilfe E-Commerce sicherer machen kann, soll hier erläutert werden.

Neben der Authentizität der Kommunikation bestehen für viele verbindliche Kommunikationsformen auch Anforderungen an die Vertraulichkeit und Anonymität. Vertraulichkeit ist eine Grundanforderung an vierlei geschäftliche und an alle private Kommunikation. Für Anonymität braucht man nicht nur auf die Drogenberatung zu verweisen. Sie ist auch im Geschäftsleben zum Beispiel beim Bezahlen mit Geldmünzen und Geldscheinen gewährleistet. Politische Wahlen erfordern sowohl Anonymität der Wählenden als auch die Authentizität ihrer Wahlberechtigung. Anonymität und Pseudonymität bilden eine Grundlage zur Datensparsamkeit und damit für eine datenschutzfreundliche Technik.

Anonymität und Datenschutz stellen technische Herausforderungen an die offenen Kommunikationsnetze dar, für die es bereits eine Reihe interessanter Lösungen gibt [Chau_85, Pfitz_87, PEM_93, PGP_95, P3P_00]. Dieser Beitrag wird aber auf Probleme der Anonymität und des Datenschutzes nicht weiter eingehen, sondern sich auf die Authentizität und Vertraulichkeit beschränken.

3 Authentizität im sozialen Kontext

Authentizität ist keine kontextfreie Eigenschaft. Sie bezieht sich immer auf Menschen, ihr Umfeld und ihre Handlungen. Eine Person kann zum Beispiel als authentisch in ihrem sozialen Kontext angesehen werden, indem ihre Herkunft und ihre Wohn- und Arbeitsumgebung überzeugend zum Ausdruck gebracht ist. Ein Dokument ist authentisch in bezug auf seinen Erzeuger und hängt von dessen Authentizität ab. Ein Vertrag wird in einer rechtlich gestalteten gesellschaftlichen Umgebung als korrekt anerkannt oder als inkorrekt verworfen.

Die Kontrolle über Authentizitätsmerkmale kann als staatliche Aufgabe angesehen werden, wie das z. B. bei Personalausweisen und Geldscheinen der Fall ist. Das sahen die ersten Ansätze zur Spezifikation von Sicherungsverfahren in der technischen Kommunikation auch vor. Die öffentlichen Schlüssel zur Verifikation digitaler Unterschriften sollten von einer nationalstaatlich organisierten Zertifizierungsinfrastruktur personalisiert und zertifiziert werden [X509_88, PEM_93].

Diese Vorgehensweise sieht eine Reihe von staatlichen Regelungsaufgaben vor. Erstens werden Personen zu Regionen und Organisationen zugeordnet. Zweitens erhalten sie als Folge davon maschinenlesbare Namen und Internetadressen. Drittens werden an die Personen kryptografische Schlüssel vergeben, mit Hilfe derer sie digital signieren können. Zur Verifikation digitaler Signaturen werden öffentlich zugängliche Verzeichnisse mit öffentlichen Schlüsseln und deren Zertifikaten eingerichtet.

Zum Beispiel könnte dann ein australisches Reisebüro die digitale Signatur eines deutschen Touristen, der spontan sein einmaliges Last-Minute-Angebot annehmen und bezahlen will, ohne weiteres als authentisch verifizieren. Und umgekehrt könnte der deutsche Tourist die Echtheit der digital übermittelten australischen Tickets feststellen.

Allerdings ist für viele Umgebungen keine staatlich beglaubigte Authentizität nötig. Zum Beispiel genügen für die Kreditwürdigkeit glaubwürdige Aussagen von Kreditorganisatio-

nen. Für den Zugang zu geschützten Ressourcen genügen ungefälschte private Berechtigungsausweise. Für die Wiedererkennung unter Freunden genügen unverwechselbare Erinnerungsmkmale. Ob nun staatlich oder privat organisiert: entscheidend für die Glaubwürdigkeit von Authentifizierungsmerkmalen ist, dass sie fälschungssicher sind und von neutralen Dritten überprüft wurden.

4 Kryptografie

Kryptografische Verfahren werden schon seit Menschengedenken eingesetzt, um über weite Entfernungen hinweg vertraulich miteinander zu kommunizieren. Die Geschichte der Spionage hat die Kryptografie wesentlich geprägt [Kah_67]. Mit Hilfe moderner Computer sind die Verschlüsselungstechniken immer angriffssicherer geworden. In den siebziger Jahren wurde der „Data Encryption Standard (DES)“ [z.B. bei BSschn_96] eingeführt und ist Grundlage der heute wohl am meisten benutzten Verschlüsselungstechnik, z.B. im Finanzdatenverkehr der Banken untereinander oder beim Vertraulichkeitsschutz militärischer Kommunikation.

Es ist das Verdienst von Diffie und Hellmann, erkannt zu haben, dass eine Verschlüsselungstechnik in offenen Netzen erst dann sicher benutzt werden kann, wenn man die zugehörigen geheimen Schlüssel nicht mehr über das Netz kommunizieren muss [DiHe_76]. Sie haben eine Technik gefordert, die so gestaltet ist, dass ein Benutzer eine Verschlüsselungsfunktion mit zwei *verschiedenen* Schlüsseln bedienen soll, von denen der eine *verschlüsselt* und der andere *entschlüsselt*. Dann kann nämlich der Benutzer den einen Schlüssel *geheimhalten* und braucht ihn auch nie herauszugeben, während er den anderen *veröffentlicht* und jedem zugänglich macht. Jeder, der ihm etwas verschlüsselt zusenden will, benutzt *des Empfängers öffentlichen Schlüssel*. Der Empfänger (und nur dieser allein) kann das Kryptogramm mit Hilfe seines geheimen Schlüssels wieder zum Klartext entschlüsseln. Seinen geheimen Schlüssel braucht er dafür niemals außerhalb seines lokalen Rechnerbereiches, z.B. auf einer persönlichen Chipkarte, herauszugeben.

Diffie und Hellmann stellten eine zweite bahnbrechende Forderung auf: Verschlüsselungsverfahren sollten derart gestaltet sein, dass man sie nur knacken kann, indem man ein bisher ungelöstes mathematisches Problem löst. Zum Beispiel kennt bis heute niemand einen „schnellen“ deterministischen Algorithmus zur Faktorisierung ganzer Zahlen oder zur Bestimmung diskreter Logarithmen. Mathematiker bezweifeln, dass es solche Algorithmen überhaupt gibt. Diffie und Hellmann unterstellen mit Recht, dass das Lösen ungelöster mathematischer Probleme die schwierigste (und möglicherweise sogar eine unerfüllbare) Herausforderung ist, die man an einen Angreifer auf ein kryptografisches Verfahren oder auf einen geheimen Schlüssel stellen kann.

Allerdings waren es erst Rivest, Shamir und Adleman [RSA_78] und später ElGamal [El-Ga_85], die konkrete Verfahren nach den Forderungen von Diffie und Hellman vorlegten. RSA beruht auf dem Problem der Faktorisierung, ElGamal auf dem Problem des diskreten Logarithmus. Die Algorithmen selbst sind öffentlich bekannt, und viele benutzen denselben Algorithmus, aber mit unterschiedlichen Schlüsselpaaren. Die Sicherheit bezieht sich nun darauf, dass trotz öffentlicher Bekanntheit der Algorithmen und der öffentlichen Schlüssel die geheimen Komponenten mit realistischem Aufwand nicht berechnet werden können, wenn die Schlüssel lang genug gewählt werden und solange keine abkürzenden schnellen Analyseverfahren bekannt sind. Vielleicht muss man mit Blick auf die Zukunft eine Einschränkung machen. Wenn massiv-parallele Rechnerarchitekturen realisierbar sind, so wie sie heute theoretisch als „DNA-Computer“ oder „Quantencomputer“ vorher-

gesagt werden, dann könnten (seriell) langsame Algorithmen durch Parallelisierung plötzlich schnell werden und damit alle kryptografischen Sicherungen unterlaufen.

5 Langsames und schnelles Rechnen

Diffie und Hellman machten die Beobachtung, dass es schnelle Rechengänge gibt, die nur langsam umkehrbar sind. Etwas lax ausgedrückt: Multiplizieren geht schnell, dividieren dauert lang. Jeder kann an sich selbst ausprobieren, dass es etwa nur wenige Minuten dauert, zwei fünfstelligen Zahlen handschriftlich nach Schulregeln miteinander zu multiplizieren. Dagegen dauert es in der Regel viele Stunden und Tage, allein und ohne Hilfe eines Computers eine zehnstellige Zahl in ihre Primfaktoren zu zerlegen, vor allem, wenn sie aus nur zwei fünfstelligen Primzahlen besteht. Dafür muss man nämlich buchstäblich milliarden von Multiplikationsversuchen unternehmen, bis man alle Möglichkeiten durchprobiert hat. Versuchen Sie es mal mit 3.105.316.187.

Diffie und Hellmans Idee zielt nun darauf, dass diejenigen, die im Besitz der richtigen Schlüssel sind, schnell rechnen dürfen, in unserem Beispiel also multiplizieren, während die Angreifer, die die Schlüssel nicht kennen, langsam rechnen müssen, in unserem Beispiel die Primfaktoren suchen. Wie kann man aber erreichen, dass sowohl der Verschlüsseler (bzw. der Signierer), als auch der berechtigte Entschlüsseler (bzw. Verifizierer einer Signatur) multiplizieren dürfen? Schließlich soll doch das Entschlüsseln (bzw. Verifizieren) zum Ausgangsergebnis *zurückführen*.

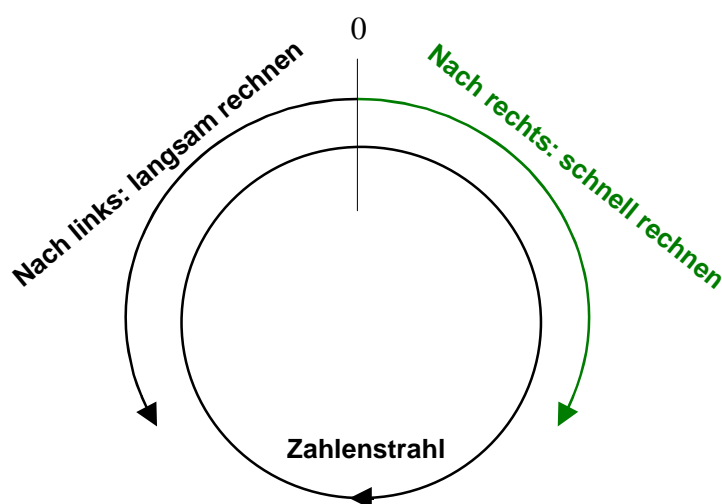


Abb. 1: „Im Kreis“ rechnen: *rechts* herum: multiplizieren; *links* herum: dividieren, logarithmieren und in Primfaktoren zerlegen

Hier hilft die Beobachtung, wie die Uhr den unendlichen Zeitverlauf in 24-Stundenkreise zusammenführt: Bei 24 Uhr fängt sie einfach wieder von vorne an: sie sieht 25 Uhr als dasselbe an wie 1 Uhr, 26 Uhr wie 2 Uhr usw. Wir lernen daraus, dass man im Zahlenraum statt nur nach rechts und links ins Unendliche hinein, sehr einfach „im Kreis“ herumrechnen kann, indem man alle Zahlen durch eine vorgegebene Zahl (bei der Uhr: 24) teilt und

6 „Symmetrische“ Verschlüsselung

Sogenannte „symmetrische“ Verschlüsselungsverfahren wie DES oder IDEA sind dadurch gekennzeichnet, dass jeder Benutzer über einen Schlüssel verfügt, mit dem er geheimzuhaltende Daten, z.B. eine Kreditkartennummer oder ein Passwort oder einen vertraulichen Brief, verschlüsselt und auch wieder entschlüsselt. Wenn zwei oder mehrere Partner denselben Schlüssel benutzen, den außer ihnen niemand kennt, können sie sich an seiner Verwendung erkennen: Sie zeigen sich gegenseitig, dass sie einen vorgegebenen Datensatz ver- und entschlüsseln können. So können sie das Verfahren nicht nur zum Verbergen ihrer Kommunikation vor unbefugten Dritten, sondern auch zur gegenseitigen Identifizierung benutzen.

Das schützt Benutzer, die einen symmetrischen Schlüssel gemeinsam benutzen, vor Angriffen auf die Integrität und Vertraulichkeit ihrer Kommunikation von außen. Aber innerhalb einer Benutzergruppe, die denselben Schlüssel benutzt, kann der Schlüssel nicht zur Unterscheidung verwendet werden. Innerhalb einer solchen Gruppe „kann es jeder gewesen sein“. Deshalb ist diese Art der Identifikation nach außen nicht beweisbar. Symmetrische Verfahren kann man nur in solchen Umgebungen einsetzen, in denen schon ein hohes Maß an Vertrauen besteht.

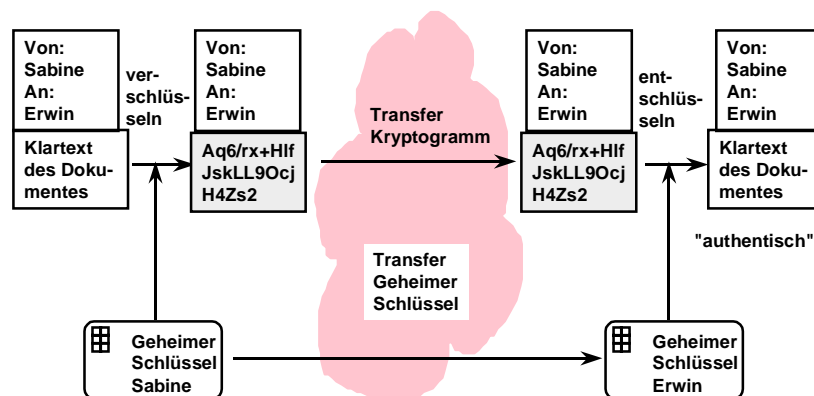


Abb. 3: Symmetrische Verschlüsselung: Derselbe Schlüssel zum Ver- und Entschlüsseln

Zum Beispiel vertrauen wir im allgemeinen unserer Bank, dass sie unsere geheimen Transaktionsnummern („TAN“) für Homebanking-Aufträge nicht ausnutzt, um in unserer Maske gegen uns zu handeln, etwa unser Konto einfach zu belasten und zu behaupten, das hätten wir selbst getan. Das ist deshalb eine vernünftige Annahme, weil unsere Bank ohnehin schon mit unserem Vertrauen über unser Geld verfügt und weil es organisatorische und gesetzliche Regelungen gibt, die das Verhältnis zwischen Bank und ihren Kunden schützen.

Auch Rechnernetze „geschlossener“, zentral kontrollierter Benutzergruppen, wie z.B. das Rechenzentrum oder die vernetzte Verwaltung einer Universität, können ohne weiteres symmetrische Verfahren einsetzen und dadurch die Sicherheit ihres Netzes vor Angriffen von außen wirkungsvoll schützen, zum Beispiel mit dem im MIT entwickelten Kerberos-System [Ker_88]. Allerdings gilt diese Art von Sicherheit nur innerhalb der geschlossenen Einsatzumgebung, die dadurch als *Sicherheitsinsel* von dem Rest der Welt, z.B. von dem Internet, *isoliert* wird.

7 „Asymmetrische“ Verschlüsselung

Sogenannte „asymmetrische“ Verschlüsselungsverfahren wie RSA und ElGamal sind dadurch gekennzeichnet, dass jeder Benutzer über ein Paar von zwei Schlüsseln verfügt. Der eine Schlüssel („Private Key“) ist der geheimzuhaltende „private Schlüssel“ seines Besitzers und darf nur von ihm verwendet und niemals nach außen mitgeteilt werden. Der andere Schlüssel („Public Key“) ist der „öffentliche Schlüssel“ seines Besitzers und wird allen seinen Kommunikationspartnern mitgeteilt.

RSA [RSA_78] ist nun so gestaltet, dass die beiden Schlüssel eines Paares zueinander invers sind: Ein Datensatz, der durch die asymmetrische Verschlüsselungsfunktion mit *einem* der beiden Schlüssel *verschlüsselt* wird, wird durch Anwendung derselben Verschlüsselungsfunktion mit dem jeweils *anderen, zugehörigen* Schlüssel wieder *entschlüsselt*. Kein anderer Schlüssel leistet die Entschlüsselung. Die Entschlüsselung ohne den zugehörigen Entschlüsselungsschlüssel ist so aufwendig, dass sie bei hinreichender Schlüssellänge in realistischer Zeit und mit realistischen Rechnerressourcen nicht zu leisten ist. Ebenso wenig lässt sich nur mit Kenntnis eines der beiden Schlüssel eines asymmetrischen Schlüsselpaares der jeweils andere Schlüssel berechnen, d.h. der private Schlüssel bleibt geheim, auch wenn alle Welt den zugehörigen öffentlichen Schlüssel kennt.

Der reversible RSA-Algorithmus ermöglicht zwei verschiedene Anwendungen: zum einen das Authentifizieren eines Datensatzes mit Hilfe der sogenannten „digitalen Signatur“, zum anderen das Verschlüsseln eines Datensatzes zum Zwecke des Verbergens vor Unbefugten.

ElGamal [ElGa_85] hat für die digitale Signatur einerseits und für die Verschlüsselung andererseits zwei verschiedene asymmetrische Algorithmen entwickelt. Ausschließlich zum Zweck der digitalen Signatur ist der entsprechende Algorithmus von ElGamal, der keine reversiblen Ver- und Entschlüsselungsvorgänge zulässt, variiert und im „Digital Signature Standard (DSA)“ [z.B. bei BSchn_96] spezifiziert worden.

Abbildung 4 veranschaulicht das Verfahren einer digitalen Signatur. Bei der digitalen Signatur verschlüsselt eine Senderin, die wir Susanne nennen wollen, den zu schützenden Dokumententext mit Hilfe ihres privaten Schlüssels. Niemand anders als sie kann das auf dieselbe Weise tun, denn niemand außer ihr selbst kennt ihren privaten Schlüssel. Der so verschlüsselte Text dient als digitale Signatur und wird gemeinsam mit dem unverschlüsselten Klartext versendet.

Mit Hilfe des öffentlichen Schlüssels von Susanne kann jeder Empfänger die digitale Signatur verifizieren, indem er sie „entschlüsselt“ und prüft, ob das Ergebnis mit dem mitgelieferten Klartext übereinstimmt. Wenn ja, dann ist nicht nur Susanne als Urheberin der digitalen Signatur festgestellt, sondern es ist auch erwiesen, dass der signierte Text im vorliegenden Wortlaut signiert worden ist. Jede Änderung auch nur eines Bits in der Signatur oder im signierten Text würde nämlich zu einer Nichtübereinstimmung zwischen Ursprungstext und „entschlüsselter“ Signatur führen. Auch die „Entschlüsselung“ der Signatur

tur mit einem anderen als Susannes öffentlichen Schlüssel würde zu einem Ergebnis führen, das nicht mit dem mitgelieferten Ursprungstext übereinstimmt.

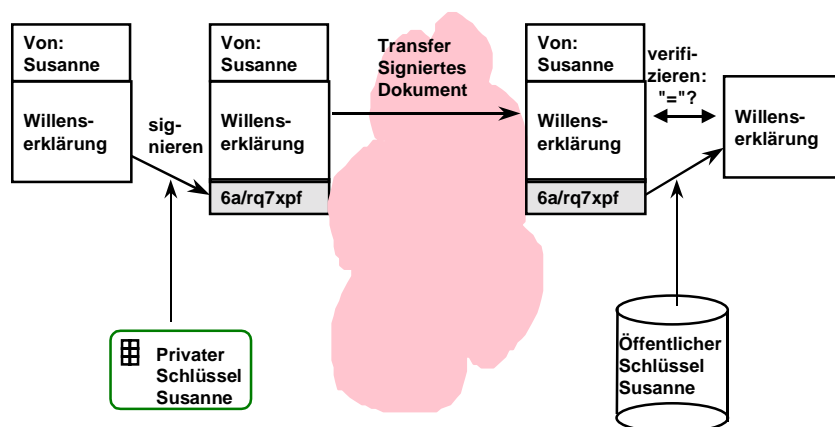


Abb. 4: Digitale Signatur

In der Praxis wird ein Klartext erst zu einem Hashwert kurzer Länge „gefaltet“ und dann der „gefaltete Text“ (d.i. der Hashwert) mit dem privaten Schlüssel verschlüsselt. Dabei verwenden alle Benutzer dieselbe Hashfunktion, etwa MD5 [z.B. in BSchn_96]. Das geschieht hauptsächlich, um das Signaturverfahren schneller, also billiger, zu machen, denn Verschlüsselungsvorgänge sind um so zeitraubender, je länger der zu verschlüsselnde Text ist, während Hash-Verfahren auch bei sehr langen Texten noch schnell sind. Einen zusätzlichen Sicherheitseffekt erzielt das „Falten“ eines Textes dadurch, dass es eine digitale Signatur irreversibel macht. Aus einem Hashwert kann man nämlich den Originaltext nicht rekonstruieren.

Eine andere Anwendung der asymmetrischen Kryptografie ist das Verbergen von Daten, die man über ein ungeschütztes offenes Netz übertragen und dabei vor unbefugten Mitlauschern schützen will. Man verschlüsselt die Daten vor dem Versenden mit dem öffentlichen Schlüssel des Empfängers. Abbildung 5 veranschaulicht das.

Um einem bestimmten Empfänger, den wir Erwin nennen wollen, eine Nachricht verschlüsselt zukommen zu lassen, die nur er und niemand sonst wieder entschlüsseln kann, besorgt sich jeder, der das tun möchte, den öffentlichen Schlüssel von Erwin, z.B. aus einem öffentlichen Verzeichnis oder indem er vorher Erwin um seinen öffentlichen Schlüssel bittet. Er verschlüsselt dann den Text mit Hilfe von Erwins öffentlichen Schlüssel. Diesen verschlüsselten Text schickt der Sender an Erwin, am besten zusammen mit dem öffentlichen Schlüssel, damit Erwin weiß, dass er gemeint ist und welcher seiner öffentlichen Schlüssel (vielleicht hat er mehrere) verwendet worden ist. Zum Entschlüsseln braucht Erwin nur das Entschlüsselungsverfahren mit seinem privaten Schlüssel auf das Kryptogramm anzuwenden, um den ursprünglichen Klartext wieder zu erhalten. Da niemand an-

deres außer Erwin über Erwins privaten Schlüssel verfügt, kann auch niemand anderes den Klartext ermitteln.

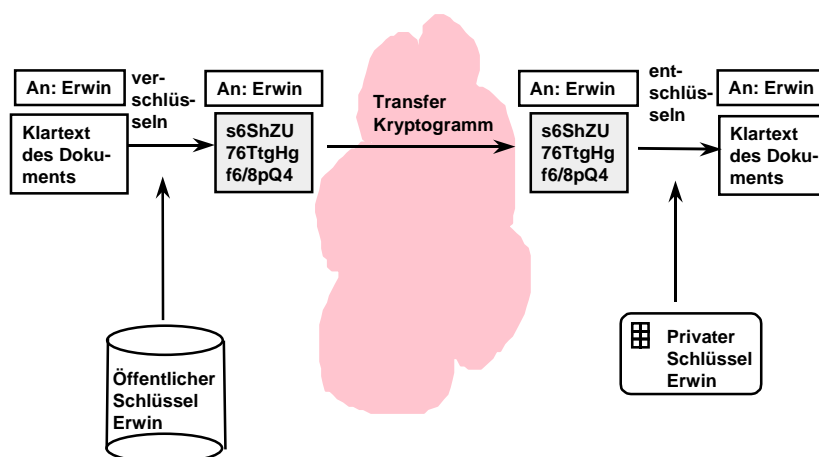


Abb. 5: Elektronische Daten asymmetrisch verschlüsseln

In der Praxis wird ein sogenanntes Hybridverfahren angewendet, das in der Summe asymmetrisch ist, das aber zur Zeitersparnis einen symmetrischen Anteil enthält: Der zu verschlüsselnde (lange) Text wird mit einem schnellen symmetrischen Algorithmus verschlüsselt, und zwar mit einem symmetrischen Schlüssel, der extra für diesen einen Vorgang vom Sender erzeugt wird. Dieser (kurze) symmetrische Schlüssel wird dann mit einem asymmetrischen Verfahren verschlüsselt und so dem Kryptogramm des Textes beigelegt. Das wird deshalb so gemacht, weil die bekannten asymmetrischen Verfahren wie RSA oder ElGamal bei langen Texten zeitaufwendig sind, während man sehr schnelle symmetrische Algorithmen kennt, z.B. DES oder IDEA, die genauso sicher sind. Das Hybridverfahren ist insgesamt ein asymmetrisches Verfahren, billiger als die reinen asymmetrischen Verfahren, aber genauso sicher.

Mit asymmetrischen Verschlüsselungsverfahren stehen also zwei Sicherheitsdienste zur Verfügung: zum einen die digitale Signatur, die die Authentizität der Kommunikationspartner, die Datenintegrität und die Nicht-Abstreitbarkeit des Ursprungs sicherstellt; zum anderen die Verschlüsselung der Kommunikation, die ihre Vertraulichkeit sicherstellt.

Bei Einsatz asymmetrischer Verfahren brauchen geheime Schlüssel nicht mehr aus der Hand gegeben zu werden. Die Benutzung eines privaten Schlüssels ist bis auf seinen Besitzer rückführbar: niemand anders als er verfügt über ihn. Bei Verwendung von persönlichen Schlüsselpaaren ist deshalb die Sicherheit auch über unsichere Netze hinweg gewährleistet, denn die Partner können durch geeignete Kodierung ihrer Daten Kryptogramme über beliebige Netze verschicken. Dadurch kann man auch über offene Netze elektronische Geschäfte sicher abwickeln.

Natürlich sind dabei hohe Sicherheitsanforderungen an die lokalen Systeme zu stellen. Zum Beispiel darf ein Besitzer seinen privaten Schlüssel nicht verlieren oder aus Versehen außerhalb seiner Chipkarte sichtbar machen können. Die lokalen Funktionen müssen korrekt implementiert und unmanipuliert sein. Die Bedienung muss so einfach und verständlich sein, dass dem Benutzer keine Fehler bei der Anwendung der Signatur oder der Verschlüsselung unterlaufen können. Besonders wichtig und oft übersehen ist die Anforderung, dass alle beteiligten Partner dieselbe Ansicht der signierten Inhalte haben müssen.

8 Zertifizierung öffentlicher Schlüssel

Asymmetrische kryptografische Verfahren für digitale Signaturen erfordern eine Sicherungsinfrastruktur für das Management von Schlüsseln und für die sichere Zuordnung von öffentlichen Schlüsseln zu ihren Besitzern. Die sichere und von jeder Seite nachvollziehbare Bindung eines öffentlichen Schlüssels an ihren Besitzer als sozialer Person, bezeichnet durch ihren Namen, nennt man die Zertifizierung eines öffentlichen Schlüssels. So ist etwa der Personalausweis ein Zertifikat, das den Namen seines Besitzers an seine soziale Existenz (als Bürger des-und-des Landes, wohnhaft da-und-da usw.) und an gewisse unverfälschbare Merkmale wie ein Passfoto bindet. Anhand des Fotos kann jeder den Namen und den sozialen Bezug seines Besitzers verifizieren.

Der Zertifizierungsprozess für digitale Signaturen kann gesetzesmäßig formalisiert sein wie beim Personalausweis. Diesen Weg beschreitet das deutsche Signaturgesetz SigG [IUK_97]. Es unterstellt die Sicherheit einer Signatur, wenn sie unter bestimmten, im Gesetz ausgeführten Bedingungen zustande gekommen ist. Kern des Gesetzes bilden Anforderungen an die Zertifizierungsstellen, welche Zuordnungen zwischen öffentlichen Schlüsseln und ihren Eigentümern beglaubigen. Der öffentliche Schlüssel wird zur Verifikation einer digitalen Signatur eingesetzt. Durch die beglaubigte Zuordnung des öffentlichen Schlüssels zu seinem Besitzer kann auch die Signatur und damit der signierte Text selbst unabstreitbar der signierenden Person zugerechnet werden. Wenn nun dabei die Regeln des Gesetzes eingehalten werden, dann würde im Streitfall ein Gericht die Sicherheitsvermutung anwenden und die Signatur zunächst als echt anerkennen [GeRo_98].

Das SigG folgt dem Prinzip der hierarchischen Zertifizierungsinfrastruktur nach [X509_88]. Dabei wird zuerst eine staatlich besonders kontrollierte einmalige „Wurzel-Zertifizierungsstelle“ etabliert, deren öffentlicher Schlüssel dadurch authentisch ist, dass er allgemein bekannt ist. Diese zertifiziert öffentliche Schlüssel von anderen Zertifizierungsstellen, die ihr auf diese Weise unmittelbar „untergeordnet“ sind. Diese können wiederum andere Zertifizierungsstellen zertifizieren, usw. In der untersten Stufe werden Personen zertifiziert, die ihrerseits keine Zertifikate mehr ausstellen. Nach dem deutschen Signaturgesetz ist dieser Zertifizierungsbaum allerdings auf zwei Ebenen beschränkt: oberste Zertifizierungsinstanz ist die Regulierungsbehörde für Post und Telekommunikation (RegTP) in Mainz; unter ihr gibt es zugelassene Zertifizierungsstellen für Personen, unter denen die Zertifizierungsstelle der Deutschen Telekom die erste war.

Allerdings funktioniert Zertifizierung auch ohne staatliche Regulierung. Private Initiativen können ohne weiteres ihre eigenen Zertifizierungsinfrastrukturen aufbauen. Das geschieht zum Beispiel im Rahmen der Europäischen Forschungsnetze, wo Zertifizierungsstellen ihre Mitglieder aus den Hochschulen und Forschungseinrichtungen zertifizieren. Ein anderes Beispiel bietet die Finanzwelt. „Identrus“ ist eine internationale Initiative von Privatbanken [Iden_00]. Sie baut eine grenzüberschreitende Zertifizierungsinfrastruktur auf, um ihren Firmenkunden zum Zweck digitaler Finanztransaktionen über das Internet zertifi-

zierte Signaturen zu ermöglichen. Für andere Zwecke sollen ihre Zertifikate keine Gültigkeit haben.

Vor allen anderen Initiativen hatte schon Anfang der 1990er Jahre eine Art „Grassroot“-Bewegung für Zertifikate „von unten nach oben“ von sich reden gemacht. Idee und Realisierung stammt von Phil Zimmermann, der im Alleingang das Verschlüsselungs- und Signaturprodukt „PGP – Pretty Good Privacy“ geschrieben hatte. Es handelt sich um leicht zugängliche frei erhältliche Software, die ihrem Anwender erlaubt, Texte mit den modernsten kryptografischen Verfahren (RSA, DSA, IDEA, MD5) digital zu signieren und zu verschlüsseln. Dabei erzeugt jeder Anwender nach freier Entscheidung einen persönlichen Namen und ein Schlüsselpaar. In der Regel setzen PGP-Benutzer ihre Email-Adresse als Namen ein.

Mit PGP kann jeder Benutzer jeden öffentlichen Schlüssel anderer Benutzer zertifizieren. Das funktioniert zwar, ist aber außerordentlich aufwendig. Es verlangt nämlich, dass jeder Kommunikationsteilnehmer mit jedem seiner Kommunikationspartner Schlüssel austauscht und diese auf Echtheit überprüft, bevor er mit ihm sicher kommunizieren kann.

Deshalb hat PGP ein weiteres Zertifizierungsverfahren implementiert, indem Personen, die einander fremd sind, durch eine dritte Person miteinander bekannt gemacht werden. Diese dritte Person heißt in der PGP-Terminologie „Introducer“. Ein „Introducer“ kann einen öffentlichen Schlüssel, den er selbst überprüft hat, digital signieren und anderen Personen weiterreichen. Wenn diese ihm als „Introducer“ vertrauen, dann werden sie die von ihm signierten öffentlichen Schlüssel für echt halten. Dadurch können nicht nur einzelne, sondern ganze Sammlungen von oft hunderten von Schlüsseln weitergereicht werden. Die Besonderheit dieses Zertifizierungsverfahrens von PGP besteht darin, dass sich jeder ohne weitere formale Qualifikation daran beteiligen kann.

Allerdings hat auch das Introducer-Verfahren ein Wachstumsproblem. Am Ende muss man eben doch ein persönliches Verhältnis zu einem Introducer haben, da seine Zertifizierungsregeln ja nicht geregelt sind. In der Praxis beschränken sich die zertifizierten Sammel Listen von PGP auf geschlossene Gruppen. PGP wird weniger zum Signieren, als zum Verschlüsseln von Nachrichten unter Freunden verwendet. PGP hat den Verdienst, die Technik der asymmetrischen Kryptografie im Internet populär gemacht zu haben.

9 Anwendungsbeispiele

Digitale Signaturen können zur Authentifizierung kommunizierender Partner verwendet werden. Beispielsweise können zwei E-Mail-Server digital signierte Erkennungsnachrichten austauschen, bevor sie eine Verbindung zueinander etablieren.

Die Mechanismen für den Integritäts- und Vertraulichkeitsschutz werden in verschiedenen funktionalen Bereichen der Kommunikations- und Kooperationstechnik eingesetzt. Das Internet-Protokoll IPv6 enthält entsprechende Sicherheitselemente zum Schutz der Verbindungen zwischen den Internet-Knoten. Sie sind spezifiziert, aber in der Praxis noch nicht eingesetzt. Das anwendungsunabhängige Sicherheitsprotokoll „Secure Socket Layer“ [SSL_96] wurde ursprünglich von Netscape zur Absicherung der Kommunikationskanäle zwischen Browser und Server im World-Wide Web eingeführt. Es funktioniert aber auch für andere Anwendungs-komponenten im Internet.

Spezielle Sicherungsverfahren für Anwendungen, wie „Secure HTTP“ für Web-Dokumente oder X.400 für Electronic Mail haben sich nicht durchgesetzt.

Das vom Internet standardisierte „Privacy Enhanced Mail“ [PEM_93], das heute im „Secure MIME“-Format fortlebt [PKCS_93] und das von Phil Zimmermann erfundene „Pretty Good Privacy“ [PGP_95] sind Sicherungsverfahren für elektronische Nachrichten. Ihre Protokollelemente sind in reinem ASCII spezifiziert und können daher innerhalb aller bestehenden Nachrichtenformate ausgetauscht werden, ohne die Nachrichtentransfersysteme oder gar die darunterliegenden Netzprotokolle zu berühren.

Auch menschliche Benutzer können sich mit Unterstützung ihrer PCs auf diese Weise voneinander authentifizieren. Populär ist bereits Homebanking über das Internet, das heute noch oft über SSL-Kanäle und PIN-TAN-Verfahren abgesichert ist. Hier steht mit dem „Home-Banking Computer Interface“ [HBCI_97] ein mächtiger Standard der deutschen Finanzinstitute bereit, der die moderne asymmetrische Kryptografie in ihrer ganzen Bandbreite einsetzt.

In prototypischen Versuchsumgebungen werden vertragsbasierte Geschäftskommunikation (E-Commerce), kommunale Verwaltung (E-Government) und Gesundheitsanwendungen (E-Health) entwickelt und erprobt. Das Ziel ist in allen Fällen, verbindliche und vertrauliche Kommunikation mit Hilfe digitaler Signaturen und Verschlüsselung zu ermöglichen. Dabei werden anwendungsspezifisch einzelne Sicherungselemente (wie Signaturen) in ihre komplexen Kommunikationsprotokolle integriert. Allein der Austausch eines unterschriftsreifen Vertrags zwischen zwei Partnern erfordert den Austausch mindestens dreier Nachrichtenblöcke mit dreifach ineinandergeschachtelten Signaturelementen, z.B. „BAKO“ in [GKW_97].

10 Zusammenfassung und Ausblick

Asymmetrische kryptografische Mechanismen sind dazu geeignet, Telekooperationen in offenen Netzen sicher zu machen. Sie können sowohl in netznahen Protokollen, als auch auf der obersten, personenbezogenen Ebene eingesetzt werden. Man kann elektronische Nachrichten signieren und verschlüsseln. Man kann elektronisch unabstreitbare Willenserklärungen abgeben und Verträge schließen. Sowohl per E-Mail, als auch im World-Wide Web lassen sich digital signierte und verschlüsselte Dokumente als Bestandteil elektronischer Geschäfte austauschen. Geheimnisse wie Passwörter oder geheime Schlüssel brauchen nicht mehr über das Netz kommuniziert zu werden.

Es muss aber noch auf ein *politisches Problem* hingewiesen werden, das einer ungehinderten Ausbreitung kryptografischer Anwendungen im Wege steht. Kryptografie wird von allen Staaten der Welt als ein Problem der nationalen Sicherheit angesehen. Es bestehen weltweit große politische Vorbehalte gegen den Aufbau von Kommunikationsnetzen, in denen Verbrechen oder feindliche Spionage verborgen unter dem Schutz öffentlich zugänglicher nicht-brechbarer Verschlüsselung verübt werden können. Zum Beispiel wecken die Entwicklungen von „digitalem Geld“ Ängste vor neuen Dimensionen des Geldwaschens.

Diese Bedenken können nicht einfach von der Hand gewiesen werden. Aber der heute noch weit verbreitete Versuch, vor allem in den USA, Kryptografie einfach zu verbieten, ist naiv. Die kryptografischen Verfahren sind bekannt, sie beruhen auf mathematisch veröffentlichten und nicht besonders schwer zu verstehenden Theorien. Ihre Implementierung ist einfach. Das Verbot der Verwendung von Kryptografie führt dazu, dass die „guten Bürger“ sich daran halten werden, während die „Mafia“ sich einfach darüber hinwegsetzen wird. Ein Verbot würde also gerade die falsche Seite stärken. Im Internet wird dazu ein treffen-

des Phil Zimmermann-Zitat verbreitet: „*When privacy is outlawed, only the outlaws will have privacy*“.

Das Problem ist politischer Art und muss politisch gelöst werden. Eine wichtige Basis dafür bilden die Aufklärung der Bürger und eine öffentliche Debatte. In Deutschland genießen wir gegenwärtig einen politisch gewollten liberalen Umgang mit Kryptografie.

Die größte Herausforderung bildet die Etablierung von vertrauensbildenden Maßnahmen (englisch „Trust“) im Internet. Die digitale Signatur kann hierfür einen grundlegenden Baustein bilden. Aber die Absicherung einzelner isolierter Aussagen genügt nicht. Vertrauen muss stabil in einem komplexen Zusammenspiel von Wollen, Wissen und Handeln bestehen können. Es scheint so, dass Zertifizierungsinfrastrukturen großer wohlorganisierter und zweckorientierter Verbände [z.B. Iden_00] den Weg zu vertrauenswürdiger Kommunikation in ihrem Anwendungsfeld (z.B. für den Geldtransfer) ebnen können. Jedenfalls sind die großen Anwendungen im offenen Internet erst im Aufbau, sei es Banking, Einkäufen und Bezahlen, Business-to-Business-Kooperation oder kommunale Verwaltung. Aus Sicht von 1999 gesprochen, hat das Electronic Commerce im Internet noch nicht wirklich begonnen.

Anhang: Überblick über das RSA-Verfahren

Für eine große, aus den Primzahlen p und q zusammengesetzte Zahl n , erzeuge man zwei Primzahlen d und e mit folgenden Eigenschaften:

- $1 < p, q < d, e < n$
- p und q sind Primzahlen (und bleiben geheim)
- $n = p \cdot q$ heißt der „Modulus“
- e ist eine systemweite, öffentlich bekannte Konstante
- d wird so gewählt, dass $d \cdot e \equiv 1 \pmod{(p-1) \cdot (q-1)}$
- n (und damit p und q) und d sind von Person zu Person verschieden
- n wird der „öffentliche Schlüssel“ einer Person
- d wird der zugehörige „private Schlüssel“ einer Person
- p und q werden jetzt „vergessen“: sie werden nicht mehr gebraucht, aber sie bilden eine Hintertür zur Berechnung von d , denn $d = e^{-1} \pmod{(p-1) \cdot (q-1)}$ ist leicht zu berechnen. Hingegen ist d allein aus Kenntnis von e und n nur dann „leicht“ zu berechnen, wenn p und q bekannt sind. Auf diese Weise beruht die Sicherheit von RSA auf dem Faktorisierungsproblem von n
- Für alle m gilt nach dem kleinen Satz von Fermat und Euler: $m^{ed} \equiv m \pmod{n}$

Digitale Signatur mit RSA:

- e ist eine systemweite, öffentlich bekannte Konstante
- Susanne besitzt ihr individuelles Schlüsselpaar (n öffentlich, d privat)
- Susanne signiert einen Text m auf folgende Weise:
- Susanne faltet m mit Hilfe einer systemweit einheitlichen Hashfunktion auf eine Bitfolge $\text{hash}(m)$, dann verwendet Susanne ihren privaten Schlüssel d und berechnet die „Signatur“ $s := \text{hash}(m)^d \pmod{n}$
- Jeder, der den Text m und seine Signatur s kennt, kann sie wie folgt verifizieren:

- er benutzt Susannes öffentlichen Schlüssel e und berechnet $x := s^e \pmod{n}$. Dann bildet er $\text{hash}(m)$ und prüft, ob $x \equiv \text{hash}(m) \pmod{n}$ gilt oder nicht. Im Falle der Übereinstimmung gilt die Signatur als verifiziert, andernfalls als falsifiziert, denn es gilt nach Fermat und Euler: $x \equiv s^e \equiv \text{hash}(m)^d \equiv \text{hash}(m) \pmod{n}$

Datenverschlüsselung mit RSA:

- e ist eine systemweite, öffentlich bekannte Konstante
- Erwin besitzt sein individuelles Schlüsselpaar (n öffentlich, d privat)
- Jeder, der Erwin eine vertrauliche Nachricht m schicken will, benutzt Erwins öffentlichen Schlüssel e und berechnet das Kryptogramm: $c := m^e \pmod{n}$
- Zur Entschlüsselung von c benutzt Erwin seinen privaten Schlüssel d , indem er berechnet: $x := c^d \pmod{n}$. Da c mit seinem öffentlichen Schlüssel e berechnet worden war, geht Erwin davon aus, dass $x = m$ der ursprüngliche Klartext ist, denn es gilt nach Fermat und Euler: $x \equiv c^d \equiv m^{ed} \equiv m \pmod{n}$

Literatur

- [BSch_96] Bruce Schneier: *Applied Cryptography. Protocols, Algorithms, and Source Code in C*. 2nd Ed. Wiley & Sons, Chichester 1996, 758 p.
- [Chau_85] Chaum, David: *Security without Identification: Transaction systems to make big brother obsolete*. Com. ACM, Vol. 24, No. 2, 1985, 1030-1044.
- [DiHe_76] W. Diffie, M.E. Hellman: *New Directions in Cryptography*. IEEE Transactions on Information Theory. Vol.IT-22, 644-654, 1976.
- [ElGa_85] T. ElGamal: *A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms*. IEEE Transactions on Information Theory, Vol.IT-31, 469-472, 1985.
- [ESig_99] EU: Directive 1999/93/EC on a community framework for electronic signatures. 13.12.1000. In: Official Journal of the European Communities, 2000. http://europa.eu.int/comm/internal_market/en/media/sign/index.htm
- [GeRo_98] M. Geppert, A. Roßnagel: *Telekommunikations- und Multimediarecht*. Contains: TelekommunikationsG, TelediensteG, TeledienstedatenschutzG, SignaturG, SignaturVO, Mediendienste-Staatsvertrag. Beck-Texte im dtv, München 1998.
- [GKW_97] P. Glöckner, S. Kolletzki, M. Wichert: *Signed Unique References - A BAKO Extension Proposal*. Proceedings of JENC8, Edinburgh 1997, pp. 431/1-9. <http://sit.gmd.de/SICA/Publications/sure/>
- [HBCI_97] SIZ – Informatikzentrum der Sparkassenorganisation, Bonn: *HBCI – Homebanking-Computer-Interface – Schnittstellenspezifikation*. Hrsg.: Bundesverband deutscher Banken e.V., Köln; Deutscher Sparkassen- und Giroverband e.V., Bonn; Bundesverband der Deutschen Volksbanken und Raiffeisenbanken e.V., Bonn; Verband öffentlicher Banken e.V., Bonn. Version 2.0, 24.7.97. <http://www.siz.de>.
- [Iden_00] *Identrus*. Providing a Global Framework for Trusted Business to Business E-Commerce. Partner Banks, among many others: Bank of America, Barclays, Canadian Imperial Bank of Commerce, Chase Manhattan, Citigroup, Deut-

- sche Bank, Dresdner Bank, Commerzbank, Hypo Vereinsbank, The Industrial Bank of Japan, Sanwa, Societe General. 2000, <http://www.identrus.com>.
- [IUK_97] B.R. Deutschland: *Informations- und Kommunikationsdienstegesetz (IuKDG)*. Enthält Teledienstegesetz (TDG, Art. 1), Teledienstedatenschutzgesetz (TDDSG, Art. 2), Signaturgesetz (SigG, Art. 3). Deutscher Bundestag, 1.6.1997, <http://www.iid.de/rahmen/>. Teilw. Auch in [GeRo98].
- [Kah_67] David Kahn: *The Codebreakers: The Story of Secret Writing*. MacMillan, New York 1967.
- [Ker_88] Steiner, J.G.; Neumann, C.; Schiller, J.I.: *Kerberos: An Authentication Service for Open Network Systems*. USENIX Winter Conference, Dallas Texas, 9-12 Feb 1988. Proceedings pp. 191-202.
- [P3P_00] W3C: *The Platform for Privacy Preferences 1.0 (P3P1.0) Specification*. W3C Working Draft, 10 May 2000. <http://www.w3.org/TR/P3P/>.
- [PEM_93] Internet IETF: *Privacy Enhancement for Internet Electronic Mail*. Part I-IV („PEM“). RFC 1421-1424, Feb 1993.
- [Pfitz_87] Pfitzmann, A.: *Diensteintegrierende Kommunikationsnetze mit teilnehmerüberprüfbarem Datenschutz*. Informatik-Fachberichte Nr. 234. Springer Verlag, Berlin usw. 1987.
- [PGP_95] Garfinkel, S.: *PGP: Pretty Good Privacy*. A Guide for PGP Users. O'Reilly & Associates, Inc., Sebastopol, CA, January 1995.
- [PKCS_93] RSA Laboratories: PKCS #1-10, *Public Key Cryptography Standards*, Nov 1, 1993. <http://www.rsa.com/pub/pkcs>.
- [RSA_78] R. Rivest, A. Shamir, L. Adleman: *A Method for Obtaining Digital Signatures and Public Key Cryptosystems*. Com ACM, Vol 21 No 2, 120-126, Feb 1978.
- [Scho_73] A. Scholz, B. Schoeneberg: *Einführung in die Zahlentheorie*. Sammlung Göschen de Gruyter, Berlin, New York 1973.
- [SSL_96] Freier, A.; Karlton, P.; Kocher, P.: *The SSL Protocol (Secure Socket Layer), Version 3.0*. Internet Draft, 18 Nov 1996, 63 pages, draft-freier-ssl-version3-02.txt. <http://home.netscape.com/eng/ssl3/>. Included in Transport Layer Security (TLS) standardization of the IETF, <http://www.ietf.org/html.charters/tls-charter.html>
- [X509_88] X.509 – *The Authentication Framework*. In: ISO/IEC 9594, ITU X.500 (1988/92): Information technology – Open Systems Interconnection – *The Directory* 1993(E).