Keine Angst um Ihr Geld!

Entwicklung des sicheren Zahlungsverkehrs im Internet

Von Michael Waidner[*]

Mit rasanter Geschwindigkeit entwickelt sich das Internet zu einem Medium, über das jeder mit jedem Geschäfte abwickeln kann. Dabei spielt es keine Rolle mehr, ob die Partner sich bereits zuvor kannten, ob sie im selben Land angesiedelt sind, oder dieselbe Sprache sprechen. Sicherheit vor Betrug und Datenschutz auf diesem globalen Marktplatz zu garantieren ist ein Problem völlig neuer Dimension. Eine der Grundfunktionen hierfür ist das sichere Bezahlen.

Sicherheit im Internet ist am ehesten mit dem Nachrichtenaustausch über Postkarten zu vergleichen: Vertraulichkeit des Inhalts ist ebensowenig gesichert wie Echtheit der Absenderangaben. Zieladressen können «gestohlen» und damit Daten an einen falschen Adressaten umgelenkt werden. Hinzu kommt, dass jeder im World Wide Web (WWW) einen «Laden» einrichten kann, etablierte vertrauenswürdige Organisationen ebenso wie Betrüger. Verfahren wie «PGP» für elektronischer Briefe oder «SSL» für die Kommunikation im WWW können die Sicherheit zwar verbessern. Es fehlt aber noch die geeignete umfassende Infrastruktur zur Zertifizierung von Schlüsseln, und den Benutzern fehlt oft das Wissen darüber, was geschützt ist und was nicht.

Kommunikationssicherheit ist nicht alles: Das für elektronischen Handel zunächst wesentlichste Problem ist das elektronische *Bezahlen*. In «Geld» verwandelte Bits stellen einige sehr spezielle Sicherheitsanforderungen.

Authentizität durch digitale Signaturen

Wie bei einem Papierscheck die Unterschrift geprüft werden kann, so muss auch bei einer elektronischen Zahlung die Echtheit verifiziert werden können. Hierzu dienen *kryptographische Authentifizierungsverfahren:* Man interpretiert eine digitale Nachricht als Zahl und wendet darauf gewisse mathematische Operationen an. In diese geht neben der Nachricht noch eine weitere Zahl ein, der sogenannte «Schlüssel». Das Ergebnis wird dann zusammen mit der Nachricht übertragen.

Bei den einfacheren *symmetrischen* Verfahren einigen sich Erzeuger und Empfänger der Nachricht zuvor auf einen gemeinsamen Schlüssel, der vor allen anderen geheimgehalten wird (etwa wie eine PIN). Der Empfänger kann dann auf Nachricht und Schlüssel diesselbe Operation wie der Erzeuger anwenden und prüfen, ob er dasselbe herausbekommt. Falls ja, war die Nachricht echt. Der Nachteil dieser Verfahren ist, dass ein Gericht niemals entscheiden kann, ob eine Nachricht vom Erzeuger authentisiert wurde oder aber vom vermeintlichen Empfänger.

Die moderneren Verfahren sind daher *asymmetrisch*: Erzeuger und Empfänger verwenden zwei *unterschiedliche* Schlüssel. Beide werden vom Erzeuger generiert. Der *Signaturschlüssel* bleibt beim Erzeuger und ist geheim. Der *Testschlüssel* wird so veröffentlicht, dass jeder potentielle Empfänger ihn später nachweislich dem Erzeuger zuordnen kann. Zum Signieren nimmt der Erzeuger die Nachricht und den Signaturschlüssel und berechnet hieraus eine *digitale Signatur*. Der Empfänger nimmt die Nachricht, diese Signatur und den Testschlüssel, und sein Test liefert als Ergebnis «authentisch» oder «falsch». Ein Dritter kann denselben Test anwenden und sich so von der Echtheit überzeugen.

---

[*] Dr. Michael Waidner ist Leiter der Gruppe «Netzwerksicherheit» am IBM Forschungslaboratorium Zürich. Mehr Informationen findet man im World Wide Web unter dem URL «http://www.zurich.ibm.com/Technology/Security».

Dieser Artikel erschien mit wenigen Veränderungen in:
Neue Zürcher Zeitung (NZZ), 8. Oktober 1996, Nr. 234, Seite B51

Sehr häufig wird für Kreditkartenzahlungen im Internet noch auf *jede* Form kryptographischer Authentifizierung verzichtet. Der einzige Echtheisnachweis ist dann die Kreditkartennummer. Da diese bei jeder Zahlung weitergegeben wird, ist das Verfahren äusserst unsicher und nur zu rechtfertigen, wenn der Kunde dabei letztlich kein Risiko zu tragen hat. Um die Verbreitung der Nummern im Internet zu beschränken, sollten diese dann aber zumindest immer *verschlüsselt* übertragen werden.

Verschlüsselung wird ebenfalls durch kryptographische Verfahren erreicht. Dabei wird die Nachricht und der Schlüssel in ein *Chiffrat* abgebildet und nur dieses übertragen. Der Empfänger kann dann mittels eines nur ihm (und eventuell noch dem Erzeuger) bekannten *Entschlüsselungsschlüssels* wieder auf die Nachricht zurückschliessen. Bei einfacheren Ansätzen (wie Verschlüsselung mit «SSL») wird die Kreditkartennummer nur auf dem Weg zum *Händler* verschlüsselt. Vollständige Zahlungssysteme wie «iKP» verschlüsseln zwischen Kunde und *Bank*, d.h. schützen auch gegen den Händler.

Autorisierung durch On-line Verifizierung oder Smartcards

Digitale Daten können leicht, perfekt und unbemerkt kopiert werden. Folglich muss der Empfänger einer Zahlung sich davon überzeugen können, dass diese auch *gedeckt* ist. In *on-line* Zahlungssystemen werden alle Zahlungen an einen Bankserver weitergereicht, der Doubletten herausfiltert und die Deckung bestätigt. In *off-line Systemen* wird die Authentifikation von einer *Smartcard* berechnet. Diese garantiert zugleich für die Deckung, indem sie den Gesamtbetrag aller Zahlungen begrenzt. Doubletten werden vom Empfänger erkannt, indem die Zahlungsnachricht teilweise vom Empfänger selbst mitgeprägt werden muß, d.h. alte Nachrichten würden nicht passen.

Grundvoraussetzung für off-line Systeme ist die *physische* Sicherheit von Smartcards. Tatsächlich gelten Smartcards als relativ sicher: ein gut ausgerüstetes physikalisches Forschungslabor könnte zwar Smartcards systematisch brechen (d.h. die geheimen Schlüssel auslesen), für einen durchschnittlichen Verbrecher gibt es aber deutlich einfachere Möglichkeiten, illegal zu Geld zu kommen. Zahlungssysteme, die grössere Geldbeträge bewegen, könnten den Brechaufwand jedoch rechtfertigen und sollten daher stets als on-line Systeme gestaltet werden.

Vertraulichkeit durch Verschlüsselung

Die Umstände und Daten einer Zahlung müssen vor unbefugter Kenntnisnahme geschützt werden.

Schutz vor völlig Unbeteiligten kann durch Verschlüsselung (s.o.) erreicht werden, etwa mittels «SSL», und ist relativ unabhängig davon, welches Zahlungssystem verwendet wird.

Anonymität ist eine typische Eigenschaft von Bargeld: im nachhinein kann man durch Anschauen des Geldes den Zahlenden nicht identifizieren, und meist kann man zwei Banknoten auch nicht ansehen, ob sie jemals vom selben Zahlenden verwendet wurden. Die Identität von elektronischem Geld gegenüber dem *Empfänger* zu verbergen ist vergleichsweise einfach: statt Namen werden *Pseudonyme* verwendet, wobei die Abbildung der Pseudonyme auf Konten nur den Banken bekannt ist. Dieser Ansatz wird z.B. von «iKP» verfolgt. Die Bargeld-artigen Systeme «ecash» und «CAFE» erreichen durch relativ komplexe kryptographische Verfahren auch Anonymität gegenüber dem Bankensystem.

An elektronische Zahlungen werden dieselben Anforderungen gestellt wie an solche in der Papierwelt: Zahlungen auf Rechnung, mit Schecks oder Kreditkarten müssen die Vertraulichkeit wahren. Alltagszahlungen, die man sonst mit Münzen erledigt hätte, sollten auch hier anonym sein.

Zahlungssysteme

	On-line Zahlungssysteme	Off-line Zahlungssysteme
Zahlungsfluss kann durch Systembetreiber kontrolliert werden	Kreditkarten: • Ohne Kryptographie: *First Virtual* • Mit Kryptographie: *CyberCash, iKP* Vorgeschlagener Standard: *SET* Schecks: • *FSTC Electronic Check* Kleinst"bar"zahlungen: • *Millicent, NetBill, CAFE, μ-iKP, PayWord.* Zahlungsvermittler: • *Globe ID(R) by GC Tech* • *OpenMarket Payment Switch*	Smartcard-basiertes elektronisches Geld: • Mit symmetrischer Kryptographie: *Danmont, Banksys Proton* • Mit digitalen Signaturen: *Europay Clip* • Typ des verwendeten Verfahrens nicht öffentlich bekannt: *Mondex*
Anonymisierte Zahlungen	• Anonymisiert durch mehrere «Wechselstuben»: *NetCash, Anonymous Creditcards* • «Anonymisierte» digitale Signaturen: *Digicash e-cash*	• «Anonymisierte» digitale Signaturen: Europäisches ESPRIT R&D Projekt *CAFE*

Abb. 1 Übersicht über Elektronische Zahlungssysteme

Von besonderer Bedeutung ist das von Europay, Mastercard und VISA als Standard vorgeschlagene Kreditkartensystem «SET», entworfen von GTE, IBM, Microsoft, Netscape, SAIC, Terisa und VeriSign. Die erste verbindliche Version wurde im Juli 1996 veröffentlicht. Ab Ende 1996 wird IBM Produkte basierend auf «SET» anbieten.

Das Grundprinzip entspricht dem der «2KP» bzw. «3KP» Variante von «iKP». «iKP» wurde Anfang 1995 von Wissenschaftlern in den IBM Forschungslaboratorien in Zürich und New York entwickelt und von Mastercard als erster Vorschlag eines Standards übernommen. Nach der Einigung mit VISA auf die Entwicklung eines gemeinsamen Vorschlags war es der Ausgangspunkt für IBM's Beitrag zu «SET». Derzeit wird in einem niederländischen Feldversuch ein in Zürich entwickelter Prototyp von «iKP» getestet.

In «iKP» spezifiziert der Händler alle Zahlungsdaten und signiert diese, wodurch der Kunde den Händler sicher identifiziert. Der Kunde verschlüsselt die Kreditkartendaten so, dass nur die Bank des Händlers, aber nicht der Händler selbst, diese Daten lesen kann, und signiert dieses Chiffrat zusammen mit den übrigen Zahlungsdaten. Der Händler reicht dieses weiter an seine Bank, die alles entschlüsselt und prüft, und hieraus eine Anfrage an das existierende Kreditkartensystem generiert. Die Antwort wird von der Bank signiert und dem Händler mitgeteilt. «2KP» und «3KP» beziehen sich auf die Anzahl der

Signaturschlüssel im System: «3KP» ist die eben skizzierte Variante. Lässt man die Signaturen des *Kunden* weg, so hat man «2KP». Dieses erfordert einen geringere Infrastruktur (da die Schlüssel der Kunden nicht mehr zertifiziert werden müssen), reduziert die Sicherheit aber auf die von Zahlungen via Telefon, sprich, die Autorisierung des Kunden ist nicht nachweisbar -- woraus folgt, dass der Kunde nicht gezwungen werden sollte, das damit verbundene Risiko selbst zu tragen.

Gleichwohl «iKP» nur kryptographische Verfahren mit hoher Sicherheit (d.h. lange Schlüssel) verwendet, ist es aus den USA exportierbar. Eine entsprechende Exportgenehmigung wird auch für «SET» erwartet.

Zukunftsmusik?

Sehr wahrscheinlich wird sich «SET» im Laufe des nächsten Jahres als bevorzugte Methode für Kreditkartenzahlungen im Internet durchsetzen. Neben Kreditkarten sind in absehbarer Zeit auch Systeme für Schecks, Überweisungen und Bargeld zu erwarten, letztere mit einem gewissen Grad an Anonymität.

Insbesondere in Europa werden derzeit diverse smartcard-basierte «elektronische Geldbörsen» eingeführt, zunächst zur Verwendung in öffentlichen Telefonen und Automaten. Mittelfristig werden aber PC's standardmässig mit Kartenlesegeräten ausgestattet werden, so dass diese Börsen auch im Internet eingesetzt werden können.

Die Verfügbarkeit von Kartenlesegeräten wird zugleich auch dazu beitragen, on-line Zahlungssysteme sicherer zu machen: Derzeit werden diese vollständig auf Standard-PC's ausgeführt. PC's sind, insbesondere wenn sie zuhause stehen und bedenkenlos Software aus zweifelhaften Quellen verwendet wird, sehr empfänglich für «Viren». Wird nun etwa ein geheimer Signaturschlüssel auf einer Smartcard gehalten, und werden alle Signaturen nur durch die Smartcard erzeugt, so ist ein Stehlen des Signaturschlüssels aus dem PC ausgeschlossen.

Der nächste Schritt in Richtung Sicherheit wird die Einführung «elektronischer Brieftaschen» sein. Eine solche signiert nicht nur Nachrichten, sondern hat auch Tastatur und Anzeige, so dass der Kunde seine geheime PIN nicht in einen unsicheren PC eintippen muss (wo sie «abgefangen» werden kann), bzw. er dem angezeigten Betrag als korrekt vertrauen kann. Äusserlich ähneln die bereits verfügbaren «elektronischen Brieftaschen» Taschenrechnern, die gerade so gross sind, dass man eine Smartcard hineinschieben kann.

Möglicherweise noch wichtiger als der Zuwachs an Sicherheit ist der Zuwachs an Mobilität: Niemand sollte einem fremden Terminal allzusehr vertrauen. Mit einer Smartcard ist ein Missbrauch zumindest zeitlich beschränkt. Mit einer elektronischen Brieftasche ist man gar nicht mehr gezwungen, einem fremden Terminal zu vertrauen.

Der nächste Schritt

Elektronische Zahlungen sind ein wichtiges, aber nicht das einzige Sicherheitsproblem im elektronischen Handel: Elektronische Ausschreibungen, Offerten, Verhandlungen, Auktionen, Verträge, Vertragserfüllungen, Rechtsstreite haben ebenso umfassende Sicherheits- und Datenschutzforderungen wie Zahlungssysteme. Diese Probleme sind Gegenstand des von der Europäischen Union und der Schweiz geförderten R&D Projektes SEMPER <www.semper.org>, dessen technische Leitung das IBM Forschungslaboratorium Zürich übernommen hat. Die Partner kommen aus den Bereichen Dienstanbieter (z.B. Otto-Versand, Hamburg), Banken (z.B. Europay International) sowie Telekommunikation und R&D in Sicherheit und Kryptographie. Neben IBM sind als weitere Schweizer Partner *Telekurs* (als Projektbegleiter) und *r3 security engineering* beteiligt.