erscheint in: à la Card aktuell, Mai 1994

Europäisches Industrie- und Forschungskonsortium entwickelt neuartiges Zahlungsverfahren

Von Michael Waidner (Universität Hildesheim und Universität Karlsruhe)
und Arnd Weber (Institut für Sozialforschung, Frankfurt)

Überblick

Sichere elektronische Zahlungen sollen von einem neuartigen Zahlungsverfahren ermöglicht werden, das im Rahmen des ESPRIT Projekts „CAFE — Conditional Access for Europe“ von 13 europäischen Industrieunternehmen und Forschungsinstituten entwickelt wird. Grundlage sind kryptographische Verfahren, insbesondere sogenannte public-key-Verfahren zur digitalen Unterschrift: alle Zahlungen werden durch den Emittenten des elektronischen Geldes digital unterschrieben und sind so gegen Fälschung sicher.

Für Zahlungen erhalten die Kunden eine Prozessorchipkarte des Emittenten oder eine Art elektronischer Geldtasche. In seiner Grundversion erlaubt das Zahlungsverfahren anonyme offline Zahlungen von Kunden an beliebige Dienstleister. Die Kunden erhalten elektronisches Geld über öffentliche Ausgabeautomaten oder über private Terminals, die über den heimischen Telefonanschluß mit einem Emittenten verbunden sind.

Zahlungen können in unterschiedlichen Währungen geleistet werden. Optional kann elektronisches Geld auch zwischen Kunden transferiert werden. Möglich ist auch die Kombination mit herkömmlichen Kredit- und Debitsystemen. Ein Übergang zu einem anonymen oder auch nichtanonymen online-Betrieb ist ebenfalls möglich, etwa für höhere Werte. Darüber hinaus ist der Kunde gegen den Verlust elektronischen Geldes durch Ausfall, Verlust oder Diebstahl seiner Karte oder seiner elektronischen Geldtasche geschützt.

Das Zahlungsverfahren setzt keinen zentralen Emittenten voraus. Statt dessen ist das Verfahren für mehrere Emittenten offen, die zudem die möglichen Optionen unabhängig voneinander auswählen können.

Ein Test der entwickelten Architektur und verschiedener Optionen soll 1995 stattfinden.

Eine elektronische Geldtasche enthält elektronisches Geld und kann zusätzlich auch die Funktionen anderer Karten oder auch digitale Quittungen und ähnliches enthalten. Technisch ist sie ein Gerät ähnlich einem Taschenrechner, also mit einer kleinen LCD-Anzeige und Tastatur, das über einen eingebauten Infrarotsender und -empfänger mit anderen Geräten kommunizieren kann. Da die Kommunikation über eine Infrarotverbindung, also kontaktlos erfolgt, sind hinsichtlich Form und zusätzlicher Funktionalität beliebig unterschiedliche elektronische Geldtaschen denkbar. Das Geld des Kunden wird von seiner elektronischen Geldtasche gespeichert und verwaltet. Alle Transaktionen des Kunden werden vom Kunden selbst über seine elektronische Geldtasche initiiert. Abhebungen und, soweit vom Kunden gewünscht, auch Zahlungen sind durch PIN-Abfrage geschützt. Die elektronische Geldtasche kann der Kunde im Prinzip von einem beliebigen Hersteller beziehen und beliebig selbst prüfen oder von Dritten prüfen lassen kann.

Daß gespeichertes elektronisches Geld nur einmal ausgegeben werden kann, wird durch ein spezielles, in eine elektronische Geldtasche einsetzbares Sicherheitsmodul des Emittenten, den sogenannten „Guardian“, erzwungen.

Die Zahlungsempfänger können zur Speicherung des erhaltenen elektronischen Geldes beliebige Speichermedien verwenden. Im Gegensatz zu elektronischen Geldtaschen benötigen POS-Terminals kein Sicherheitsmodul. Die Kommunikation mit dem Gerät des Kunden erfolgt, je nach Systemvariante, über einen Chipkartenleser oder einen Infrarotsender und -empfänger.

Ziele und Grundlagen

Etwas vereinfacht ausgedrückt, versucht das Projekt mit seinem Zahlungsverfahren aufzuzeigen, was man mit den heutigen technischen Möglichkeiten hinsichtlich Betrugssicherheit, Datenschutz, Offenheit und Flexibilität erreichen kann. Das Zahlungsverfahren wird daher hinsichtlich dieser Eigenschaften weit über das heute übliche hinausgehen.

Die Unfälschbarkeit elektronischen Geldes wird durch sogenannte digitale Unterschriften erreicht: Sie sollen für elektronisch dargestellte Dokumente dasselbe leisten wie die eigenhändige Unterschrift für Papierdokumente.

Ihre Verwendung im Zahlungsverfahren ist im Prinzip sehr einfach: Ein Emittent erklärt digitale Dokumente bestimmter Gestalt, die von ihm digital unterschrieben sind, als geldwert. Der Kunde erhält also eine Art elektronische Banknote. Die Echtheit der digitalen Unterschrift wird durch seine elektronische Geldtasche oder seine Karte geprüft.

Wesentlich für den Emittenten ist die Fälschungssicherheit seiner digitalen Unterschrift. Auf den ersten Blick erscheinen fälschungssichere digitale Unterschriften unmachbar: Jede digitale Nachricht kann perfekt kopiert werden. Einfaches Hinzufügen einer eingescannten echten Unterschrift, oder ähnliches, genügt also sicher nicht. Auch die Methoden der klassischen Kryptographie sind unzureichend: Dort kennt der Unterschreibende ein Geheimnis, seinen geheimen Schlüssel, mit dessen Hilfe er aus dem digitalen Dokument eine Pseudounterschrift ableitet. Zur Überprüfung benötigt der Überprüfer aber *ebenfalls* den geheimen Schlüssel. Er könnte daher die Unterschrift beliebig nachmachen. Nichtsdestotrotz verwenden allerdings viele Zahlungsverfahren solche eigentlich ungeeigneten Pseudounterschriften, etwa in der Gestalt von MACs und TANs, und auch indirekt über PIN-Prüfungen.

Der erste Blick trügt jedoch. Wie unfälschbare digitale Unterschriften realisiert werden könnten, zeigten 1976 die beiden Kryptographen Whitfield Diffie und Martin Hellman und revolutionierten damit die gesamte Kryptographie: Sie stellten eine neue Klasse von mathematischen Verfahren vor, die sogenannten Einwegfunktionen mit Geheimnis. Eine Einwegfunktion ist eine mathematische Funktion, die jedermann einfach berechnen kann, die aber aus Aufwandsgründen praktisch nicht umkehrbar ist. Als Beispiel nennt Diffie die Multiplikation: Jeder kann schnell z. B. die Primzahlen 127 und 997 multiplizieren. Aus dem Produkt, 126619, kann man umgekehrt die beiden Faktoren wieder eindeutig bestimmen, aber nur mit sehr viel größerem Rechenaufwand als zur Multiplikation erforderlich war. Haben die beiden Primfaktoren eine Länge von etwa 77 Dezimalstellen, so ist mit heutiger Rechnertechnologie die Umkehrung praktisch nicht mehr möglich. Eine Einwegfunktion *mit Geheimnis* ist ebenfalls praktisch nicht invertierbar, es sei denn, man kennt das Geheimnis der Funktion, einen geheimen Schlüssel. Im Prinzip kann der Besitzer des Geheimnisses mit einer solchen Funktionen direkt digital unterschreiben: Mittels seines geheimen Schlüssels kehrt er die Funktion um und bestimmt einen Wert, auf den angewandt die Einwegfunktion als Ergebnis gerade das zu signierende Dokument ergibt. Dieses kann niemand außer ihm tun. Aber jeder kann prüfen, daß die Funktion, angewandt auf diesen Wert, also auf die digitale Unterschrift, tatsächlich wieder das Dokument ergibt. Die einfachsten Verfahren zur digitalen Unterschrift arbeiten tatsächlich nach diesem Prinzip. Aus Sicherheits- und Effizienzgründen ist die Konstruktion allerdings meist etwas komplizierter.

Aus Datenschutzsicht ist die direkte und einfache Verwendung elektronischer Banknoten allerdings noch unbefriedigend: Bezahlt ein Kunde mit einer solchen Banknote und löst der Empfänger sie später ein, so ist der Zahlungsfluß, also wer an wen zahlte, offensichtlich. Nun könnte man elektronische Banknoten auch anonym kaufen, etwa gegen Bargeld an Automaten. Jedoch könnten die betreffenden Transaktionen leicht deanonymisiert werden, etwa wenn jemand Zahlungen anhand einer Kartennummer verfolgt (was in den meisten vergleichbaren digitalen Zahlungsverfahren möglich ist), oder wenn man anbietet, auch vom Girokonto aus nachladen zu können.

Statt dessen gewährt das im Projekt entwickelte Zahlungsverfahren perfekten Datenschutz. Dieser wird mit Hilfe einer 1982 von dem Kryptographen David Chaum vorgeschlagenenen Erweiterung digitaler Unterschriften erreicht: Der Kunde rechnet eine vom Emittenten erhaltene elek-

tronisch Banknote so um, daß zwar deren Gültigkeit erhalten bleibt, sie aber bei Zahlungseingang nicht mehr mit der ursprünglich ausgegebenen in Beziehung gesetzt werden kann.

Durch die digitalen Unterschriften ist elektronisches Geld praktisch unfälschbar. Wie jede digitale Information könnte es aber im Prinzip beliebig kopiert und damit unerlaubt mehrfach ausgegeben werden. Dieses Kopieren ist ausgeschlossen, solange das Sicherheitsmodul des Emittenten, der „Guardian“, sicher arbeitet. Das Zahlungsverfahren sorgt aber im Gegensatz zu den meisten bisherigen digitalen Kartenzahlungsverfahren auch für den Fall vor, daß dieses Sicherheitsmodul gebrochen wird:

Das Brechen eines Sicherheitsmoduls hat keine Auswirkung auf die Gesamtsicherheit. Die Module enthalten keine Daten, deren Geheimhaltung für das Gesamtsystem wesentlich wäre.

Im schlimmsten Fall kann ein Betrüger mit Hilfe eines gebrochenen Sicherheitsmoduls elektronische Banknoten mehrfach verwenden. Übersteigt der Betrug aber eine bestimmte Grenze und verwendet der Betrüger dieselbe Banknote mehrmals, so wird automatisch der Inhaber der zum gebrochenen Sicherheitsmodul gehörenden elektronischen Geldtasche oder Karte identifiziert. Der Betrug ist damit nachweisbar.

Die Verwendung von digitalen Unterschriften erfordert aus Sicherheitsgründen arithmetische Berechnungen mit bis zu 154-stelligen Dezimalzahlen. Solche Berechnungen sind sehr zeitaufwendig. Um Verarbeitungszeiten ähnlich denen heutiger Kartensysteme zu erreichen, werden in allen Geräten spezielle Mikroprozessoren mit kryptographischem Koprozessor verwendet.

Ein wesentliches Ziel bei der Entwicklung des Zahlungsverfahrens ist, daß die Architektur für möglichst viele Jahre und für die verschiedensten elektronischen Dienste verwendet werden kann. Sicherheitsexperten aus dem Bankenbereich verglichen den Ansatz des Projektes anschaulich mit einer 10 Meter hohen Mauer, deren Überspringen für Betrüger so aussichtslos sei, daß diese es nicht einmal versuchen würden. Diese äußerst hohe Sicherheit macht es auch möglich, auf sogenannte „Gucklöcher“ im System zu verzichten, die man sonst vorhalten müßte, um eventuelle Eindringlinge in das System zu entdecken.

Jeder Emittent elektronischen Geldes muß nur seinen eigenen elektronischen Banknoten, also seinen eigenen digitalen Unterschriften vertrauen. Hierauf beruht im Kern die Offenheit des Zahlungsverfahrens. Der Emittent behält seinen „Float“ aufgrund der Vorausbezahlung, kann selbst seinen Teil des Systems kontrollieren und unabhängig von anderen Emittenten spezielle Optionen auswählen.

Meinungen

Über 300 Nutzer existierender Kartenzahlungssysteme in Deutschland, Frankreich, Großbritannien, Italien und der Schweiz wurden zu unterschiedlichen Aspekten elektronischer Zahlungsverfahren befragt.

Ungefähr die Hälfte der Befragten äußerte die Meinung, ein elektronisches Zahlungsverfahren müsse dieselbe Anonymität wie Münzen anbieten, also perfekten Datenschutz.

Das Konzept der vom Konsortium entwickelten elektronischen Geldtasche stieß bei etwa zwei Dritteln der Befragten auf Interesse. Als besonders vorteilhaft für die Sicherheit wird dabei angesehen, daß der Kunde die elektronische Geldtasche während der Bezahlung nicht aus der Hand geben muß. Ein Händler kann auch nicht irrtümlich einen zu großen Betrag aus dem Guthaben abrufen, da der Kunde den Vorgang über die Anzeige seiner elektronischen Geldtasche direkt verfolgen kann und jede Zahlung durch Knopfdruck bestätigen muß.

Überraschenderweise bejahten etwa zwei Drittel der befragten Kartennutzer die Frage, ob sie es begrüßen würden, Zahlungen auch in ECU leisten zu können. Als Grund wurde angeführt, daß der ECU Preise transparenter machen würde und Belege langfristig nur in einer Währung ausgestellt würden. Ferner erhofften die Befragten, daß dadurch die Kosten von Zahlungen im Ausland gesenkt würden. Dementsprechend sieht das Zahlungsverfahren vor, daß neben existierenden Währungen auch ein elektronischer ECU verwendet werden kann.

Die Befragung zeigte auch, daß für Benutzer herkömmlicher Debit- und Kreditkarten der Schutz gegen Geldverlust bei Verlust oder Diebstahl einer Karte zu deren wichtigsten Eigenschaften gehört. Dementsprechend ist es notwendig, auch elektronisches Geld zumindest optional und für höhere Werte gegen Verlust zu schützen. Ein solcher Schutz ist auch notwendig, um technische Defekte der Sicherheitsmodule, elektronischen Geldtaschen und Chipkarten tolerieren zu können. Der vom Konsortium verfolgte Ansatz ermöglicht diese Verlusttoleranz: Da das elektronische Geld nur einmal verwendet werden kann, ist es möglich, nichtbenutztes Geld zu erstatten. Dafür muß der Kunde beim Laden der Karte oder Geldtasche eine (an sich wertlose), zur Wahrung seines Datenschutzes von ihm verschlüsselte Sicherungskopie der geladenen Banknotennummern erstellen.

Verlauf des Projekts

Nach erfolgreichem Abschluß der für 1995 geplanten Erprobung des Zahlungsverfahrens wird eine Architektur zur Verfügung stehen, die über die heutigen inkompatiblen, monofunktionalen Wertkarten, z.B. Telefonwertkarten, Kopierkarten und Kantinenkarten, hinausweist. Die Offenheit des Systems macht es möglich, daß Emittenten ihre eigenen Ziele verfolgen, ohne Interoperabilität einzubüßen.

Erprobt werden Chipkarten und elektronische Geldtaschen mit Infrarotschnittstelle. Statt elektronischer Geldtaschen könnten aber auch andere ausreichend intelligente Geräte und andere Kommunikationsmedien verwendet werden. Sinnvolle Gerätekombinationen sind z. B. Notebook-Rechner und Personal Digital Assistants mit PCMCIA-Einschubkarte für das Sicherheitsmodul und sowohl Infrarot als auch Modemverbindungen. Digitale Mobilfunktelefone kommen ebenfalls in Betracht.

Neben der Benutzung für offline Zahlungen bietet sich das Zahlungsverfahren natürlich auch für die direkte Abrechnung von Netzwerkdiensten an. So könnte etwa eine online Datenbank ohne vorherige Einschreibung benutzt werden, da ja sofort bezahlt würde.

Im weiteren Verlauf des Projektes soll, entsprechend dem recht allgemeinen Projekttitel „Conditional Access for Europe“, die elektronische Geldtasche zu einer Art elektronischer Brieftasche ausgebaut werden. Diese könnte z.B. einfache Zugangsberechtigungen oder auch andere digital unterschriebene Dokumente enthalten, von einfachen Quittungen bis hin zu einem elektronischen Ausweis oder elektronischen Führerschein.

Das Projekt wird im Rahmen des ESPRIT-Programms der Europäischen Union gefördert. Das Projektkonsortium vereinigt Sozialwissenschaftler und Unternehmensberater — Institut für Sozialforschung (D), Cardware (GB) — Hersteller von Soft- und Hardware — die Firmen DigiCash (NL), Gemplus (F), Ingenico (F), Siemens (D) — und Entwerfer kryptographischer Verfahren aus den Forschungsinstituten der niederländischen und französischen PTT, des Sintef Delab (N) und der Universitäten Århus (DK), Hildesheim (D) und Leuven (B). Die Projektleitung liegt beim niederländischen Forschungsinstitut CWI und dem Projektkoordinator, David Chaum.

Es ist vorgesehen, die genauen Charakteristika der Architektur in einem öffentlichen Prozeß zu definieren. Insofern ist jegliches Feedback an das Projektkonsortium höchst willkommen.

Michael Waidner, Institut für Rechnerentwurf und Fehlertoleranz, Universität Karlsruhe, 76128 Karlsruhe; Fax. (0721) 370455; Tel. (0721) 608 4024

Arnd Weber, Institut für Sozialforschung, Senckenberganlage 26, 60325 Frankfurt (Main); Fax. (069) 749907; Tel. (069) 756183 12