4. GMD-SmartCard Workshop, Darmstadt, 8. und 9. Februar 1994

Das ESPRIT-Projekt "Conditional Access for Europe"

Michael Waidner*

"Conditional Access for Europe" (CAFE) ist ein von der Europäischen Union im Rahmen von ESPRIT gefördertes Forschungs- und Entwicklungsprojekt. Ziel ist die Entwicklung von Autorisierungssystemen, insbesondere digitalen Zahlungssystemen. Grundlage sind kleine, tragbare Benutzergeräte, *Wallets* genannt, die in Größe und Erscheinungsbild Taschenrechnern oder PDAs ähneln. Wallets können untereinander und mit anderen Geräten per Infrarotkanal kommunizieren.

Hauptmerkmal von CAFE ist die hohe Sicherheit aller Beteiligter unter geringstmöglichen Anforderungen an das gegenseitige Vertrauen: Die Sicherheit vieler herkömmlicher Systeme basiert darauf, daß alle Beteiligten dem Betreiber vertrauen. Oft hängt die Sicherheit aller Beteiligter auch noch von manipulations- und ausforschungssicheren Geräten ab, etwa von Chipkarten, oder von den Besitzern der POS-Terminals. Die Benutzer können diese Geräte nicht kontrollieren, müssen aber dennoch deren Korrektheit vertrauen. In CAFE genügt es für die Integrität und Vertraulichkeit, wenn jeder Beteiligte nur solchen Geräten vertraut, die er vollständig kontrolliert und die keine Geheimnisse vor ihm haben. Hauptstütze der Sicherheit sind kryptographische Verfahren, insbesondere digitale Signaturen.

Hauptgegenstand von CAFE sind digitale offline Zahlungssysteme, die den Benutzern Unbeobachtbarkeit (Datenschutz) und Sicherheit garantieren. Unbeobachtbarkeit und Sicherheit der Benutzer gegen Geldverlust basieren allein auf Kryptographie. Die Sicherheit des Betreibers basiert ebenfalls auf Kryptographie und zusätzlich auf der Manipulations- und Ausforschungssicherheit eines Bestandteils der Wallets, der *Guardians*. Sollte ein Guardian wider Erwarten ausgeforscht werden, so wird dem Betreiber zumindest garantiert, daß für jeden unerlaubt ausgegebenen Betrag der Betrüger eindeutig identifiziert und damit zur Rechenschaft gezogen werden kann. Die Sicherheit eines Benutzers hängt *nicht* vom Guardian seines Wallets ab.

Das für einen Feldversuch 1995 vorgesehene Zahlungssystem wird die Bezahlung in mehreren Währungen (z. B. ECU und DM) erlauben und schützt die Benutzer selbst dann vor Geldverlust, wenn sie ihr Wallet verlieren.

1 Das Projekt

1.1 Wer steckt hinter CAFE?

Das Akronym CAFE steht für *Conditional Access for Europe*, ein von der Europäischen Union gefördertes ESPRIT Projekt[1]. Die Arbeiten in CAFE begannen im Dezember 1992 und werden voraussichtlich im Dezember 1995 abgeschlossen sein.

CAFE vereinigt Sozialwissenschaftler (Univ. Frankfurt, Cardware), Hersteller von Soft- und Hardware (DigiCash, Gemplus, Ingenico, Siemens) und Entwerfer kryptographischer Verfahren (CWI Amsterdam, PTT NL, SEPT, Sintef Delab Trondheim,

* Univ. Karlsruhe, Inst. f. Rechnerentwurf u. Fehlertoleranz, 76128 Karlsruhe *und* Univ. Hildesheim, Inst. f. Informatik, 31113 Hildesheim • Tel. 0721/608 4024 • email WAIDNER@IRA.UKA.DE

1 Projekt 7023

Universitäten Århus, Hildesheim, Leuven). Die Projektleitung liegt beim CWI mit David Chaum als Projektkoordinator.

1.2 Was ist CAFE?

Gegenstand von CAFE sind **Autorisierungssysteme**, d. h. digitale Systeme, die gewisse Rechte ihrer Benutzer verwalten. Dabei kann es sich um die digitale Nachbildung von Ausweisdokumenten handeln, den geschützten Zugriff auf vertrauliche Daten, den geschützten Zugang zu Gebäuden oder — wichtigstes Beispiel für CAFE — um digitale Zahlungssysteme.

Ein **digitales Zahlungssystem** ist ein informationstechnisches System, mit dessen Hilfe Geld zwischen Benutzern transferiert werden kann.[2] Bislang konzentrierte sich CAFE fast ausschließlich auf digitale Zahlungssysteme. Dementsprechend beschränkt sich die folgende Darstellung ebenfalls auf digitale Zahlungssysteme.

Technologische Basis für CAFE sind **elektronische Wallets**. Ein Wallet ist ein kleiner, tragbarer Rechner, ähnlich einem Taschenrechner oder PDA[3], mit eigener Stromversorgung, eigener Tastatur und Anzeige und der Möglichkeit, direkt mit anderen Wallets zu kommunizieren. In CAFE wird dies ein Infrarotkanal sein. Jeder Benutzer des Systems besitzt und verwendet sein eigenes Wallet, das seine Rechte verwaltet und für seine Sicherheit garantiert.

In einer realen Anwendung kann es unterschiedliche Typen von Wallets geben, je nach den unterschiedlichen Anforderungen und Bedürfnissen der Benutzer. Durch die Kopplung per Infrarotkanal ist die Kompatibilität zwischen unterschiedlichen Typen leicht herzustellen. Luxusversionen könnten die CAFE-Funktionen mit denen eines universellen PDAs, eines Mobiltelefons oder auch eines Notebooks kombinieren. Einfachste Versionen würden nur die CAFE-Funktionen unterstützen und dementsprechend nur die minimal notwendige Benutzerschnittstelle besitzen. In einem Feldversuch innerhalb von CAFE werden aus Aufwandsgründen nur relativ einfache Wallets realisiert und erprobt werden.

Das **CAFE-Grundsystem** wird ein prepaid offline Zahlungssystem sein. „Prepaid“ bedeutet, daß ein Benutzer, bevor er eine Zahlung leisten kann, „elektronisches Geld“ beim Systembetreiber kaufen und in sein Wallet laden muß.[4] „Offline“ bedeutet, daß

---

2 Der Begriff „digitales Zahlungssystem“ entstammt der Informatik, genauer, dem kryptographischen Protokollentwurf. Im Sprachgebrauch der Geldwirtschaft wäre ein „digitales Zahlungssystem“ eher ein Zahlungsverfahren, etwa wie Euroscheck oder Kreditkarte.

3 PDA = Personal Digital Assistent, z. B. der Apple Newton.

4 Generell unterscheidet man Zahlungssysteme anhand der Relation zwischen einer Zahlung und der Belastung des Kontos des Zahlenden in „prepaid“ (Belastung vor der Zahlung, etwa wie bei Telefonwertkarten), „pay-now“ (Belastung während der Zahlung, typisch für online Zahlungssysteme) und „pay-later“ (Belastung nach der Zahlung, etwa wie bei Kreditkarten).

zur Abwicklung einer Zahlung in der Regel kein Kontakt zu einer Zentrale notwendig ist.[5]

Gedacht ist dieses Grundsystem primär für Zahlungen von Wallets an POS-Terminals[6]. Es erlaubt daher nur den einmaligen Transfer elektronischen Geldes, d. h. erhält ein Benutzer elektronisches Geld in einer Zahlung, so kann er dessen Echtheit zwar lokal überprüfen, muß es aber beim Zahlungssystembetreiber zur Gutschrift einreichen, bevor er es für eine eigene Zahlung verwenden kann (ähnlich wie bei Annahme eines Reiseschecks).

Für das Grundsystem existieren folgende Erweiterungen:

- **Transferierbarkeit**, d. h. ein Zahlungsempfänger kann digitales Geld, das er in einer Zahlung erhalten hat, sofort für eine neue Zahlung verwenden, ohne es zuvor beim Betreiber einzureichen.
- **Mehrere Währungen**, d. h. ein Benutzer kann das in seinem Wallet gespeicherte elektronische Geld in einer von mehreren Währung ausgeben, z. B. in ECU oder DM.
- **Verlusttoleranz**, d. h. verliert ein Benutzer sein Wallet, oder wird es defekt oder gestohlen, so erhält er dennoch den Gegenwert des im Wallet gespeicherten elektronische Geldes zurück.

Das CAFE-Grundsystem ist in viererlei Hinsicht ein **offenes System**:

- Wie Bargeld ist das CAFE-Grundsystem als **universelles Zahlungssystem** konzipiert. Ein Benutzer soll mit seinem Wallet beliebige Dienstleistungen bezahlen können, nicht nur einen oder wenige spezielle Dienste.
- Das Zahlungssystem läßt mehrere unabhängige Betreiber zu, wobei natürlich Zahlungen zwischen Kunden unterschiedlicher Betreiber möglich sein sollen.
- Das CAFE-Grundsystem spezifiziert nur gewisse Protokolle, nicht genaue Soft- und Hardwarekomponenten. Damit ist das Grundsystem prinzipiell offen für weitere Hardwareplattformen und läßt die Integration in andere Systeme zu.
- Da das Grundsystem ein prepaid Zahlungssystem ist, werden im Gegensatz zu Kreditkartensystemen keine Anforderungen an die Kreditwürdigkeit der Benutzer gestellt. Einfache Wallets sollten bei hoher Stückzahl preiswert herzustellen sein. Die Bedienung der Wallets und POS-Terminals kann (und wird im Feldversuch) sehr einfach gestaltet werden.[7] Damit schließt das Grundsystem per se keine Benutzer aus.

---

5 Generell unterscheidet man Zahlungssysteme in „online Systeme“ und „offline Systeme“. Bei online Systemen muß für jede Zahlung ein Kontakt zum Betreiber hergestellt werden. Sie verursachen daher höhere Kosten (mehr Kommunikation, höhere Verarbeitungsleistung beim Betreiber), können aber dem Betreiber eine höhere Sicherheit bieten.

6 POS = Point of sale

7 Die Minimalanforderung ist, daß das Wallet dem Zahlenden die Höhe des vom Zahlungsempfänger geforderten Betrags anzeigt und der Zahlende die Bezahlung aktiv bestätigt, indem er eine „OK“-Taste auf seinem Wallet drückt.

Der Entwurf des Grundsystems und seiner Erweiterungen wird bis Mitte 1994 abgeschlossen sein, so daß das Grundsystem, voraussichtlich erweitert um Verlusttoleranz und mehrere Währungen, bis Anfang 1995 implementiert und dann in einem Feldversuch erprobt werden kann.

Aufbauend auf dem Grundsystem sind für die Zukunft Entwicklungen weiterer Autorisierungssysteme geplant, etwa ein online Zahlungssystem zur Zahlung größerer Beträge und Anwendungen des Wallets zur Speicherung von medizinischen Notfalldaten, als elektronischer Ausweis, elektronischer Schlüssel usw.

Generell sollen die CAFE-Systeme einerseits den Bedürfnissen des Marktes und andererseits auch den gesetzlichen Anforderungen der Mitgliedsstaaten der EU entsprechen. Zur Erforschung dieser Bedürfnisse und Anforderungen wurden und werden existierende vergleichbare Systeme ausgewertet und deren Benutzer und Experten aus Banken, Verbraucherverbänden, Verwaltungen usw. befragt.

1.3 Worin unterscheiden sich CAFE-Zahlungssysteme von anderen digitalen offline Zahlungssystemen?

Der wesentlichste Unterschied zwischen den CAFE-Systemen und anderen universellen digitalen offline Zahlungssystemen, etwa Danmønt oder den diversen Citycards, liegt in den äußerst hohen Sicherheitsanforderungen von CAFE.

1.3.1 Mehrseitige Sicherheit

Die meisten existierenden digitalen Zahlungssysteme sind als Systeme mit **einseitiger Sicherheit** konzipiert: Die Sicherheit aller Parteien basiert auf der Verläßlichkeit einzelner Parteien, meist des Systembetreibers.

Einseitige Sicherheit ist jedoch für Zahlungssysteme ungeeignet, da sie den Beteiligten keine Rechtssicherheit bieten kann. Als Beispiel betrachte man Geldausgabeautomaten:

Benutzt ein Bankkunde seine ec-Karte an einem Geldausgabeautomaten, so basiert seine Sicherheit vollständig auf der Verläßlichkeit der Bank. Alles, was er weiß, weiß auch die Bank. Alles, was er kann, könnte daher auch ein betrügerischer Bankinsider tun, und kein Gericht kann unterscheiden, ob eine Auszahlung durch den Kunden oder einen solchen betrügerischen Bankinsider initiiert wurde. Damit herrscht für *keine* der beiden Parteien „Bank“ und „Kunde“ Sicherheit vor Betrugsmöglichkeiten.

Hieran ändert sich auch dann nichts, wenn man akzeptiert, daß zumindest manchen Banken als Institution mehr vertraut wird als einzelnen Kunden. In diesem Fall würde man dann für die Bank entscheiden, wenn diese durch ihre internen Sicherheitsmaßnahmen glaubhaft machen kann, daß Betrugsversuche durch Insider ausgeschlossen sind. Leider ist es aber sehr unwahrscheinlich, daß es eine Bank gibt, die dies tatsächlich nachweisen kann. Zum einen gibt es zahlreiche Beispiele von erfolgreichen Insiderangriffen trotz scheinbar unumgehbarer Sicherheitsmaßnahmen [Ande 93,

Neum 92]. Zum anderen ist der Kreis der zu betrachtenden Insider unüberschaubar groß: Er umfaßt nicht nur die Mitarbeiter der Bank, sondern auch die all derjenigen Einrichtungen, die zur Betreibung, Herstellung oder Wartung mit der Hard- oder Software des betrachteten Zahlungssystems zu tun haben oder hatten.

Entscheidet ein Gericht dagegen im Zweifel gegen die Bank, so ist die Bank damit umgekehrt vor betrügerischen Kunden völlig unsicher.

Um solche unentscheidbaren Situationen zu vermeiden, werden die CAFE-Systeme als Systeme mit **mehrseitiger Sicherheit** entworfen: Alle Sicherheitsforderungen einer Partei werden möglichst ohne vorausgesetztes Vertrauen dieser Partei in andere Parteien erfüllt. Keinesfalls wird gegenseitiges Vertrauen von Parteien mit widerstrebenden Interessen (wie oben Bank und Bankkunde) vorausgesetzt. Idealerweise muß eine Partei nur sich selbst und gewissen Entscheidungsinstanzen, z. B. Gerichten, vertrauen.

Mehrseitige Sicherheit ist für alle Beteiligten von Vorteil:

- Mehrseitige Sicherheit erhöht die Rechtssicherheit, da keine unklärbaren Situationen wie bei der einseitigen Sicherheit auftreten können. Mehrseitige Sicherheit garantiert, daß stets genügend Beweismittel für eine eindeutige Entscheidung vorhanden sind.
- Zahlungssysteme mit einseitiger Sicherheit haben einen natürlichen Sicherheitsengpaß, d. h. sie sind sehr empfindlich gegen Angriffe durch Insider. Bei mehrseitiger Sicherheit sind die Benutzer vor solchen Angriffen sicher.
- Mehrseitige Sicherheit erhöht die Akzeptanz eines Zahlungssystems durch die Bürger und ist für die Betreiber ein gutes zusätzliches Werbeargument für ihr System.

Die Forderung nach mehrseitiger Sicherheit hat unmittelbare Konsequenzen für die CAFE-Architektur und die zu verwendenden Sicherheitstechniken:

- Jeder Benutzer muß über ein Gerät verfügen, dem er vertrauen und mit dem er zuverlässig kommunizieren kann. In CAFE sind dies die Wallets. Für die zuverlässige Kommunikation zwischen Benutzer und Wallet benötigt ein Wallet eine eigene Tastatur und Anzeige. Ohne diese wären die von Geldausgabeautomaten oder POS-Terminals bekannten Betrugsmöglichkeiten durch gefälschte Terminals möglich.
- Der Betreiber benötigt in jeder offline Transaktion, die seine Sicherheitsforderungen berührt, ein Gerät, dem er vertrauen kann, auch wenn dieses physikalisch unter der Kontrolle eines nicht notwendigerweise vertrauenswürdigen Benutzers ist. In CAFE sind dies ausforschungssichere Prozessorchipkarten, die sogenannten **Guardians**. Hierauf wird in Abschnitt 2.2.1 näher eingegangen.

- Es müssen digitale Signaturen verwendet werden [DiHe 76, Denn 82, GoMR 88]. Nur digitale Signaturen können eigenhändige Unterschriften ersetzen, und ein solcher Ersatz ist zur Sicherstellung von Beweismitteln unerläßlich [PWP 90, Grim 93].[8]
- Die Sicherheit einer Partei soll nicht von Geräten abhängen, die für diese Partei unausforschbar oder vor ihr manipulationssicher sind. Damit scheiden für CAFE z. B. alle Systeme aus, deren Sicherheit ausschließlich auf der Sicherheit von Chipkarten basiert.
- Alle Entwürfe (Software und Hardware), die für die Sicherheit einer Partei wesentlich sind, müssen dieser Partei zur Überprüfung zugänglich sein. Für CAFE scheiden daher geheimgehaltene Algorithmen aus.

Eine Voraussetzung mehrseitiger Sicherheit ist das Vertrauen der Parteien in die eigenen Geräte: Damit ein Benutzer seinem Wallet trauen kann, muß dessen Entwurf (Software und Hardware) korrekt sein, wobei Korrektheit auch die Erfüllung der Sicherheitsanforderungen des Benutzers einschließt. Zusätzlich muß das konkrete Wallet des Benutzers dem Entwurf entsprechen, also korrekt hergestellt sein. Die wenigsten Benutzer werden in der Lage sein, die Entwürfe und Geräte selbst zu verifizieren. Statt dessen muß es hinreichend viele kompetente Prüfinstanzen geben, so daß jeder Benutzer darauf vertrauen kann, daß sich darunter wenigstens eine verläßliche Prüfinstanz befindet (denkbar wären etwa Prüfinstanzen des TÜV und der Verbraucherverbände).

1.3.2 Datenschutz

Die CAFE-Systeme sind als Massensysteme für den Alltagsgebrauch gedacht. Damit sollen die CAFE-Zahlungssysteme vor allem für kleine Beträge geeignet sein, wie sie bei kleineren Einkäufen, Telefonieren oder Benutzen öffentlicher Verkehrsmittel anfallen.

Würde man z. B. für jede Zahlung eine Kreditkarte verwenden, so erhielte die Kreditkartenorganisation ein umfangreiches Kaufprofil des Benutzers. Sie würde erfahren, wann der Benutzer wo einkauft, wann er telefoniert, wann er welche Fahrt mit einem Bus macht, usw. Aus Datenschutzsicht wäre dies eine unerwünschte Situation.

Verwendet man statt einer Kreditkarte Münzgeld für eine Zahlung, so ist diese Zahlung **unbeobachtbar:** Die verwendeten Münzen identifizieren den Benutzer nicht, weder gegenüber dem Zahlungsempfänger noch gegenüber der Notenbank. Zudem sind die Zahlungen eines Benutzers untereinander unverkettbar, denn man sieht zwei Münzen nicht an, ob sie vom selben Benutzer stammen oder nicht.

Diese Unbeobachtbarkeit soll auch für die Benutzer der CAFE-Systeme gelten: Im CAFE-Grundsystem soll der Zahlende perfekt unbeobachtbar sein, d. h. zu einer Zahlung soll weder der Zahlungsempfänger noch der Betreiber notwendigerweise die

---

[8] Leider werden sehr häufig auch symmetrische Authentisierungsverfahren, d. h. solche, bei denen zum Signieren und zum Testen dieselben Schlüssel verwendet werden, als „Signaturen“ bezeichnet. Als Beweismittel sind diese aber völlig untauglich, vgl. Abschnitt 2.1.2.

Identität des Zahlenden erfahren, noch sollen unterschiedliche Zahlungen desselben Benutzers untereinander verkettbar sein. Wie bei Bargeld schließt dies nicht aus, daß der Zahlende unabhängig vom Zahlungssystem identifiziert wird, sei es unbeabsichtigt oder gewollt, etwa durch ein kryptographisches Identifizierungsprotokoll.

Für den Zahlungsempfänger wird *keine* Unbeobachtbarkeit gefordert. Der Grund ist, daß die Hauptanwendung des CAFE-Grundsystems der Kauf von Waren oder Dienstleistungen von dem Zahlenden ohnehin bekannten Anbietern sein wird.

Im Gegensatz zu Zahlungen sind Abhebungen und Einreichungen beobachtbar, d. h. hier muß sich der Abheber oder Einreicher gegenüber dem Betreiber identifizieren.

Hinsichtlich der Voraussetzungen für die Unbeobachtbarkeit gilt dasselbe wie für die mehrseitige Sicherheit[9]: Der Schutz der Daten eines Benutzers soll nur von der Verläßlichkeit der Geräte dieses Benutzers selbst abhängen.

Trotz des Datenschutzes müssen natürlich die sonstigen Sicherheitsanforderungen erfüllt werden. Für die Zahlungshöhe kann eine obere Grenze vorgesehen werden, ab der die Unbeobachtbarkeit des Zahlenden aufgehoben wird, d. h. dieser sich gegenüber dem Zahlungsempfänger und evtl. auch gegenüber dem Betreiber (z. B. ab DM 5000) identifizieren muß. Die Sicherheit für den Betreiber ist von der Höhe dieser Grenze allerdings unabhängig, da das CAFE-Grundsystem ohne Rückgriff auf Gerätesicherheit (also nur durch Kryptographie) garantiert, daß im Betrugsfall der Betrüger ohnehin identifiziert wird.

Ein verbesserter Datenschutz nützt offensichtlich den Benutzern, aber auch den Betreibern: Zum einen erhöht Datenschutz die Akzeptanz eines Zahlungssystems durch die Bürger und kann daher als zusätzliches Werbeargument verwendet werden. Zum anderen vereinfacht sich für den Betreiber das Problem des Schutzes der bei ihm gespeicherten Daten, da er weniger personenbezogene Daten über seine Kunden erhält.

2 Das CAFE-Grundsystem

Im folgenden wird die für das CAFE-Grundsystem gewählte Architektur zusammen mit den Grundideen der dafür aus der Literatur bekannten Protokolle vorgestellt. Die CAFE-Protokolle orientieren sich insbesondere an den Protokollen in [Bran1 93], sind jedoch im Detail noch projektvertraulich und können daher nicht ausführlich beschrieben werden.

2.1 Vorbemerkungen

Im folgenden wird zur Vereinfachung nur ein kleiner Ausschnitt der tatsächlichen CAFE-Architektur verwendet: Es werden nur die wesentlichsten Transaktionen betrachtet, und es wird von nur einem Zahlungssystembetreiber ausgegangen.

---

9 Genauer gesagt ist technischer Datenschutz ein Teil der Sicherheit.

2.1.1 Begriffe

Es werden zwei Ebenen betrachtet: Die *Benutzerebene* enthält die Zahlenden, Zahlungsempfänger, Betreiber und Gerichte. Die *Systemebene* enthält die Geräte, die die für die Benutzer notwendigen Funktionen realisieren, also im wesentlichen Wallet, Guardian und POS-Terminal, und die Geräte des Betreibers zum Geldtransfer mit den Benutzern.

Betrachtet werden hier nur die drei wichtigsten Transaktionen:

- **Abheben**, durch das der Zahlende vom Betreiber elektronisches Geld erhält (z. B. gegen Abbuchung von einem Bankkonto),
- **Bezahlen**, durch das der Zahlende elektronisches Geld zum Zahlungsempfänger transferiert (dies ist die einzige offline Transaktion), und
- **Einreichen**, durch das der Zahlungsempfänger elektronisches Geld an den Betreiber transferiert (z. B. gegen eine entsprechende Gutschrift auf sein Konto).

Daneben werden natürlich noch weitere Transaktionen benötigt, etwa die zur Initialisierung des Gesamtsystems — an der auch die Gerichte beteiligt sein müssen, die später evtl. anhand digital signierter Nachrichten Streitfälle entscheiden müssen — und zur Initialisierung der einzelnen Benutzer und Geräte.

Sicherheitsanforderungen werden auf Benutzerebene formuliert. Zur Erfüllung einer Sicherheitsanforderung eines bestimmten Benutzers muß man davon ausgehen, daß die Geräte, die die Interessen dieses Benutzers auf Systemebene vertreten, verläßlich entworfen und hergestellt wurden.

2.1.2 Sichere Geräte und Kryptographie

Wesentlich für digitale Zahlungssysteme sind zwei Klassen von Sicherheitshilfsmitteln, *sichere Geräte* und *Kryptographie*.

Ein **sicheres Gerät** soll einem Angreifer standhalten, der direkten physischen Zugriff auf das Gerät hat. Ziel des Angreifers ist die Ausforschung von im Gerät gespeicherten vertraulichen Daten.

Wie die meisten offline Zahlungssysteme, so verwendet auch das CAFE-Grundsystem *Prozessorchipkarten* als sichere Geräte [GuUQ 92, Scha 92]. Im Feldversuch wird dies eine Chipkarte von Gemplus mit einem Siemens Kryptokoprozessor sein. Deren Sicherheit wird im allgemeinen als befriedigend hoch eingeschätzt, hängt aber letztlich von den Fähigkeiten eines konkreten Angreifers ab. Aus diesem Grund muß auch für den (hoffentlich nicht eintretenden) Fall, daß eine Prozessorchipkarte ausgeforscht worden ist, ein befriedigender *Notfalldienst* angeboten werden.

Kryptographie taucht in Zahlungssystemen mit mehrseitiger Sicherheit vorwiegend in der Gestalt *digitaler Signatursysteme* auf [DiHe 76].

Digitale Signatursysteme bilden die eigenhändige Unterschrift kryptographisch nach und sind daher für mehrseitige Sicherheit in digitalen Zahlungssystemen unerläßlich: Ein Signatursystem besteht aus (wenigstens) drei Algorithmen:

- Der Algorithmus ***gener*** erzeugt bei jedem Aufruf ein zufälliges Schlüsselpaar (s, t). Prinzipiell kann *gener* von jedem Benutzer selbst ausgeführt werden, und für mehrseitige Sicherheit sollte dies auch jeder Benutzer selbst tun. Hat Benutzer X ein Schlüsselpaar (s_X, t_X) erzeugt, so hält er s_X geheim und macht t_X für alle potentiellen Empfänger von Signaturen von X öffentlich.
- Der Algorithmus ***sign*** dient zum Signieren von Nachrichten und benötigt hierzu den geheimen Schlüssel s_X.
- Der Algorithmus ***test*** dient zum Testen von Nachrichten. Um zu testen, ob eine Nachricht mit s_X signiert wurde, wird der Schlüssel t_X benötigt.

Ein Signatursystem ist sicher, wenn kein Angreifer eine Signatur fälschen kann, der nur t_X und eine Reihe von mit s_X signierten Nachrichten (die er evtl. sogar selbst bestimmen kann) kennt. „Nicht können" ist dabei im komplexitätstheoretischen und probabilistischen Sinne zu verstehen, d. h. die Wahrscheinlichkeit einer Fälschung ist vernachlässigbar klein, falls der Angreifer nur (in einem Sicherheitsparameter polynomial) begrenzt viel rechnen kann.

Bekannte Signatursysteme sind RSA [RSA 78], ElGamal [ElGa 85], GMR [GoMR 88], DSS [DSS 92] und das für den Einsatz in Zahlungssystemen besonders interessante Schnorr-System [Schn 91]. Wie die Sicherheit aller kryptographischer Systeme mit öffentlichen Schlüsseln, so basiert auch die Sicherheit von Signatursystemen auf gewissen mathematischen Problemen, etwa auf dem der Faktorisierung (z. B. RSA, GMR) oder diskretem Logarithmus (ElGamal, DSS, Schnorr).[10] Die Schwierigkeit dieser Probleme ist im komplexitätstheoretischen Sinne zwar nicht genau bekannt, wird aber als sehr hoch eingeschätzt. Zumindest haben die Probleme allen bisherigen Versuchen, sie effizient zu lösen, widerstanden.

Symmetrische Authentisierungssysteme (oft MAC, *Message Authentication Code*, genannt und z. B. auf DES basierend) sind als Ersatz für die eigenhändige Signatur prinzipiell ungeeignet. „Signierer" und „Tester" besitzen dieselbe Schlüsselinformation, so daß ein Außenstehender, etwa ein Gericht, nie entscheiden kann, wer von beiden eine bestimmte Authentisierung erzeugte. Damit kann der Tester nie eine Signatur als glaubwürdiges Beweismittel gegen den Signierer verwenden.

Eine für unbeobachtbare Zahlungssysteme wichtige Variante digitaler Signatursysteme sind **blind geleistete Signaturen** [Chau 85]: Dies ist ein Protokoll zwischen zwei Parteien, dem Signierer und dem Signaturempfänger. Das Resultat des Protokolls besteht darin, daß der Signaturempfänger eine vom Signierer signierte Nachricht erhält. Diese Nachricht ist dem Signierer aber *unbekannt* (daher „blind"), erfüllt aber gewisse Eigenschaften. Effiziente Varianten zur blinden Signierung gibt es z. B. für RSA [Chau 85, Ferg 93] und das Schnorr-Schema [Bran 93, Bran1 93].

---

[10] „Basieren" bedeutet im Idealfall, daß das mathematische Problem und das Fälschungsproblem äquivalent, also gleich schwierig sind. Von den oben genannten Systemen konnte dies allerdings bislang nur für die Äquivalenz von GMR und Faktorisierung gezeigt werden.

Typischerweise werden blind geleistete Signaturen für Zahlungssysteme wie folgt verwendet [Chau 85]: Elektronisches Geld wird durch vom Betreiber signierte Nachrichten einer bestimmten Gestalt dargestellt, den *elektronischen Münzen*. Beim Abheben läßt sich der Zahlende eine elektronische Münze vom Betreiber blind signieren. Wird diese elektronische Münze später vom Zahlungsempfänger eingereicht, so bleibt der Zusammenhang zwischen dem Abheben und dem Einreichen verborgen: Die Münze ist unter allen Münzen desselben Wertes verborgen, die Transaktionen sind unverkettbar.

2.2 Konzept des CAFE-Grundsystems

2.2.1 Starke Integrität für den Betreiber durch sichere Geräte

Die wesentlichste Sicherheitsforderung des Betreibers ist die nach **starker Integrität** (im Gegensatz zur schwachen, wie in Abschnitt 2.2.3 erläutert). Starke Integrität bedeutet, daß innerhalb des Zahlungssystems elektronisches Geld nicht fälschbar ist: die Gesamtsumme elektronischen Geldes entspricht stets den ausgeführten Abhebungen und Einreichungen.

Nun ist digitale Information aber beliebig kopierbar. Also muß man für starke Integrität den Zahlenden davon abhalten, bereits ausgegebenes elektronisches Geld ein weiteres mal auszugeben.

In online Systemen ist dies sehr einfach möglich, da der Betreiber aktiv an jeder Zahlung beteiligt ist.

In offline Systemen wird statt dessen auf Systemebene für die Transaktion Zahlung ein sicheres Gerät des Betreibers verwendet, das sich physisch aber beim Benutzer befindet. Im Feldversuch für das CAFE-Grundsystem wird dieses sichere Gerät eine Prozessorchipkarte sein (siehe Abschnitt 2.1.2).

In vielen Zahlungssystemen realisiert das sichere Gerät des Betreibers nicht nur die Aufgaben des Betreibers, sondern zugleich auch die des Zahlenden. Dieser Ansatz widerspricht der mehrseitigen Sicherheit:

- Betreiber und Zahlender müssen demselben Gerät vertrauen. Im Konfliktfall darf man nicht erwarten, daß der Zahlende einem Gerät des Betreibers vertraut.
- Der Zahlende kann mit „seinem“ sicheren Gerät nur indirekt, über ein Terminal, kommunizieren. Damit muß er auch diesem Terminal vertrauen.

In CAFE wird daher zwischen dem Gerät des Betreibers, dem Guardian, und dem Gerät des Zahlenden, dem Wallet, unterschieden.[11] Der Guardian verhindert, daß elektronisches Geld mehrfach ausgegeben wird, und das Wallet kontrolliert den Guardian aus Sicht des Zahlenden.

---

[11] Diese Unterscheidung ist allerdings nicht für jede Realisierung zwingend, d. h. die Funktionen *beider* Geräte könnten auch in nur *einem* Gerät realisiert werden. Dies kann aus Kompatibilitätsgründen zu existierenden POS-Terminals sinnvoll sein, reduziert aber die mehrseitige Sicherheit gegenüber der Zwei-Geräte-Lösung.

Wesentlich für die genaue Verwendung von Wallet und Guardian sind zwei Probleme: Wie kann verhindert werden, daß der Guardian die Unbeobachtbarkeit des Zahlenden gefährdet, und wie kann ein akzeptabler Notdienst für den Fall, daß ein Guardian wider Erwarten doch ausgeforscht wird, angeboten werden?

2.2.2 Unbeobachtbarkeit des Zahlenden

Die naive Verwendung von Wallet und Guardian ist die folgende: Das Wallet dient nur als Ein- und Ausgabegerät für den Zahlenden und zum Testen und Speichern von Beweismitteln, z. B. von signierten Quittungen. Das eigentliche Zahlungsprotokoll wird durch den Guardian ausgeführt.

Bei dieser Verwendung erhält der Guardian aber alle Information über die Zahlungen des Zahlenden. Die Unbeobachtbarkeit des Zahlenden hängt daher vollständig davon ab, daß sein Guardian keine vertraulichen Daten weitergibt (z. B. während einer Abhebung). Dies widerspricht der mehrseitigen Sicherheit, d. h. ist für CAFE untauglich.

Statt dessen verwendet CAFE das folgende, in [Chau 92] vorgeschlagene Konzept:[12]

Der Guardian wird physikalisch daran gehindert, direkt mit einem anderen Gerät außer dem Wallet zu kommunizieren: Der Guardian wird vollständig in das Wallet eingeschoben, d. h. das Wallet dient als physische Schirmung, und es besitzt keine Kommunikationsschnittstelle außer der zum Wallet. Damit kann das Wallet kontrollieren, welche Informationen zwischen Guardian und Umgebung fließen.

Die Fähigkeit zu bezahlen, wird auf Wallet und Guardian verteilt, d. h. beide müssen kooperieren, damit eine Zahlung stattfinden kann. Auf diese Weise kann der Guardian verhindern, daß ein Betrag mehrfach ausgegeben wird.

Unter der *Sicht* eines Beteiligten auf eine Transaktion versteht man die Zusammenstellung all der Information, die dieser Beteiligte nach dieser Transaktion hat (z. B. alle von dieser Instanz gesendeten und empfangenen Nachrichten).

Das Protokoll für die Transaktion Zahlung ist so gestaltet, daß gilt:

- Es gibt keine versteckten Kanäle zwischen Guardian und Außenwelt, d. h. es gibt keine Möglichkeit für den Guardian, unbemerkt mit einer Partei außerhalb des Wallets zu kommunizieren.[13]
- Die Sicht des Guardians auf eine Zahlung ist mit den Sichten der Parteien der Umgebung nicht verkettbar, d. h. es gibt in den Sichten keine Gemeinsamkeiten, anhand derer ein Angreifer sie später als zusammengehörend erkennen würde.[14]

---

12 In [Chau 92] wird statt von Guardian von Observer gesprochen.

13 Der einzige Kanal, der nicht geschlossen werden kann, besteht darin, daß der Guardian jederzeit und für die Umgebung feststellbar das Protokoll unterbrechen und hierdurch Information nach außen geben kann. Man kann aber erreichen, daß hierdurch nur ein Bit signalisiert werden kann.

14 Verfügt der Guardian über eine Realzeituhr, so können die Sichten einer Transaktion allerdings meist unabhängig vom Protokoll anhand der Zeit, zu der die Transaktion stattfand, verknüpft werden. Die Existenz einer autonomen Realzeituhr in einer Prozessorschipkarte als Guardian ist allerdings mangels

Beide Eigenschaften werden erreicht, indem das Wallet die Nachrichten vom Guardian an die Außenwelt und umgekehrt „verwürfelt“, d. h. sie werden so transformiert, daß sie zwar alle notwendigen Eigenschaften beibehalten, aber innerhalb aller möglichen Nachrichten mit diesen Eigenschaften gleichverteilt erscheinen. Die Varianten im Protokollablauf werden auf möglichst wenige reduziert (etwa so, daß sie nur von den unterschiedlichen zu bezahlenden Beträgen abhängen), so daß auch hierdurch verschiedene Sichten nicht verkettbar werden.

Zur Sicherstellung eines akzeptablen Notfalldienstes (siehe Abschnitt 2.2.3) müssen im CAFE-Grundsystem Zahlungen vom Betreiber vorautorisiert werden. Anschaulich kann man sich vorstellen, der Zahlende erhielte in der Transaktion Abheben eine Münze oder einen Scheck vom Betreiber, den er dann für eine Zahlung verwenden kann. Zum Abheben muß sich der Zahlende identifizieren, da der abgehobene Betrag von einem nicht-anonymen Konto abgebucht wird.

Zur Unbeobachtbarkeit muß daher zusätzlich dafür gesorgt werden, daß die Sicht des Betreibers zu einer Abhebung nicht mit der Sicht des Zahlungsempfängers zu der entsprechenden Zahlung verkettet werden kann. Vereinfacht wird dies erreicht, indem der Betreiber die Vorautorisierung blind signiert (vgl. Abschnitt 2.1.2).

Das Konzept von Wallet und Guardian wird unabhängig von Zahlungssystemen ausführlicher beschrieben in [Chau 92] und, zusammen mit einigen Protokollen, in [ChPe1 93, CrPe 93, BrCh 93].

2.2.3 Schwache Integrität durch Kryptographie im Notfalldienst für den Betreiber

Wird der Guardian ausgeforscht, so verliert er seine Sicherungsfunktion für den Betreiber, und der Zahlende kann das vorhandene elektronische Geld möglicherweise beliebig oft ausgeben.

Der im CAFE-Grundsystem realisierte Notfalldienst stellt aber sicher, daß in diesem Fall der Betreiber einen solchen Betrug zumindest erkennen und dem betrügerischen Zahlenden nachweisen kann. Diese Eigenschaft basiert alleine auf kryptographischen Techniken, ist also unabhängig von der Sicherheit eines Gerätes. Die erreichte Sicherheit wird **schwache Integrität** genannt.

Die Grundidee ist relativ einfach: Zahlungen werden nur in festen Einheiten, der Einfachheit halber *elektronische Münzen* genannt, geleistet. Der eigentlich zu bezahlende Betrag muß daher eventuell durch mehrere Münzen dargestellt und in mehreren Zahlungen transferiert werden. Beim Abheben wird in jede Münze die Identität des Zahlenden eincodiert. Durch blinde Signierung werden die Münzen durch den Betreiber vorautorisiert. Wird die Münze für eine Zahlung verwendet, so muß der Zahlende dem Zahlungsempfänger einen Teil der Codierung verraten. Verwendet der

---

eigener Stromversorgung ausgeschlossen. Eine theoretisch denkbare Funkuhr scheitert an der physischen Schirmung durch das Wallet.

Zahlende die Münze zweimal, so muß er mit großer Wahrscheinlichkeit zwei verschiedene Teile der Codierung verraten. Die Codierung ist nun so gewählt, daß aus zwei Teilen die Identität bestimmt werden kann, wohingegen ein Teil alleine keine Information über die Identität verrät.

Beim Einreichen erhält der Betreiber die Münzen und Codierungsteile von den Zahlungsempfängern und muß — aufwendigster Teil des Verfahrens — alle erhaltenen Münzen daraufhin untersuchen, ob eine zweimal vorkommt und gegebenenfalls die beiden Teile zur Berechnung der Identität des Betrügers nutzen.

Diese Grundidee wurde, unabhängig vom Konzept von Wallet und Guardian und zusammen mit einem ersten Protokoll, in [ChFN 90] vorgeschlagen. Effizientere Lösungen wurden später in [Bran 93, Bran1 93, Ferg 93, FrYu 93] veröffentlicht und teilweise auf das Wallet-und-Guardian-Konzept übertragen [Bran 93, Ferg1 93]. Das CAFE-Grundsystem orientiert sich an den Protokollen in [Bran 93], deren Sicherheit auf einer Variante des Problems des diskreten Logarithmus bzw. auf digitalen Signaturen nach dem Schnorr-Schema [Schn 91] beruht.

Die Darstellung von Beträgen durch Münzen hat zwei Nachteile: Der Zeit- und Speicherbedarf erhöht sich gegenüber Systemen, die keinen Notfalldienst dieser Art anbieten, denn jede Münze muß getrennt gespeichert und verarbeitet werden. Zudem können die vom Münzgeld bekannten Probleme auftreten, wenn der Zahlende den zu bezahlenden Betrag nicht darstellen kann, d. h. nicht „passend hat“.

Zur Lösung beider Probleme sind zwei Ansätze bekannt, die auch im CAFE-Grundsystem verwendet werden (neben weiteren Spezialkonstruktionen) [OkOh 92, Ferg 93]: Zum einen gibt es Vorschläge, Münzen in mehrere Teilmünzen aufspalten zu können (z. B. eine 8-ECU-Münze in eine 4-ECU-Münze und zwei 2-ECU-Münzen), zum anderen Vorschläge, Münzen mehrfach verwenden zu können (z. B. eine 8-ECU-Münze achtmal als 1-ECU-Münze ausgeben zu können). Beide Ansätze reduzieren zwar etwas die Unbeobachtbarkeit (da mehrfach verwendete Münzen untereinander verkettbar sind), leisten aber die gewünschte schwache Integrität im Notfall.

2.3 Erweiterungen

2.3.1 Transferierbarkeit

Hauptproblem für die Transferierbarkeit, also die mehrmalige Weitergebbarkeit elektronischen Geldes, im CAFE-Grundsystem ist die schwache Integrität im Notfall. Die Nachweisbarkeit der unerlaubten Mehrfachverwendung einer Münze muß auch für den zweiten und jeden nachfolgenden Transfer gelten, und im Betrugsfall darf nur der Betrüger, nicht aber jeder ehemalige Besitzer der Münze deanonymisiert werden. Die prinzipielle Idee zur Lösung dieses Problems ist in [ChPe 93] beschrieben.

2.3.2 Mehrere Währungen

Das Hauptproblem bei der Verwendung mehrerer Währungen ist die Verfügbarkeit eines verbindlichen Wechselkurses zum Zeitpunkt der Zahlung. Für dessen Festlegung gibt es unterschiedliche Möglichkeiten, z. B. für einen längeren Zeitraum feste Wechselkurse oder die für eine gewisse Zeit gültige Eincodierung des Wertes einer Münze in mehreren Währungen während des Abhebens.

2.3.3 Verlusttoleranz

Dies ist die aus Anwendersicht vermutlich wichtigste Erweiterung des CAFE-Grundsystems: Verliert ein Zahlender sein Wallet, oder wird dieses defekt oder gestohlen, so verliert er *ohne* Verlusttoleranz zugleich auch alles im Wallet gespeicherte elektronische Geld. Durch Verlusttoleranz wird dieser Verlust minimiert.

Die Grundidee für Verlusttoleranz ist, die im Wallet gespeicherten elektronischen Münzen zusätzlich in einem zweiten Gerät abzuspeichern [WaPf 90, WaPf 91]. Die Abspeicherung muß so erfolgen, daß die Unbeobachtbarkeit des Zahlenden nicht beeinträchtigt wird, also z. B. auf einer Backup-Karte des Benutzers oder in verschlüsselter Form beim Betreiber. Im Verlustfall liefert der Benutzer seine Backup-Karte oder den verwendeten Verschlüsselungsschlüssel beim Betreiber ab, der dann die abgespeicherte Information auswertet: Alle Münzen, die das Wallet noch nicht ausgegeben hatte, werden dem Besitzer des Wallets gutgeschrieben. Bereits ausgegebene Münzen werden anhand des Verfahrens zur Entdeckung von mehrfach ausgegebenen Münzen (vgl. Abschnitt 2.2.3) erkannt.

Im Idealfall erhält ein Benutzer alle verlorenen Münzen zurück. Beschränkt wird die Verlusttoleranz durch zwei Faktoren:

Ist elektronisches Geld mehrfach transferierbar (was im Grundsystem nicht der Fall ist), so ist die Sicherung der nicht direkt vom Betreiber erhaltenen Münzen schwierig und nicht in jedem Fall möglich.

Ist ein verlorenes oder gestohlenes Wallet für den Finder oder Dieb *ohne* PIN verwendbar, so kann der Besitzer des Wallets die dabei ausgegebenen Münzen nicht mehr zurück erhalten. Um diesen Verlust zu begrenzen, muß der Gesamtbetrag, der ohne zwischenzeitliche Eingabe einer PIN ausgegeben werden kann, begrenzt werden.

2.3.4 Andere Erweiterungen

Neben den drei genannten Erweiterungen sind weitere für spezielle Anwendungen geplant, etwa für das Bezahlen von Telefongesprächen (sehr viele geringwertige Zahlungen in kurzer Zeit) oder von Fahrkarten im Nahverkehr (mit Bestpreisabrechnung, z. B. am Monatsende, unter Wahrung der Unbeobachtbarkeit).

2.4 Zusammenfassung: Was leistet das CAFE-Grundsystem?

Das CAFE-Grundsystem ist ein universelles prepaid offline Zahlungssystem.

Zahlungen eines Benutzers sind unbeobachtbar, d. h. niemand, auch nicht die Zahlungspartner und Betreiber, können innerhalb des Zahlungssystems Zahlende identifizieren oder verschiedene Zahlungen desselben Zahlenden miteinander in Beziehung bringen. Dies ist der vom Bargeld her gewohnte Datenschutz. Technisch basiert dies nur auf der Verläßlichkeit des Wallets des Zahlenden und, je nach Implementierung, zusätzlich auf der Sicherheit gewisser kryptographischer Verfahren.

Die Sicherheit eines Benutzers hängt nur von der Verläßlichkeit seines Geräts, also eines Wallets (Zahlender) oder POS-Terminals (Zahlungsempfänger), und der Sicherheit gewisser kryptographischer Verfahren ab. Sie ist unabhängig von der Verläßlichkeit der Geräte anderer Benutzer oder des Betreibers. Insbesondere ist der Guardian für die Sicherheit des Benutzers des zugehörigen Wallets bedeutungslos (von der Gesamtverfügbarkeit einmal abgesehen).

Die Sicherheit des Betreibers hängt ebenfalls nur von der Verläßlichkeit seiner Geräte und von der Sicherheit gewisser kryptographischer Verfahren ab. Zu den Geräten des Betreibers gehören allerdings auch die Guardians, die physikalisch sicher sein müssen. Sind diese tatsächlich sicher, so wird dem Betreiber starke Integrität garantiert, d. h. er kann nicht betrogen werden. Sind sie unsicher, so kann der Betreiber aber zumindest noch jeden Betrug entdecken und dem Betrüger nachweisen (schwache Integrität).

3 Ausblick

Bis etwa Mitte 1994, also bis zum Ende der ersten Projekthälfte, werden sich die Arbeiten in CAFE auf die Erforschung der Wünsche der potentiellen Benutzer und Betreiber, die Entwicklung des CAFE-Grundsystems nebst Erweiterungen und die Vorbereitung der praktischen Erprobung des Grundsystems konzentrierten. Die zweite Projekthälfte wird der eigentlichen Erprobung und einer zweiten Entwurfsphase gewidmet sein. Diese zweite Entwurfsphase dient einerseits der Fortentwicklung des CAFE-Grundsystems und andererseits der Entwicklung weiterer Autorisierungssysteme auf der Basis des CAFE-Wallets und -Guardians.

Für Kritik und Kommentare danke ich *Birgit Baum-Waidner, Malte Borcherding, Winfried Görke, Birgit Pfitzmann* und *Arnd Weber*.

4 Literatur

Ande 93 R. Anderson: Why Cryptosystems Fail; 1st ACM Conference on Computer and Communications Security, ACM, New York 1993, 215-227.

Bran 93 S. Brands: An Efficient Off-line Electronic Cash System Based On The Representation Problem; CWI, Computer Science/Departement of Algorithmics and Architecture, Rep. CS-R9323, 1993.

Bran1 93 S. Brands: Electronic Cash Systems Based on The Representation Problem In Groups Of Prime Order; Crypto '93, Pre-proceedings, Santa Barbara, August 1993, 26.1-26.15.

BrCh 93 S. Brands, D. Chaum: Distance-Bounding Protocols; Eurocrypt '93, Pre-proceedings, Lofthus, Mai 1993, W70-W88.

BüPf 89 H. Bürk, A. Pfitzmann: Digital Payment Systems Enabling Security and Unobservability; Computers & Security 8/5 (1989) 399-416.

Chau 85 D. Chaum: Security without Identification: Transaction Systems to make Big Brother Obsolete; Communications of the ACM 28/10 (1985) 1030-1044.

Chau 92 D. Chaum: Achieving Electronic Privacy; Scientific American (August 1992) 96-101.

ChFN 90 D. Chaum, A. Fiat, M. Naor: Untraceable Electronic Cash; Crypto '88, LNCS 403, Springer-Verlag, Berlin 1990, 319-327.

ChPe 93 D. Chaum, T. Pedersen: Transferred Cash Grows in Size; Eurocrypt '92, LNCS 658, Springer-Verlag, Berlin 1993, 390-407.

ChPe1 93 D. Chaum, T. Pedersen: Wallet Databases with Observers; Crypto '92, LNCS 740, Springer-Verlag, Berlin 1993, 89-105.

CrPe 93 R. Cramer, T. Pedersen: Improved Privacy in Wallets with Observers; Eurocrypt '93, Pre-proceedings, IACR, Lofthus, Mai 1993, W58-W69.

Denn 82 D. Denning: Cryptography and Data Security; Addison-Wesley Publishing Company, Reading 1982; Reprinted with corrections, January 1983.

DiHe 76 W. Diffie, M. E. Hellman: New Directions in Cryptography; IEEE Transactions on Information Theory 22/6 (1976) 644-654.

DSS 92 The Digital Signature Standard Proposed by NIST; Comm. of the ACM 35/7 (1992) 36-40.

ElGa 85 T. ElGamal: A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms; IEEE Transactions on Information Theory 31/4 (1985) 469-472.

Ferg 93 N. Ferguson: Single Term Off-Line Coins; Eurocrypt '93, Pre-proceedings, Lofthus, Mai 1993, W46-W57.

Ferg1 93 N. Ferguson: Extensions of Single-Term Coins; Crypto '93, Pre-proceedings, Santa Barbara, August 1993, 25.1-25.11.

FrYu 93 M. Franklin, M. Yung: Secure and Efficient Off-Line Digital Money; 20th International Colloquium on Automata, Languages and Programming (ICALP), LNCS 700, Springer-Verlag, Heidelberg 1993, 265-276.

GoMR 88 S. Goldwasser, S. Micali, R. L. Rivest: A Digital Signature Scheme Secure Against Adaptive Chosen-Message Attacks; SIAM J. Comput. 17/2 (1988) 281-308.

Grim 93 R. Grimm: Das Gleichgewichtsmodell für verbindliche Telekooperation; Datenschutz und Datensicherung DuD 17/2 (1993) 94-107.

GuUQ 92 L. Guillou, M. Ugon, J. Quisquater: The Smart Card: A Standardized Security Device Dedicated to Public Cryptology; Gustavus J. Simmons: Contemporary Cryptology – The Science of Information Integrity; IEEE Press, Hoes Lane 1992, 561-613.

Neum 92 P. G. Neumann: Inside Risks: Fraud by computers; Communications of the ACM 35/8 (1992), 154.

OkOh 92 T. Okamoto, K. Ohta: Universal Electronic Cash; Crypto '91, LNCS 576, Springer Verlag, Berlin 1992, 324-337.

PWP 90 B. Pfitzmann, M. Waidner, Andreas Pfitzmann: Rechtssicherheit trotz Anonymität in offenen digitalen Systemen; Datenschutz und Datensicherung DuD 14/5-6 (1990) 243-253, 305-315.

RSA 78 R. L. Rivest, A. Shamir, L. Adleman: A Method for Obtaining Digital Signatures and Public-Key Cryptosystems; Comm. of the ACM 21/2 (1978) 120-126, reprinted: 26/1 (1983) 96-99.

Scha 92 I. Schaumüller-Bichl: Sicherheitsmanagement – Risikobewältigung in informationstechnologischen Systemen; BI Wissenschaftsverlag, Mannheim 1992.

Schn 91 C. P. Schnorr: Efficient Signature Generation by Smart Cards; Journal of Cryptology 4/3 (1991) 161-174.

WaPf 90 M. Waidner, B. Pfitzmann: Loss-Tolerance for Electronic Wallets; Proceedings 20th International Symp. on Fault-Tolerant Computing (FTCS 20), Newcastle upon Tyne (UK), 140-147.

WaPf 91 M. Waidner, B. Pfitzmann: Loss-tolerant electronic wallet; David Chaum (ed.): Second International Smart Card 2000 Conference, North-Holland, Amsterdam 1991, 127-150.