Sicheres Bezahlen für Informationsdienste in zukünftigen Mobilnetzen

Hans-Joachim Hitz, Günther Horn
Siemens AG
Zentralabteilung Technik
Information und Kommunikation

1 Zusammenfassung

Schon heute werden Mehrwert-Informationsdienste in Mobilnetzen angeboten. Durch die Entwicklung leistungsfähigerer Endgeräte sowie die Bereitstellung von neuen Diensten in zukünftigen Netzen wird die Vielfalt der angebotenen Informationsdienste sowie der Anbieter zunehmen. Dieser Beitrag beschreibt ein sicheres, flexibles und effizientes Bezahlungsverfahren für solche Dienste, das auf der Verwendung von Micropayments beruht, und seine Implementierung in einem Demonstrator. Das Verfahren ist auch in einer allgemeineren Umgebung einsetzbar.

2 Einleitung

Die Verbreitung der Mobilkommunikation hat seit der Einführung von Systemen, die auf dem GSM-Standard basieren, sehr stark zugenommen und wird voraussichtlich weiterhin stark wachsen. Mobilsysteme werden nach wie vor überwiegend für Sprachdienste genutzt, wenn auch Datendienste verfügbar sind. Neben den angebotenen Basisdiensten sind auch, abhängig vom jeweiligen Diensteanbieter, vielfältige Mehrwertdienste (z.B. Börseninformation, Pannenhilfe) verfügbar, deren Gestaltungsmöglichkeiten jedoch durch die technischen Randbedingungen der heutigen GSM-Systeme (insbesondere Bandbreite und Display) beschränkt sind. Die Bezahlung für die Inanspruchnahme dieser Mehrwertdienste erfolgt heute auf der Basis der Subskription sowie der Nutzungsdauer des Mehrwertdienstes. Das Mißbrauchspotential von Mehrwertdiensten (in Festnetzen und Mobilnetzen) ist sehr hoch und ist wohlbekannt. Es wäre wünschenswert, mit zunehmender Reduzierung der technischen Beschränkungen durch neue Netze und Dienste auch ein Bezahlungsverfahren einzusetzen, das

einerseits den wachsenden Darstellungmöglichkeiten durch größere Flexibilität Rechnung trägt und andererseits deutlich mehr Sicherheit bietet als das heutige Abrechnungsverfahren.

Ein zweites Gebiet der Kommunikation, auf dem gegenwärtig ein enormes Wachstum zu beobachten ist, ist das Internet, insbesondere das WorldWideWeb. Hier ist der leichte Zugriff auf ansprechend graphisch aufbereitete Informationsquellen mit Hilfe eines Browsers den meisten inzwischen wohl vertraut. Parallel zum Wachstum des Internet werden auch seine Nutzungsmöglichkeiten für Zwecke des elektronischen Handels diskutiert. Während erste Lösungen bereits vorliegen, ist der erwartete große Aufschwung für den elektronischen Handel bisher noch nicht eingetreten, da noch wesentliche Fragen ungeklärt sind. Eine zentrale dieser Fragen ist die Sicherheit. Die Sicherheit betrifft eine ganze Reihe von Aspekten, wie die Vertraulichkeit von Benutzerinformationen, die Abwicklung von Bestell- und Liefervorgängen, die Bindewirkung von elektronischen Verträgen und insbesondere die Bezahlung über das Internet. Auf dem letzten Gebiet gibt es inzwischen eine wahre Flut von Vorschlägen für die verschiedensten Zwecke. Eine Klasse von Bezahlungsverfahren ist diejenige der Micropayments, die gedacht ist für die Bezahlung von Information, die pro abgerufener Informationseinheit nur einen relativ geringen Wert hat, der den Einsatz aufwendigerer Verfahren nicht rechtfertigt.

Es wird erwartet, daß mobile Telekommunikationssysteme und das Internet in Zukunft nicht mehr so streng getrennt sein werden wie heute. Zum einen werden erstere einen komfortableren Zugang zum Internet erlauben als heute, zum anderen werden auch Internet- und insbesondere WorldWideWeb-Anwendungen und -Protokolle in mobilen Telekommunikationssystemen vermehrt sinnvoll zum Einsatz kommen können. Dies ist heute aufgrund der technischen Beschränkungen der Mobilsysteme nur bedingt möglich. Diese Entwicklung wird dann auch eine Realisierung von mobilen Mehrwert-Informationsdiensten auf der Basis von WorldWideWeb-Technologie ermöglichen. Spätestens dann stellt sich auch die Frage nach adäquaten Bezahlungsverfahren für solche Dienste in verstärkter Weise. Die Anbieter von mobilen Mehrwert-Informationsdiensten könnten dann profitieren von Verfahren, die ursprünglich für das Internet vorgeschlagen wurden. Jedoch muß sichergestellt sein, daß diese Verfahren mit den besonderen technischen Beschränkungen in einer mobilen Umgebung, die in abgemilderter Form nach wie vor bestehen werden, verträglich sind. In diesem Beitrag wird die Realisierung eines bestimmten

Verfahrens aus der Klasse der Micropayment-Verfahren betrachtet.

Es soll hier ausdrücklich betont werden, daß der Einsatz des vorgestellten Bezahlungsverfahrens keineswegs auf mobile Dienste beschränkt ist, und daß bei seinem Einsatz für mobile Dienste die Verwendung von WorldWideWeb-Technologie nicht Voraussetzung ist. Jedoch sind die technischen Randbedingungen im Fall von Mobildiensten besonders anspruchsvoll und die Attraktivität von mobilen Informationsdiensten bei Verwendung von WorldWideWeb-Technologie besonders hoch. Darüber hinaus ist in einem Mobilnetz ein Benutzer von vornherein mit einer Chipkarte ausgestattet, was die Lösung der Sicherheitsprobleme erheblich erleichtert. Aus diesen Gründen wurde der Einsatz des Bezahlungsverfahrens am Szenario mobiler Mehrwert-Informationsdienste demonstriert.

Der Rest des Beitrags ist wie folgt aufgebaut:

In Kapitel 3 wird ein kurzer Überblick über die heutige sowie die zu erwartende zukünftige Situation bei Netzen, Basisdiensten, Mehrwertdiensten und Endgeräten gegeben.

In Kapitel 4 wird ein Abriß elektronischer Bezahlungsverfahren gegeben, um dem Leser die Einordnung des hier ausgewählten Verfahrens zu erlauben. Dabei kommen die Anforderungen an solche Systeme ebenso zur Sprache wie die gängigsten Eigenschaften der Systeme und eine grobe Klassifizierung.

In Kapitel 5 wird das zu Grunde gelegte Abrechnungsmodell dargestellt, in dem die Rollen der an der Bereitstellung des Informationsdienstes und am Bezahlvorgang beteiligten Parteien erläutert werden.

In Kapitel 6 werden die verwendeten Protokolle ausführlich beschrieben. Diese bestehen aus einem Vereinbarungsprotokoll mit gegenseitiger Authentifikation, das für Mobilanwendungen optimiert ist, sowie dem eigentlichen Bezahlungsprotokoll.

In Kapitel 7 wird ein Demonstrator beschrieben, der im Rahmen des EU-Förderprojekts ASPeCT (**A**dvanced **S**ecurity for **Pe**rsonal **C**ommunication **T**echnologies) entwickelt wurde. Dabei werden sowohl die Architektur als auch die Konfiguration des Demonstrators beschrieben. Ferner wird kurz auf einen im selben Rahmen geplanten Feldversuch eingegangen.

In Kapitel 8 werden schließlich die Einsatzmöglichkeiten von

Chipkarten im gegebenen Zusammenhang sowie die Realisierung im Demonstrator dargestellt.

3 Technische Umgebung für mobile Informationsdienste - heute und in Zukunft

3.1 Netze und Basisdienste

GSM hat sich als Standard für zellulare Mobilsysteme in Europa und weiten Teilen der Welt etabliert. GSM bietet heute, neben dem Sprachdienst, Datendienste bis zu einer Bitrate von 9,6 kbit/s sowie den Short Mpatenteessage Service (SMS), der für die Realisierung von Mehrwertdiensten heute von besondere Bedeutung ist. Der SMS ermöglicht die Übertragung von Nachrichten bis zu 160 Zeichen Länge, die dann auf dem Display des Mobiltelephons dargestellt werden. Nachrichten werden in einem Short Message Center zwischengespeichert. In naher Zukunft werden - in Phase 2+ von GSM - zwei neue Datendienste zur Verfügung stehen, die auch die Bereitstellung hochwertiger Informationsdienste erheblich erleichtern werden, der High Speed Circuit Switched Data (HSCSD) Service und der General Packet Radio Service (GPRS). Beide Dienste werden wesentlich höhere Bitraten bieten, als dies heute der Fall ist. Der leitungsvermittelte HSCSD-Dienst erlaubt die Kombination von bis zu 8 Kanälen zu je 9.6 kbit/s, bietet also insbesondere die Bitrate eines ISDN-Kanals von 64 kbit/s, der GPRS erlaubt Bitraten von bis zu 100 kbit/s und ist aufgrund seiner Eigenschaft als paketvermittelnder Dienst besonders für Informationsdienste geeignet, die Internetprotokolle verwenden.

Neben GSM kann auch DECT für die Anbieter von mobilen Informationsdiensten von Interesse werden, wenn auf DECT basierende Cordless Telephone Mobility (CTM) eine hinreichende Verbreitung erhält. Darauf soll hier jedoch nicht näher eingegangen werden.

Die oben genannten Systeme gehören der sogenannten zweiten Generation der Mobilsysteme an, die in einigen Jahren durch ein Mobilsystem der dritten Generation, dem Universal Mobile Telecommunications System (UMTS) ergänzt werden. UMTS wird die Funktionalität der Systeme der zweiten Generation umfassen und darüber hinaus Multimediadienste in hoher Qualität ermöglichen. Die Bitraten sollen ISDN-Raten (flächendeckend) sowie bis zu 2 Mbit/s (in ausgewählten Gebieten wie Stadtzentren oder

Industriegebieten) betragen. UMTS wird bei ETSI SMG standardisiert und gleichzeitig vom UMTS Forum, einem Zusammenschluß von Telekommunikationsnetzbetreibern, -herstellern und regulierenden Behörden vorangetrieben. Das UMTS Forum erwartet die Einführung von UMTS-Diensten auf kommerzieller Basis für das Jahr 2002 [UMTS].

3.2 Mehrwertdienste

Wer heute einen Vertrag mit einem Diensteanbieter für ein GSM-basiertes Mobilnetz eingeht, erhält damit in der Regel auch eine ganze Palette von Mehrwertdiensten angeboten. Zur Illustration seien hier einige aufgelistet: Pannen-Service, Travel-Service, Verkehrsinformations-Service, Vermittlungs-Service, medizinische Hilfe unterwegs, Sekretariats-Service, Börseninformations-Service und viele andere mehr. Diese Dienste sind heute auf die GSM-Bitraten und das Display eines GSM-Telefons, also auf die Anzeige einer geringen Anzahl von Zeichen beschränkt. Es bedarf keiner großen Phantasie, sich vorzustellen, daß viele dieser Dienste erheblich an Attraktivität gewinnen würden, wenn sie durch detaillierte Graphik - wenn möglich in Farbe - unterstützt werden könnten. Dies gilt vermehrt, wenn ein solcher Mehrwertdienst die spezifischen Vorteile der Mobilität ausnutzen kann, zum Beispiel durch Kombination mit dem Global Positioning System (GPS). Als ein Beispiel sei ein europaweiter Pannendienst für Autofahrer betrachtet: Dieser könnte einem Autofahrer die nächstgelegene (geöffnete) Werkstatt mitteilen, abhängig von seiner durch GPS ermittelten Position und eventuell Tag und Uhrzeit. Der Weg dorthin würde beschrieben durch eine Landkarte, die dem Benutzer über das Mobilsystem auf das Display seines Endgerätes übermittelt würde. Solche mobilen Mehrwertdienste sind keine bloße Zukunftsmusik mehr. Sie werden bereits in Feldversuchen erprobt (siehe [GeHa]).

3.3 Endgeräte

Die meisten der heute verwendeten Endgeräte für GSM besitzen ein kleines Display, das nur die Darstellung weniger Zeichen erlaubt. Es ist damit für einen anspruchsvollen Mehrwertdienst der oben beschriebenen Art nur bedingt geeignet. Verwendet man als Endgerät zur Darstellung des Mehrwertdienstes einen mobilen Rechner (Laptop PC), den man über ein Funkmodem an ein GSM-Endgerät anschließt, so hat man sich zwar von den Beschränkungen

des Displays weitgehend befreit, die Datenrate der von GSM angebotenen Dienste bleibt jedoch ein Problem.

Ungeachtet dessen werden schon heute in zunehmendem Maße Endgeräte entwickelt, die erweiterte Funktionalität bereitstellen, z.B. durch Integration eines Browsers und Anpassung der verwendeten Protokolle an die Besonderheiten des Mobilfunks. Die Vielfalt solcher Endgeräte, die die Funktionen eines Mobilterminals und eines Laptop PCs oder handgehaltenen Computers vereinen, wird noch zunehmen.

4 Elektronische Bezahlungsverfahren

4.1 Anforderungen an ein Bezahlungsverfahren für mobile Mehrwertdienste

Die Abrechnung für heutige Mehrwertdienste besteht aus einer Basisgebühr für die Inanspruchnahme des Basisdienstes - der für die Übermittlung der Information zwischen dem Benutzer und dem Anbieter von Mehrwertdiensten sorgt - und einer "Prämie" für den Mehrwert, den der Informationsdienst bietet. Beide Teile der Gebühr beruhen auf der Subskription und einer zur Nutzungsdauer des Dienstes proportionalen Komponente. Für die Zukunft wäre jedoch aufgrund der größeren Vielfalt der angebotenen Dienste ein **flexibleres** Abrechnungsverfahren, zumindest für die "Prämie" wünschenswert. Diese Flexibilität bezieht sich auf verschiedene Aspekte:

- die Parameter, von denen die Gebühr abhängt, (Neben der Nutzungsdauer könnte das übertragene Datenvolumen berücksichtigt werden sowie, noch wichtiger, der Inhalt der Information.)
- die Mischung verschiedener möglicher Tarife,
- die Leichtigkeit, mit der ein Tarif gewechselt werden kann.

Wesentlich ist auch die **Effizienz** des gewählten Bezahlungsverfahrens. Wie schon oben kurz erwähnt, muß der Aufwand, der für einen Bezahlungsvorgang getrieben werden muß, in vernünftiger Relation stehen zum Wert der zu bezahlenden Ware, hier der erworbenen Information. Dies ist bei vielen vorgeschlagenen elektronischen Bezahlungsverfahren für Warenwerte im Bereich von einem ECU (European Currency Unit) oder darunter nicht der Fall,

z.B. wegen vorgeschriebener Rückfragen bei einem zentralen Server. Ferner muß auch die Abwicklung des Bezahlungsprotokolls vereinbar sein mit den technischen Gegebenheiten auf der Nutzerseite, auf der Seite des Servers, der die Bezahlung abwickelt sowie des Kommunikationsmediums, hier des Mobilnetzes, d.h. das Bezahlungsprotokoll muß möglichst wenig Rechenaufwand erfordern und möglichst kurze Nachrichten enthalten.

Selbstverständlich muß ein Bezahlungsverfahren auch **sicher** sein gegen jede Form von Mißbrauch. Auch hier gilt jedoch wieder, daß der Aufwand für die Sicherheit des Verfahrens in Relation stehen muß zum Wert des zu schützenden Gutes. Ein Aspekt der Sicherheit, der zunehmend an Bedeutung gewinnt, ist die **Unanfechtbarkeit** der Gebührenabrechnung. Diese bedeutet, daß während des Bezahlungsverfahrens Daten erzeugt werden, auf deren Grundlage später entschieden werden kann - nicht nur von den beteiligten Parteien, sondern auch von neutralen Dritten -, ob ein Dienst auch tatsächlich in Anspruch genommen wurde oder ob es sich bei der Gebührenabrechnung um eine ungerechtfertigte Zahlungsforderung handelt.

4.2 Eine Klassifikation von Bezahlungsverfahren

Eine große Zahl von Bezahlungsverfahren ist für den Gebrauch im Internet vorgeschlagen worden. Literaturübersichten finden sich z.B. in [Gang], [Pete].

Die Terminologie, die für die Bezeichnung der Rollen der an dem Bezahlungsverfahren beteiligten Parteien in der Literatur verwendet wird, variiert. Typischerweise werden drei Rollen unterschieden:

- der Käufer oder Kunde: Er möchte einen Dienst in Anspruch nehmen, eine Information oder ein Stück Software kaufen und dafür elektronisch bezahlen,
- der Verkäufer oder Händler: Er bietet einen Dienst an oder verkauft eine Information oder ein Stück Software und möchte dafür elektronisch bezahlt werden,
- der Makler oder die Bank oder der Bezahlungssystemanbieter, auch "Issuer/Acquirer" in kreditkartenbasierten Systemen: Er betreibt das Bezahlungssystem und bietet die dafür notwendigen Dienste an. Die spezifische Rolle hängt von den Besonderheiten des Bezahlungsverfahrens ab. In den meisten Systemen ist er

Mittler bei den Zahlungen des Kunden an den Händler, in einigen Systemen (z.B. Mondex) ist es aber auch möglich, daß Zahlungen einer Partei an eine zweite ohne Einschaltung der Bank erfolgen.

Die Rollen der an dem in diesem Beitrag betrachteten Verfahren beteiligten Instanzen werden im Kapitel 5 beschrieben.

Häufig werden die Bezahlungsverfahren nach folgenden nützlichen Kriterien unterschieden:

- **online vs. offline:** Ein online-Verfahren erfordert den online-Zugang zu einem Autorisierungsserver, typischerweise betrieben von einer Bank oder einem "Acquirer", bei jeder Zahlung. Beispiele für solche Systeme sind kreditkartenbasierte Systeme sowie Netbill [Netb]. In einem offline-System gibt es keine Notwendigkeit, neben Kunde und Händler noch eine dritte Instanz an der Bezahlung online zu beteiligen. Elektronische Geldbörsen sind Beispiele für offline-Systeme.
- **kreditbasiert vs. debitbasiert**: In einem kreditbasierten System wird das Konto des Kunden erst belastet, nachdem er die Zahlung geleistet hat, in einem debitbasierten System ist es umgekehrt.
- **Verwendung von Kryptographie**: Fast alle vorgeschlagenen Verfahren verwenden kryptographische Methoden, um das geforderte Sicherheitsniveau zu erreichen. Es gibt jedoch auch Ausnahmen [Firs]. Ferner wird unterschieden zwischen Verfahren, die **secret-key Kryptographie** und solchen, die **public-key Kryptographie** verwenden. Zur ersten Klasse gehören z.B. elektronische Geldbörsen, zur zweiten anonyme electronic cash-Systeme. Die Verwendung von public-key Kryptographie bringt typischerweise eine höhere Rechen- und Kommunikationskomplexität mit sich. Ein Vorteil ist dagegen die größere Flexibilität des Schlüsselmanagements.
- **ausschließliche Verwendung von Software vs. Verwendung von "tamper-resistant" Hardware**: In einigen Systemen ist die Verwendung von "tamper-resistant" Hardware, sowohl auf der Seite des Kunden als auch auf der des Händlers, zwingend, um **Mißbrauch durch die Beteiligten** auszuschließen. Alle

elektronische Geldbörsen fallen in diese Kategorie. Andere Systeme können auch ausschließlich in Software realisiert werden. Hierunter fällt z.B. das SET-Protokoll als ein Beispiel für ein kreditkartenbasiertes System. Jedoch ist es oft auch bei dem letzteren Typ von Systemen auf der Seite des Kunden wünschenswert, "tamper-resistant" Hardware einzusetzen, beispielsweise, um den geheimen Schlüssel **vor dem Zugriff Dritter** zu schützen.

- **Anonymität und Unverfolgbarkeit**: Einige Bezahlungsverfahren bieten starke Garantien für die Unverfolgbarkeit des Bezahlungsvorgangs, wie bei realem Bargeld erlaubt der Bezahlungsvorgang keine Rückschlüsse auf die Identität des Käufers. Dies gilt auch bei Verfolgung über mehrere Bezahlungsvorgänge hinweg. Electronic cash-Systeme wie [ecas], [CAFE] bieten diese Art von Garantie. Erkauft wird diese Garantie mit einem Overhead an notwendigen kryptographischen Berechungen. Kreditkartenbasierte Systeme können keine Unverfolgbarkeit bieten, da der Käufer ein Konto beim Kreditkartenunternehmen haben muß. Jedoch können diese Verfahren noch Anonymität im dem Sinn bieten, daß der Käufer gegenüber dem Händler ein Pseudonym verwendet.
- **Unanfechtbarkeit**: siehe Kapitel 4.1

Häufig werden Bezahlungsverfahren anstatt durch die obigen Eigenschaften auch an Hand ihrer Analoga in der Welt herkömmlicher Bezahlungsverfahren klassifiziert. (Wir haben schon einige dieser Begriffe verwendet.)

- **Kreditkartenbasierte Systeme**: Diese Systeme emulieren die Transaktionen, die heute bei der Bezahlung mit Kreditkarte vorgenommen werden. Diese Verfahren sind online, kreditbasiert und benützen public-key Kryptographie. Das SET-Protokoll hat sich als Defacto-Standard etabliert [SET]. Diese Systeme sind geeignet für die Bezahlung von Beträgen von ECU an aufwärts, nicht jedoch für die Bezahlung kleiner und sehr kleiner Beträge, hauptsächlich aufgrund der Kosten der online-Autorisierung.
- **Elektronische Geldbörsen**: Diese Systeme sind typischerweise

offline, debitbasiert und verwenden secret-key Kryptographie. Sie erfordern "tamper-resistant" Hardware sowohl auf der Seite des Kunden als auch auf der des Händlers, was ein Nachteil ist. Sie sind effizient einsetzbar auch für die Bezahlung kleiner Beträge. (Sie könnten daher auch als Micropayment Systeme (s.u.) betrachtet werden, auch wenn sie üblicherweise nicht unter diesen Begriff subsumiert werden.)

- **Electronic cash-Systeme**: Ihre hervorstechende Eigenschaft ist die Unverfolgbarkeit. Die Analogie zu realem Geld wird in einigen Ländern (wie z. B. in Deutschland) relativiert durch die gesetzliche Anforderung, für die Kunden bei der Bank Schattenkonten einzurichten. Sie sind auch geeignet für die Bezahlung kleiner Beträge.
- **Micropayment-Systeme**: Diese Systeme wurden entworfen zu dem Zweck, effizient eine Bezahlung kleiner Beträge über das Internet zu unterstützen. Für eine Übersicht über die Vielzahl der gemachten Vorschläge siehe wiederum [Pete]. Hier soll nur auf einige wenige eingegangen werden. Interessanterweise wurde innerhalb kurzer Zeit derselbe kryptographische Mechanismus, der ursprünglich in [Lam] für Authentifikationssysteme vorgeschlagen worden war, von vier Autoren [Pede, PayW, ikP, Netc] für die Anwendung in Micropayment-Systemen vorgeschlagen. Dieser Mechanismus bewirkt, daß die durch eine digitale Signatur gegebene Garantie sich - außer auf den signierten Wert selbst - auch auf viele davon mittels einer Einwegfunktion abgeleiteten Werte erstreckt. Diese Werte sind sehr effizient zu berechnen und werden zur Bezahlung verwendet. (Wem dies noch etwas kryptisch vorkommt, der sei auf das Kapitel 6 verwiesen.)
- Anwendungen für Micropayment-Verfahren erstrecken sich von elektronischem Publizieren über Kommunikationsdienste, Informationsdienste und Video-on-Demand bis zum Verkauf von Software. Um den angestrebten Effizienzgewinn zu erzielen, sollten allerdings im Abrechnungszeitraum mehrere Zahlungen eines Kunden an einen Händler erfolgen, um die Kosten für die Zahlungsabwicklung mit dem Makler zu minimieren.
- Micropayment-Verfahren können in vielen Varianten ausgestaltet

werden: sie können online oder offline sein (oder eine Mischung davon), sie können kredit- oder debitbasiert sein. Man muß jedoch anmerken, daß Micropayment-Verfahren, die für jeden Bezahlungsvorgang online-Autorisierung erfordern, viel von den Vorteilen verlieren, die sie durch die Verwendung effizienter kryptographischer Mechanismen gewinnen. Sinnvoll wäre in jedem Fall, die Notwendigkeit einer online-Autorisierung vom bezahlten - oder aufgelaufenen - Betrag abhängig zu machen.

4.3 Das Tick Payments-Verfahren

Wir legen in diesem Beitrag das von T. Pedersen in [Pede] beschriebene "Tick Payments"-Verfahren zugrunde. Es wurde ursprünglich für die Abrechnung von Telefongesprächen entwickelt, woraus sich auch der Name ableitet (von "phone ticks", dem Ticken des Gebührenzählers). Für die Details des Verfahrens siehe Kapitel 6. Es ist ein Micropayment-Verfahren, das im Projekt ASPeCT in einer online- und einer offline-Variante implementiert wurde. Es gibt sowohl eine kreditbasierte als auch eine debitbasierteVariante. Im Projekt ASPeCT wurde die kreditbasierte Variante implementiert, da sie näher am Abrechnungsmodell der üblichen Telephonrechnung liegt.

5 Abrechnungsmodell

Ein logistisches Problem, mit dem sich ein Anbieter eines Micropayment-Bezahlverfahrens konfrontiert sieht, ist die Zusammenführung all der kleinen Beträge, die ein Benutzer bei verschiedenen Anbietern von Informationsdiensten bezahlt hat, zu einer Rechnung. Dies ist ein nicht-triviales Problem und führt schon heute dazu, daß sich Internet Service Provider mit Telephongesellschaften zusammentun, da diese große Erfahrung mit Abrechnungssystemen haben, vgl. [CWI]. Es ist daher sinnvoll, das Abrechnungsmodell für Micropayments von vornherein so anzulegen, daß es vorhandene Abrechungsstrukturen optimal nutzt. Dies wird in dem von uns betrachteten Fall dadurch erleichtert, daß wir Mehrwert-Informationsdienste in Mobilnetzen betrachten, uns also schon in einer Telekommunikationsumgebung befinden. Der Benutzer soll, wie heute auch, nur eine Rechnung für die Inanspruchnahme von Mehrwertdienste verschiedener Anbieter erhalten, zusammen mit seiner Telephonrechnung.

Wir beschreiben hier nur den Fall, in dem das Micropayment-

Verfahren als offline-Verfahren verwendet wird.

An der Abrechnung sind drei Instanzen beteiligt: Der mobile Benutzer, der Anbieter des Mehrwertdienstes und der Anbieter der Mobilnetzdienste (z.B. ein GSM Service Provider). Voraussetzung für das Funktionieren des Modells ist, daß zwischen dem Benutzer und dem Mobilnetz-Diensteanbieter einerseits und letzterem und dem Anbieter des Mehrwertdienstes andererseits vertragliche Beziehungen bestehen. Die erste Beziehung ist dabei eine gewöhnliche Subskription.

Die Abwicklung des Zahlungsvorgangs wird in Abbildung 1 illustriert:

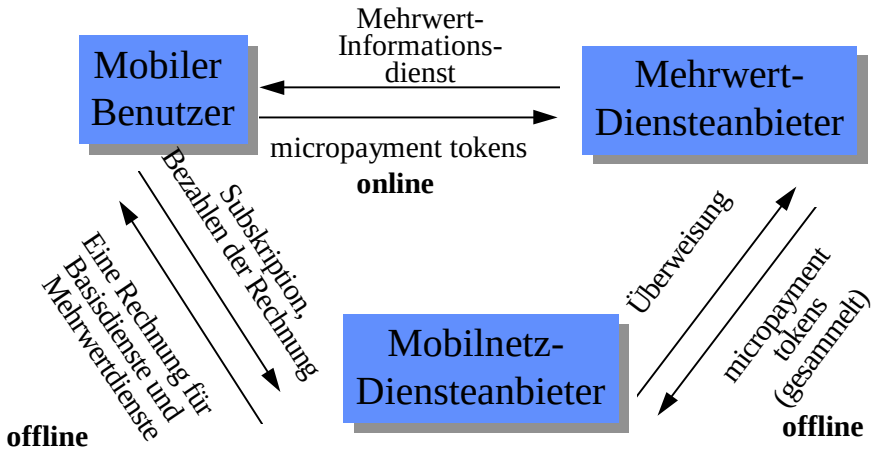


Abbildung 1: Abwicklung des Zahlungsvorgangs

Während ein mobiler Benutzer einen Mehrwertdienst in Anspruch nimmt, leistet er fortwährend Zahlungen in Form von Micropayment-Tokens an den Anbieter des Dienstes. Das Protokoll, das diese Zahlungen realisiert, ist in Kapitel 6 beschrieben. Der Anbieter des Mehrwertdienstes prüft die erhaltenen Micropayment-Tokens, sammelt diese als Nachweise für die Zahlungen des Benutzers und schickt diese gebündelt in festen Abständen - z.B. täglich oder wöchentlich - zur Abrechnung an den Mobilnetz-Diensteanbieter. Dieser prüft die erhaltenen Abrechnungsdaten (insbesondere auf Duplikate) und belastet sie dem Gebührenkonto des Benutzers. Der entsprechende Betrag wird auf das Konto des Anbieters des Mehrwertdienstes überwiesen. Am Monatsende schickt er dem Benutzer die übliche Telephonrechnung, in der die Gebühren für die Inanspruchnahme der Mehrwertdienste berücksichtigt sind. Diese

wird dann vom Benutzer auf üblichem Wege bezahlt.

Die einzige online-Beziehung für Bezahlungszwecke besteht also zwischen dem Benutzer und dem Anbieter des Mehrwertdienstes.

6 Protokolle

Die Abwicklung des Bezahlungsvorgangs geschieht in zwei Phasen:

In der Initialisierungsphase authentifizieren sich der Benutzer U (für User) und der Mehrwert-Diensteanbieter V (für Value Added Service Provider) gegenseitig. Dabei verpflichtet sich der Benutzer mittels einer digitalen Signatur auch - in unanfechtbarer Weise - auf einen Startwert für das Micropayment-Verfahren und auf weitere Information, die für die Berechnung der Gebühren wesentlich ist, wie z.B. den anzuwendenden Tarif, Datum, Uhrzeit, etc. Das Authentifikationsprotokoll in der hier vorgestellten Form ist auch bei ETSI SMG für die Authentifikation zwischen Benutzer und Netzwerk vorgeschlagen [ETS]. Der Startwert wird durch n-fach iterierte Anwendung einer Einwegfunktion auf einen vom Benutzer zufällig gewählten Wert berechnet.

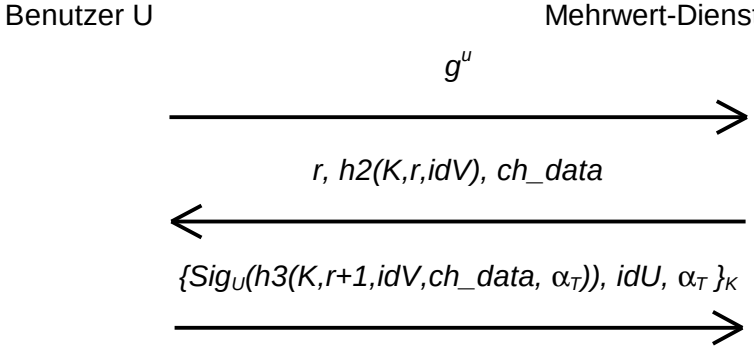
In der Datenübertragungsphase bezahlt der Benutzer, indem er Urbilder des Startwertes preisgibt. Diese bilden die kleinste Einheit für die Bezahlung, sogenannte „Ticks“ (Micropayment-Tokens). Der Wert eines solchen Ticks wird während der Initialisierungsphase festgelegt. Der Benutzer ist der einzige, der solche Ticks berechnen kann, daher gelten sie für den Mehrwert-Diensteanbieter als Nachweis für die Rechnung an den Benutzer. Der Mehrwert-Diensteanbieter rechnet mit dem UMTS Service Provider des Benutzers ab und kann dort die protokollierten Ticks als Nachweis vorlegen. Die hohe Effizienz des Verfahrens kommt daher, daß der Benutzer mit einer einzigen Signatur eine große Anzahl von Zahlungsvorgängen authentifiziert. Diese Zahlungsvorgänge bestehen dann aus einer sehr schnellen Berechnung einer Einwegfunktion und der Übertragung der Ticks, die deutlich kleiner sind als typische Signaturen.

Im folgenden werden die den beiden Phasen entsprechenden Protokolle dargestellt, wobei wir der Klarheit wegen auf ein drittes Protokoll nicht näher eingehen. In diesem, dem "Reinitialisierungs-Protokoll", vereinbaren der Benutzer und der Mehrwert-Diensteanbieter eine neue Anzahl von Ticks, wenn der Benutzer während einer Verbindung die im Authentifikations-Protokoll vereinbarte Anzahl verbraucht hat.

6.1 Voraussetzungen

- Es ist eine kryptographisch starke endliche Gruppe G mit erzeugendem Element *g* allgemein bekannt (d.h. das diskrete Logarithmus-Problem in G ist hart).
- Es gibt Einwegfunktionen *f* und *h2* und Hash-Funktionen *h1* und *h3*. (Es würde zu weit führen, hier die präzisen Anforderungen an diese Funktionen zu beschreiben.)
- $\{\ \}_K$ bezeichnet eine symmetrische Verschlüsselung mit dem Schlüssel K.
- $Sig_A()$ bezeichnet die Signatur eines Benutzers A mit seinem geheimen Signatur-Schlüssel.
- Der Mehrwert-Diensteanbieter V hat einen allgemein bekannten öffentlichen Schlüssel g^v zur Vereinbarung von Sitzungsschlüsseln.

6.2 Authentifikations-Protokoll



Der Benutzer U erzeugt eine Zufallszahl u, berechnet g^u und schickt das Ergebnis an V.

Wenn V dies erhält, kennt er die Identität von U nicht. V erzeugt eine Zufallszahl *r*, berechnet $(g^u)^v$ und einen Sitzungsschlüssel $K := h1((g^u)^v,r)$ und $h2(K,r,idV)$, um zu beweisen, daß er *K* kennt. V hat jetzt die Möglichkeit, Daten *ch_data* für die Gebührenberechnung an U zu schicken, die U signieren muß.

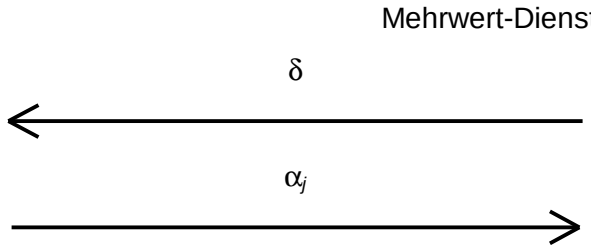
Nach Erhalt der zweiten Nachricht berechnet *U* den Sitzungsschlüssel $K = h1((g^v)^u,r)$. Dann prüft er den Wert $h2(K,r,idV)$

und weiß, daß *V* den Sitzungsschlüssel *K* besitzt. *U* verschlüsselt seine Identität *idU* und den Startwert α_T für das Bezahlungs-Protokoll zusammen mit dem signierten Hashwert aus der Konkatenation von *K, r+1, idV, ch_data,* und α_T. Durch seine Signatur bestätigt U einmal, daß er *K* kennt und zum zweiten, daß er g^u als Startwert für die Schlüsselvereinbarung gewählt und zu *V* geschickt hat. Diese Signatur wird mit *K* verschlüsselt, um die Anonymität von U zu gewährleisten.

Nach Erhalt der dritten Nachricht entschlüsselt *V* mit *K* die verschlüsselten Teile und erfährt so die Identität *idU* von U und weiß, welchen öffentlichen Schlüssel er aus seiner Datenbank braucht, um die Signatur zu verifizieren.

6.3 Bezahlungs-Protokoll

Für das Bezahlungs-Protokoll wählt der Benutzer U zufällig einen Wert α_0 während der Ausführung des Authentifikations-Protokolls. Auf dieses α_0 wendet er *T*-mal eine Einwegfunktion *f* an und berechnet $\alpha_1=f(\alpha_0)$ bis $\alpha_T = f(\alpha_{T-1})$. Der Wert α_T ist der Startwert für das Bezahlungs-Protokoll und wird an den Mehrwert-Diensteanbieter V geschickt. Die Zahlung von einem Tick wird von U geleistet, indem U das Urbild α_{j-1} von α_j unter *f* an V schickt. V kann prüfen, daß $\alpha_j = f(\alpha_{j-1})$ gilt und unter der Voraussetzung, daß *f* eine Einwegfunktion ist, konnte nur U den Wert α_{j-1} kennen (j = 1, . . . T).



Wenn der Mehrwert-Diensteanbieter V eine Bezahlung vom Benutzer U anfordern will, schickt er einen Wert δ an U, der angibt, wieviel Ticks bezahlt werden sollen. Der Benutzer U kontrolliert diese Forderung und sendet den Wert α_j als Bezahlung, falls die Forderung korrekt ist. Wenn wir mit α_i den aktuellen Wert bezeichnen, der bei V bekannt ist, gilt $f^{\delta}(\alpha_j) = \alpha_i$.

7 Der Demonstrator

7.1 Konfiguration des Demonstrators

Der im Rahmen des ACTS-Projektes ASPeCT entwickelte Demonstrator zeigt die Einbettung eines Micropayment-Verfahrens als sicheres Bezahlungsverfahren für Mehrwert-Informationsdienste für mobile Benutzer. Der mobile Benutzer des Demonstrators hat ein leistungsfähiges Terminal in Form eines Laptops, der über ein GSM-Mobiltelefon eine Datenfunk-Verbindung mit dem Diensteanbieter bzw. mit dessen Server herstellen kann. Der GSM-Datenfunk ist dabei der Basisdienst, der vom Netzbetreiber zur Verfügung gestellt wird und der Mehrwert-Informationsdienst wird vom Server erbracht. In dem hier vorgestellten Demonstrator wählt sich der Benutzer in das Siemens Intranet ein, in dem der Server eingebunden ist. Wichtige Teile der Sicherheitsfunktionen auf Benutzerseite werden von einer persönlichen Chipkarte erbracht, worauf in Kapitel 8 näher eingegangen wird.

Der im Demonstrator verwendete Mehrwert-Informationsdienst ist ein WorldWideWeb-Dienst, auf dem Laptop des Benutzers läuft als Anwendungssoftware ein WWW-Browser, auf dem Server-Rechner des Diensteanbieters läuft ein WWW-Server.

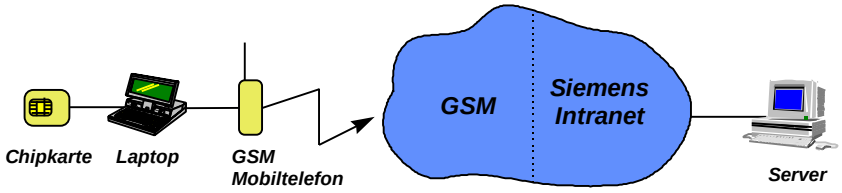


Abbildung 2: Konfiguration des Demonstrators

7.2 Einbindung des Bezahlungsverfahrens

Für die Einbindung eines Bezahlungsverfahrens in einen Mehrwert-Informationsdienst bieten sich zwei Optionen an, zum einen die Integration in die Applikationsprogramme und zum anderen die Realisierung in zusätzlichen Software-Komponenten, die an die Applikationsprogramme anzubinden sind. Für die erste Variante spricht die einfachere Kopplung an das Applikationsprotokoll, für die zweite Variante spricht eine gewisse Unabhängigkeit von den verwendeten Applikationsprogrammen. Für den hier beschriebenen

Demonstrator haben wir die zweite Variante gewählt, wobei die Anbindung des Bezahlungsverfahrens an das Applikationsprotokoll durch eine speziell hierfür entwickelte Zwischenschicht zwischen den Applikationsprogrammen und der Kommunikationsschicht realisiert wird:

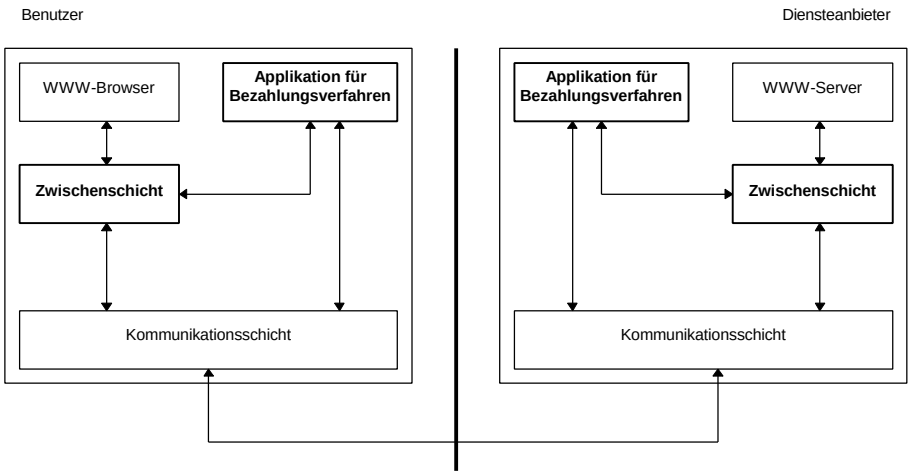


Abbildung 3: Architektur des Demonstrators

Die Anbindung des Bezahlungsverfahrens mit einer Zwischenschicht zwischen Applikationsprogrammen und der Kommunikationsschicht hat den Vorteil, daß Applikationsprogramme von beliebigen Herstellern verwendet werden können, solange sie die gleiche Kommunikationsschnittstelle verwenden. Für WWW-Applikationsprogramme ist dies gewährleistet, da sie stets auf Windows Sockets als Schnittstelle für TCP/IP-Kommunikation aufsetzen. Damit sind einfache Abrechnungsverfahren direkt möglich, flexiblere Abrechnungsverfahren lassen sich realisieren, indem in der Zwischenschicht das Applikationsprotokoll interpretiert wird, um Vorgänge auf Applikationsebene zu erkennen. Hervorzuheben wäre noch, daß das hier vorgestellte Konzept nicht nur unterschiedliche WWW-Applikationsprogramme ermöglicht, sondern prinzipiell auch für andere Mehrwert-Informationsdienste einsetzbar ist, sofern sie Windows Sockets als Schnittstelle zur Kommunikationsschicht verwenden.

7.3 Erweiterung durch eine Trusted Third Party

Ein großer Vorteil von public-key Kryptographie liegt darin, daß zwei

kommunizierende Parteien ein Vertrauensverhältnis aufbauen können, wenn sie eine gemeinsame Instanz haben, der sie beide vertrauen. Solche Instanzen werden als Trusted Third Parties (TTP) bezeichnet. Sie erstellen die Zertifikate, die in den verwendeten Protokollen eine wichtige Rolle spielen. Für den Fall, daß Benutzer und Diensteanbieter während der Kommunikation Bedarf nach aktualisierten Zertifikaten haben, kann eine online erreichbare TTP in das Protokoll einbezogen werden. Auch dieses erweiterte Protokoll ist in unserem Demonstrator realisiert. Ein Rechner, der die Rolle der TTP wahrnimmt, ist im Siemens Intranet verfügbar.

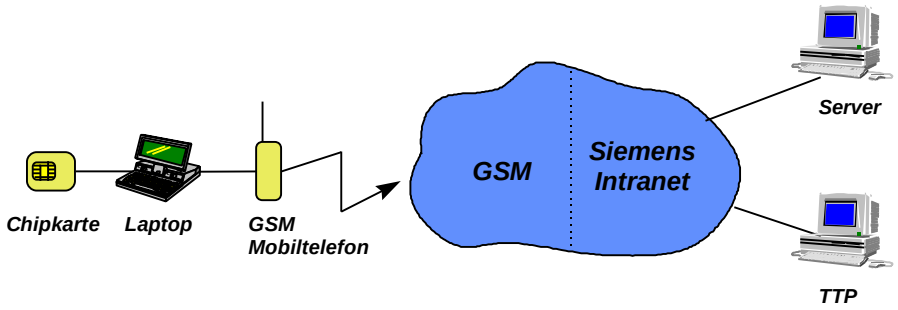


Abbildung 4: Konfiguration mit TTP

7.4 Geplanter Feldversuch

In Kooperation mit dem ACTS-Projekt EXODUS ist ein Feldversuch mit einem UMTS-Testnetzwerk geplant. UMTS wird geeignete Kommunikationsdienste für die Realisierung attraktiver mobiler Mehrwert-Informationsdienste bieten.

8 Der Einsatz von Chipkarten

Um eine hohe Sicherheit für die verwendeten Protokolle zu gewährleisten, werden Chipkarten für die zentralen Funktionen auf der Seite des mobilen Benutzers eingesetzt. Sämtliche Schritte des Authentifikations-Protokolls wie auch des Reinitialisierungs-Protokolls können auf Chipkarten ausgeführt werden. Prinzipiell gilt dies auch für das eigentliche Bezahlungs-Protokoll, jedoch ist hier der mögliche Verlust begrenzt und eine hohe Performanz auf der Chipkarte schwer zu erreichen, so daß dieses Protokoll eventuell besser in dem Terminal des Benutzers realisiert werden sollte. Schon heute haben die Benutzer von Mobilfunknetzen standardmäßig eine Chipkarte, deren Nutzung sich für weitere

Anwendungen geradezu anbietet.

Das hier verwendete Authentifikations-Protokoll ist für UMTS als Standard vorgeschlagen [ETS] und wurde im Rahmen des ASPeCT-Projektes bereits vollständig auf Chipkarte realisiert, jedoch wird diese Realisierung nicht in dem hier vorgestellten Demonstrator verwendet. Im Rahmen dieses Demonstrators wird die Chipkarte für die Kernfunktion der Authentifikation verwendet, nämlich für die Erstellung der Signatur mit dem persönlichen geheimen Schlüssel des mobilen Benutzers. Dadurch liegt dieser besonders sicherheitskritische Schlüssel niemals außerhalb der Chipkarte vor, wodurch die Möglichkeiten zum Betrug sogar mit einem manipulierten Terminal stark eingeschränkt sind.

Um eine ausreichende Performanz zu erreichen, werden im ASPeCT-Projekt Chipkarten verwendet, die zusätzlich zu dem Hauptprozessor noch einen speziellen Crypto-Coprozessor enthalten, beides integriert in dem Chip SLE44CR80S von Siemens. Darüber hinaus ermöglicht dieser Chip durch seinen großen Speicher (das EEPROM hat 8K) die Realisierung der Authentifikation mit den hier vorgestellten Protokollen und einer kompletten Anwendung für GSM-Dienste auf einem Chip, so daß mit einer Chipkarte im GSM-Netz telefoniert werden kann und sie auch für die Authentifikation in UMTS verwendbar ist. Die Speichergröße von Chipkarten - auch solchen mit Crypto-Coprozessor - wird in nächster Zukunft noch stark wachsen, so daß keine Speicherplatzprobleme zu erwarten sind.

9 Literatur

[CAFE] J.-P- Boly et.al., The ESPRIT project CAFE: "High Security Digital Payment Systems", ESORICS ‘94, LNCS 875, Springer Verlag, Berlin 1994, S. 217-238.

[Chen] L. Chen, H.-J. Hitz, G. Horn, K. Howker, V. Kessler, L. Knudsen, C. J. Mitchell, C. Radu: "The use of Trusted Third Parties and Secure Billing in UMTS", ACTS Mobile Telecommunications Summit, Granada, Nov 1996.

[ecas] ecash home page, http://www.digicash.com/ecash/ecash-home.html.

[ETS]ETSI SMG SG DOC 73/95. "A public-key based protocol for UMTS providing mutual authentication and key agreement", Sept 1995.

[Firs] First Virtual Holdings Inc., http://www.fv.com/.

[Gang] http://ganges.cs.tcd.ie/mepeirce/Project/oninternet.html.

[GeHa] E. Geulen, J. Harmer: "A Medium-Term Solution for Multimedia Using the OnTheMove Mobility Gateway", ACTS Mobile Telecommunications Summit, Granada, Nov 1996.

[iKP] R. Hauser, M. Steiner, M. Waidner: "Micro-payments based on iKP", Proc. Securicom Conference, Paris, 1996.

[Lamp] L. Lamport: "Password Authentication with insecure communication", Communications of the ACM, 24 (11), 770-771, Nov 1981.

[Netb] The Netbill electronic commerce project, http://www.ini.cmu/NETBILL/home.html.

[Netc] Anderson R et al: "NetCard - A practical electronic cash system". http://www.cl.cam.ac.uk:80/users/rja14/

[PayW] R.L.Rivest, A. Shamir: "PayWord and MicroMint: Two simple micropayment schemes", May 1996, available from the authors under {rivest, shamir}@theory.lcs.mit.edu.

[Pede] T. P. Pedersen: "Electronic payments of small amounts", DAIMI PB-495, Computer Science Department, Aarhus University, August 1995.

[Pete] H. Petersen: "Anonymes elektronisches Geld", Datenschutz und Datensicherheit 21 (1997) 7, 403-410.

[SET]Secure Electronic Transactions (SET). http://www.mastercard.com/set.

[UMTS] UMTS Forum: "A regulatory framework for UMTS", Report No. 1 from the UMTS Forum, June 1997.