Kommunikation mit persönlichen Mobilgeräten - Möglichkeiten und Absicherung

Holger Reif

SmartRing GmbH

Zusammenfassung Diese Arbeit betrachtet die verschiedenen heut am Markt befindlichen Technologie für die mobile Speicherung und Verarbeitung von persönlichen Informationen unter besonderer Berücksichtigung von Sicherheitsaspekten und des Mobilfunkstandards GSM.

1 Motivation

Information und Kommunikation sind bereits seit geraumer Zeit Schlagworte, die das sich verändernde Wesen unserer Gesellschaft charakterisieren. In zunehmendem Maße ist eine Verschmelzung der beiden zu beobachten. Hinzu kommt der sich verstärkende Aspekt der Mobilität, der an die Speicherung und Übermittlung der Kommunikation enorme Anforderungen stellt. Die vom ehemaligen Chef der Firma Microsoft, Bill Gates, gezeichnete Vision der "Information at your fingertips" wird mehr und mehr Realität.
Entsprechend wachsen die Sicherheitsanforderungen, da es sich oftmals um vertrauliche oder personenbezogene Daten handelt. Es muß die Gewißheit bestehen, daß nur der Eigentümer oder der berechtigte Empfänger diese Datensätze einsehen kann. Auch die Nutzung dieser Informationen in Form von digitalisierten Transaktionen schafft neue Forderungen. So muß der Absender einer übermittelten Entscheidung zweifelsfrei feststellbar sein und es darf keine Möglichkeit des Abstreitens bestehen.
Betrachtet man die Wichtigkeit des Zugriffs auf Informationen zu jedem Zeitpunkt und berücksichtigt man weiterhin die in jüngster Zeit immer häufigeren Dienstblockadeangriffe, offenbart sich eine weitere wichtige Forderung, nämlich die nach der Verfügbarkeit von Informationen. Dies soll allerdings nicht Gegenstand dieser Arbeit sein.
Im Kapitel 2 werden die am häufigsten anzutreffenden Gerätetypen mit ihren technischen Merkmalen vorgestellt. Das Kapitel 3 gibt einen Überblick über mögliche Kommunikationsmedien mit ihren Sicherheitseigenschaften im allgemeinen, während Kapitel 4 im besonderen die Entwicklung auf dem GSM-Sektor beleuchtet. Ein Ausblick schließt die Arbeit ab.

2 Geräteklassen

Dieses Kapitel bietet eine Möglichkeit der Klassifizierung von tragbaren, Informationen speichernden Geräten an. Diese will weder ausschließlich noch umfassend sein. Eine vollständige Auflistung ist angesichts der rasanten technischen Entwicklung nicht möglich und würde den Rahmen dieser Arbeit sprengen. Unter Berücksichtigung anderer Unterscheidungskriterien sind weitere Klassifikationen möglich.

2.1 Mobilfunkgeräte

Das Mobiltelefon, oder Handy, ist der Inbegriff der mobilen Gesellschaft mit Kommunikation zu jeder Zeit an jedem Ort schlechthin. Die Penetration steigt rasant und nähert sich in Deutschland der Marke von 50 Prozent. Die Ausstattung der Endgeräte wird immer reichhaltiger. Die aktuelle und verbreitete Technologie für die Funkstrecke ist GSM, siehe Kapitel 4. Darüber hinaus gibt es nach wie vor Geräte für weitere Funkdienste.

2.1.1 Funktionsumfang

Bereits die allerersten GSM Mobiltelefone erlaubten die Speicherung von rudimentären Kontaktinformationen in Form eines Telefonbuches. Dieses wird auf der SIM Karte abgelegt und ist somit sogar portabel, d.h. bei einem Wechsel des Telefons bleiben die Einträge erhalten. Die Zahl der Einträge wird durch die Speicherkapazität der SIM Karte beschränkt und bei deren Personalisierung durch den Netzbetreiber festgelegt. Üblich sind ca. 125 Einträge. Einige Modelle erlauben das nichtportable Ablegen von Telefonbucheinträgen auch im Speicher des Telefons, wobei hier die Beschränkungen recht großzügig sind. Darüber hinaus werden Funktionen wie mehrere Rufnummern pro Eintrag und Gruppenzuordnung angeboten. Neuere Modelle ermöglichen sogar die Verwaltung von Adreßinformationen.
Meist besitzen die Geräte eine Uhr mit Alarmfunktion. Eine darauf aufbauende, bei Geräten der gehobenen Klasse implementierte Funktion ist der Terminplaner. Bedingt durch die Displaygröße und das Fehlen einer alphanumerischen Tastatur kann er meist nur stark eingeschränkt benutzt werden. Eine Synchronisation ist nur mit speziellen PC-Programmen möglich.
Die für eine einseitige Informationsübertragung ausgelegten Pager (Telmi, Scall usw.) besitzen demgegenüber nur ein einzeiliges alphanumerisches oder ein kleines grafisches Display und wenige Tasten zur Interaktion. Lediglich einige Geräte für den professionellen Einsatz, z.B. zur Übermittlung von Börseninformationen, besitzen eine großzügige, vollgrafische Anzeige.
Betriebsfunkgeräte verfügen meist über keine geeignete Tastatur, aber oft über ein mehrzeiliges alphanumerisches Display. Damit können Nachrichten dargestellt und eventuell auch quittiert werden.

2.1.2 Anwendungen

Pager besitzen üblicherweise keine Möglichkeiten zum Ausführen von Anwendungen. Falls sie mehr als Anzeigen und ggf. Abspeichern von Textnachrichten beherrschen, sind die Anwendungen mit der Auslieferung des Gerätes vorgegeben.
Angaben zu GSM Geräten finden sich in Kapitel 4.
Betriebsfunkgeräte können keine Anwendungen ausführen.

2.2 PDA

Als Persönliche Digitale Assistenten (PDA) bezeichnet man eine ganze Reihe von unterschiedlichen Geräten. Die Abgrenzung zu anderen Geräteklassen wie Terminplaner oder (Sub)Notebook ist nicht klar definiert. Im allgemeinen werden jedoch alle Geräte verstanden, deren Größe ein Mitführen in der Jackentasche erlaubt, die mehrere Anwendungen mitbringen und weitere Anwendungen nachladen können. Eine grobe Unterteilung in die zwei Klassen mit/ohne Tastatur ist möglich.

2.2.1 Tastaturlose PDA (Stift-PDA)

Die bekanntesten Vertreter dieser Klasse dürften die Geräte der Firma Palm darstellen. Derzeit sind verschiedene Gerätefamilien mit unterschiedlichen Eigenschaften am Markt. Dazu kommen kompatible Nachbauten von Firmen wie TRG oder Handspring. Ebenfalls einen tastaturlosen PDA hat die Firma HP mit dem Journada im Programm.
Gemeinsam ist allen Geräten ein ein- oder mehrfarbiges, berührungsempfindliches Display, über das Eingaben mittels Stift möglich sind. Texte werden entweder mittels Schrifterkennung oder durch eine stilisierte Tastatur im Display eingegeben.
Das Betriebssystem ist auf kooperatives Arbeiten aller Anwendungen angewiesen, Speicherschutzkonzepte beispielsweise sind nicht implementiert. Als Betriebssystemroutinen vorgehaltene Sicherheitsfunktionen können jedoch einige Abhilfe schaffen. Applikationen werden über die serielle Schnittstelle nachgeladen.
Ausgestattet sind diese Geräte üblicherweise mit einem seriellen und oftmals mit einem Infrarot Anschluß. Der Palm VII enthält ein zuschaltbaren Sende- und Empfangsteil für einen speziellen Funkdienst, der in allen größeren Städten der USA angeboten wird. Die Palm-Nachbauten verfügen über einen Erweiterungssteckplatz für Zusatzmodule, der z.B. ein Modem aufnehmen kann. Weitere Module können über die serielle Schnittstelle angeschlossen werden.
Die Rechenleistung der Geräte ist, wohl auch im Interesse einer langen Batterielebensdauer, relativ eingeschränkt.

2.2.2 PDA mit Tastatur

Den Gegenpart zu den vorher genannten Palms bilden in dieser Klasse Geräte von Psion. Abgesehen vom Vorhandensein einer Tatstatur sind die übrigen Merkmale vergleichbar, weshalb hier auf eine weitergehende Erläuterung verzichtet wird.
Es sei erwähnt, daß für einige Stift-PDAs zusammenklappbare Tastaturen als Zusatzgeräte angeboten werden.

2.2.3 Anwendungen

Im Lieferumfang sind meist alle üblichen Büroanwendungen im Kleinformat enthalten, dazu zählen Kalender, Termin-, Adreß- und Dateiverwaltung, Editor, Tabellenkalkulation und oftmals noch ein Mini-Browser für Informationen. Dazu kommen Anwendungen speziell für den Mobileinsatz, wie Alarmfunktionen oder Weltzeit.
Darüber hinaus gibt es vielfältigste Software für verschiedene Verwendungszwecke, darunter auch Sicherheitsanwendungen wie Homebanking mit HBCI (Homebanking Computer Interface). Allerdings sind diese nicht sehr weit verbreitet.
Entwicklungsumgebungen oder Skriptunterstützung ermöglichen bei Bedarf die Erstellung von eigenen Anwendungen durch den Nutzer.

2.3 Chipkarte

Die Chipkarte wird hier mit aufgeführt, da sie zum einen selbst eine Art Kleinstrechner darstellt (unter Ausschluß der Speicherkarten) und zum anderen gerade im Bereich von Sicherheitsanwendungen eine wichtige Rolle spielt. Allerdings benötigt sie normalerweise ein Hostsystem und kann damit strenggenommen nicht als eigenständiges Gerät angesehen werden.
Chipkarten gelangen überwiegend in zwei Formaten im Einsatz, im Scheckkarten- und im Plug-in-Format (z.B. GSM Telefon). Kartenherstellern beziehen die Chips von einer Handvoll Halbleiterproduzenten. Sie erhalten das meist herstellereigene Betriebssystem und anwendungsspezifische Software. Danach erfolgt gewöhnlich eine Personalisierung entsprechend den Vorgaben des Anwenders.
Es existieren zwar Standards für multifunktionale Karten, das prominenteste Beispiel ist dabei die Geldkarte der deutschen Kreditwirtschaft, der tatsächliche Einsatz deckt aber im Regelfall nur eine Anwendung ab. Ein Nachladen von Anwendungen ist möglich, aber selten implementiert und erfordert einen hohen logistischen Aufwand zur Wahrung der Systemsicherheit und der Verhinderung von Angriffen. Das Anwendungsspektrum ist breit und reicht von der Zugangskontrolle über Bankinganwendungen (z.B. HBCI) bis zu Signaturanwendungen gemäß deutschem Signaturgesetz.
Die Leistungsfähigkeit von Chipkarten ist recht gering. Moderne Karten besitzen lediglich einen nichtflüchtigen Schreib-Lese-Speicher von maximal 64 kByte, die Verarbeitungsleistung der CPU ist recht gering (8-Bit-Prozessor bei einer Taktfrequenz von wenigen Megahertz). Die Kommunikation mit dem Hostsystem

erfolgt über eine serielles Interface, daß üblicherweise kontaktbehaftet und selten kontaktlos realisiert ist.

2.4 Zukünftige Entwicklungen

Es ist klar, daß unterwegs vor allem zwei Grundfunktionalitäten benötigt werden: Sprachkommunikation (Telefonieren) und Datenkommunikation auf der einen und Informationsspeicherung auf der anderen Seite. Beide Funktionen werden bislang durch unterschiedliche Geräte erbracht, deren Funktionsumfang sich immer mehr ausweitet. Betrachtet man die Geräteentwicklungen, lassen sich zwei gegensätzliche Trends beobachten: das multifunktionale (all-in-one) und das modulare Gerätekonzept.

2.4.1 Multifunktionale Geräte

Kennzeichen dieser Geräteklasse ist das Verschmelzen der Informations- und Kommunikationsfunktionen zu einer Einheit. Die Initiative für diese Entwicklung geht vor allem von Telefonherstellern aus.
Der wohl erste Vertreter war der Nokia Communicator. Er verband ein GSM-Telefon mit einem PDA. Der Sende- und Empfangsteil kann vom PDA genutzt werden, um beispielsweise Faxe oder Emails per IMAP über TCP/IP zu empfangen.
Eine echte Integration ist dabei jedoch nur teilweise gelungen. So werden zwei separate Telefonbücher verwaltet. Der liebevolle Beiname "Informationsbrikett" deutet auf das beträchtliche Gewicht, verbunden mit einem nicht optimalen Formfaktor hin, was zusammen mit dem recht hohen Preis und der geringen Verfügbarkeit einen echten Durchbruch verhinderte.
Der nächste Versuch zur Etablierung dieser Geräteklasse wird derzeit von Ericsson unternommen. Das R380s soll im Herbst 2000 verfügbar sein. Im Gegensatz zum Communicator verzichtet es auf Minitasten und benutzt statt dessen ein berührungsempfindliches Display. Der Clou dabei ist Nutzung eines Displays für Telefon- und Organizerfunktionen und die Realisierung der Telefontastatur über die Berührungssensoren des Displays.
Es ist abzuwarten, inwieweit das R380s sich auf dem Markt behaupten kann.
Aus Richtung traditioneller PDA-Anbieter sind bislang nur Ansätze zu erkennen. So integriert zwar der Palm VII ein Funkmodem, benötigt aber ein spezielles, nur in den Großstädten der USA verfügbares Funknetz. Unterstützung des europäischen GSM-Systems ist angekündigt, allerdings wird kein konkreter Realisierungszeitraum genannt.
Das Konzept des Pocket PC mit dem Betriebssystem WinCE 3 beinhaltet auch die Integration eines Mobiltelefons, die bislang verfügbaren Geräte beschränken sich jedoch auf Kabel- und Infrarotverbindungen.
Ein Grund für die zögerliche Umsetzung seitens der traditionellen PDA-Hersteller mag in der unterschiedlichen Batterielaufzeit liegen. Während ein ständig betriebsbereites Handy alle 2 oder 3 Tage nachgeladen werden muß, laufen die nur bedarfsweise eingeschalteten Organizer mehrere Wochen mit einem Batteriesatz.

2.4.2 Modulare Geräte

Derzeit propagiert vor allem die Firma Siemens den Ansatz von miteinander kommunizierenden, spezialisierten Einzweckgeräten. Mit der Kombination aus S/C35 als GSM-Telefon und IC35 als Organizer zeigt sie bereits ihre Vorstellungen. Die immer wieder problematische, weil unübersichtliche Verwaltung von Informationen im Handy (z.B. Telefonbuch) gelingt viel komfortabler auf dem größeren Display des Organizers, auch das Abrufen von WAP-Angeboten ist damit viel angenehmer. Zum Telefonieren dagegen braucht der Nutzer kein unförmiges Gerät, sondern nimmt das schlanke Handy. Der IC35 besitzt verschiedene Erweiterungsmöglichkeiten über den CompactMedia Slot sowie einen Einschub für Chipkarten, was seinen Einsatz für Sicherheitsanwendung interessant macht.
Ein wichtiger Nachteil ist die Kommunikation mittels Infrarot, was eine direkte Sichtverbindung zwischen beiden Geräten erfordert. Mit der Einführung von Bluetooth (siehe nächstes Kapitel) ist dort aber schon eine sehr wirksame Abhilfe in Sicht, die sicher dem modulare Gerätekonzept starke Impulse geben wird.

3 Kommunikationsmöglichkeiten

Dieses Kapitel beschreibt und vergleicht verschiedene technische Möglichkeiten, mit anderen Systemen zu kommunizieren. Dabei ist prinzipiell zwischen lokaler und nicht-lokaler Kommunikation zu unterscheiden. Kennzeichnend für die erstgenannte Gruppe ist die Überbrückung von kurzen Distanzen, meist wenige Meter. Direkt angeschlossen werden meist andere Mobilgeräte oder PCs, mitunter dient die Gegenstelle als Relais für nicht-lokale Kommunikation.

3.1 Kabel

Praktisch jedes tragbare Gerät ermöglicht den Anschluß per Kabel (bzw. im Falle der Chipkarte per Kontakt). Teilweise ist damit auch gleich ein Laden der Akkus verbunden. Besonders clever ist dabei die "Hot-Sync"-Lösung des PalmPilot, der nach Einstecken in die Ladestation sofort einen Datenabgleich vornimmt. Die Übertragung erfolgt meist serielle, übliche Datenraten liegen zwischen 9.6 kBit/s bis 115 kBit/s.
Die direkte Kommunikation per Kabel ermöglicht nur einen geringen Einsatzradius von wenigen Metern, ist aber sehr sicher. Ein Abhören oder Verändern der Daten während der Übertragung ist praktisch ausgeschlossen.

3.2 Infrarot

Der IrDA-Standard der Infrared Data Association definiert eine Punkt-zu-Punkt Verbindung und benutzt zur Übertragung infrarotes Licht . Die maximale Entfernung zwischen beiden Endpunkten beträgt einen Meter, und es muß eine Sichtverbindung bestehen. Sender und Empfänger müssen relativ exakt ausrichtet sein, der

Aussendewinkel beträgt 30°. Die Übertragungsgeschwindigkeiten können zwischen 9.6 kBit/s und 16 Mbit/s liegen.
Bereits heute sind über 150 Mio. Geräte mit einer IrDA-Schnittstelle ausgestattet, darunter Laptops, Handhelds und Mobiltelefone ab der Mittelklasse.
Die Datenübertragung erfolgt ungesichert, die direkte Ausrichtung schützt keinesfalls vor Ausspähen und Einspeisen von Daten mittels Spezialausrüstung. Eine Absicherung der Kommunikation muß unbedingt auf Anwendungsebene erfolgen.

3.3 Bluetooth

Der recht neue Standard wird durch führende Unternehmen im Bereich Kommunikation und Mobilgeräte entwickelt und lizenzfrei zur Nutzung angeboten. Er wurde in der vorliegenden Version 1.0 als Kabelersatz konzipiert. Im lizenzfreien 2.4 GHz Band wird eine Spread Spectrum Technik eingesetzt, die recht robust gegenüber Störungen ist. Die Reichweite beträgt bei Standardtransmittern 10 Meter, bei solchen mit erhöhter Sendeleistung und Empfangsempfindlichkeit 100 Meter. Eine direkte Sichtverbindung ist nicht erforderlich.
Bis zu 7 Geräte bilden ein Piconet, das sämtliche Kommunikation über den Master abwickelt. Mehrere Piconets können gleichzeitig ohne nennenswerte Beeinträchtigungen nebeneinander existieren. Jedes Gerät hat eine eindeutige Geräteadresse von 48 Bit. Die erzielbare maximale Nettodatenrate hängt von der Anzahl der Teilnehmer eines Piconets ab und beträgt ca. 700 kBit/s.
Die Übertragung zwischen den einzelnen Geräten kann verschlüsselt erfolgen. Die Schlüssel werden nach einer Authentifikation per PIN berechnet. Damit ist die Gefahr des Abhörens gering. Allerdings skaliert die PIN-basierte Schlüsselvereinbarung (peering) nicht, eine Verbindlichkeit allein über diesen Standard ist damit ebenfalls nicht realisierbar. Allerdings eröffnen sich interessante Möglichkeiten, wenn das Sicherheitsmodul mit dem Gerät, das die eigentliche Anwendung abarbeitet, mittels abgesicherter Bluetooth-Verbindung kommuniziert. Praktisch alle Mobilgerätehersteller haben bekundet, den Standard unterstützen und einsetzen zu wollen, was für eine rasche Verbreitung sorgen sollte.

3.4 DECT

DECT (Digital Enhanced Cordless Telecommunications) ist ein etablierter digitaler Funkstandard im Frequenzband um 1.9 GHz. Er ermöglicht eine Übertragungsrate pro Kanal von 24 kBit/s. Verwendung findet er vor allem im Bereich der schnurlosen Telefonie, am Markt werden aber auch Lösungen mit Kanalbündelung angeboten, insbesondere für den schnurlosen Zugang zu einer ISDN Basisstation. Die Reichweite beträgt 50 Meter in Gebäuden und bis 300 Meter im Freien.
Authentifikation der Endgeräte bei der Basisstation, eindeutige Geräteadressen und Verschlüsselung der Kanäle sind die Sicherheitsmerkmale einer DECT-Verbindung.
Von Mobilgeräteherstellern wird DECT bislang kaum unterstützt, es existieren einzelne Geräte, die sowohl GSM als auch DECT implementieren.

3.5 Mobilfunk

GSM ermöglicht heute standardmäßig verbindungsorientierte Verbindungen mit Datenraten von bis zu 9600 Bit/s. Durch Kanalbündelung per HSCSD (High Speed Circuit Switched Data) lassen sich derzeit Datenraten bis 38.4 Kbit/s, erweiterbar auf 56 kBit/s erzielen. Dieser Dienst wird in Deutschland noch nicht flächendeckend angeboten. GPRS (General Paket Radio Service) ermöglicht eine paketorientierte Übertragung mit bis zu 115 kBit/s. Allerdings werden Endgeräte erst zum Jahresende 2000 zur Verfügung stehen, eine flächendeckende Verfügbarkeit wird noch später.
Kurznachrichten (SMS, Short Message Service) übertragen 160 Textzeichen kodiert in 140 Byte. Die Übertragungsgeschwindigkeit liegt bei ca. 6 bis 10 Nachrichten pro Minute.
Die Bandbreite von Nicht-GSM-Netzen liegt ebenfalls meist bei 9.6 kBit/s. Erst UMTS (Universal Mobile Telephone Service) wird deutlich größere Bandbreiten zur Verfügung stellen, theoretisch bis 2 Mbit/s, praktisch zunächst bis ca. 384 kBit/s.

4 GSM-basierte Kommunikation

Insbesondere in Europa ist das von ETSI (European Telecommunications Standards Institute) entwickelte und von über 300 Netzbetreibern in mehr als 100 Ländern für 330 Mio. Kunden eingesetzte GSM (Global System for Mobile Communication) der Standard zur Mobilkommunikation. Dieses Kapitel soll deshalb einen tieferen Einblick in die Sicherheitskonzepte, die für Transaktionen zum Einsatz kommen können.

4.1 GSM Luftschnittstelle

Die Verbindung zwischen mobilem Endgerät und Basisstation bezeichnet man als Luftschnittstelle. Da Funkübertragung ein Rundsendemedium darstellt, sieht der Standard zur Authentifikation und zur Vermeidung des Abhörens von Gesprächen eine Verschlüsselung der Aussendungen vor. Dies betrifft sowohl den Daten- als auch den Signalisierungskanal. Das eingesetzte symmetrische Verschlüsselung wird als mittel bis stark wirksam eingeschätzt. Ab der Basisstation wird der Verkehr über VPNs der Netzwerkbetreiber geleitet.
Applikationen auf dieser Sicherheitsstufe können also davon ausgehen, daß vertrauliche Daten höchstens dem Netzbetreiber bekannt werden. Die Authentizität der Daten ist gering bis mittel, und hängt vor allem von der Vertrauenswürdigkeit des Netzbetreibers ab.
Typische Anwendungen benutzen den Kurznachrichtendienst SMS zur Übermittlung von Informationen wie Kontostände, Börsennachrichten, Staumeldungen etc. Echte Transaktionen sind üblicherweise nicht zu finden.

4.2 SIM Application Toolkit

Die SIM-Karte (Subscriber Identity Module) ermöglicht das Ausführen von meist menübasierten Applikationen. Die Anwendungen können dabei die Ein- und Ausgabekanäle des Telefons weitgehend verwenden, so können spezielle Kurznachrichten direkt empfangen oder gesendet werden. Die dazu nötigen Schnittstellen zwischen Chipkarte und Endgerät sind als SIM Applikation Toolkit (SAT) spezifiziert und seit etwa einem Jahr standardmäßig auf den Karten integriert.
Zur Manipulation der SIM-Karte durch den Betreiber nach deren Erstpersonalisierung und Auslieferung, dazu gehören Parameteränderungen oder das Laden von Applikationen, wurde zeitgleich mit SAT die OTA (Over The Air) Technologie eingeführt. Mittels einer entsprechenden OTA-Plattform kann der Operator auf die Karte so zugreifen, als befände sie sich in einem angeschlossenen Kartenleser. Kern von OTA ist eine Spezifikation zur abgesicherten Übertragung von Informationen unter Nutzung von Kurznachrichten als Träger.
Für Authentifikation und Verschlüsselung wird das sehr sichere symmetrische 3-DES-Verfahren eingesetzt. Die benötigten Schlüssel werden bei der Personalisierung auf der Karte abgelegt und vom Netzbetreiber verwaltet. Der Schutz der Nachrichten erstreckt sich also von Endgerät bis in die Rechenzentren des Netzbetreibers und ist unabhängig von Übertragungswegen. Dienstanbieter können die Sicherheit der Applikationen nicht allein kontrollieren, sondern sind auch hier auf den Netzbetreiber angewiesen.
Wegen des höheren logistischen Aufwands zur Schlüsselverwaltung haben sich bislang kaum Dienste etabliert, die auf SAT aufsetzen und gleichzeitig die Sicherheitsmerkmale zur Absicherung einsetzen. Die wenigen vorhandenen Beispiele werden fast ausschließlich durch den Netzbetreiber selbst angeboten.

4.3 WAP

Mit dem WAP-Standard (Wireless Application Protocol) versucht die Mobilkommunikationsindustrie mit derzeit noch mäßigem Erfolg, das starke Wachstum der Internetnutzung auf das Mobiltelefon zu übertragen. Spezielle codierte Seiten in der HTML-ähnlichen Sprache WML (Wireless Markup Language) werden über normale Datenverbindungen übertragen und mit einem in das Endgerät integrierten Browser dargestellt.
Mit WTLS (Wireless Transport Layer Security, inkompatibel zum im Internet gebräuchlichen TLS) definiert WAP einen Standard zur Absicherung auf Transportebene. Die Authentifikation und Schlüsselvereinbarung erfolgt mittels starken asymmetrischen Verfahren. Der Nachteil einer WTLS-Lösung ist der Verschlüsselungsendpunkt. Da WML-Seiten einer spezielle, platzsparende Binärkodierung in einem sog. WAP-Gateway unterworfen werden, endet der WTLS-Tunnel vor diesem Gateway. Falls der Dienstanbieter ein solches Gateway nicht selbst betreibt, ist der Netzbetreiber weiterhin in Teil der Vertrauenskette.
Ein Ausweg liegt in der Nutzung einer speziellen Funktion der WML Skriptsprache. Diese erlaubt das Signieren von Texten mit einem auf einem privaten Schlüssel. Der signierte Text wird vom Netzbetreiber nicht verändert. Somit kann zumindest der

Dienstanbieter eine nichtabstreitbare Signatur vom Kunden erhalten, der umgekehrte Weg, beispielsweise für Quittungen, ist derzeit noch nicht spezifiziert. Der private Schlüssel des Kunden befindet sich auf dem Sicherheitsmodul WIM (Wireless Identification Modul).
Mittels der beschriebenen Funktionen lassen sich auch Dienste mit höheren Sicherheitsanforderungen realisieren. Angedacht sind Gebiete wie Banking, Brokerage und andere m-Commerce-Anwendungen. Derzeit sind allerdings weder WIMs noch Endgeräte, die mit diesen Sicherheitsmodulen zusammenarbeiten können, am Markt erhältlich.

4.4 Andere Lösungen auf Anwendungsebene

Wegen der oben aufgezeigten, eher unbefriedigenden Situation und dem Wunsch, trotzdem sichere Dienstleistungen für mobile Endgeräte anzubieten, wurden verschiedene herstellerspezifische Entwicklungen unternommen, die sich grob in zwei Klassen unterteilen lassen.
Zum einen betrachten einige Anbieter das Mobiltelefon nur als Übertragungsmittel, womit eine Unabhängigkeit von der Sicherheit von GSM erzielt wird. Die eigentliche Anwendung wird auf einem PDA realisiert. Die Verbindung zum Handy als GSM-Modem erfolgt dann meist über Infrarot. Allerdings werden hierfür Geräte der gehobenen Klasse benötigt. Prominentes Beispiel für diesen Ansatz sind HBCI-konforme Bankinganwendungen. Bezüglich der Sicherheit solcher Anwendungen gilt das im Abschnitt zu PDAs Gesagte.
Der andere Weg besteht in der Erweiterung der Funktionalität der SIM-Karte um Public-Key-Algorithmen und deren Einbindung in SAT. Auf diese Weise können auch mit heute handelsüblichen Endgeräten Signaturen erzeugt werden, auf die der Serviceprovider Anwendungen aufsetzen kann. Im Einsatz ist diese Technik vor allem im Finanzbereich für Mobilbanking. Eine Variante dieses Ansatzes benutzt zusätzliche Steckplätze für separate Chipkarten (dual slot).
Beiden Ansätzen haftet der Makel der fehlenden Standardisierung an. Außerdem sind Lösungen verschiedener Anbieter möglicherweise nicht kompatibel. Dementsprechend ist die Unterstützung nur zögerlich, da keiner teuere Fehlinvestitionen tätigen will.

5 Ausblick

Zusammenfassend läßt sich feststellen, daß die heute verfügbaren Geräte und Technologien noch keine echte Benutzung von m-Commerce erlauben. Allenfalls der erste Schritt, die gezielte Informationsübermittlung, ist möglich. Transaktionen hingegen sind von einigen Risiken begleitet.
Eine echte Besserung ist vermutlich erst dann möglich, wenn es gelingt, dem Nutzer ein Gerät oder Sicherheitsmodul zur Verfügung zu stellen, das er universell einsetzen kann, ob mobil, im Internet oder für lokale Anwendungen. Dann wird auch der Nutzer bereit sein, wenigstens einen Teil der Kosten für eine entsprechende Infrastruktur zu

übernehmen. Allerdings findet sich derzeit auf dem Markt keine Lösung, die diese Ansprüche erfüllen könnte.