Kapitel 8

VPNs für E- und M-Business

Der große Vorteil von VPNs ist die Flexibilität in der Absicherung ganz unterschiedlicher Protokolle und Applikationen. Wegen der Sicherheitsfunktionen auf IP-Ebene brauchen sich Programmierer, Anbieter von Produkten und Dienstleistungen sowie Anwender keine Gedanken über die Sicherheit der Verbindung zu machen. Hacker haben beim Einsatz sicherer Verfahren mit genügend großen Schlüssellängen keine Chance.

8.1 Geschäftsabwicklung über Netzwerke

Öffentliche Netze, insbesondere das Internet, haben eine zentrale Bedeutung im Leben jedes Einzelnen gewonnen. Einkäufe, Reisebuchungen und andere finanzielle Transaktionen sind dabei im Zentrum des Interesses. Die Stichworte »E-Business« und »M-Business« stehen für die neue Flexibilität bei der Abwicklung von Geschäften. Der Begriff E-Business bezeichnet ganz allgemein die Abwicklung von geschäftlichen Transaktionen über öffentliche Netzwerke, M-Business bedeutet hingegen die Durchführung dieser Vorgänge über das Mobilfunknetz mittels Mobiltelefon oder Communicator (Abb. 8.1).

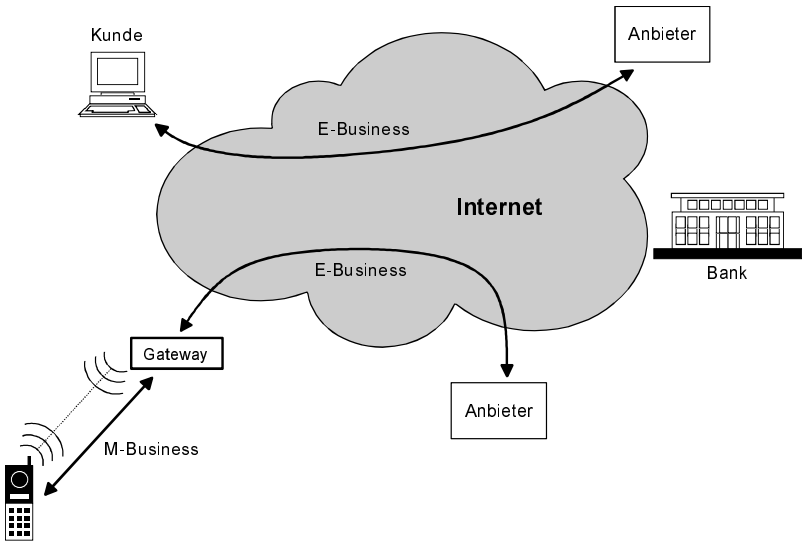

Abb. 8.1: E- und M-Business

Das Thema Sicherheit ist ein zentrales Element innerhalb der benötigten Infrastruktur. Authentikation, Verschlüsselung, digitale Signatur und die damit verbundene juristische Beweisbarkeit von Transaktionen sind Anforderungen, zu deren Erfüllung von technischer Seite her VPNs hervorragend geeignet sind.

- Im Bereich des E- und M-Commerce (elektronischer Handel) können VPNs die bei Angeboten, Bestellungen und finanziellen Transaktionen ausgetauschten Daten sichern.
- ASP (Application Service Provider) bieten komplette Rechenzentrums-Infrastrukturen inklusive der benötigten Software-Lizenzen an. Der Zugriff erfolgt über das Internet. Die zwischen Kunden und ASP ausgetauschten Daten können durch ein VPN gesichert werden.
- Der weitere Ausbau von B2B-Infrastrukturen (»Business to Business«), z. B. zwischen Zulieferern und Fertigungsbetrieben, verlagert sich auf öffentliche Netze mit Absicherung durch VPNs. Auch elektronische Marktplätze wie Auktionshäuser können durch temporäre VPNs abgesichert werden, die alle an der Geschäftsabwicklung beteiligten Gruppierungen verbinden.

Heutige Systeme zum E-Commerce arbeiten aus der Sicht des Endkunden nach einem recht starren Schema: Der Kunde verbindet sich über seinen Client mit einem Web-Server. Diese Verbindung wird über ein gesichertes Protokoll vor unberechtigten Zugriffen geschützt. Mit der Auswahl bestimmter Menüpunkte auf den Web-Seiten werden die Transaktionen initiiert. Praktisch die gesamte »Intelligenz« der Verarbeitung liegt auf der Server-Seite, eine VPN-Infrastruktur besteht nicht.

Mit der VPN-Technologie wäre im Internet eine Vereinheitlichung ungeahnten Ausmaßes möglich. Durch den großflächigen Einsatz von Protokollen wie IPSec auch bei Privatnutzern könnte eine Sicherheit bei der Kommunikation über das Internet erzielt werden, wie sie heute kaum vorstellbar erscheint.

Dabei wird auch mittelfristig die Abgrenzung von VPN-Strukturen und anderen Sicherheitsmechanismen durch das Verhältnis zwischen den Kommunikationspartnern definiert. Ein VPN kommt zum Einsatz, wenn mehrfache oder sogar permanente Kommunikation zwischen beiden den Aufbau und Betrieb einer VPN-Infrastruktur rechtfertigt. Bei gelegentlichen Zugriffen, die zudem mehr oder weniger anonym sind (z. B. Einkauf im Internet), lohnt sich der Aufwand für ein VPN hingegen nicht.

8.2 Risiken von E- und M-Business ohne VPN

8.2.1 Internet-Zugang über PC

Die meisten Benutzer wickeln ihre Online-Geschäfte mit einem herkömmlichen Web-Browser ab. Als Kommunikationsprotokoll dient dabei fast immer SSL. SSL unterstützt neben der Authentikation des Servers auch die des Clients. Das wird

aber nur in den seltensten Fällen (etwa durch SmartCards) realisiert, meist beweist nur der Server seine Identität. Damit sind Angriffe gegen SSL möglich, wenn der Angreifer sich in die Netzwerkverbindung des Kunden einklinken kann (»Man in the Middle«). Das soll am Beispiel eines lokalen Netzwerks beschrieben werden, von dem aus ein Benutzer Online-Banking durchführen möchte. Unter der Voraussetzung, dass sich der Angreifer im gleichen lokalen Netzwerk befindet, kann er folgendermaßen vorgehen:

- Falls sich ein Switch zwischen dem Hacker und dem Opfer befindet, wird der Rechner des Opfers mit einem gezielten Netzwerkpaket (»ARP-Spoofing«) dazu veranlasst, den Zugang ins Internet über den Rechner des Angreifers umzuleiten. Er sendet ab sofort alle Netzwerkpakete an den »Angreifer-PC«, dieser leitet sie ins Internet weiter.
- Um mit dem Browser auf den Server seiner Bank zugreifen, stellt der »Opfer-PC« eine DNS-Anfrage nach dessen IP-Adresse. Diese Anfrage passiert zunächst den Angreifer, der sie mit seiner eigenen IP-Adresse beantwortet (»DNS-Spoofing«). Ab jetzt werden Pakete an die Bank explizit an den Hacker gerichtet, der sie zunächst unverändert weiterleitet.
- Wird nun die SSL-Verbindung aufgebaut, präsentiert der Angreifer ein zuvor erzeugtes SSL-Serverzertifikat, das er selbst unterschrieben hat (»Root-Zertifikat«). Der Benutzer wird von seinem Browser aufgefordert, das Zertifikat zu akzeptieren. Tut er das, wird eine SSL-Verbindung zwischen dem Opfer und dem Hacker aufgebaut.
- Der Hacker baut dann eine zweite SSL-Verbindung mit der Bank auf. Ohne Client-Authentikation ist das ohne Schwierigkeiten möglich. Alle Daten der Verbindung können abgehört und nach Belieben manipuliert werden.

Ein zusätzliches Risiko sind die Schwächen des bei der SSL-Verschlüsselung hauptsächlich eingesetzten schwachen RC4-Algorithmus, der (zumindest in der Theorie) für Angreifer kein unüberwindbares Hindernis darstellt.

8.2.2 Kommunikation über Mobiltelefon

Mit der zunehmenden Mobilität in unserer Gesellschaft müssen auch immer mehr Geschäftsprozesse von unterwegs erledigt werden, z. B. über Mobiltelefone. Das Bezahlen von Waren über Tastenkombinationen auf dem Telefon ist längst keine Zukunftsmusik mehr. Allerdings sind in den heutigen Geräten meist keine ausreichend sicheren Algorithmen implementiert. Authentikation und Verschlüsselung sind zwar vorhanden, doch die proprietären Algorithmen A8 (Schlüsselaustausch), A5 (Verschlüsselung) und A3 (Authentikation) arbeiten mit dermaßen geringen Schlüssellängen, dass A5 »geknackt« ist und die anderen als stark gefährdet gelten (/Schmi02/). Erst UMTS bietet durch seine wesentlich größere Bandbreite und die Auswahl besserer Algorithmen eine passable Sicherheit.

Interessanterweise wird in der mobilen Telefonie einzig die Client-Authentikation über die SIM-Karte des Telefons genutzt, der Zugangspunkt braucht seine Identität nicht nachzuweisen. Angreifer können also eine eigene Sendestation in die Nähe des Opfers stellen, dessen Telefon sich dort einloggen lassen und die gesamte Kommunikation als »Man in the Middle« abhören und manipulieren.

Beim Versand von SMS-Nachrichten fehlt die Authentikation sogar ganz, so dass das Fälschen (»Spoofing«) von Nachrichten über allgemein zugängliche Seiten im Internet problemlos möglich ist. Das unbefugte Mitlesen von SMS-Nachrichten wird durch deren Zwischenspeicherung auf Servern des Netzwerkbetreibers erleichtert.

Sollen Mobiltelefone für sichere Kommunikation genutzt werden, muss deshalb auf proprietäre Lösungen ausgewichen werden. Einige Spezialhersteller bieten SIM-Karten an, bei denen auf Hardwareebene eine starke Verschlüsselung implementiert ist. Die Kommunikation zweier Mobiltelefone, die beide mit SIM-Karten desselben Anbieters bestückt sind, können dann eine End-to-End-Security aufbauen. Nur dann haben Angreifer bei Zugriffen auf die vertraulichen Nutzdaten keine Chance.

8.2.3 Internet-Zugang über Mobiltelefon

Eine mobile Alternative zum PC ist der Zugang ins Internet über das Mobiltelefon. Dabei ist nicht der Einsatz als Modem für einen Laptop gemeint, sondern der direkte Zugriff über das WAP-Protokoll. Wird das Telefon als Modem eingesetzt, gelten die Überlegungen für den Internet-Zugang für PCs.

Bei der in den meisten Mobiltelefonen implementierten WAP-Version 1.x wird zwischen dem Mobiltelefon und dem WAP-Gateway beim Mobilfunk-Betreiber die aus dem SSL-Standard abgeleitete Protokollschicht WTLS eingesetzt. Zur Kommunikation zwischen dem WAP-Gateway und dem eigentlichen WAP-Server mit der Applikation ist eine Konvertierung von WTLS in das IP-basierte SSL-Protokoll nötig. Hier entsteht eine temporäre Sicherheitslücke, da die Daten auf dem Gateway für einen gewissen Zeitraum unverschlüsselt vorliegen. Dazu kommen die bei WAP 1.x eingesetzten geringen Schlüssellängen von 40 Bit und weniger, die Angriffe wesentlich erleichtern.

Die Probleme der Konvertierung am Gateway und der geringen Schlüssellängen wurden in der WAP-Version 2.0 angegangen. Hier kommen bis zu 1 024 Bit zum Zuge, so dass die Sicherheit zumindest nicht geringer ist als bei der Arbeit mit dem PC.

8.2.4 Fazit

Im Gegensatz zur internen Kommunikation bei Firmen und Behörden werden im Verhältnis zwischen Endkunden und Anbietern die im Vergleich zu einem VPN weniger sicheren Client-Server-Protokolle WTLS und SSL eingesetzt. Es ist deshalb nötig, dass in der Zukunft mehr und mehr »Intelligenz« auf den Client des Endkunden verlagert wird, so dass auch hier die Mechanismen eines VPN zum Einsatz kommen können. Das setzt allerdings eine drastische Steigerung der Leistungsfähigkeit der Endgeräte voraus, kompakte Bauweise und lange Standby-Zeit sind dann nicht mehr die maßgeblichen Design-Kriterien. Im Mobilfunkbereich ist mit dem neuen Übertragungsstandard UMTS als Ersatz für GSM wegen der dann endlich passablen Bandbreite in einigen Jahren mit einem Boom im M-Commerce zu rechnen.

8.3 VPN-Systeme zum E-Commerce

An der Verarbeitung einer Transaktion sind im Normalfall mehrere Institutionen beteiligt. Der Anbieter einer kostenpflichtigen Leistung arbeitet mit einem Provider (beispielsweise einer Bank) zusammen, der in seinem Namen das Geld vom Kunden einzieht. Außerdem ist die Bank des Kunden am Geschäft beteiligt. Es ist sinnvoll, zwischen diesen Parteien ein oder mehrere Business-to-Business-VPNs (»B2B-VPNs«) einzurichten. Die Abbildungen 8.2 und 8.3 geben Implementierungs-Beispiele für einen SSL-Zugriff über das Internet und für einen WAP/WTLS-Zugriff mittels Mobiltelefon.

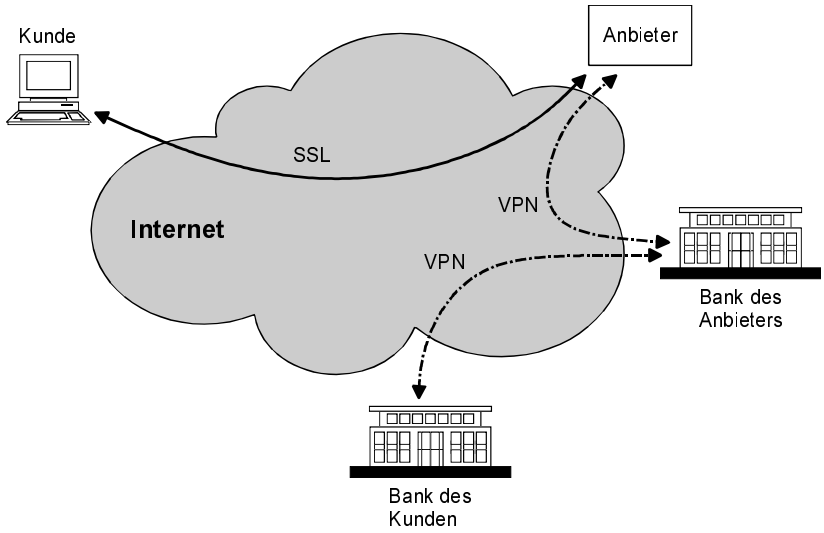

Abb. 8.2: SSL und VPN

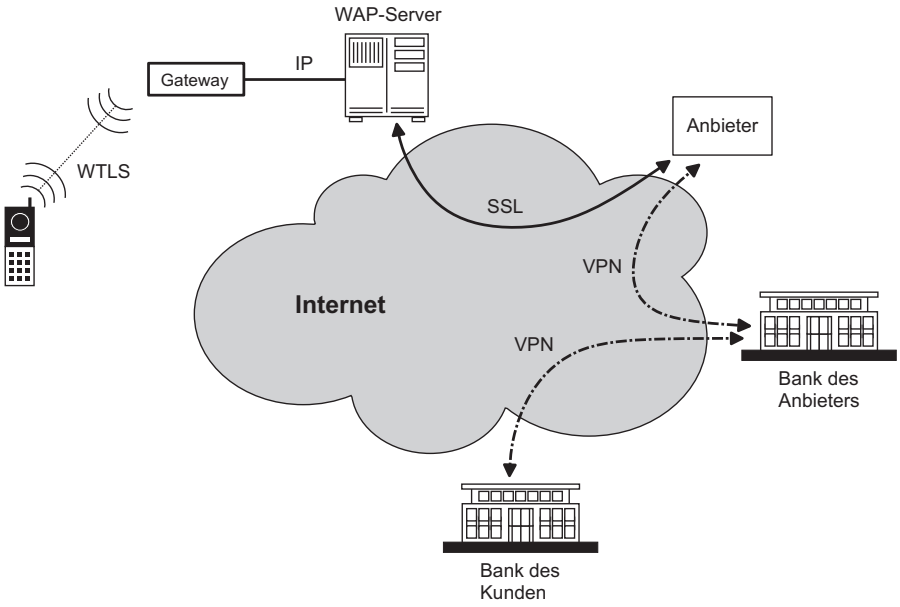

Abb. 8.3: WAP und VPN

8.4 Das »Jedermann-VPN«

Mit der zu erwartenden Verbreitung des E-Business auch für Endkunden muss immer mehr der beim Geschäftsvorgang benötigten »Intelligenz« auf den Client des Kunden verlagert werden. Angebote müssen beispielsweise automatisch recherchiert, mit den Wünschen des Interessenten verglichen und in einer Vorauswahl gegenübergestellt werden. Die dann benötigte Flexibilität im Umgang mit Zertifikaten, Internet-Protokollen und den dazugehörigen Anwendungen lässt eine Migration hin zu einem »echten« VPN erwarten, an dem der Endkunde über seinen Internet-Provider partizipiert. Die Kopplung der beteiligten Rechner zu einem VPN wäre dabei nur temporär und auf einen Geschäftsvorgang beschränkt. Auch Privatleute untereinander könnten für einen Datenaustausch auf die Online-Sicherungsmechanismen von VPNs setzen (Abb. 8.4).

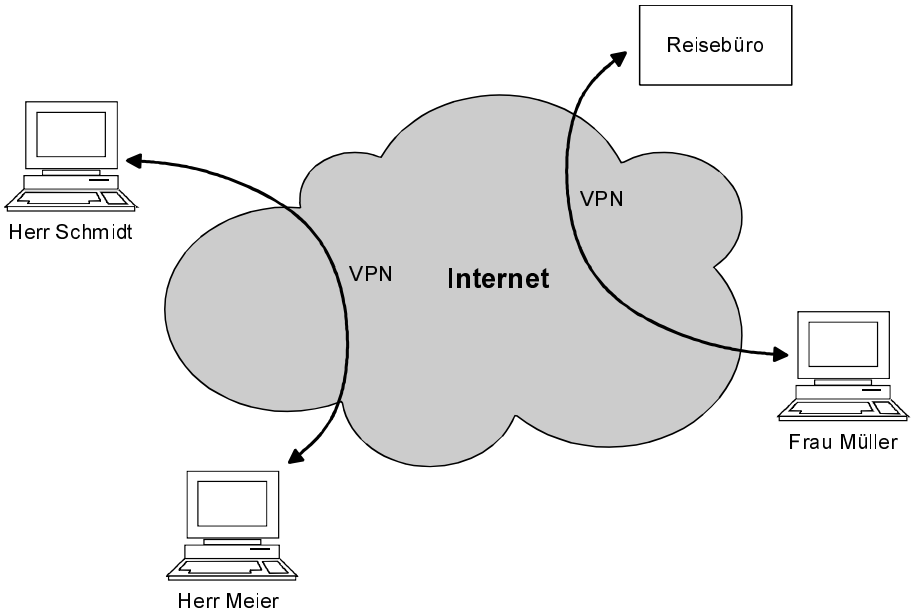

Abb. 8.4: Temporäre VPNs für den privaten Gebrauch

8.5 Protokolle im E- und M-Business

Da es noch auf absehbare Zeit eine Koexistenz zwischen WTLS, SSL und den allgemeineren VPNs geben wird, wird an dieser Stelle ein kurzer Überblick über die in diesem Buch bisher noch nicht behandelten Protokolle gegeben. Die Absicherung von öffentlichen Schlüsseln geschieht bei ihnen völlig identisch zu den bisher beschriebenen Mechanismen, so dass bei Bedarf dieselbe Infrastruktur aus CAs und RAs genutzt werden kann.

Ein immer wichtiger werdendes Protokoll im E-Business ist SET, mit dem ein bargeldloser Zahlungsverkehr über unsichere Netze implementiert werden kann. SET ist – im Gegensatz zu den innerhalb des Netzwerkstacks angesiedelten SSL und WTLS – innerhalb des Protokollstacks auf der Applikationsebene angesiedelt. Alle drei Protokolle liefern eine sichere Verbindung für ganz bestimmte Anwendungen. Sie kommen immer dann zum Einsatz, wenn ein »festes« VPN nicht erwünscht oder nicht praktikabel ist, wie zum Beispiel in einer losen Kunden-Händler-Relation. In einer Gesamtlösung, die auch den internen Netzwerkverkehr der Händler und der Banken mit seinem hohen Sicherheitsbedarf berücksichtigt, kommt es dann zu einer Koexistenz eines oder mehrerer VPNs mit den anderen Sicherheits-Protokollen.

8.5.1 Secure Socket Layer (SSL)

Das von Netscape entwickelte Protokoll SSL wird auch TLS (Transport Layer Security) bezeichnet. Es setzt auf der Transportschicht des Netzwerk-Stacks auf. Prinzipiell könnte es mit jedem Protokoll dieser Ebene kooperieren, doch in der Praxis sind nur Implementierungen für TCP bekannt.

SSL nimmt alle für Authentizität, Vertraulichkeit und Unversehrtheit der Daten benötigten Aufgaben wahr. Dazu verhandeln Client und Server über Algorithmen zur Datenkompression, Verschlüsselung und digitalen Signatur. Basis dieser »Vorverhandlungen« sind öffentliche Schlüssel des Servers und optional des Clients, die mithilfe von Zertifikaten von Zertifizierungsinstanzen (Certification Authorities, CAs) bestätigt werden. Wie bei VPNs werden langsame asymmetrische Private/Public-Key-Algorithmen mit symmetrischen Verfahren kombiniert.

Beschreibung des Verfahrens

SSL ist ein zustandsbehaftetes Protokoll. Mit ihm können zwischen zwei Rechnern ein oder mehrere Sitzungen aufgebaut werden, die ihrerseits jeweils eine oder mehrere Verbindungen enthalten können. Die Nutzdaten werden vor dem Senden fragmentiert, komprimiert, um eine digitale Signatur ergänzt und verschlüsselt. Der Empfänger kehrt die Reihenfolge der Operationen um und führt die Nutzdaten der nächsthöheren Ebene des Netzwerkstacks zu. Diese Aufgaben werden im SSL Record Layer wahrgenommen.

Zusätzlich zu diesem transparenten Teil setzen drei weitere Protokolle auf dem SSL Record Protocol auf, die aber nicht in höhere Schichten übermittelt werden (Abb. 8.5):

- Das *SSL Handshake Protocol* nimmt interne SSL-Kommunikations- und Verwaltungsaufgaben auf den beteiligten Rechnern wahr, wie etwa die (gegenseitige) Authentikation oder die Wahl des Verschlüsselungsverfahrens.
- Das *»change cipher spec«-Protokoll* teilt dem Partner den Wechsel in den zuvor ausgehandelten Verschlüsselungsalgorithmus mit. Vom Prinzip her hätte dieses Protokoll in die Familie des SSL Handshakes gehört, doch bestünde dann die Gefahr von Deadlocks.
- Das *Alert Protocol* schließlich wird im Fehlerfall aktiv.

Zum Austausch von Schlüsseln während des Handshakes stehen die Verfahren RSA, Diffie-Hellman und Fortezza zur Verfügung.

Die SSL-Kommunikation wird über reservierte TCP/IP-Ports abgewickelt:

- Port 443 lässt SSL-Verbindungen zu Webservern zu. Diese Art der Verbindung ist die einzige, die bisher in praktischen Implementierungen realisiert ist.
- Port 465 ist für SSL in Verbindung mit dem E-Mail-Protokoll SMTP reserviert.
- Port 563 schließlich ist für SSL in Verbindung mit Newsgroups reserviert.

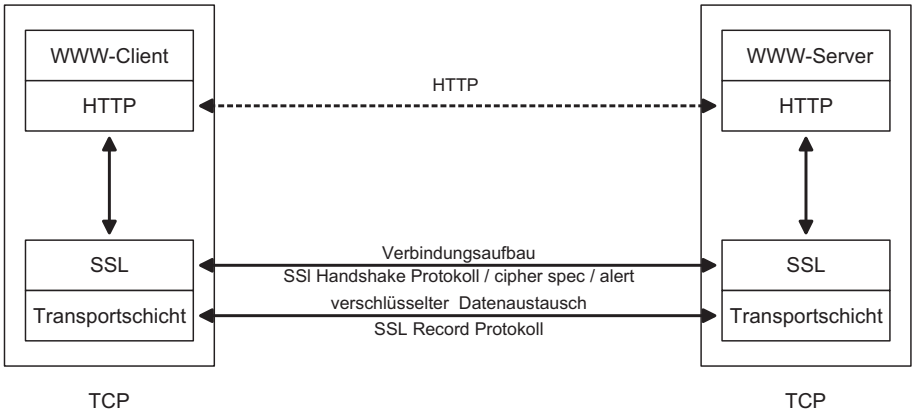

Abb. 8.5: Das Prinzip von SSL

Hier zeigt sich der Unterschied zwischen SSL und einer allgemeinen VPN-Definition: Ein VPN stellt eine für die verschiedenen Applikationen transparente Netzwerkverbindung zwischen beliebigen Netzwerkknoten her. Das sitzungsorientierte SSL ist hingegen nur für bestimmte Client-Server-Applikationen definiert, mit denen die wichtigsten Dienste im Internet abgedeckt werden.

Kryptographische Verfahren

In der aktuellen SSL-Version sind folgende Verfahren zur Verschlüsselung der Daten definiert:

- keine Verschlüsselung
- Stromverschlüsselung nach RC4 mit einer Schlüssellänge von 40 oder 128 Bit, mit allen Risiken und Nebenwirkungen
- Blockverschlüsselung mit CBC nach RC2 (40 oder 128 Bits), DES (40 oder 56 Bits), Triple-DES, IDEA und Fortezza

Für die digitale Signatur stehen folgende Optionen zur Verfügung:

- keine Signatur
- MD5
- SHA-1

Bewertung der Sicherheit

Wird nicht gerade RC4 genutzt, kann SSL als kryptographisch ausreichend abgesichert betrachtet werden. Die Kombination Triple-DES und SHA-1 entspricht dem Stand der Technik, AES wird in kommende Versionen einfließen. Leider handeln Client und Server die eingesetzten Protokolle ohne Einflussmöglichkeit durch den Benutzer aus, so dass RC4 in der Regel nicht vermieden werden kann. Vorsicht ist also geboten.

8.5.2 Wireless Application Protocol (WAP)

Der WAP-Standard wurde vom WAP-Forum für die langsamen Übertragungsraten von Mobiltelefonen definiert. Er stellt einen kompletten Netzwerk-Stack für diese Geräte zur Verfügung. Im Folgenden wird zunächst die heute übliche Version 1 beschrieben, die Neuerungen von WAP 2.0 folgen im Anschluss.

Beschreibung des Verfahrens

Auf der untersten Ebene wird die Verbindung durch den jeweiligen Träger – zum Beispiel GSM – gebildet. Darüber befindet sich die Transportschicht »Wireless Datagram Protocol« (WDP), die eine dem IP-Protokoll analoge Transportfunktion hat. Sie trennt die physikalische Übertragung von der darüber liegenden Sicherungsschicht »Wireless Transport Layer Security« (WTLS). WTLS weist eine große Ähnlichkeit mit SSL auf, im Unterschied zu SSL ist aber zusätzlich eine gesicherte Kommunikation zwischen zwei Clients möglich. Damit können beispielsweise zwei Mobiltelefone Visitenkarten austauschen.

Da das WAP-Protokoll primär für den Client-Server-Einsatz im Internet konzipiert wurde, haben sich die Entwickler für die Integration einer Transaktions-Ebene entschieden (»Wireless Transaction Protocol«, WTP). Damit wurde einer der Hauptnachteile von gewöhnlichen Internet-Verbindungen, das zustandslose HTTP-Protokoll und die damit nur schwer realisierbaren Transaktionen, von vornherein vermieden. Da nicht alle WAP-Zugriffe Transaktionen sind, bietet WTP drei unterschiedliche Dienste an:

- eine nicht abgesicherte Einweg-Anfrage (One Way Request)
- eine abgesicherte Einweg-Anfrage
- eine abgesicherte Zweiwege-Transaktion mit Request und Reply

Alle denkbaren WAP-Zugriffe müssen sich in Abfolgen dieser drei Transaktionen zerlegen lassen.

Der TCP- bzw. UDP-Ebene im IP-Stack entspricht das »Wireless Session Protocol« (WSP), bei dem zwei unterschiedliche Dienste definiert sind:

- Der verbindungsorientierte Dienst nutzt das Transaktions-Protokoll WTP und die darunter liegenden Schichten.
- Der verbindungslose Dienst hingegen greift direkt auf das Datagramm-Protokoll WDP zu.

Als Applikationsebene unter WAP wurde das »Wireless Application Environment« (WAE) definiert, das im Wesentlichen aus der an HTML angelehnten Sprache »Wireless Markup Language« (WML), einem JavaScript-Derivat namens »WMLScript« sowie Telefon-, Kalender- und anderen kleinen Anwendungen besteht.

Abbildung 8.6 verdeutlicht die WAP-Architektur grafisch. Abbildung 8.7 zeigt, wie deren Elemente in der Praxis unterschiedlich zu Netzwerk-Stacks kombiniert werden können. Die Grafik links zeigt, wie ein Benutzer über die Handy-Oberfläche Transaktionen ausführt. In den beiden anderen Grafiken kommunizieren Anwendungen direkt miteinander.

Abbildung 8.7 zeigt auch, dass die höheren Schichten von WAP alternativ über UDP/IP miteinander kommunizieren können. Hier könnte ein Ansatz zu einer Integration der beiden Stacks zu einer dann universell einsetzbaren VPN-Realisierung liegen.

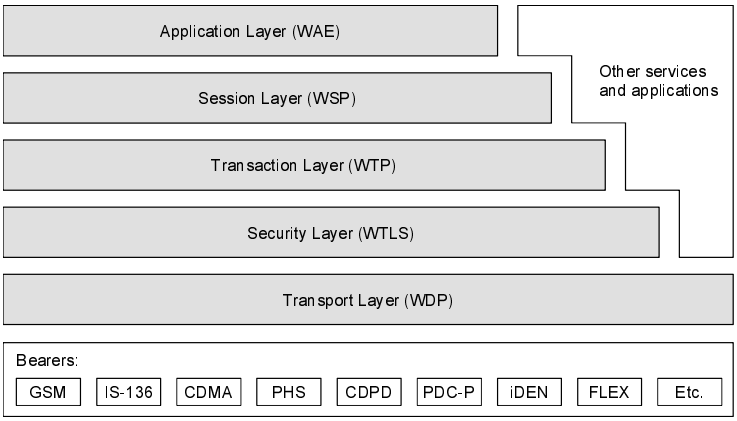

Abb. 8.6: WAP-Architektur

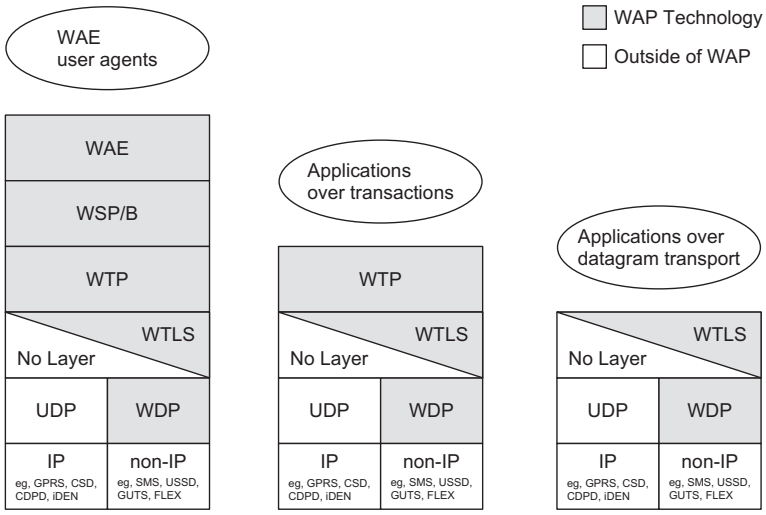

Abb. 8.7: WAP-Stacks

Kryptographische Verfahren

Die kryptographisch abgesicherte Ebene des WAP-Stacks (WTLS) wurde aus SSL abgeleitet. Die in diesem Kapitel beschriebenen Verfahren von SSL kommen im Wesentlichen auch unter WAP zum Einsatz, allerdings in extrem »abgespeckten« Versionen:

- Die Berechnung von Initialisierungs-Vektoren für die Verschlüsselung geschieht nach einem linearen Verfahren, so dass die Vektoren vorhersehbar sind.
- Die DES-Schlüssellänge von 35 Bit ist absolut unzureichend.
- Einer der für die Berechnung von MAC-Hashwerts vorgesehenen Algorithmen führt ein primitives 40 Bit-XOR durch.
- Gegen die gemäß dem Standard PKCS#1 implementierten RSA-Verfahren zur Verschlüsselung und digitalen Signatur hat Daniel Bleichenbacher einen Angriff entwickelt. Aus einer großen Zahl von gesendeten Nachrichten und der Reaktion des Opfers (PKCS#1-kombatibel oder nicht) kann eine Analyse begonnen werden, die deutlich schneller als Brute-Force zum gewünschten Ergebnis führt.
- Die beim Schlüsselaustausch über Diffie-Hellman benutzten Primzahlen haben nur eine Länge von 512 oder 768 Bit.

Bewertung der Sicherheit

WAP 1.x mit WTLS muss aus heutiger Sicht als völlig unzureichend für den Einsatz im M-Business angesehen werden. Wegen der Notwendigkeit der Konvertierung von WTLS in SSL am WAP-Gateway des Providers ist eine End-to-End-Verschlüsselung nicht möglich. Die geringen Schlüssellängen tun ihr Übriges.

Verbesserungen in WAP 2.0

Der Netzwerkstack von WAP 2.0 unterscheidet sich komplett von dem seiner Vorgänger-Versionen. WTLS als Sicherungsschicht wurde komplett gestrichen und durch das herkömmliche SSL (TLS) ersetzt, das seinerseits auf TCP/IP aufsetzt. Die WAP-Gateways wurden durch WAP-Proxies ersetzt, die ein Routing der Pakete unterhalb der SSL-Schicht vornehmen, ohne die verschlüsselten Nutzdaten anzutasten. Damit ist nun auch eine End-to-End-Sicherheit möglich.

Weniger spektakulär sind die eingesetzten Verfahren: RSA mit (nur) 1 024 Bit Schlüssellänge ist im Gespräch, ebenso wie Algorithmen auf Basis von Ellipsen (ECC). Käufer von Geräten sollten sich nicht mit RSA abspeisen lassen, sondern auf dem bisher als “starkes Verfahren” geltenden ECC bestehen.

8.5.3 Secure Electronic Transaction (SET)

Der SET-Standard (Secure Electronic Transaction) soll einen bargeldlosen Zahlungsverkehr über unsichere Netze ermöglichen. Das Verfahren wurde von IBM in Zusammenarbeit mit einigen Kreditkartenfirmen entwickelt. Die bei SET ausgetauschten Protokolle basieren, wie auch bei VPNs, auf der Kombination von symmetrischen und asymmetrischen Verschlüsselungsverfahren, wobei zur Absicherung der öffentlichen Schlüssel Gebrauch von X.509-Zertifikaten gemacht wird.

Bei SET sind fünf Partner involviert:

- Der Kunde, in der Regel der Besitzer einer Kreditkarte, kauft Waren oder Dienstleistungen über das Netz ein.
- Der Händler ist der Gegenpart des Kunden während der Abwicklung des Geschäfts.
- Das Geldinstitut des Kunden berechtigt den Kunden zum Zahlungsverkehr über SET und garantiert die Auszahlung von rechtmäßig angeforderten Beträgen.
- Das Geldinstitut des Händlers nimmt dessen Anforderungen nach Bezahlung an und zieht die entsprechenden Beträge vom Geldinstitut des Kunden ein.
- Das »Payment Gateway« ist ein von Geldinstitut des Händlers oder einer Drittfirma betriebener Rechner mit besonderen Funktionen.

Die Ziele von SET sind die Authentikation des Kunden, des Händlers und seines Geldinstituts sowie die Vertraulichkeit und Unversehrtheit der während des Zahlungsvorgangs ausgetauschten Daten.

Beschreibung des Verfahrens

SET definiert eine Reihe von Transaktionen, die jeweils aus einer ganzen Serie ausgetauschter Protokolle bestehen. Bei einer Transaktion gibt es immer nur zwei Partner, womit sich die Kommunikation der insgesamt fünf beteiligten Seiten in ihrer Komplexität stark reduziert. Folgende Transaktionen sind definiert (Abb. 8.8):

- Die **Registrierung des Kunden** umfasst seine Anmeldung bei einer CA, wobei ihm ein Zertifikat für seinen öffentlichen Schlüssel zur Verfügung gestellt wird.
- Die **Registrierung des Händlers** dient zu seiner Anmeldung bei einer CA, wobei ihm zwei Zertifikate zur Verfügung gestellt werden. Diese sichern seine beiden öffentlichen Schlüssel ab, die zum Schlüsselaustausch beziehungsweise zu seiner digitalen Unterschrift dienen. Neben dem Händler besitzen auch CA und Payment Gateway zwei Schlüsselpaare, der Kunde hingegen nur eins.
- Die **Kaufanforderung** dient zur Bestätigung der Kaufabsicht des Kunden an den Händler.
- Bei der anschließenden **Autorisierung der Zahlung** überprüft der Händler durch Anfrage an das Payment Gateway die Kreditwürdigkeit des Kunden. Bei positivem Bescheid kann er die Waren zum Kunden senden.

- Mit der **Anforderung zum Geldeinzug** setzt der Händler nach Auslieferung der Ware den Mechanismus der Geldüberweisung in Gang. Damit ist aus der Sicht von SET der Vorgang abgeschlossen.

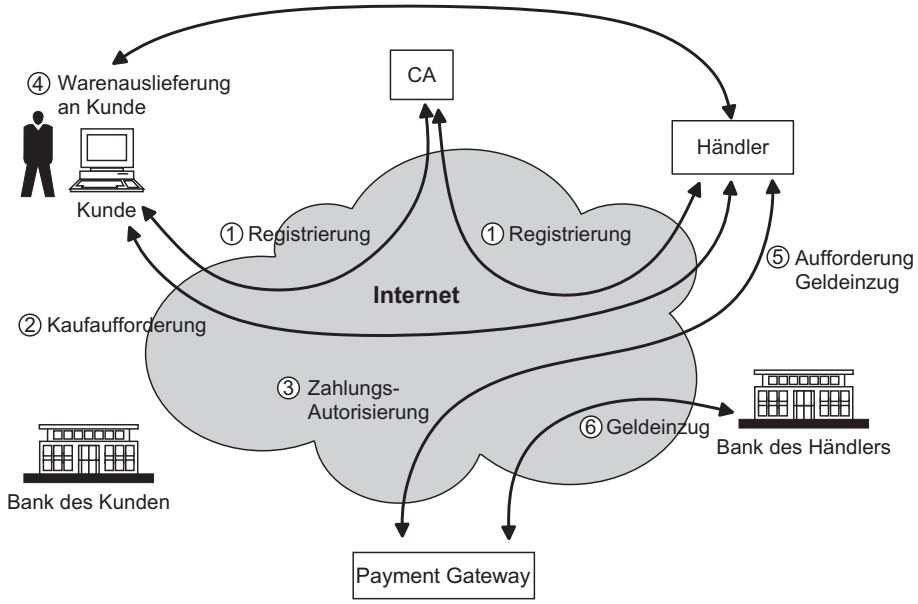

Abb. 8.8: Secure Electronic Transaction (SET)

Kryptographische Verfahren

SET lässt den Programmierern von Applikationen keine Freiheitsgrade in der Auswahl und Ausgestaltung der kryptographischen Algorithmen:

- Bei allen Operationen mit öffentlichen/privaten Schlüsseln wird RSA eingesetzt, meist mit einer Schlüssellänge von nur 1 024 Bit. Einzig bei den Root-CAs, der letzten Instanz in der Kette der Vertrauensverhältnisse der CAs untereinander, wird eine Schlüssellänge von 2 048 Bit eingesetzt.
- Die symmetrische Verschlüsselung wird mittels normalen DES (56 Bit Schlüssellänge) im CBC-Mode geleistet.
- Alle Hash-Werte werden mit SHA-1 gebildet.

Bewertung der Sicherheit

Die bis auf den SHA-1-Hash unzureichenden Schlüssellängen und Verfahren der Version 1 werden im Standard SET 2 optional erweitert. Triple-DES und AES (beide symmetrisch) sowie ECC im Bereich der asymmetrischen Verfahren schaffen dann eine akzeptable Sicherheit.