Sicherheit im WAP-Banking

keyon

Technische Lösung mit Live-Demonstration

Martin Christinat, keyon
christinat@keyon.ch
www.keyon.ch

Martin Christinat
Dipl. El.-Ing. HTL

Martin Christinat ist Gründungsmitglied von keyon und als Chief Technology Officer verantwortlich für die Produkte und Entwicklungen im Bereich WAP-Sicherheit.

WAP-Mobilgeräte

keyon

- Persönliches Gerät
- Keine Gefahr von Viren
- Nicht alle WAP-Handys unterstützen sichere Verbindungen
- Begrenzte Ressourcen
- Übertragungsgeschwindigkeiten für Daten vergleichsweise gering
- Gerätefähigkeiten sehr unterschiedlich

WAP Mobilgeräte sind sehr persönliche Geräte und daher bestens geeignet für sicherheitskritische Anwendungen wie mobile Banking. Im Gegensatz zu PCs, besteht in den meisten Fällen keine Gefahr von Hackern und Viren, da keine zusätzliche Software geladen werden kann.

Sicherheit ist im WAP Standard nur als optionale Eigenschaft vorgesehen. Das bedeutet, dass nicht jedes WAP Mobilgerät für mobiles Banking eingesetzt werden kann. Auch die Stärke und Art der Verschlüsselung ist flexibel definiert, was die Auswahl der verwendbaren Geräte zur Zeit ebenfalls noch einschränkt.

Die begrenzten Ressourcen der Mobilgeräte, allen voran die geringe Displaygrösse und Auflösung, erfordern eine entsprechend angepasste Datenaufbereitung. Die Informationen müssen auf das Notwendigste beschränkt werden und so benutzerfreundlich wie möglich dargestellt werden. Multimediale Applikationen sind nicht möglich.

Zur Zeit beträgt die Übertragungsgeschwindigkeit 9600 Bits pro Sekunde. Mit einem analogen Modem ist für den Internetzugang heute die fünffache Übertragungsgeschwindigkeit üblich. Die geringe Datenrate stellt meisten jedoch kein Problem dar, da bedingt durch die geringe Grösse der Anzeige auch dementsprechend weniger Daten übertragen werden müssen. Das WAP Protokoll wurde explizit entwickelt, um auch bei geringen Übertragungsgeschwindigkeiten eine akzeptable Performance zu erzielen. Die nächste Generation von Mobilfunknetzen und Entwicklungen wie GPRS werden die Übertragungsgeschwindigkeit drastisch erhöhen.

Die verfügbaren und geplanten WAP-Geräte bieten eine zum Teil sehr unterschiedliche Unterstützung für die Beschreibungssprache WML, die für die Darstellung der Inhalte eingesetzt wird. So gibt es z.B. nur wenige Geräte, die Tabellen darstellen können. Ein weiteres Problem stellen die unterschiedlichen Bildschirmgrössen und Formate dar. Idealerweise muss die Darstellung für jedes Mobilgerät spezifisch generiert werden, was technisch durchaus kein unlösbares Problem darstellt.

WAP-Sicherheit

keyon

- WAP-Standard sieht WTLS (Wireless Transport Layer Security) als optionales Sicherheitsprotokoll vor
- WTLS bietet
  - Authentisierung
  - Verschlüsselung (128 Bit)
  - Integritätsschutz
- Nicht an Mobilfunkprovider gebunden
- Keine neue SIM-Karte notwendig

Als Sicherheitsprotokoll wurde im WAP Standard WTLS (Wireless Transport Layer Security) spezifiziert.

Dieses speziell für WAP entwickelte Protokoll bietet eine gleichwertige Sicherheit wie das für Internet-Banking verwendete Sicherheitsprotokoll SSL (Secure Socket Layer).

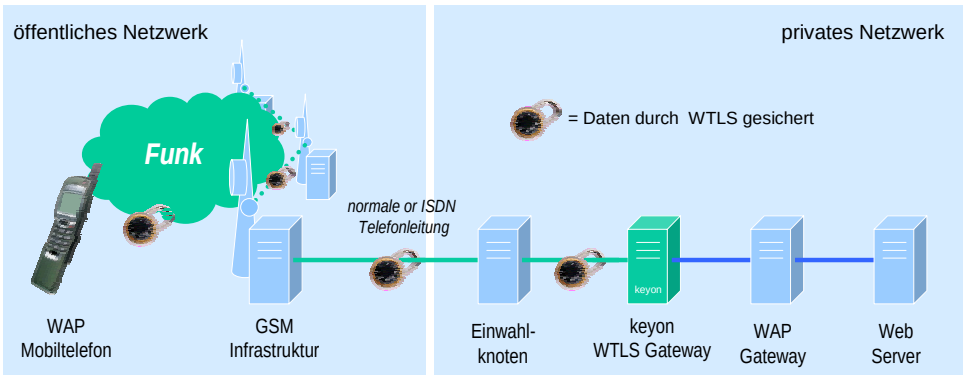
Die Aufgaben des WTLS Protokolls sind wie folgt:

- Die Gegenstelle wird über ein digitales Zertifikat authentisiert. Damit wird sichergestellt, dass man tatsächlich mit der korrekten Gegenstelle, d.h. der Bank verbunden ist.
- Alle übermittelten Daten werden verschlüsselt. Wie im Internet werden auch in WTLS beim Banking 128 Bit lange Schlüssel eingesetzt, ein Mitlesen ist für Dritte unmöglich.
- Die Integrität aller übermittelten Daten wird sichergestellt. Die übermittelten Daten können nicht manipuliert werden.

Als offene Lösung ist WTLS nicht an einen Mobilfunkprovider gebunden, eine spezielle SIM-Karte ist nicht notwendig. (SIM steht für Subscriber Identification Module und bezeichnet diejenige Chipkarte, welche für den Betrieb des Mobilfunkgeräts vorausgesetzt wird.)

WAP-Infrastruktur

keyon



Die Grafik stellt vereinfacht die beteiligten Systeme und den Datenfluss beim mobile Banking über WAP dar.

WAP benötigt einen WAP-Gateway, um über das WAP-Protokoll auf einen normalen Web-Server zugreifen zu können. Falls das WTLS Protokoll eingesetzt wird, so werden die Daten nur zwischen WAP-Mobilgerät und WAP-Gateway verschlüsselt. Das bedeutet, dass am Standort des WAP-Gateways auf alle gesichert übermittelten Daten zugegriffen werden kann. Daher muss eine Bank, die sicheres mobile Banking anbieten will, selber einen sicheren WAP-Gateway betreiben. Das bedeutet auch, dass sich der Kunde für mobile Banking direkt in die Bank einwählen muss.

Live-Demonstration

keyon

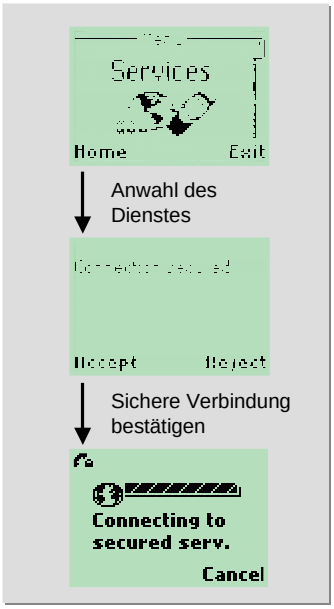
- Die gesamte WAP-Infrastruktur läuft für die Demonstration auf einem Notebook
- Als WAP-Handy wird ein Nokia 7110 simuliert
- Es wird nur eine einfache Beispielanwendung gezeigt
- Sicht des Benutzers

Zweck der Demonstration ist es zu zeigen, wie sicheres WAP Banking funktionieren kann und wie der Benutzer die Sicherheit wahrnimmt.

Der Nokia 7110-Simulator ist im Verhalten wie auch in der Anzeige identisch zu den aktuell verkauften Nokia 7110 Geräten. Mobilgeräte anderer Hersteller können von dem hier gezeigten Gerät stark abweichen, gerade was z.B. die Sicherheitsanzeigen betreffen.

Anwahl

keyon



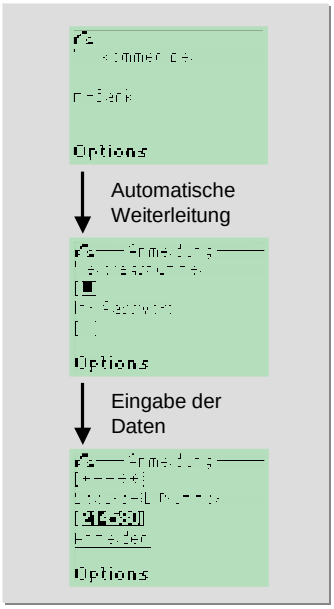
- WAP-Dienst auswählen
- Anwahl auf Telefonnummer der Bank
- Bestätigen der sicheren Verbindung
- Visuelles Feedback beim Bestehen der sicheren Verbindung

Um eine sichere Verbindung zur Bank aufzubauen, muss die Einwahlnummer der Bank angewählt werden. Der WAP-Gateway des Providers (Swisscom, diAx, Orange) kann nicht für mobile Banking verwendet werden.

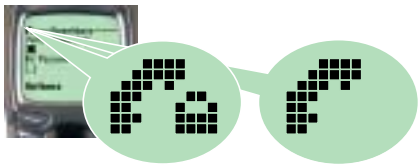
Das Nokia 7110 gibt entsprechende Meldungen aus, sobald eine sichere Verbindung besteht.

Anmelden

keyon



- Visuelles Feedback bei sicherer Verbindung



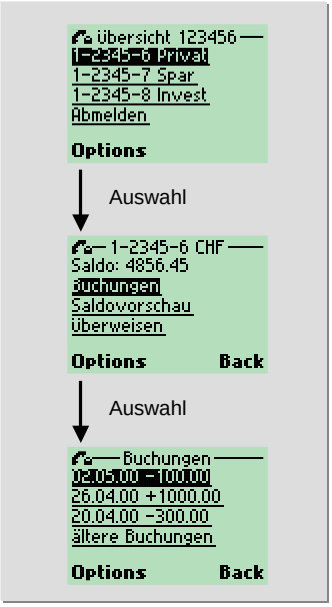
- Gleiche Anmeldedaten wie für Internet-Banking können verwendet werden

Ist die Einwahl erfolgreich, so besteht nun eine sichere Verbindung zur Bank, und der Benutzer kann seine Identifizierung eingeben. Das Nokia 7110 stellt in der linken oberen Ecke ein kleines Icon dar, wenn eine sichere Verbindung besteht. Der Benutzer kann somit sicher sein, dass die übermittelten Daten verschlüsselt sind und nur von der Bank wieder entschlüsselt werden können.

Zu den Anmeldedaten gehören üblicherweise eine Vertragsnummer, ein Passwort sowie eine Transaktionsnummer von einer Streichliste oder einem kleinen Hardwaregerät (SecureID).

Banking

keyon

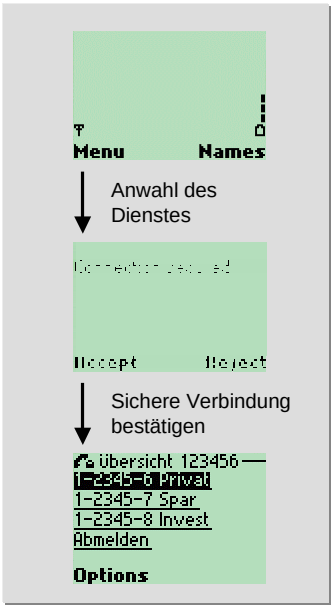


- Durchführen der gewünschten Aktivitäten wie
  - Kontostand abfragen
  - Buchungen vornehmen
  - etc.

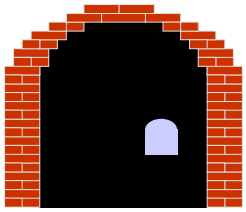
Nachdem die Bank die Anmeldedaten geprüft hat, kann der Benutzer auf seine Konten zugreifen.

Empfangsprobleme

keyon



- Unterbruch



- Neuanmelden nicht unbedingt erforderlich
- Ideal auch für Trading-Applikationen

Der Schrecken aller Mobiltelefonierer ist wohl die Versorgungslücke, oft anzutreffen in Form eines Tunnels. Eine solche Versorgungslücke kann zum Abbruch der Verbindung führen, was angesichts der doch aufwendigen Anmeldungsprozedur unangenehm ist. WTLS bietet hier jedoch eine elegante Lösung an. Der beim Etablieren der sicheren Verbindung ausgetauschte Geheimcode, welcher als Basis für die Verschlüsselung verwendet wird, ist auch nach einem Abbruch gültig.

Bei einer erneuten Anwahl versucht das Mobilgerät die Verbindung basierend auf dem ausgetauschten Geheimcode wiederaufzunehmen. Lässt dies die Bank zu, so kann sie den Benutzer anhand dieses Geheimcodes eindeutig identifizieren, er muss sich also nicht erneut anmelden. Eine erhöhte Sicherheit kann durch Abfragen eines einfachen PINs erreicht werden, damit z.B. der Verlust des Geräts kein Risiko darstellt.

Es liegt an der Bank, die Zeitdauer festzulegen, in der eine Wiederaufnahme möglich ist. Das Endgerät gibt die maximale Dauer vor, beim Nokia 7110 sind es z.B. 24 Stunden. Das eröffnet auch die Möglichkeit, sich einmal am Morgen anzumelden, und während des ganzen Tages immer wieder kurz „anzurufen“ , beispielsweise um Aktien zu handeln.

Zusammenfassung

keyon

- Sicheres Mobile-Banking ist schon jetzt möglich durch
  - sichere Mobilgeräte
  - entsprechende Infrastrukturen bei der Bank
- Die Sicherheit ist dank 128 Bit - Verschlüsselung genau so hoch wie beim Internet-Banking
- Dienste und Inhalte müssen auf die Ressourcen der Mobilgeräte abgestimmt werden
- Unterbrüche sind zwar unangenehm, stellen aber für die Sicherheit und den Ablauf kein grosses Problem dar
- Die vorgestellte Lösung ist unabhängig vom Mobilfunkanbieter