

M-Commerce Security

Inhalt

- ◆ Einleitung/ Überblick
- ◆ Technologie, Funktionsweise und Sicherheit
 - GSM
 - GPRS
 - UMTS
- ◆ Netzfunktionsweise
 - Aufbau
 - Sicherheit/ Realisierung
 - ◆ Vertraulichkeit der Identität des Benutzers
 - ◆ Benutzerauthentifikation
 - ◆ Daten- & Verbindungssicherheit
- ◆ WAP/ WML/ WTLS
- ◆ SIM Application Toolkit, MExE
- ◆ Ausblick/ Fragen

Technologie

- ◆ GSM (Global System for Mobile Communications)
 - Von ETSI standardisiert
 - ◆ TIA/ EIA-136
 - Von UWCC für USA, Kanada, Süd Amerika, Israel
- > Kooperation: EDGE (und später UMTS)

Datenübertragungsraten:

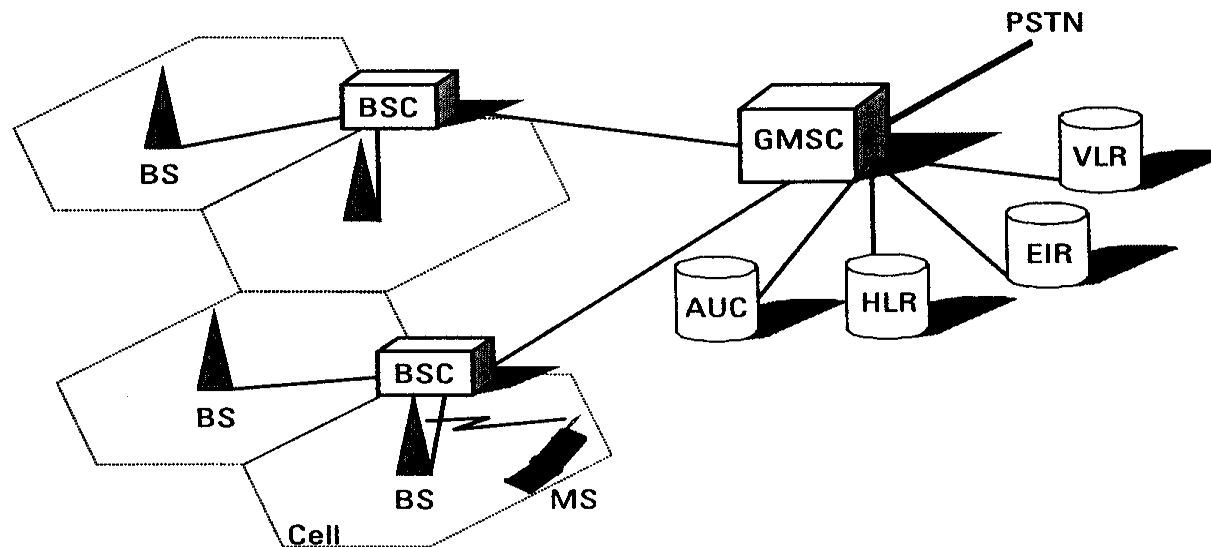
„Circuit Switched“ GSM: 14.4Kbps

GPRS: 50 Kbps

EDGE: 384 Kbps

UMTS: 2Mbps

GSM Netzwerk Modell



BS: Base Station

BSC: Base Station Controller

MS: Mobile Station

GMSC: Gateway Mobile Services Switching Center

PSTN: Public Switched Telephone Network

VLR: Visitor Location Register

AUC: Authentication Center

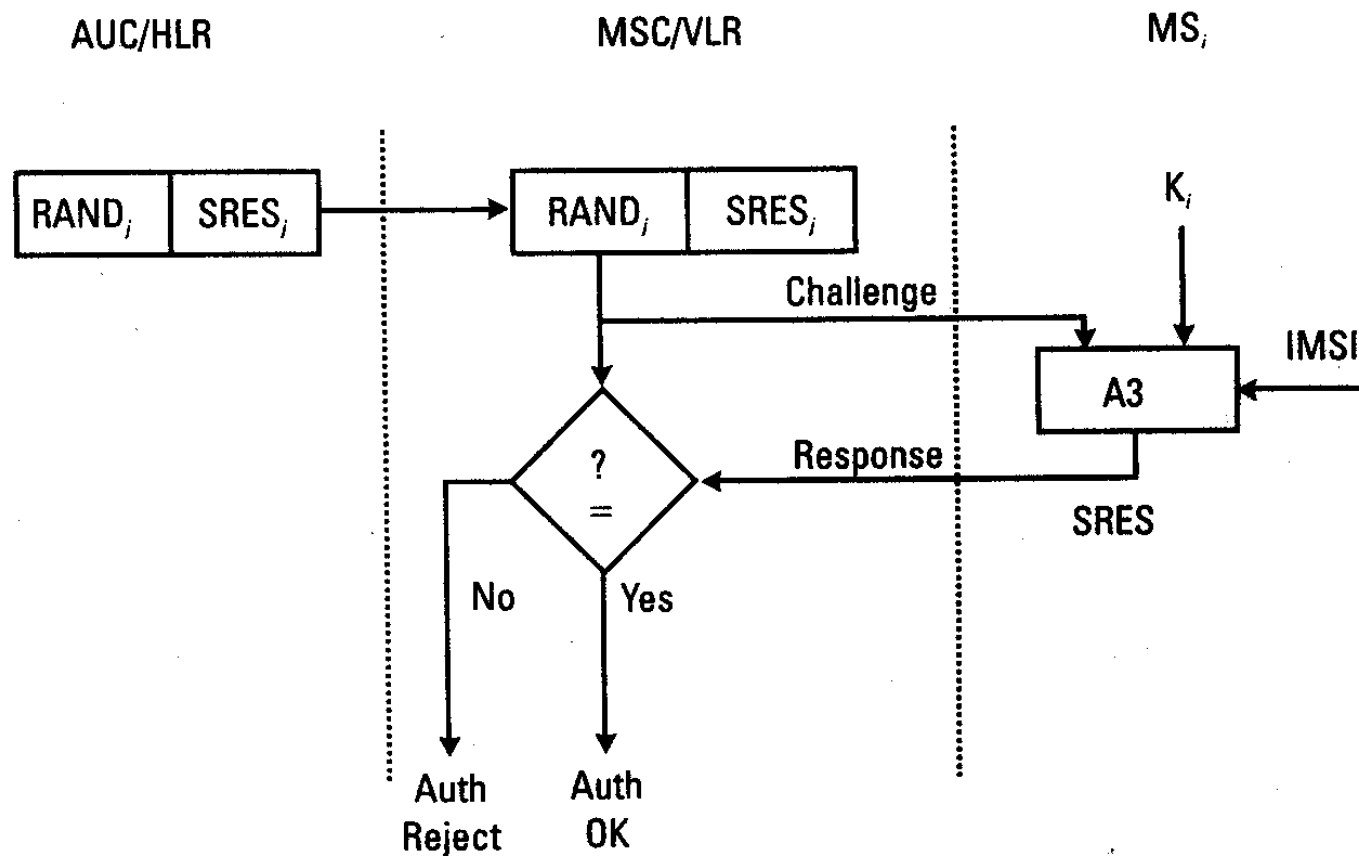
EIR: Equipment Identity Register

HLR: Home Location Register

Sicherung

- ◆ Vertraulichkeit der Identität des Benutzers
 - Geheimhaltung von benutzerspezifischen Informationen
 - IMSI nie in Klartext übertragen
 - Sicherheitslücke VLR Pos. Update eines neuen MSC...
- ◆ Benutzerauthentifikation
 - Nach Challenge Response Verfahren
 - IMSI & K_i müssen unbedingt geheim bleiben
- ◆ Daten- & Verbindungssicherheit
 - Erzeugung eines 64 Bit Schlüssels K_c für Daten/ Sprachübertragung
 - Bereits erfolgreich angegriffen von Biryukov & Shamir

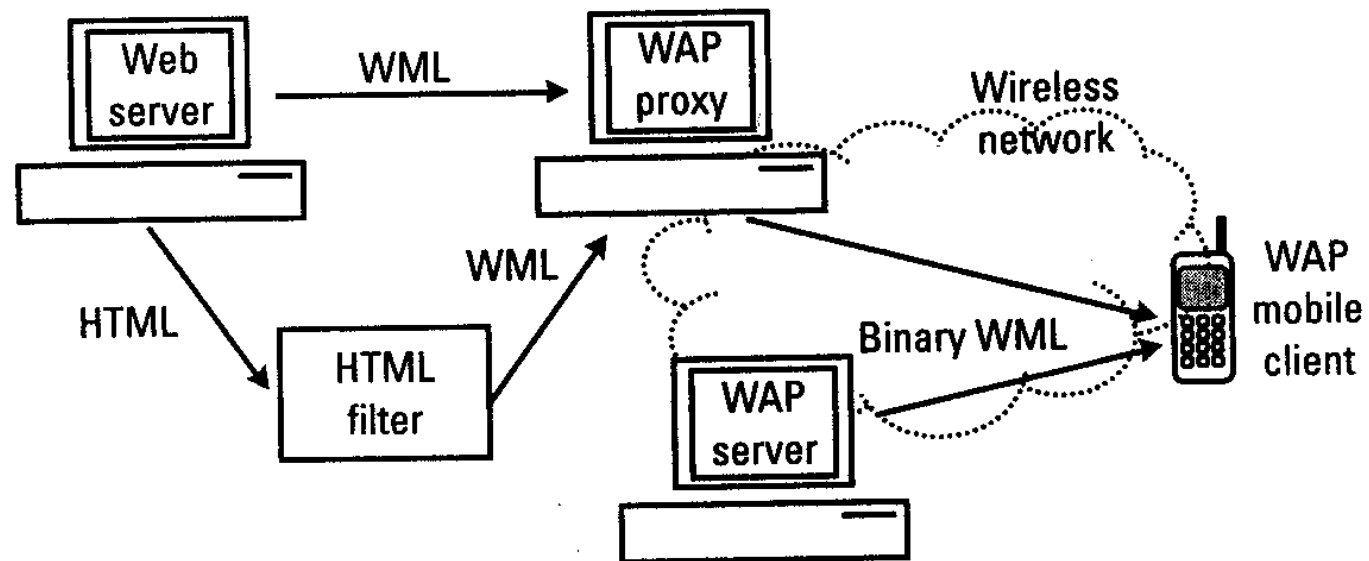
Benutzerauthentifikation



WAP

- ◆ E-Mails lesen, Bankgeschäfte durchführen, im Web surfen...
- ◆ Basierend auf Client/ Server Prinzip
- ◆ Sprache WML (compiliert) für Clients WAP Browser (meist Microbrowser)
- ◆ Decks und Cards steuern Zugangsberechtigung
- ◆ Sicherheitsprotokoll WTLS
- ◆ Sicherheitsrelevante Informationen im WIM

WAP Konfiguration



SIM Application Toolkit

- ◆ Ab GSM 11.14
- ◆ ‚Werkzeugkasten‘ für SIM Karte
- ◆ Basiert auf Client/ Server Prinzip
- ◆ Funktionen updatebar/ neu installierbar durch herunterladen aus Netzwerk
- ◆ Hohe Sicherheit durch kryptografische Funktionen
- ◆ Anderes Konzept als WAP
aber kann WAP komplementieren



MExE

- ◆ Mobile Station Application Execution Environment
- ◆ Erweiterung von SIM & Mobilem Gerät
- ◆ Standardisierte plattformunabhängige Kommunikation
- ◆ JVM fügt neue Funktionen und Möglichkeiten hinzu

Ausblick

- ◆ 2003: 66 Billionen US Dollar für mobile Transaktionen veranschlagt
- ◆ Mobile Geräte werden zu den Wichtigsten im elektr. Bezahlen (banking/ broking)
- ◆ Aber Hindernisse: Benutzerauthentifiation & Signaturen bei WAP
- ◆ WAP wirklich sinnvoll??
- ◆ ...Fragen?