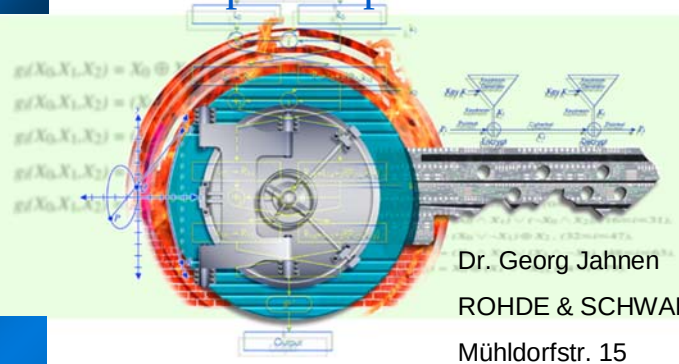
IT Sicherheit für Daten und Sprache in mobiler Vernetzung am Beispiel TopSec GSM

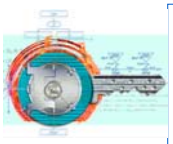


Dr. Georg Jahnen

ROHDE & SCHWARZ SIT GmbH

Mühldorfstr. 15
D-81671 München
georg.jahnen@sit.rohde-schwarz.com

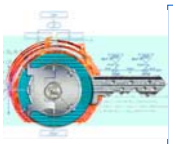
ROHDE&SCHWARZ



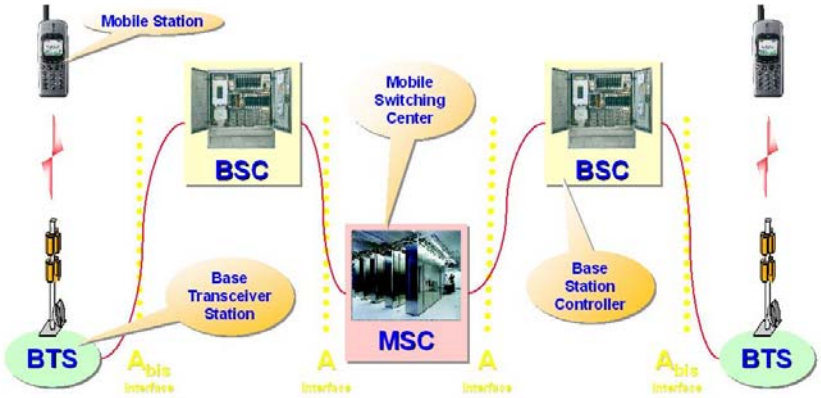
Übersicht

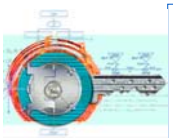
- Kommunikation in GSM Netzen, Abhörmöglichkeiten
- Verschlüsselung am Beispiel TopSec
- Datenverschlüsselung
- Verschlüsselte GSM Sprachübertragung
- GSM Datendienste
- Anpassungen für GSM Datenübertragung
- Erfahrungen mit heutiger Lösung
- Eigenschaften einer zukünftigen Lösung

ROHDE&SCHWARZ



Kommunikation in GSM Netzen





Schwachstellen und Abhörmöglichkeiten im GSM

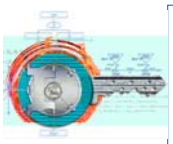
Verschlüsselung

- Beschränkt auf Luftschnittstelle – Abhören ab Basisstation möglich (Leitung ab Basisstation, Vermittlung, Richtfunkstrecke)
- Verwendeter Algorithmus (A5) weist Schwachstellen auf – Schlüssel können mit entsprechendem Aufwand bestimmt werden
- Verschlüsselung kann vom Netz her abgeschaltet werden

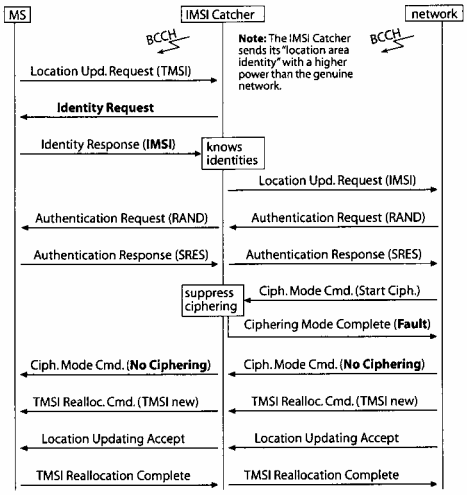
Authentisierung

- Nur das Mobiltelefon authentifiziert sich gegenüber dem Netz, nicht die Basisstation gegenüber dem Mobiltelefon – Basisstationen, die nicht dem Netzbetreiber gehören, können “untergeschoben“ werden

“IMSI-Catcher“ können einem Mobiltelefon aktiv eine Basisstation vorgaukeln. Die Zulassung der Verwendung von IMSI-Catchern ist in Deutschland in der Telekommunikationsverordnung geregelt.

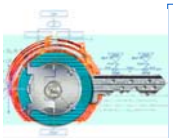


GSM-Netz: Mögliches Abfangen von IMSIs und Unterdrückung der Verschlüsselung

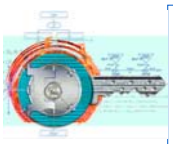


IMSI = International Mobile Subscriber Identity

Quelle: Hannes Federrath, Protection in Mobile Communications, 1999

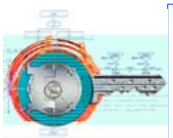


Verschlüsselung am Beispiel TopSec

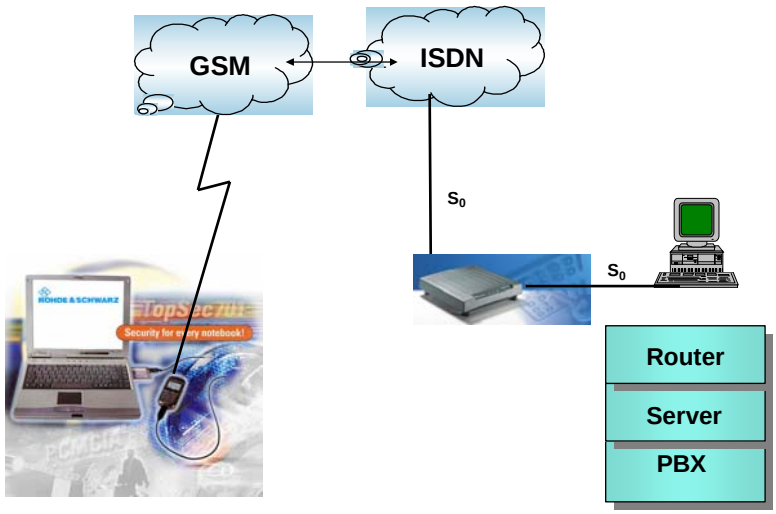


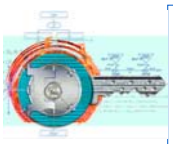
Prinzip der Verschlüsselung mit TopSec

- Ende zu Ende (e2e) Sicherheit
- Endgeräte werden nicht modifiziert
- Verschlüsselungsgeräte werden zwischen Endgerät und öffentlichem Netz geschaltet
- Zuverlässige starke Verschlüsselung
  - Starke Algorithmen
  - Anerkanntes Schlüsseleinigungsverfahren
  - Authentisierung der Partner
- Einfache Handhabung und Administration
  - Keine Schlüsselverteilung
  - Keine Schlüsselspeicherung (Einsatz von asymmetrischer Schlüsseleinigung)



Datenverschlüsselung mit TopSec





Beurteilung der Lösung

Vorteile

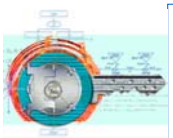
- keine Software Installationen auf dem Laptop
- Verschlüsselungskarte verhält sich wie ein Modem

Schwierigkeiten des Anwenders

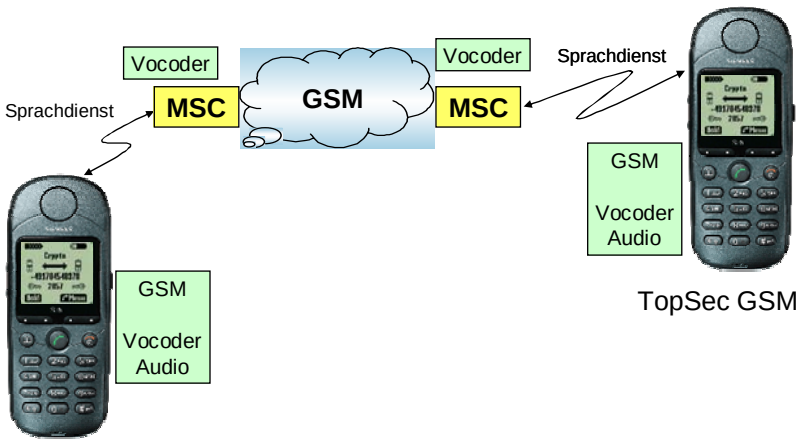
- Mit Verschlüsselung wird Anwendung oft erst eingeführt
- Verschlüsselungskarte ist erste PCMCIA Karte die zum Einsatz kommt
- Remote LAN Access ist sehr zeitaufwendig (Laufzeiten)
  (z.B. Anzeige von Verzeichnis unter Windows Explorer dauert Minuten)
- Mit „passenden“ Anwendungen kann gut gearbeitet werden
  (Replizierung von Datenbanken, Mail, ...)

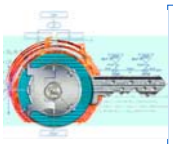
Fazit:

- Vertrieb im Rahmen von Projektlösungen



GSM Sprachübertragung





Situation in GSM Netzen

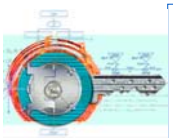
- Komprimiertes Sprachsignal wird bei der Vermittlung (Mobile Switching Center; MSC) wieder dekomprimiert
- Netzinterne Übertragung nicht notwendig transparent
- Übergang in das ISDN Netz nicht definiert

Folge:

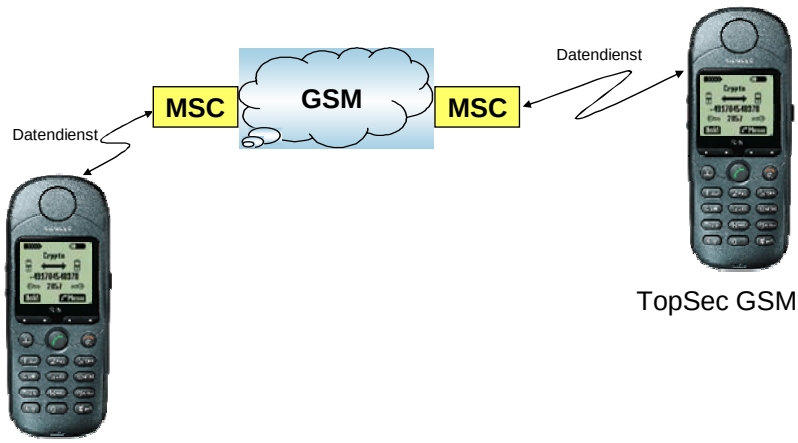
Bei Nutzung des GSM Sprachkanals mit Verschlüsselung des Vocoder Signals erfordert Modifikation des GSM Netzes

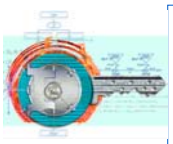
Alternative:

- Nutzung des Datendienstes



Verschlüsselte GSM Sprachübertragung

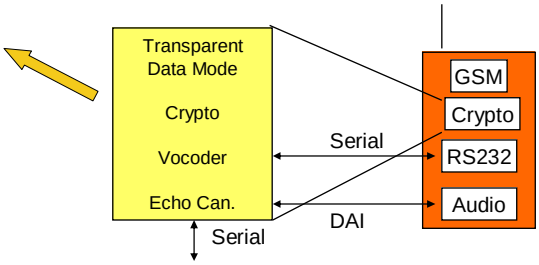


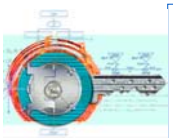


Realisierung mit Kryptomodul

32 x 34 mm²
Krypto Modul

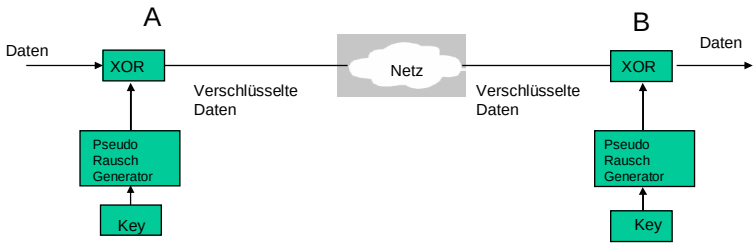
Dicke < 2 mm

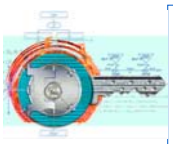




Symmetrische Verschlüsselung

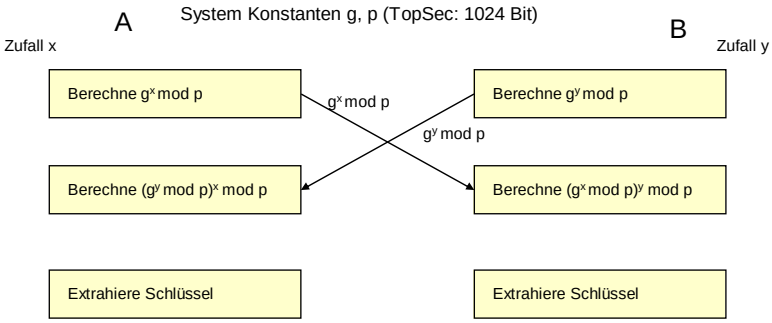
- Datenrate bis zu 64 kbps pro Kanal
- Symmetrischer Algorithmus als Stromchiffre (128 Bit)
- Geeignet für 16 Bit Digitale Signal Prozessoren (DSP)

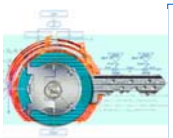




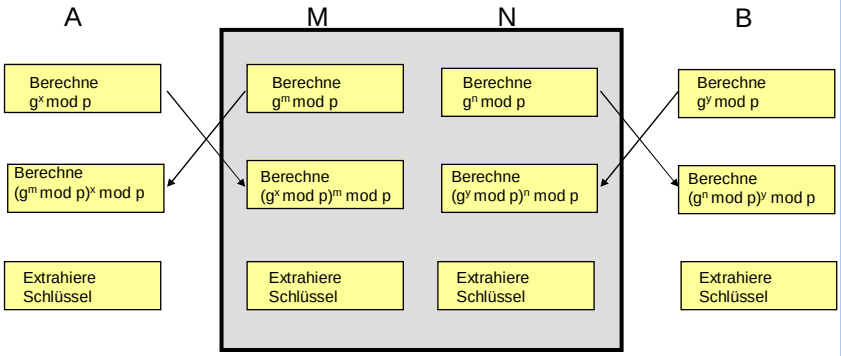
Asymmetrischer Schlüsselaustausch

Public Key Verfahren nach Diffie, Hellmann





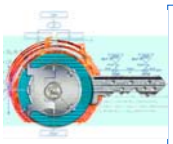
Problem bei Diffie-Hellmann: „Man in the Middle“-Angriff



Man in the Middle

“Man in the Middle” Angriff:
Geräte A und B arbeiten mit Geräten des Angreifers, nicht miteinander.

Abwehr: Authentisierung



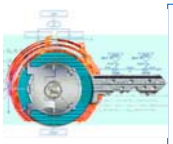
Authentisierung

Sprachkommunikation: Authentisierung durch Anwender

- Extrahiere 4 stellige Sicherheitszahl
- Anwender vergleicht beide Zahlen
- Sind Zahlen unterschiedlich, dann sind Schlüssel unterschiedlich: STOP!

Datenkommunikation

- Geräte wie PC, Router etc. können keine Sicherheitszahlen vergleichen.
- Authentisierung der Endgeräte normalerweise nicht möglich
- -> Nutze Authentisierung der TopSec Geräte



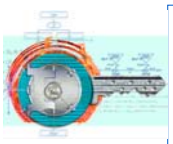
Authentisierung mit RSA Algorithmus

Generierung eines Schlüsselpaares

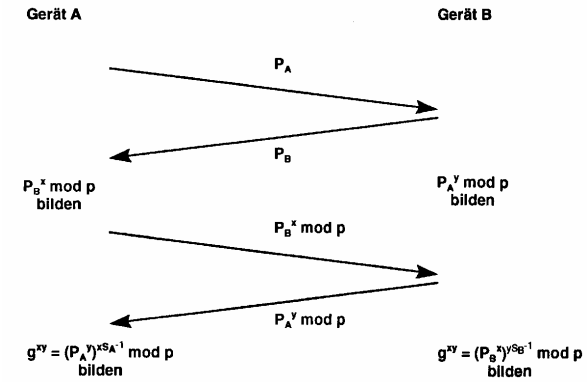
- Erzeuge
  - **Geheimer Schlüssel**, um Zertifikate zu signieren
  - **Öffentlicher Schlüssel**, um Echtheit von Zertifikaten zu überprüfen
- Generiere individuelles Zertifikat für jedes Gerät mit korrekter Signatur (Nutzung des geheimen Schlüssels)
- Gebe jedem Gerät den öffentlichen Schlüssel um Signaturen prüfen zu können

TopSec

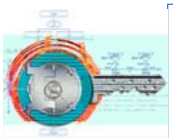
- Eine PC basierte Anwendung realisiert Zertifikatserstellung
- Zertifikat wird in sicherer Umgebung geladen
- Weiterer Zugriff auf die Geräte erfolgt über Netz



Verbindungsaufbau mit Diffie Hellman und RSA (kombiniert)



+ Weitere Meldungen zum Signalisieren von Verbindungsstatus



GSM Datendienste

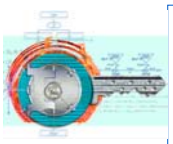
Datenübertragungsrate
- 9600 bps, Non Transparent
- 7680 bps, Transparent

Laufzeit
- bis zu 1.4 Sekunden, Non Transparent
- ca. 300 ms, Transparent

Dauer Verbindungsaufbau
- V.110 sehr schnell
- V.32, komplettes Modemtraining wird durchgeführt (ca. 10 Sek.)

Auswahl Sprache: Transparenter Datendienst, V.110
- Bei Störungen wird leise geschaltet

Auswahl Daten: Non Transparenter Datendienst, V.110
- Viele Mobiltelefone unterstützen nur diesen Dienst

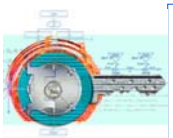


Kommunikation GSM - ISDN

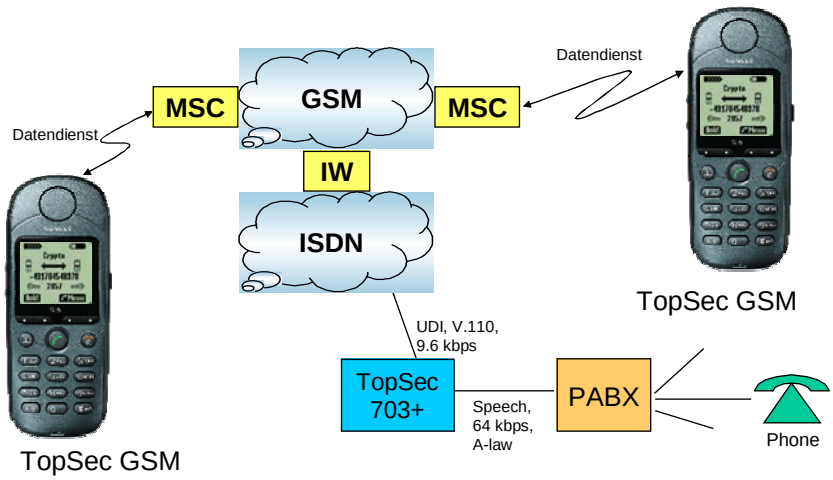
Protokoll

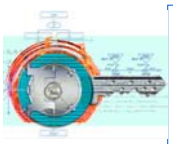
- UDI (Unrestricted Digital Information)
- V.110
- 9600 bps

Auswahl des beim Übergang verwendeten Protokolls durch das anrufende Gerät



Verschlüsselte Sprachübertragung zwischen GSM und ISDN

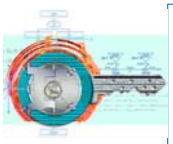




Grenzen der Verschlüsselung im GSM

- Es existiert installierte Infrastruktur
- Datendienst nicht immer „wie gewohnt“ verfügbar
- Übergang GSM <-> ISDN standardisiert, aber nicht immer vollständig implementiert
- Realisierung der Netze regional unterschiedlich
- Technische Weiterentwicklung von Infrastruktur
- Verbindungsinformation nach wie vor unverschlüsselt

- “Bedienung” von Verschlüsselung
- Einschränkungen durch Verschlüsselung (geringe Akzeptanz)
  - Einsatz von „gewohntem“ Zubehör
  - Interoperabilität zwischen Netzen
  - Schlüsseleinigung (Dauer für Verbindungsaufbau)
- ...



Verfügbarkeit der GSM Datendienste

Deutschland GSM <-> GSM

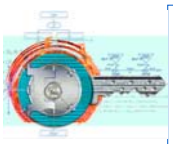
- Gute Verfügbarkeit, jedoch deutlich geringer als Sprachdienst
- Netzübergreifende Kommunikation möglich (z.B. D1 <-> D2)

Deutschland GSM <-> ISDN

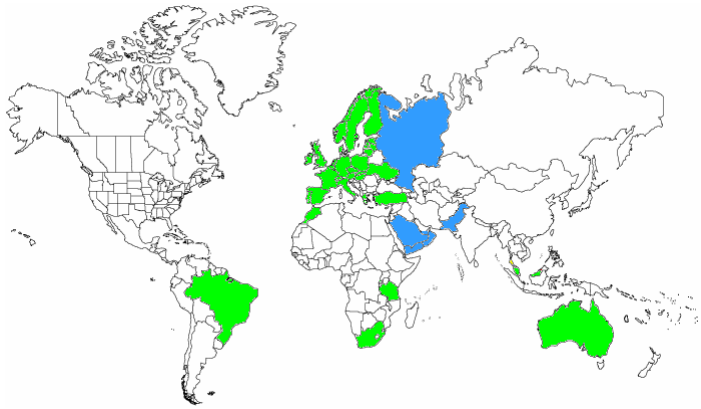
◆ E-Plus	Arbeitet einwandfrei
◆ O_2	Arbeitet nach Modifikation (MSC) einwandfrei
◆ D1	Geringe Einschränkungen (Wenige Orte)
◆ D2	Einschränkungen regional unterschiedlich

International

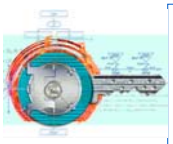
◆ V.110	Sehr starke Einschränkungen
◆ V.32	Deutlich besser verwendbar



Verfügbarkeit der GSM Datendienste

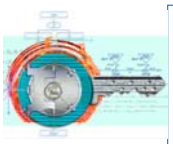


Grün	V.110 „erfolgreich“ getestet	Rot	keine Funktion
Blau	Nur V.32 Betrieb	Weiß	keine Information



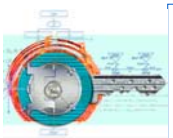
Anpassungen für GSM Datenübertragung

- Implementierung des V.32 Protokolls im TopSec GSM
  - Bei vielen Netzen im Ausland ist V.110 nicht implementiert
  - Vorteil bei Netzübergängen, die nicht digital realisiert sind
  - Vorteile bei internationaler Kommunikation
- Implementierung V.32 für Festnetzgegenstelle in Prüfung
  - Analoge Schnittstellen bevorzugt
  - Beschränkung auf 9600 bps möglich
- Implementierung spezieller Modems für Datenübertragung über Sprachdienst geplant
  - Bessere Verfügbarkeit (abhängig von Übertragungsqualität)
  - Sehr geringe Datenraten (2400 bps)
  - Einsatz stark komprimierender Vocoder (~1200 bps)
  - Geringe Sprachqualität (nur verwendbar für Notbetrieb)



Erfahrungen mit heutiger Lösung

- Anwender vergleicht Verschlüsselungsgerät mit Mobiltelefonen
  -> Forderung nach aktuellen Modellen
- Anwendung auch in USA gewünscht
  -> Basis auf Tri-Band Gerät
- Verzögerung mit transparentem Datenmodus akzeptabel
  -> Heutige Mobiltelefone arbeiten mit Non-Transparent Modus, Modifikationen daher notwendig
- Im Vergleich zu Mobiltelefonen relativ teuer
  -> Vereinfachung des Herstellprozesses, größere Stückzahlen
- Einschränkungen beim Betrieb mit Freisprechanlagen
  (Gerät arbeitet im Datenmodus, Ansteuerung entsprechend)



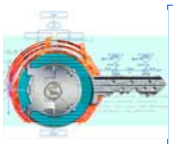
Eigenschaften einer zukünftigen Lösung

GSM

- Unabhängigkeit von aktuellen Mobiltelefonen
- Basis auf Tri-Band Gerät
- Integration des transparenten Datenmodus
- Verwendung von angepassten Modems zur Datenübertragung über Sprachdienst
- Vereinfachung des Herstellprozesses, größere Stückzahlen
- Breite Einsatzmöglichkeiten (Behörden, Industrie, Export)

Neue Mobilfunknetze (EDGE, GPRS, UMTS)

- Vorteile
  - höhere Datenraten
- Nachteile
  - Verfügbarkeit
  - Laufzeiten durch Paketorientierung



Zusammenfassung

- Anforderungen der Verschlüsselung an Übertragungsnetze
- Prinzip der heutigen Lösung
- Probleme mit den heutigen Möglichkeiten zur Datenkommunikation
- Wichtige Eigenschaften einer zukünftigen Lösung