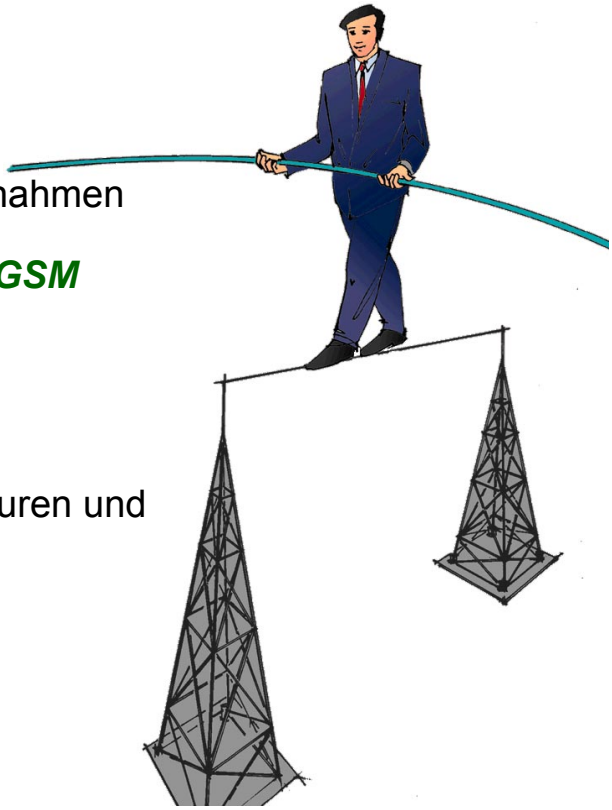
Sicherheit in der Mobilkommunikation

1 Mobilkommunikation und mehrseitige Sicherheit

1.1 Mobilkommunikation
1.2 Mehrseitige Sicherheit
1.3 Angreifermodell
1.4 Abgeleitete Sicherheitsmaßnahmen

2 Mobilkommunikation am Beispiel GSM

2.1 Allgemeines
2.2 Struktur von GSM
2.3 Datenbanken des GSM
2.4 Sicherheitsrelevante Prozeduren und Funktionen



Sicherheit in der Mobilkommunikation

3 Mobilitäts- und Verbindungsmanagement am Beispiel GSM

3.1 Location Management allgemein
3.2 Erstellbarkeit von Bewegungsprofilen allgemein
3.3 Location Update Prozeduren
3.4 Rufaufbau (Call Setup) im GSM
3.5 Erstellbarkeit von Bewegungsprofilen im GSM
3.6 Bekannte Angriffe auf GSM-Sicherheitsfunktionen
3.7 Zusammenfassung der Sicherheitsprobleme

4 Verfahren zum Schutz von Aufenthaltsinformation

4.1 Allgemeines
4.1 Systematik

Sicherheit in der Mobilkommunikation

5 Methoden mit ausschließlichem Vertrauen in die Mobilstation

- 5.1 Vermeidung von Lokalisierungsinformation
- 5.2 Variable implizite Adressen
- 5.3 Methode der Gruppenpseudonyme

6 Methoden mit zusätzlichem Vertrauen in einen eigenen ortsfesten Bereich

- 6.1 Adreßumsetzungsmethode mit Verkleinerung der Broadcast-Gebiete
- 6.2 Explizite Speicherung der Lokalisierungsinformation in einer Trusted Fixed Station
- 6.3 Pseudonymumsetzung in einer vertrauenswürdigen Umgebung mit der Methode der temporären Pseudonyme
- 6.4 Sicherheitsbetrachtungen

Sicherheit in der Mobilkommunikation

7 Methoden mit zusätzlichem Vertrauen in einen fremden ortsfesten Bereich

- 7.1 Organisatorisches Vertrauen: Vertrauen in eine Trusted Third Party
- 7.2 Methode der kooperierenden Chips
- 7.3 Mobilkommunikationsmixe

8 Mobilität im Internet

- 8.1 Mobile IP: Prinzip und Sicherheitsfunktionen
- 8.2 Mobile IP und Schutz von Aufenthaltsorten

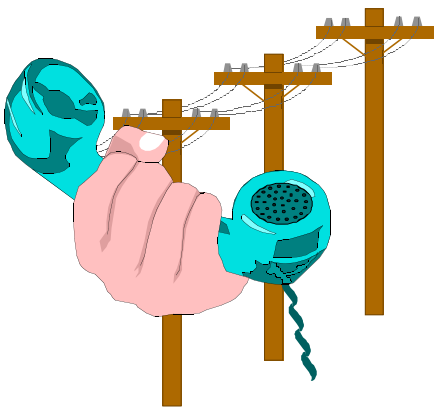
9 Zusammenfassung

Organisatorisches

- ***Lehrbeauftragter***
  - Dr.-Ing. Hannes Federrath
  - E-Mail: federrath@inf.tu-dresden.de
- ***Art der Lehrveranstaltung***
  - Wahlpflichtlehrveranstaltung, 2 SWS Vorlesung
  - Zuordnung zur Vertiefungsrichtung «Technischer Datenschutz»
- ***Erwünschte Vorkenntnisse***
  - Grundlagen Rechnernetze/verteilte Systeme
  - Grundkenntnisse Datensicherheit/Kryptographie
- ***Lehrveranstaltungsmaterial:***
  - http://www.inf.tu-dresden.de/~hf2/mobil/
- ***Form des Abschlusses:***
  - Mündliche Prüfung oder Schein

Mobilkommunikation – Einführung

- ***Unterschiede Festnetz- und Mobilkommunikation***
  - Teilnehmer bewegen sich
  - Bandbreite auf der Luftschnittstelle knapp
  - Luftschnittstelle störanfälliger als Leitungen des festen Netzes:
    - zeitweilige Diskonnektivität
  - Luftschnittstelle bietet neue Angriffsmöglichkeiten:
    - erleichterte Abhörmöglichkeit
    - Peilbarkeit



Mobilkommunikation – Einteilungsmöglichkeiten

1. Mobilitätsformen

- ***Terminal Mobility:***
  - Beispiel: **Funktelefon**
    - drahtlose Kommunikationsschnittstelle
    - mobiles Endgerät
- ***Personal Mobility:***
  - Beispiel: **öffentliche Terminals**
    - Teilnehmer ist mobil
    - bewegungsunabhängige Adresse
    - Endgerät ist nicht notwendigerweise mobil
- ***Session Mobility:***
  - «**Einfrieren einer Session**» und spätere Reaktivierung an einem anderen Ort oder/und Endgerät.

Mobilkommunikation – Einteilungsmöglichkeiten

2. Wellenbereiche

- Funkwellen (f = 100 MHz bis mehrere GHz)
- Lichtwellen (infrarot)
- Schallwellen (bisher ungebräuchlich)

3. Zellengröße

– Pikozellen	d < 100 m
– Mikrozellen	d < 1 km
– Makrozellen	d < 20 km
– Hyperzellen	d < 60 km
– Overlay-Zellen	d < 400 km

Weitere

- Punkt-zu-Punkt-Kommunikation, Broadcast (Pagerdienste)
- Analog, Digital
- Simplex, Duplex

Beispiele für mobile Netze

- *Pagerdienste (Scall, TeLMI)*
- *Datendienste (Modacom)*
- *Sprachdienste = Massenmarkt*
  - 1. Generation: analog
    - C-Netz, Cordless Telephone, AMPS
  - 2. Generation: digital
    - GSM, DCS-1800, DECT
  - 3. Generation: diensteintegrierend
    - UMTS/IMT-2000/FPLMTS

- *Satellitendienste*
  - Iridium, Inmarsat, Globalstar, Odyssey
  - GPS (Global Positioning System)
- *Internet (Mobile IP)*

Sicherheitsanforderungen an mobile Systeme

- *Bsp. f. Sicherheitsanforderungen: Cooke, Brewster (1992)*
  - protection of user data
  - protection of signalling information, incl. location
  - user authentication, equipment verification
  - fraud prevention (correct billing)
- *Allgemein*
  - Schutz der Vertraulichkeit
  - Schutz der Integrität
  - Zurechenbarkeit
  - Verfügbarkeit
- *Mobiles Umfeld kann nicht als vertrauenswürdig vorausgesetzt werden*

Vertraulichkeit, Integrität, Zurechenbarkeit, Verfügbarkeit

- ***Schutz der Inhaltsdaten («Worüber?»)*** — **Inhalte**
  - vor allen Instanzen außer den Kommunikationspartnern!
- ***Schutz der Verkehrsdaten («Wer mit wem?»)*** — **Senden**, **Empfangen**
  - Möglichkeit zur anonymen und unbeobachtbaren Kommunikation
  - auch gegenüber dem Netzbetreiber!
- ***Schutz des Aufenthaltsorts («Wo?»)*** — **Ort**
  - Schutzziel: Verhindern der Erstellbarkeit von Bewegungsprofilen

- ***Schutz vor (Ver)-Fälschung*** — **Inhalte**
  - Inhalte und Absender

- ***Sende- und Empfangsnachweise*** — **Absender**, **Empfänger**
  - Digitale Signaturen
- ***Sichere Abrechnungsverfahren*** — **Bezahlung**
  - auch gegenüber dem Netzbetreiber!
  - Anonymität und Unbeobachtbarkeit muß erhalten bleiben!

- ***Verfügbarkeit***

Was ist zu schützen?

Kommunikationsgegenstand WAS?	***Kommunikationsumstände WANN?, WO?, WER?***
Vertraulichkeit	**Anonymität Unbeobachtbarkeit**
Inhalte	**Sender**, **Ort**, **Empfänger**
Integrität	**Zurechenbarkeit Rechtsverbindlichkeit**
Inhalte	**Absender**, **Bezahlung**, **Empfänger**

Juristisch: personenbezogene Daten

Technisch: Inhaltsdaten und Verkehrsdaten

Maximal berücksichtigte Stärke des Angreifers

Schutz vor einem allmächtigen Angreifer ist unmöglich.

- Rollen des Angreifers (Außenstehender, Benutzer, Betreiber, Wartungsdienst, Produzent, Entwerfer …), *auch kombiniert*
- Verbreitung des Angreifers
- Verhalten des Angreifers
  - passiv / aktiv
  - beobachtend / verändernd (bzgl. seiner erlaubten Handlungen)
- dumm / intelligent
  - Rechenkapazität:
    - unbeschränkt: informationstheoretisch
    - beschränkt: komplexitätstheoretisch

Geld

Zeit

Angreifermodell

- ***Aktive oder passive Rolle des Angreifers***
  - Was kann der Angreifer maximal passiv beobachten?
  - Was kann der Angreifer maximal aktiv kontrollieren?
  - Was kann der Angreifer aktiv verändern?

  Konkret:
  - Angreifer außerhalb des Netzes (Outsider):
    nur passive (abhörend, beobachtend)
  - Angreifer innerhalb den Netzes (Insider):
    passive und aktive (hier: Daten verändernde Angriffe)
  - Generell: Insider und Outsider können Verfügbarkeit auf der Funkschnittstelle stören

Angreifermodell

- ***Mächtigkeit des Angreifers***
  - Wieviel Rechenkapazität besitzt der Angreifer?
  - Wieviel finanzielle Mittel besitzt der Angreifer?
  - Wieviel Zeit besitzt der Angreifer?
  - Welche Verbreitung hat der Angreifer? Oder spezieller: Welche Leitungen, Kanäle, Stationen kann der Angreifer beherrschen?

  Konkrete Verbreitung
  - Endgerät: sicher gegen Manipulation = Vertrauensbereich
  - Netzkomponenten: sicher gegenüber Outsidern, unsicher gegenüber Insidern
  - Funkschnittstelle: Peilbarkeit sendender Funkstationen (Insider und Outsider)

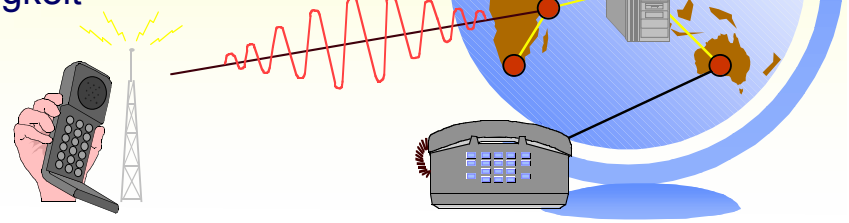
Sicherheitsmaßnahmen

	Vertr.	Integr.	Verf.
Ende-zu-Ende-Sicherung der Inhalte	x	x	
zusätzliche Verschlüsselung der Signalisierdaten	x	x	(x)
Schutz vor Peil- und Ortbarkeit:Spread Spectrum	x		x
Schutz der Kommunikationsbeziehungen	x		
Schutz des Aufenthaltsortes / Datenschutzgerechte Verwaltung der Aufenthaltsorte	x		
Gegenseitige Authentikation der Teilnehmer, aber auch der Netzkomponenten untereinander		x	x
Organisatorische Aspekte: Befugnisse des Wartungsdienstes genau definieren	x	x	x
(Hersteller)-Unabhängigkeit der Netzkomponenten	x		x
Anonyme Netzbenutzung (Wertkarten)	x		
Mehrseitig sichere, ggf. anonyme Abrechnung	x	x	(x)

Mobilkommunikation am Beispiel GSM

– Ursprünglich: Groupe Spéciale Mobilé der ETSI

- ***Leistungsmerkmale des Global System for Mobile Communication***
  - hohe, auch internationale Mobilität
  - hohe Erreichbarkeit unter einer (international) einheitlichen Rufnummer
  - hohe Teilnehmerkapazität
  - recht hohe Übertragungsqualität und -zuverlässigkeit durch effektive Fehlererkennungs- und -korrekturverfahren
  - hoher Verfügbarkeitsgrad (Flächendeckung zwischen 60 und 90%)
  - als Massendienst geeignetes Kommunikationsmedium
  - flexible Dienstgestaltung
    - Dienstevielfalt
    - Entwicklungsfähigkeit



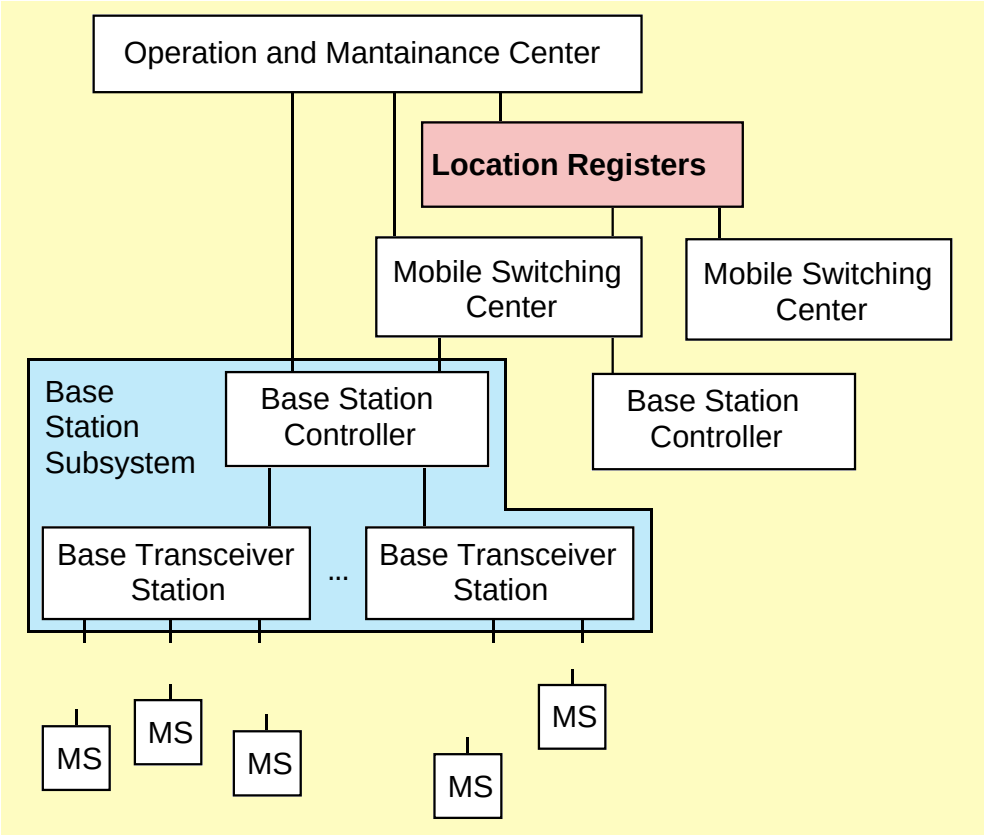
Mobilkommunikation am Beispiel GSM

– Ursprünglich: Groupe Spéciale Mobilé der ETSI

- ***Leistungsmerkmale des Global System for Mobile Communication***
  - eingebaute Sicherheitsmerkmale
    - Zugangskontrolldienste (PIN, Chipkarte)
    - Authentikations- und Identifikationsdienste
    - Unterstützung von temporären Identifizierungsdaten (Pseudonymen)
    - Abhörsicherheit für Outsider auf der Funkschnittstelle
  - relativ niedriges Kostenniveau
  - priorisierter Notrufdienst
  - Ressourcenökonomie auf der Funkschnittstelle durch FDMA, TDMA, Sprachkodierung, Warteschlangentechniken, OACSU (Off Air Call Setup)

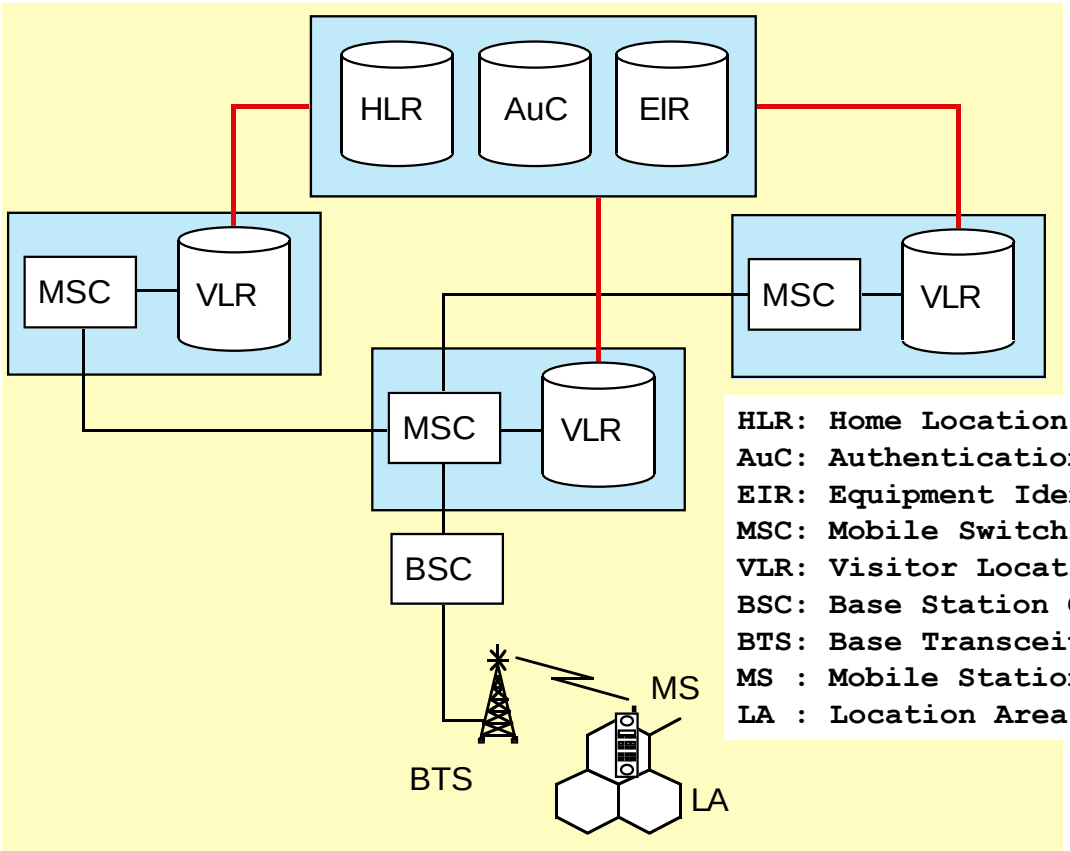
Struktur von GSM

- *Architekturkonzept – die Erste*



Struktur von GSM

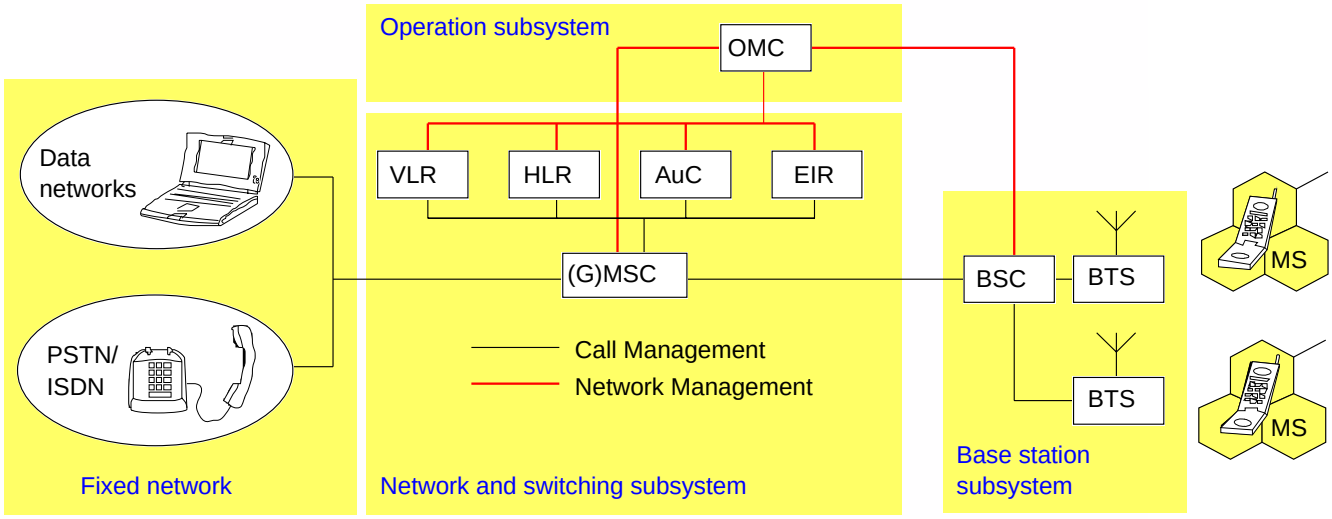
- *Logischer Netzaufbau*



HLR: Home Location Register
AuC: Authentication Center
EIR: Equipment Identity Register
MSC: Mobile Switching Center
VLR: Visitor Location Register
BSC: Base Station Controller
BTS: Base Transceiver Station
MS : Mobile Station
LA : Location Area

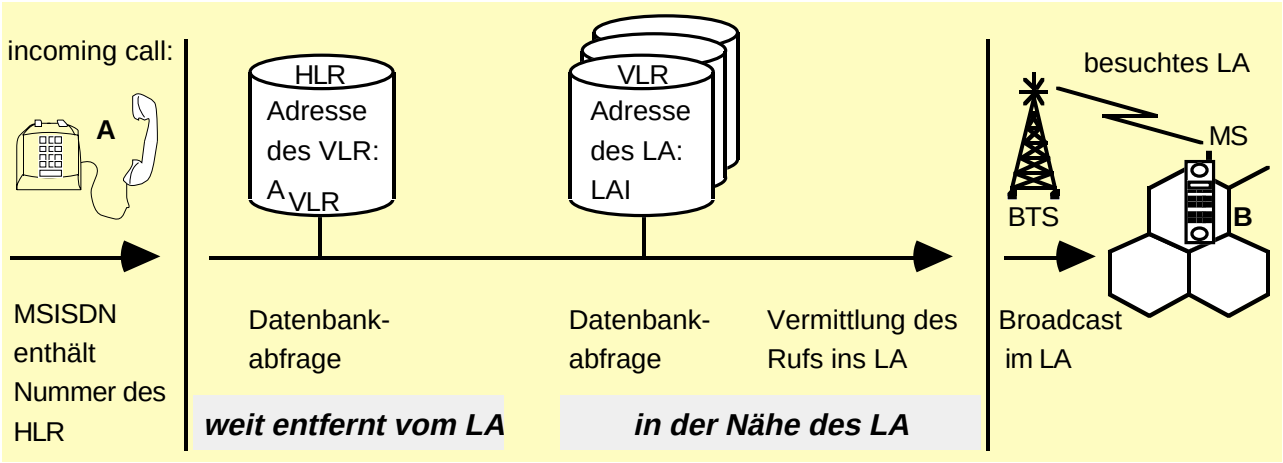
Struktur von GSM

- *Architekturkonzept – die Zweite*



Location Management im GSM

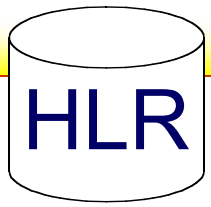
- *Grundprinzip verteilte Speicherung*
  - Verteilte Speicherung über Register
    - *Home Location Register* und *Visitor Location Register*
  - Netzbetreiber hat stets globale Sicht auf Daten
  - Bewegungsprofile sind erstellbar



Security deficits of existing mobile networks

- *Example of security demands: Cooke, Brewster (1992)*
  - protection of user data
  - protection of signaling information, incl. location
  - user authentication, equipment verification
  - fraud prevention (correct billing)
- *Security deficits of GSM (selection)*
  - Only symmetric cryptography (algorithms no officially published)
  - Weak protection of locations (against outsiders)
  - No protection against insider attacks (location, message content)
  - No end-to-end services (authentication, encryption)
- *Summary*
  - GSM provides protection against external attacks only.
  - "…the designers of GSM did not aim at a level of security much higer than that of the fixed trunk network." Mouly, Pautet (1992)

Datenbanken des GSM

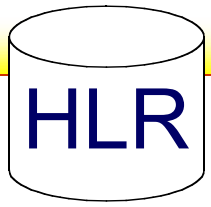


- *Home Location Register (HLR)*

Semipermanente Daten

- **IMSI** (International Mobile Subscriber Identity): max. 15 Ziffern
  - Mobile Country Code (MCC, 262) + Mobile Network Code (MNC, 01/02) + Mobile Subscriber Identification Number (MSIN)
- **MSISDN** (Mobile Subscriber International ISDN Number): 15 Ziffern
  - Country Code (CC, 49) + National Destination Code (NDC, 171/172) + HLR-Nummer + Subscriber Number (SN)
- **Bestandsdaten** über den Subscriber (Name, Adresse, Kto.-Nr. etc.)
- gebuchtes **Dienstprofil** (Prioritäten, Anrufweiterleitung, Dienstrestriktionen, z.B. Roaming-Einschränkungen)

Datenbanken des GSM



- ***Home Location Register (HLR)***

  Temporäre Daten

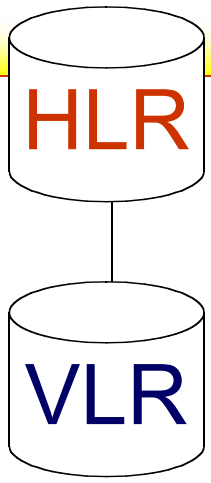
  – VLR-Adresse, MSC-Adresse

  – **MSRN** (Mobile Subscriber Roaming Number): Aufenthaltsnummer
    - CC + NDC + VLR-Nummer

  – Authentication Set, bestehend aus mehreren **Authentication Triples**:
    - RAND (128 Bit),
    - SRES (32 Bit) ,
    - Kc (64 Bit)

  – Gebühren-Daten für die Weiterleitung an die Billing-Centres

Datenbanken des GSM



- ***Home Location Register (HLR)***

- ***Visitor Location Register (VLR)***

  – IMSI, MSISDN

  – **TMSI** (Temporary Mobile Subscriber Identity)

  – MSRN

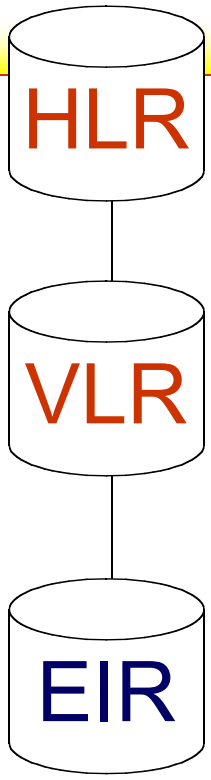
  – **LAI** (Location Area Identification)

  – MSC-Adresse, HLR-Adresse

  – Daten zum gebuchten Dienstprofil

  – Gebühren-Daten für die Weiterleitung an die Billing-Centers

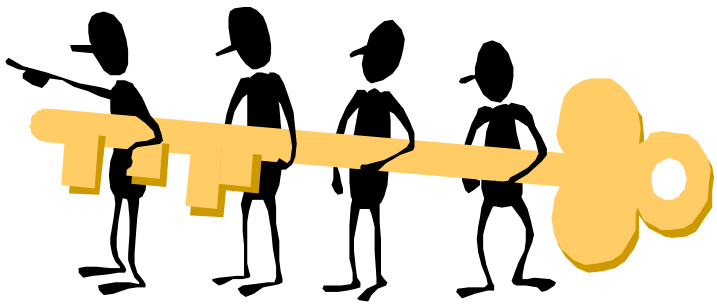
Datenbanken des GSM



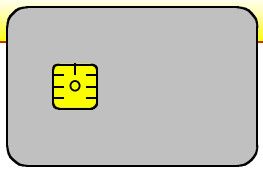
- *Home Location Register (HLR)*
- *Visitor Location Register (VLR)*
- *Equipment Identity Register (EIR)*
  - **IMEI** (International Mobile Station Equipment Identity): 15 Ziffern = Seriennummer der Mobilstation
    - **white-lists** (zugelassene Endgeräte, nur verkürzte IMEI gespeichert)
    - **grey-lists** (fehlerhafte Endgeräte, die beobachtet werden)
    - **black-lists** (gesperrte)

Security functions of GSM

- *Overview*
  - **Subscriber Identity Module** (SIM, smart card)
    - Admission control and crypto algorithms
  - **Authentication** (Mobile station → network)
    - Challenge-Response-Authentication (A3)
  - **Pseudonymization of users** on the air interface
    - Temporary Mobile Subscriber Identity (TMSI)
  - **Link encryption** on the air interface
    - Generation of session key: A8
    - Encryption: A5



Subscriber Identity Module (SIM)



- **Spezielle Chipkarte mit Rechenkapazität**

Gespeicherte Daten:

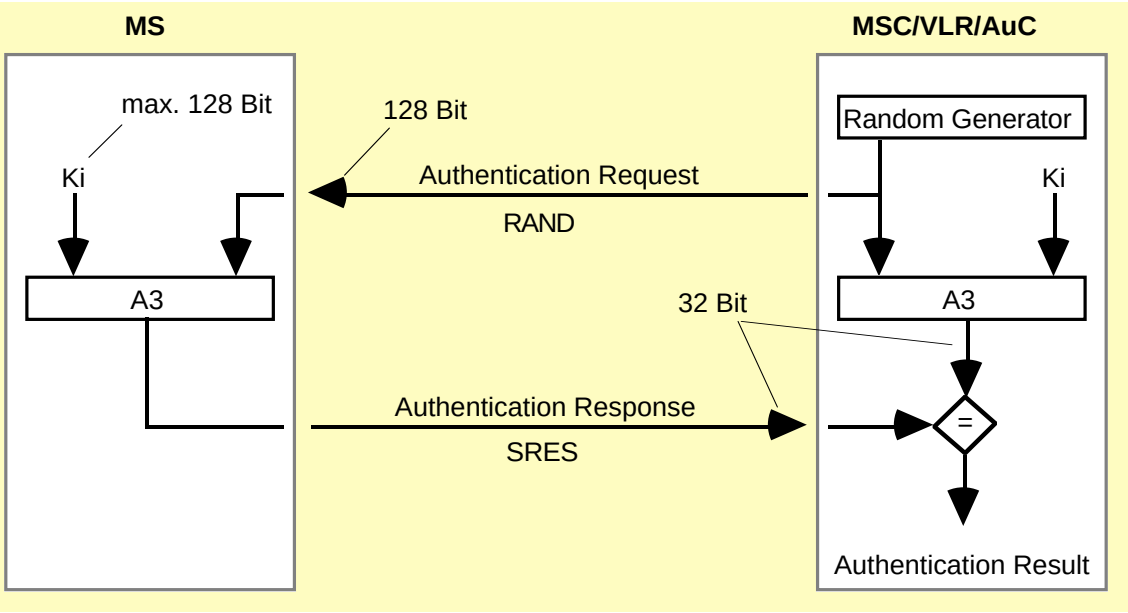
– IMSI (interne Teilnehmerkennung)
– teilnehmerspezifischer symmetrischer Schlüssel Ki (Shared Secret Key)
– PIN (Personal Identification Number) für Zugangskontrolle
– TMSI
– LAI

Krypto-Algorithmen:

– Algorithmus A3 für Challenge-Response-Authentikationsverfahren
– Algorithmus A8 zur Generierung von Kc (Session Key)

Challenge-Response-Authentication

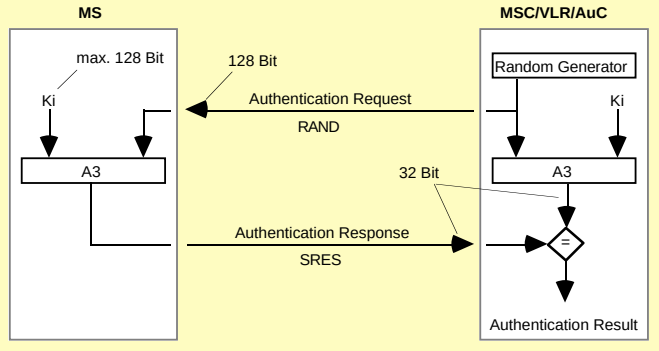
- **When initialized by the mobile network?**
  – Location Registration
  – Location Update when changing the VLR
  – Call Setup (both directions)
  – Short Message Service
- **Protocol**



Challenge-Response-Authentication

- ***Algorithm A3***
  - Implemented on SIM card and in Authentication Center (AuC)
  - Cryptographic one way function A3:

    SRES' = A3(Ki, RAND) (Ki: individual user key)
  - Interfaces are standardized, cryptographic algorithm not standardized
- ***Specific algorithm can be selected by the network operator***
  - Authentication data (RAND, SRES) are requested from AuC by the visited MSC
  - visited MSC: only compares SRES == SRES'
  - visited MSC has to trust home network operator



Attacks – Telephone at the expense of others

- ***SIM cloning***
  - –Weakness of authentication algorithm
- ***Interception of authentication data***
  - –Eavesdropping of internal communication links
- ***IMSI catcher***
  - –Man-in-the-middle attack on the air interface

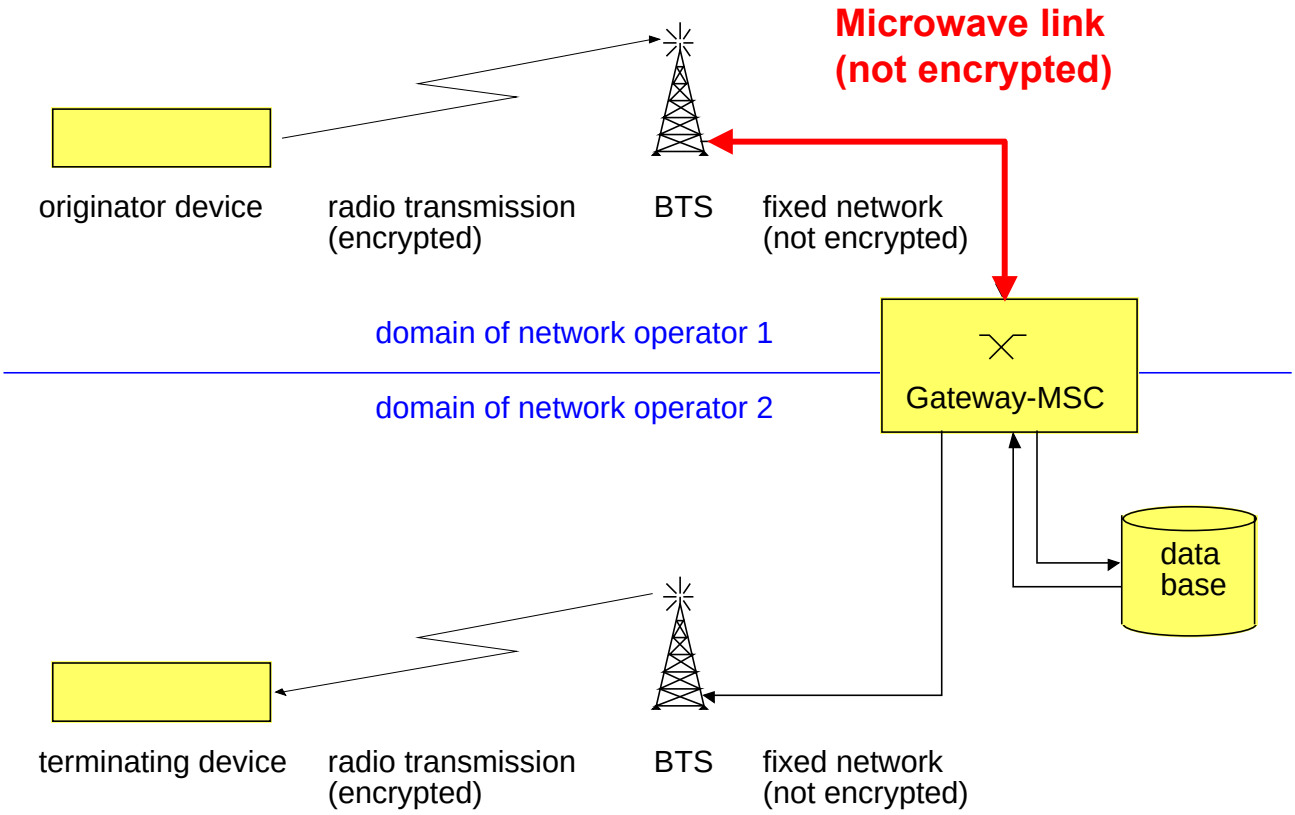
SIM cloning

- **Scope**
  - Telephone at the expense of others
  - Described by Marc Briceno (Smart Card Developers Association), Ian Goldberg and Dave Wagner (both University of California in Berkeley)
  - http://www.isaac.cs.berkeley.edu/isaac/gsm.html
  - Attack uses a weakness of algorithm COMP128, which implements A3/A8
  - SIM card (incl. PIN) must be under control of the attacker for at least 8-12 hours
- **Effort**
  - Approx. 150.000 calculations to determine Ki (max. 128 bit)
  - 6,25 calculations per second only, due to slow serial interface of SIM card

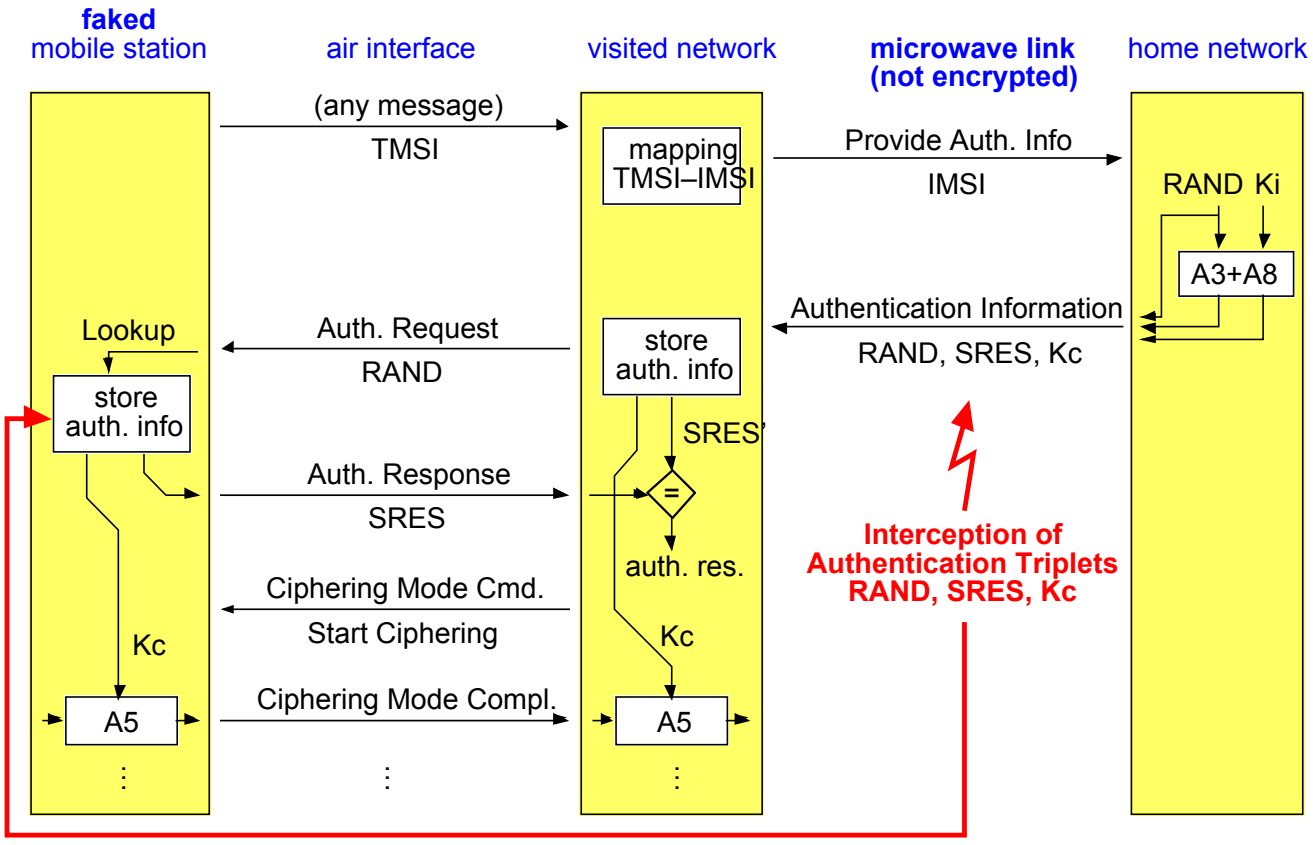
Interception of authentication data

- **Scope**
  - Telephone at the expense of others
  - Described by Ross Anderson (University of Cambridge)
  - Eavesdropping of unencrypted internal transmission of authentication data (RAND, SRES) from AuC to visited MSC
- **Weakness**
  - GSM standard only describes interfaces between network components.
  - They forgot the demand for internal encryption.
  - Microwave links are widely used for internal linkage of network components.

No encryption of internal links

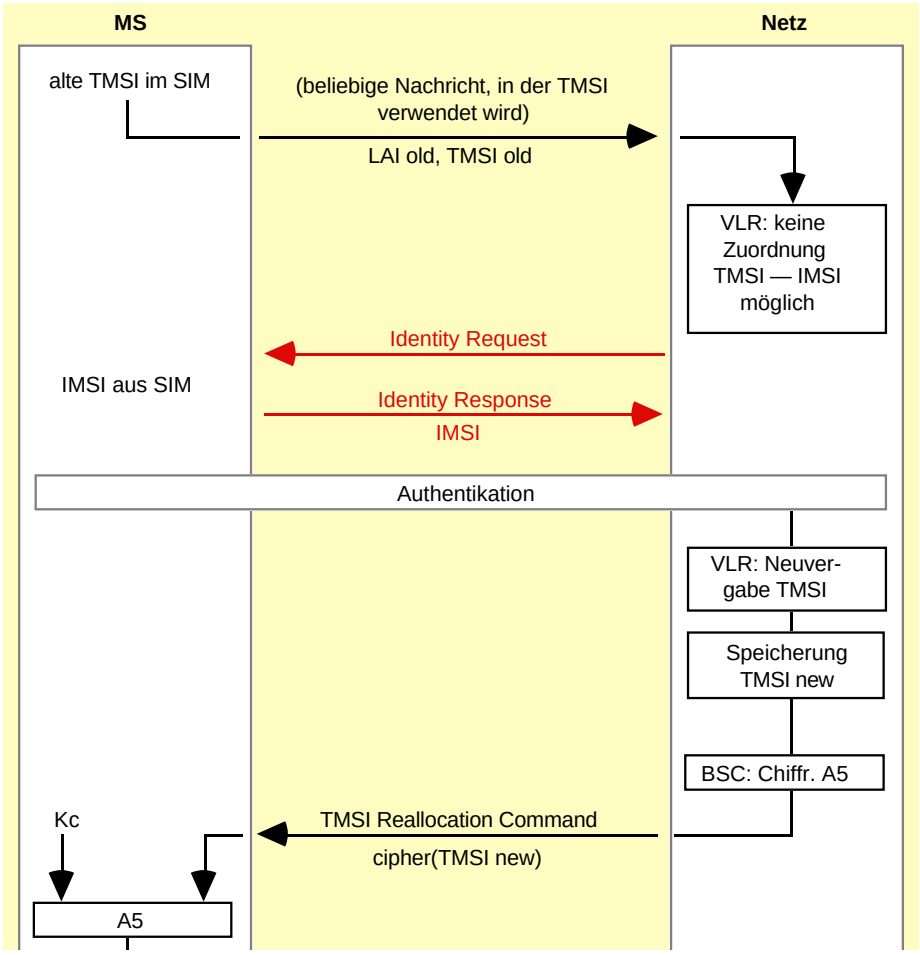


Interception of authentication data



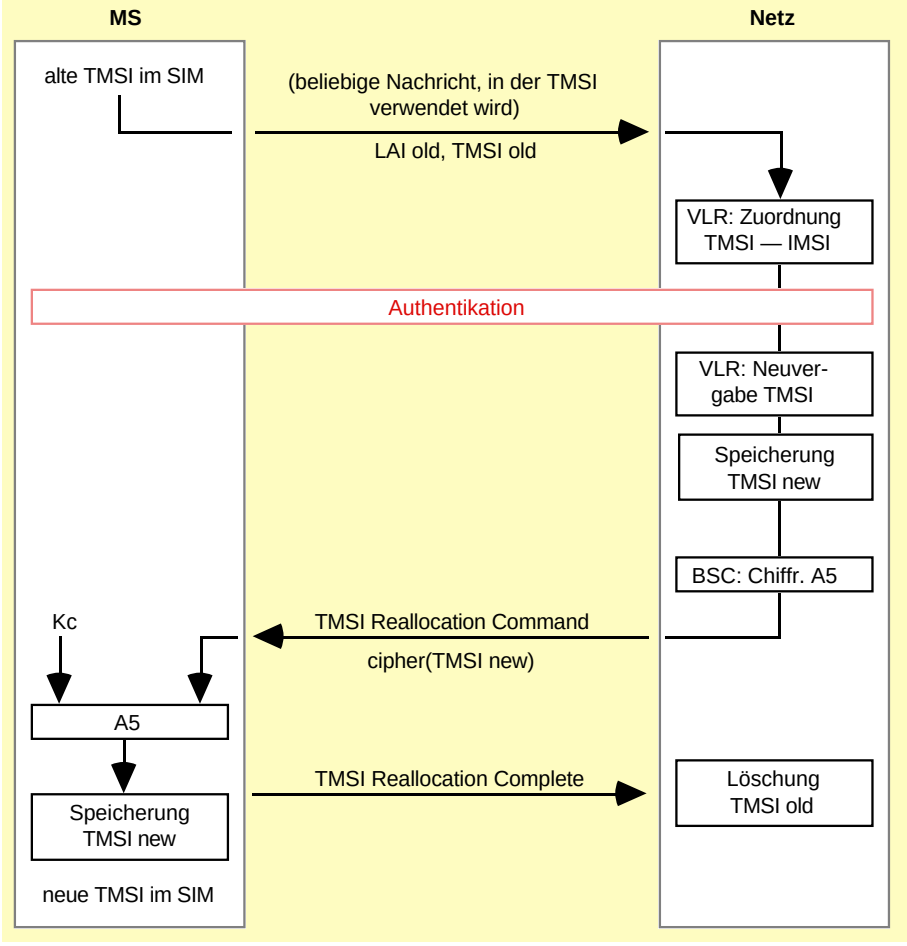
Pseudonymisierung auf der Funkschnittstelle

- ***TMSI (Temporary Mobile Subscriber Identity)***
  - soll Verkettung von Teilnehmeraktionen verhindern
  - Algorithmus zur Generierung der TMSI legt Netzbetreiber fest
  - bei erster Meldung (oder nach Fehler) wird IMSI übertragen
- ***Neuvergabe einer TMSI bei unbekannter alter TMSI***
  - Identity Request
  - ... kann jederzeit von Netz gesendet werden



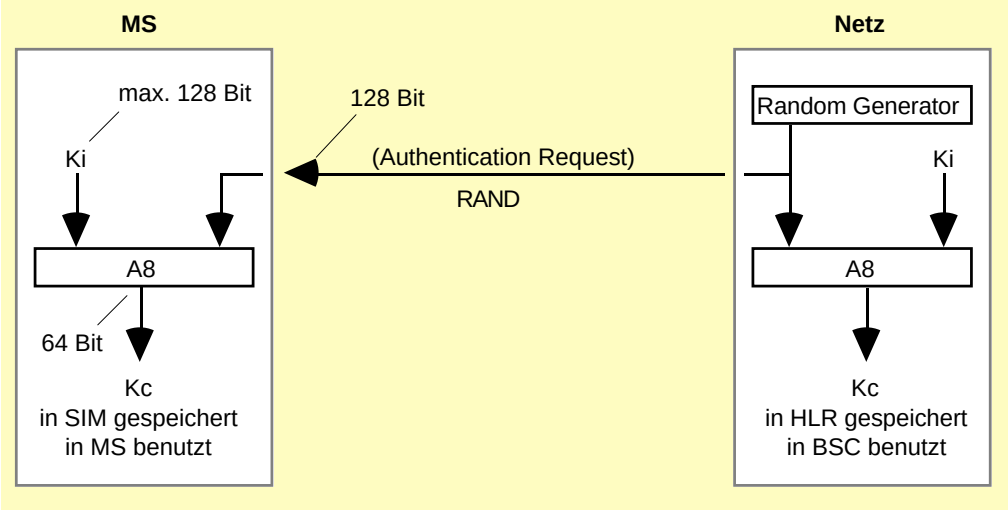
Pseudonymisierung auf der Funkschnittstelle

- ***TMSI (Temporary Mobile Subscriber Identity)***
  - soll Verkettung von Teilnehmeraktionen verhindern
  - Algorithmus zur Generierung der TMSI legt Netzbetreiber fest
  - bei erster Meldung (oder nach Fehler) wird IMSI übertragen



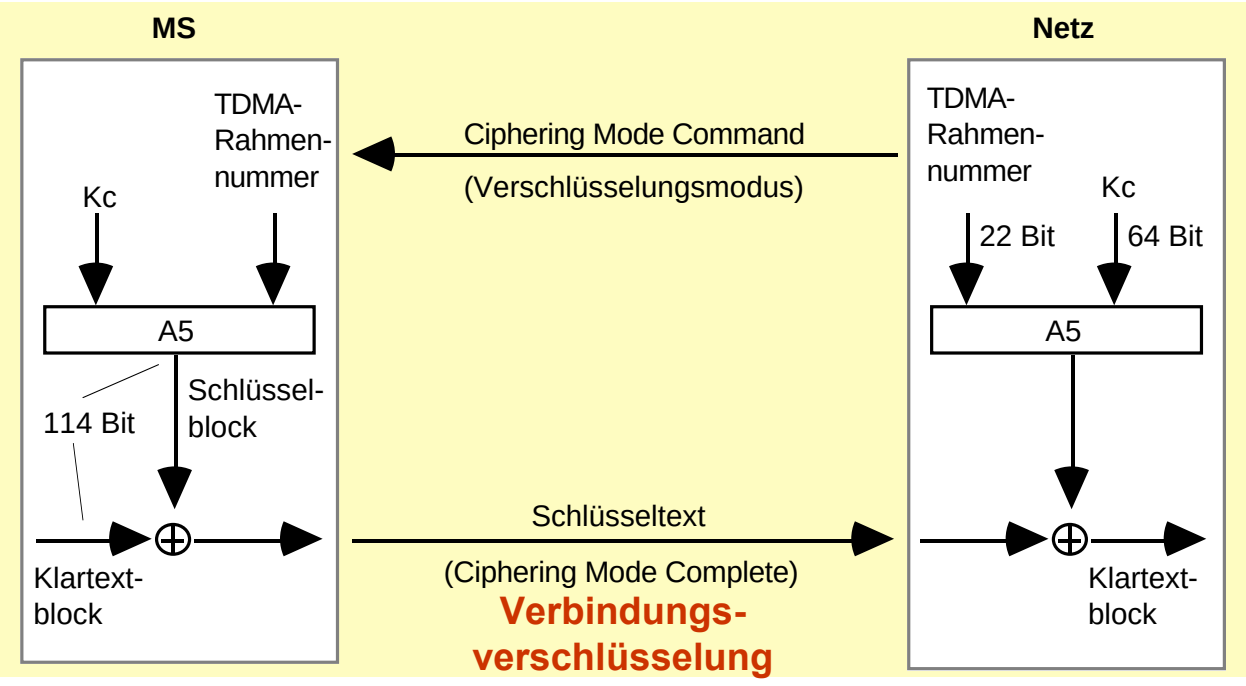
Verschlüsselung auf der Funkschnittstelle

- **Schlüsselgenerierung: Algorithmus A8**
  - auf SIM und im AuC untergebracht
  - mit Ki parametrisierte Einwegfunktion
  - nicht (europaweit, weltweit) standardisiert
  - kann vom Netzbetreiber festgelegt werden
  - Schnittstellen sind standardisiert
  - Kombination A3/A8 bekannt als COMP128



Verschlüsselung auf der Funkschnittstelle

- **Datenverschlüsselung: Algorithmus A5**
  - in der Mobilstation (nicht im SIM !) untergebracht
  - europa- bzw. weltweit standardisiert
  - schwächerer Algorithmus A5* oder A5/2 für bestimmte Staaten



Verschlüsselung auf der Funkschnittstelle

- **Ciphering Mode Command (GSM 04.08)**

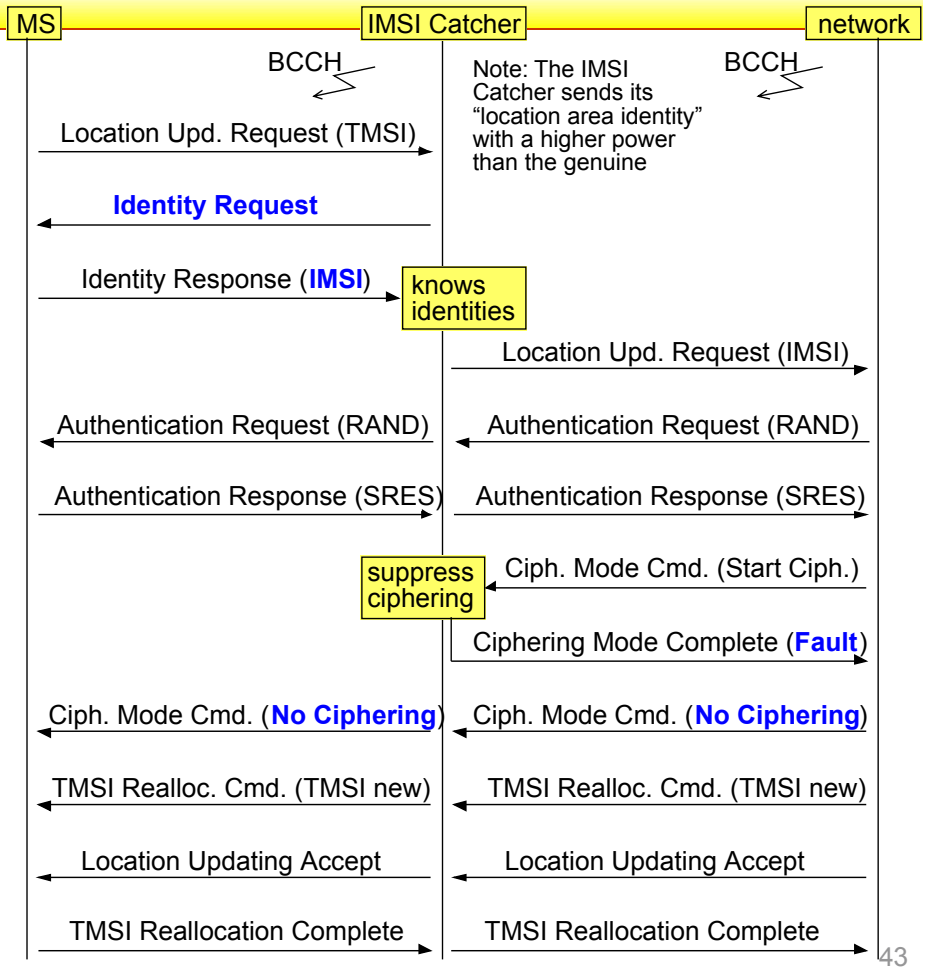
Informationselement	Länge in Bit
Protocol discriminator Transaction discriminator Message type	16
Ciphering mode setting	8

- **Cipher mode setting information element**

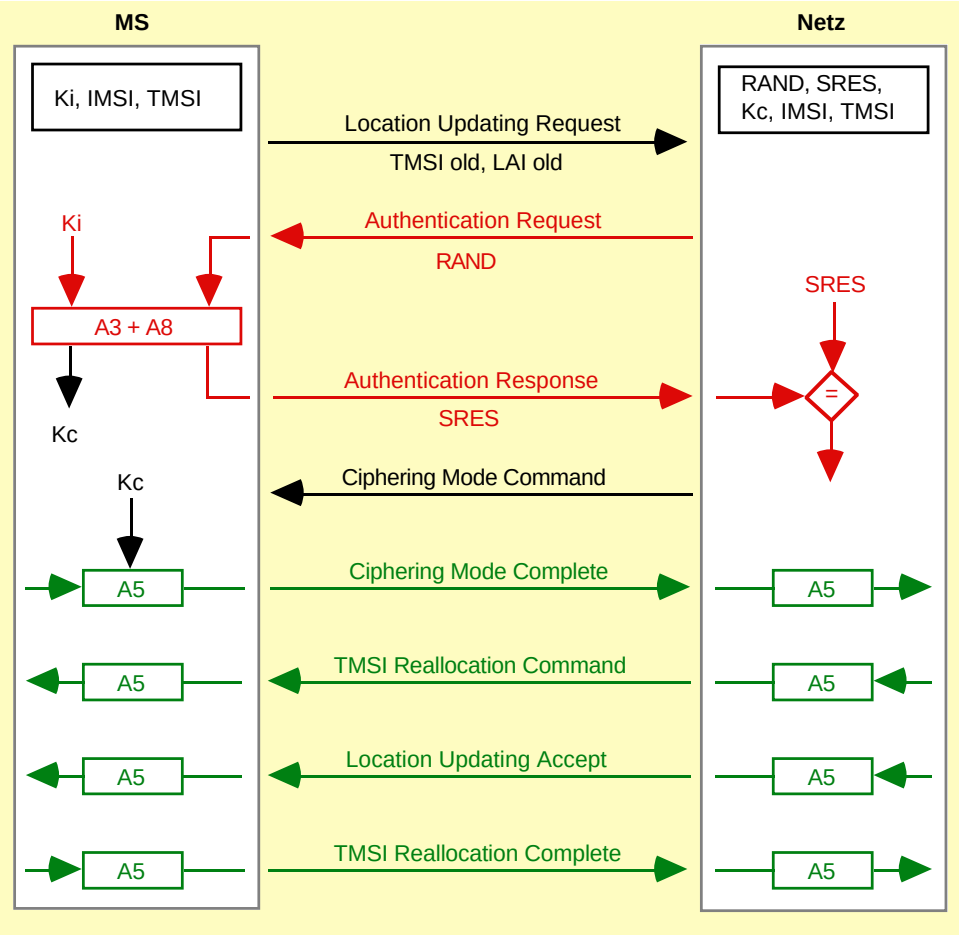
8	7	6	5	4	3	2	1	
1	0	0	1	0	0	0	SC=0	**No chiphering**
	Ciph mode set IEI			Spare	Spare	Spare	SC=1	**Start ciphering**

IMSI-Catcher

- **Scope**
  - Identities of users of a certain radio cell
  - Eavesdropping of communications
  - (Telephone at the expense of others)
- **Man-in-the-middle attack (Masquerade)**
- **Weakness**
  - No protection against malicious or faked network components

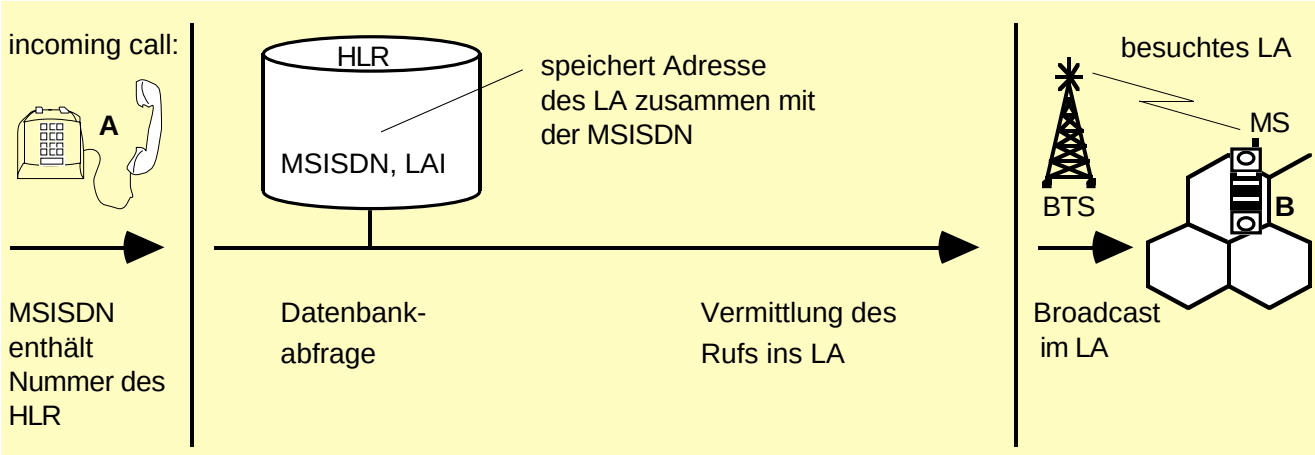


Zusammenspiel der Sicherheitsfunktionen



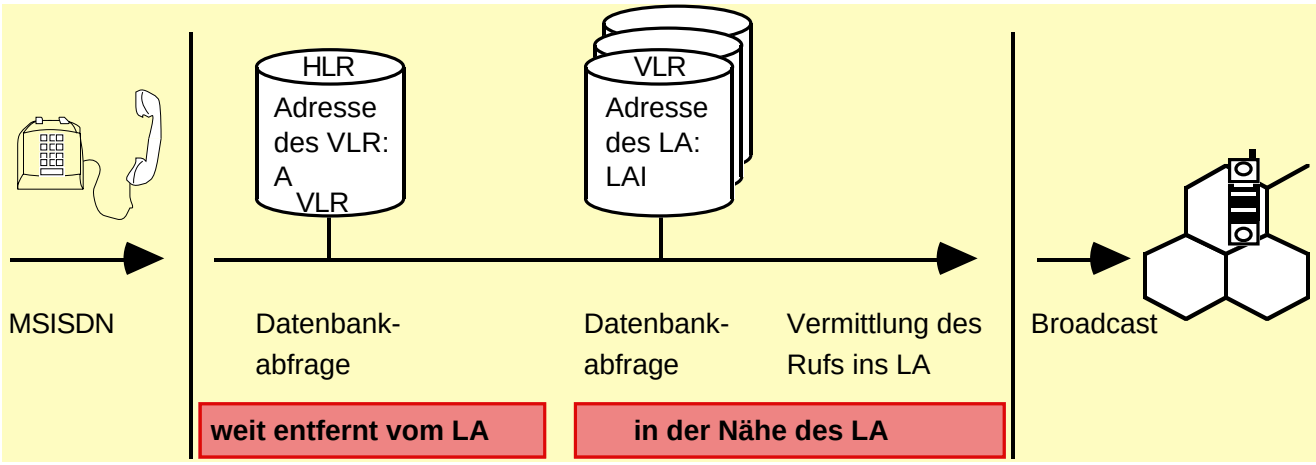
Location Management allgemein

- ***Zentral***
  - Jede Aktualisierung, d.h. Wechsel des Location Area (LA), erfordert Kommunikation mit Home Location Register (HLR)
  - Ineffizient bei großer Entfernung zwischen HLR und und aktuellem Aufenthaltsort bzw. hoher Location Update Rate (LUP-Rate)
- ***Diese Form der Speicherung wird bei Mobile IP verwendet***
  - HLR entspricht dem Home Agent



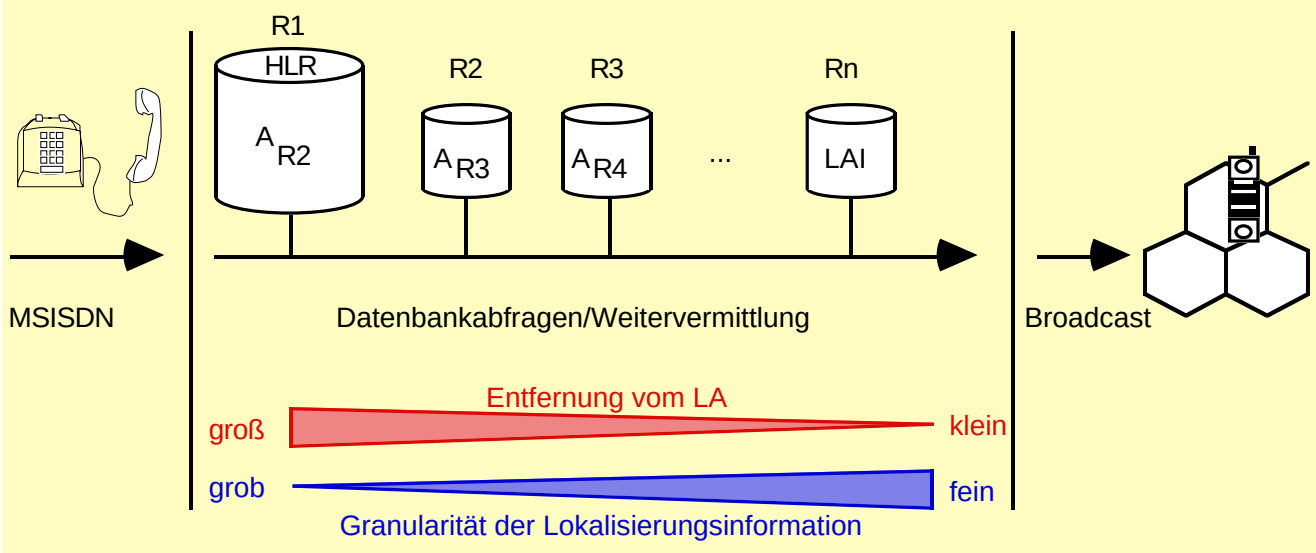
Location Management allgemein

- **Zweistufig**
  - Wechsel des LA wird dem Visitor Location Register (VLR) signalisiert
  - Ein VLR bedient einen begrenzten geographischen Bereich (VLR-Area)
  - Wechsel des VLR-Area wird dem HLR signalisiert
  - Zweck: Reduzieren der Signalisierlast im Fernbereich
  - Tradeoff: Verzögerung des Rufaufbaus (mobile terminated) durch zusätzliche Datenbankanfrage an VLR

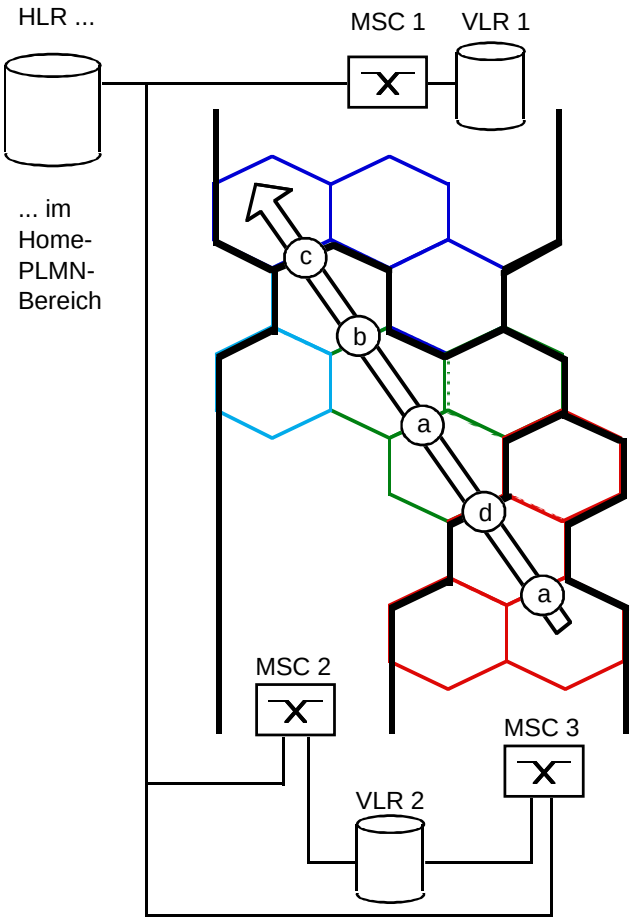


Location Management allgemein

- **Mehrstufig**
  - Verallgemeinerung des mehrstufigen Falls
  - Für Systeme der sogenannten 3. Generation vorgesehen (UMTS, FPLMTS, IMT-2000)
  - Register sind nicht zwingend hierarchisch, z.B. bei »Forwarding«



Location Update Situationen



Zeichenerklärung:

a) Wechsel der Funkzelle

b) Wechsel des LA

c) Wechsel des VLR/MSC-Bereichs

d) Wechsel des MSC-Bereichs

LA 1 (gehört zu MSC 1 und VLR 1)

LA 2 (gehört zu MSC 2 und VLR 2)

LA 3 (gehört zu MSC 2 und VLR 2)

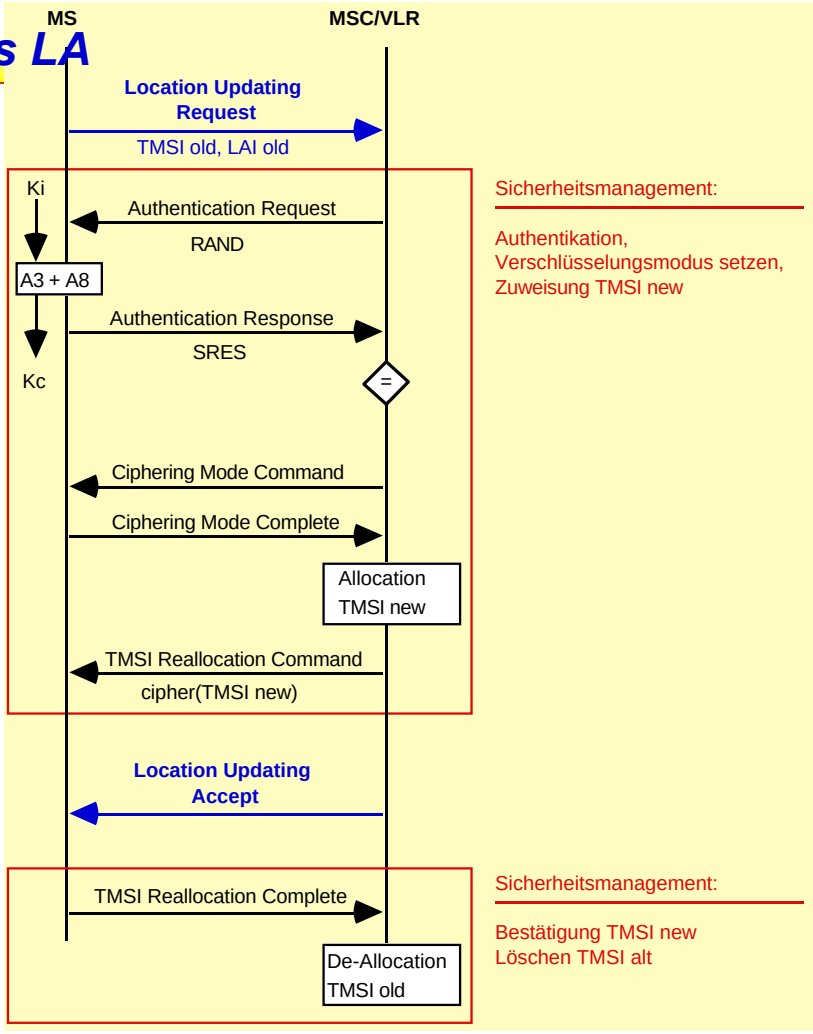
LA 4 (gehört zu MSC 3 und VLR 2)

Bewegung der MS

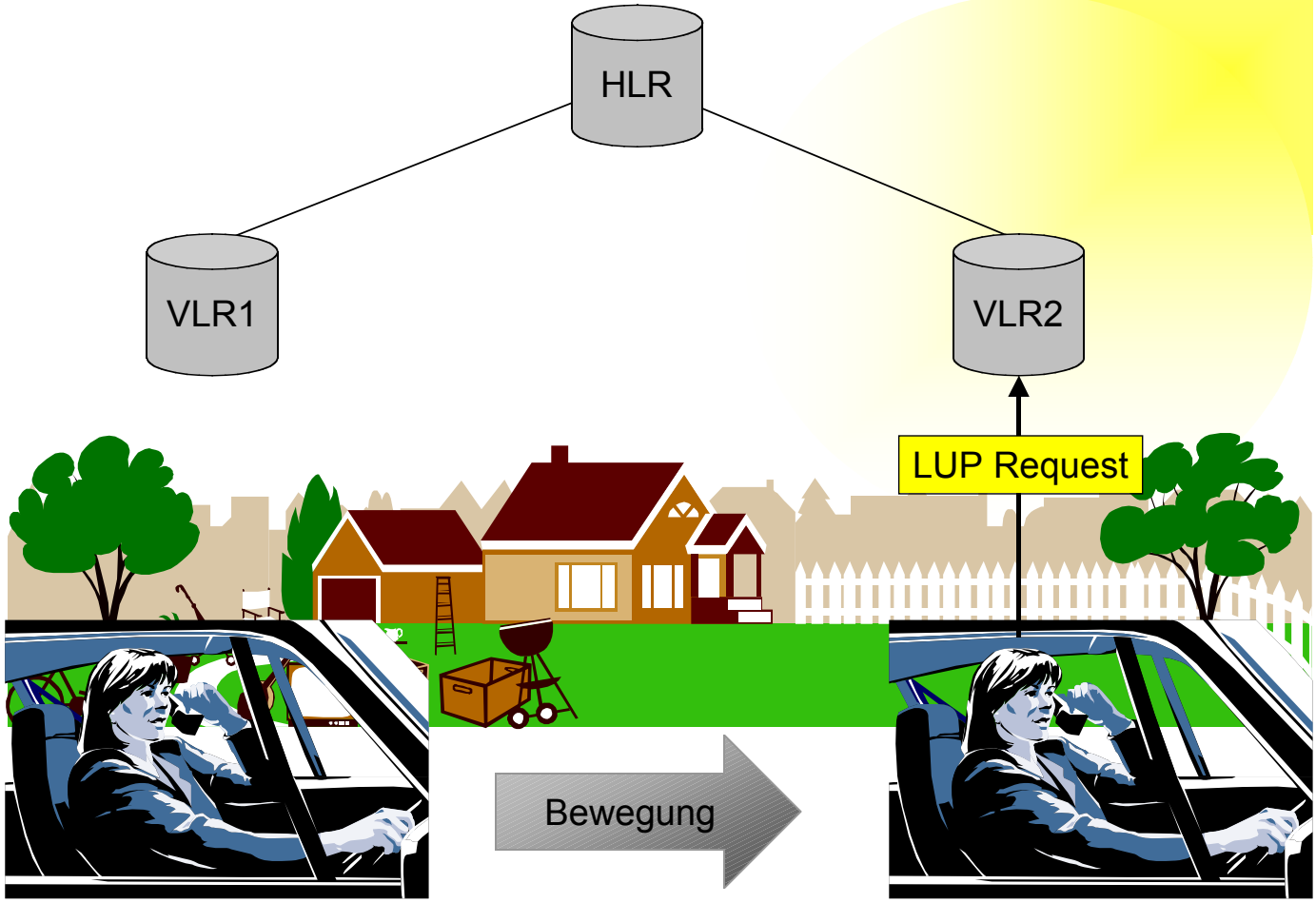
Funkzelle

Location Update: neues LA

- ***Neues LA, aber altes VLR (TMSI bekannt)***
  - Location Updating Request $(TMSI, LAI)_{old}$
  - SicherheitsImanagement
    - Authentication
    - Ciphering Mode
    - TMSI Reallocation
  - Location Updating Accept

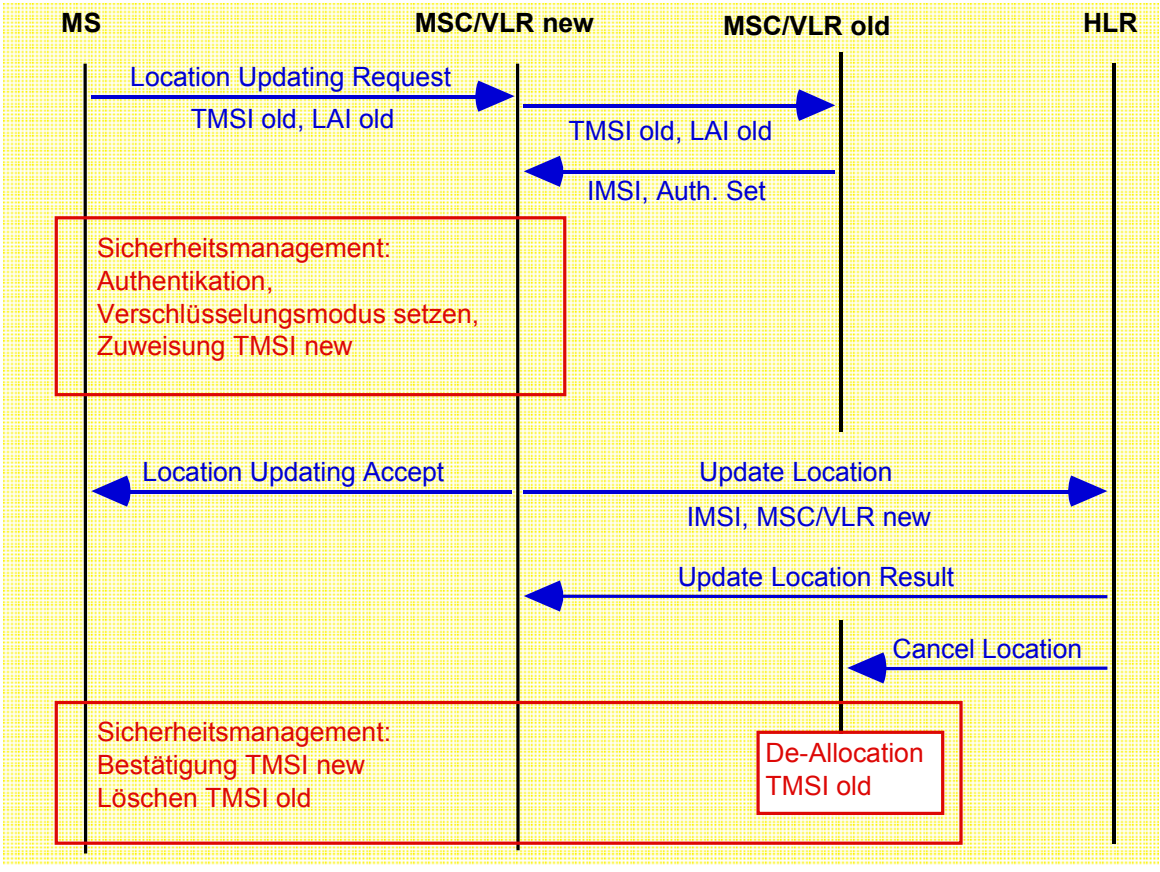


Location Update: VLR-Wechsel

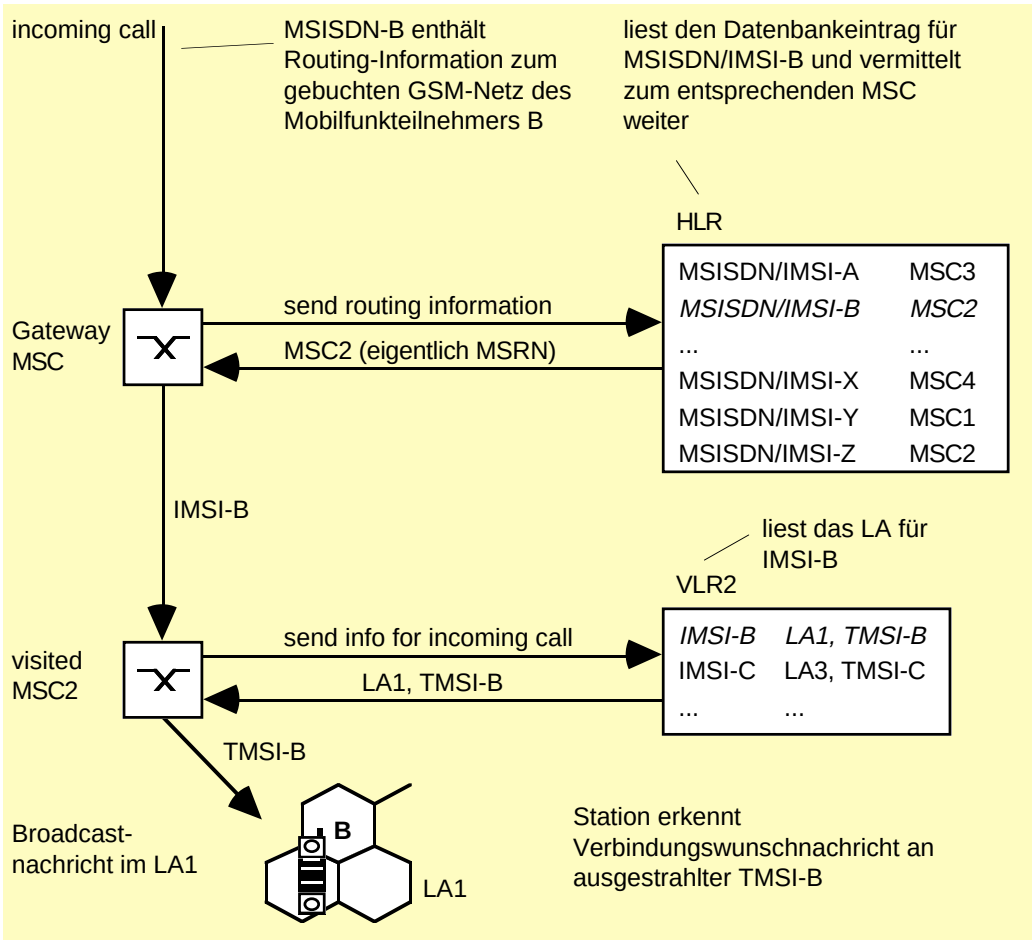


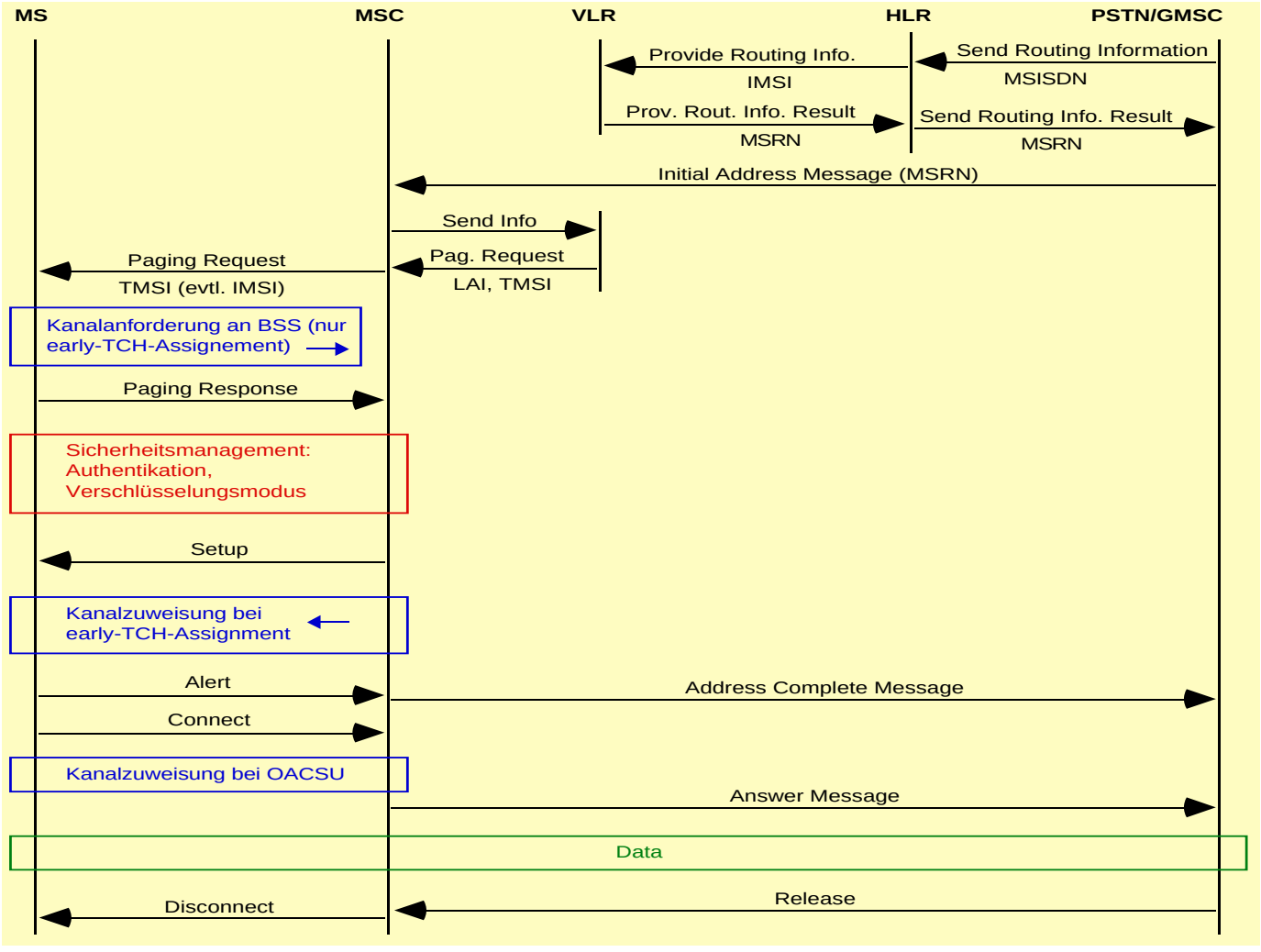
Location Update: VLR-Wechsel

- *Neues VLR (altes VLR erreichbar)*



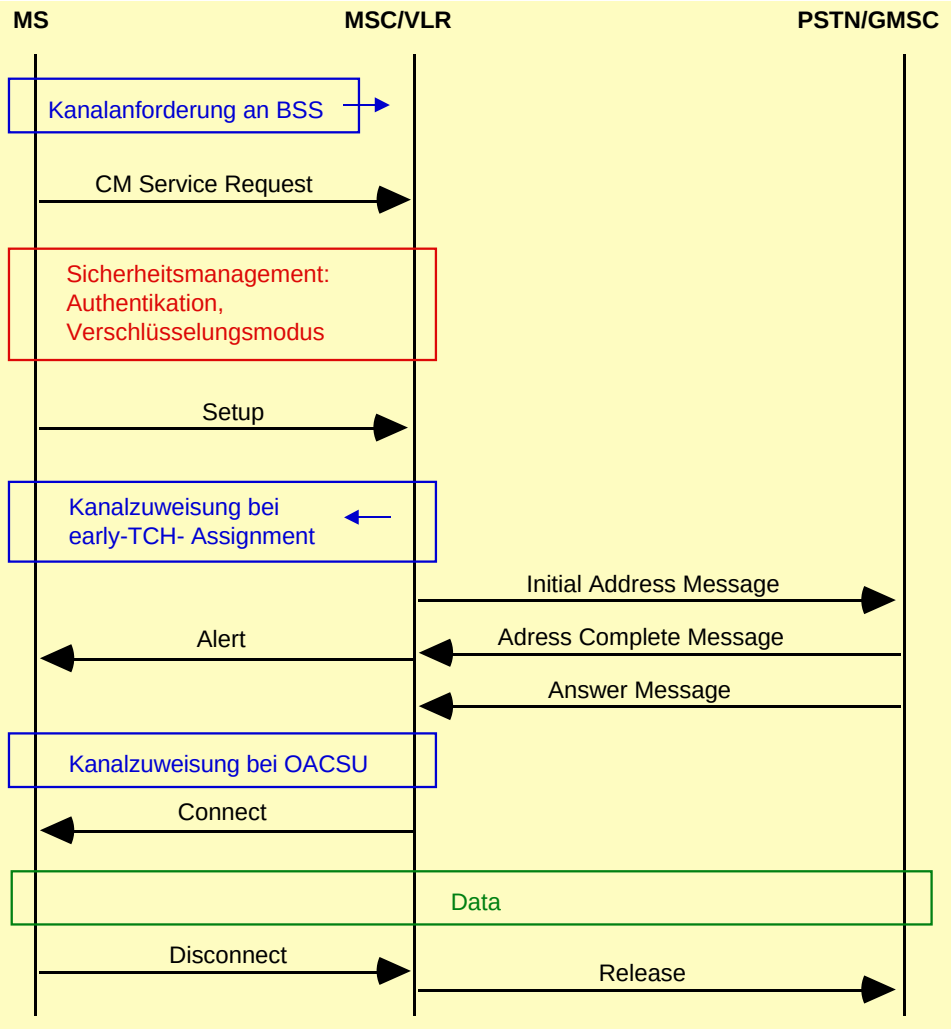
Mobile Terminated Call Setup im GSM





Mobile Originated Call Setup

- *Protokoll*



Nachrichtenaufbau GSM 04.08

8	7	6	5	4	3	2	1	
TI flag	TI value			Protocol discriminator				octet 1
0	N(SD)	Message type						octet 2
Nachrichtenelement								octet 3 …

Nachrichtenaufbau GSM 04.08

- **Protocol discriminator**

4 3 2 1	bit number
0 0 1 1	call control, packet-mode, connection control and call related SS msgs
0 1 0 1	mobility management messages
0 1 1 0	radio resources management messages
1 0 0 1	short message service messages
1 0 1 1	non call related SS messages
1 1 1 1	reserved for tests procedures

All other values are reserved

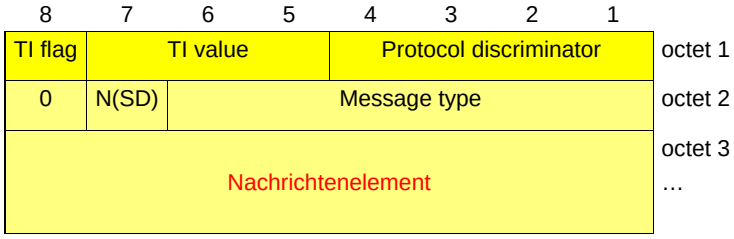
- **Transaction identifier (TI)**

dient zur Unterscheidung paralleler Aktivitäten einer MS

8	bit number = TI flag
0	message sent from the originated TI side
1	message sent to the originated TI side

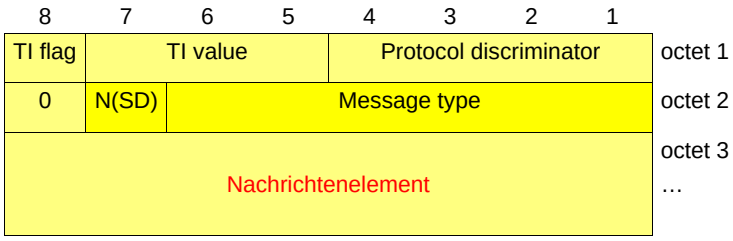
- **TI value**

Zahl von 000…110 (bin:0…6)
111 reserviert



Message type

- **Identifiziert die Funktion der Nachricht**
- **3 Klassen:**
  - radio ressources management
  - mobility management
  - call control
- **N(SD)**
  - Sequenznummer bzw. Extension Bit



Message type (1)

- *Radio ressources management*

```
8 7 6 5 4 3 2 1        bit number
-----------------------------------------------------
0 0 1 1 1 - - - Channel establishment messages
          0 1 1        ADDITIONAL ASSIGNMENT
          1 1 1        IMMEDIATE ASSIGNMENT
          0 0 1        IMMEDIATE ASSIGNMENT EXTENDED
          0 1 0        IMMEDIATE ASSIGNMENT REJECT
0 0 1 1 0 - - - Ciphering messages
          1 0 1        CIPHERING MODE ASSIGNEMT
          0 1 0        CIPHERING MODE COMPLETE
0 0 1 0 1 - - - Handover messages
          1 1 0        ASSIGNEMT COMMAND
          0 0 0        ASSIGNEMT COMPLETE
          1 1 1        ASSIGNMENT FAILURE
          0 1 1        HANDOVER COMMAND
          1 0 0        HANDOVER COMPLETE
          0 0 0        HANDOVER FAILURE
          1 0 1        PHYSICAL INFORMATION
0 0 0 0 1 - - - Channel release messages
          1 0 1        CHANNEL RELEASE
          0 1 0        PARTIAL RELEASE
          1 1 1        PARTIAL RELEASE COMPLETE
0 0 1 0 0 - - - Paging messages
          0 0 1        PAGING REQUEST TYPE 1
          0 1 0        PAGING REQUEST TYPE 2
          1 0 0        PAGING REQUEST TYPE 3
          1 1 1        PAGING RESPONSE
0 0 0 1 1 - - - System information messages
          0 0 1        SYSTEM INFORMATION TYPE 1
          0 1 0        SYSTEM INFORMATION TYPE 2
          0 1 1        SYSTEM INFORMATION TYPE 3
          1 0 0        SYSTEM INFORMATION TYPE 4
          1 0 1        SYSTEM INFORMATION TYPE 5
          1 1 0        SYSTEM INFORMATION TYPE 6
0 0 0 1 0 - - - Miscellaneous messages
          0 0 0        CHANNEL MODE MODIFY
          0 1 0        RR-STATUS
          1 1 1        CHANNEL MODE MODIFY ACKNOWLEDGE
          1 0 0        FREQUENCY REDEFINITION
          1 0 1        MEASUREMENT REPORT
          1 1 0        CLASSMARK CHANGE
```


Message type (2)

- *Mobility management*
  - Bits 7 und 8 („00“) reserviert als extension bits
  - Bit 7:
    - nur mobile originated: „1“, falls Sequenznummer gesendet wird

```
8 7 6 5 4 3 2 1      bit number
-----------------------------------------------
0 x 0 0 - - - - Registration messages
        0 0 0 1      IMSI DETACH INDICATION
        0 0 1 0      LOCATION UPDATING ACCEPT
        0 1 0 0      LOCATION UPDATING REJECT
        1 0 0 0      LOCATION UPDATING REQUEST
0 x 0 1 - - - - Security messages
        0 0 0 1      AUTHENTICATION REJECT
        0 0 1 0      AUTHENTICATION REQUEST
        0 1 0 0      AUTHENTICATION RESPONSE
        1 0 0 0      IDENTITY REQUEST
        1 0 0 1      IDENTITY RESPONSE
        1 0 1 0      TMSI REALLOCATION COMMAND
        1 0 1 1      TMSI REALLOCATION COMPLETE
0 x 1 0 - - - - Connection management messages
        0 0 0 1      CM SERVICE ACCEPT
        0 0 1 0      CM SERVICE REJECT
        0 1 0 0      CM SERVICE REQUEST
        1 0 0 0      CM REESTABLISHMENT REQUEST
0 x 1 1 - - - - Connection management messages
        0 0 0 1      MM STATUS
```

Message type (3)

- **Call control**
  - Bei nationalen Nachrichten folgt in den nächsten Oketts der eigentliche Nachrichtentyp
  - Bits 7 und 8 („00“) reserviert als extension bits
  - Bit 7:
    - nur mobile originated: „1“, falls Sequenznummer gesendet wird

```
8 7 6 5 4 3 2 1     bit number
----------------------------------------
0 x 0 0 0 0 0 0     Escape to nationally
                    specific message types
0 x 0 0 – – – – Call establishment messages
        0 0 0 1     ALERTING
        1 0 0 0     CALL CONFIRMED
        0 0 1 0     CALL PROCEEDING
        0 1 1 1     CONNECT
        1 1 1 1     CONNECT ACKNOWLEDGE
        1 1 1 0     EMERGENCY SETUP
        0 0 1 1     PROGRESS
        0 1 0 1     SETUP
0 x 0 1 – – – – Call information phase
messages
        0 1 1 1     MODIFY
        1 1 1 1     MODIFY COMPLETE
        0 0 1 1     MODIFY REJECTED
        0 0 0 0     USER INFORMATION
0 x 1 0 – – – – Call clearing messages
        0 1 0 1     DISCONNECT
        1 1 0 1     RELEASE
        1 0 1 0     RELEASE COMPLETE
0 x 1 1 – – – – Miscellaneous messages
        1 0 0 1     CONGESTION CONTROL
        1 1 1 0     NOTIFY
        1 1 0 1     STATUS
        0 1 0 0     STATUS ENQUIRY
        0 1 0 1     START DTMF
        0 0 0 1     STOP DTMF
        0 0 1 0     STOP DTMF ACKNOWLEDGE
        0 1 1 0     START DTMF ACKNOWLEDGE
        0 1 1 1     START DTMF REJECT
```

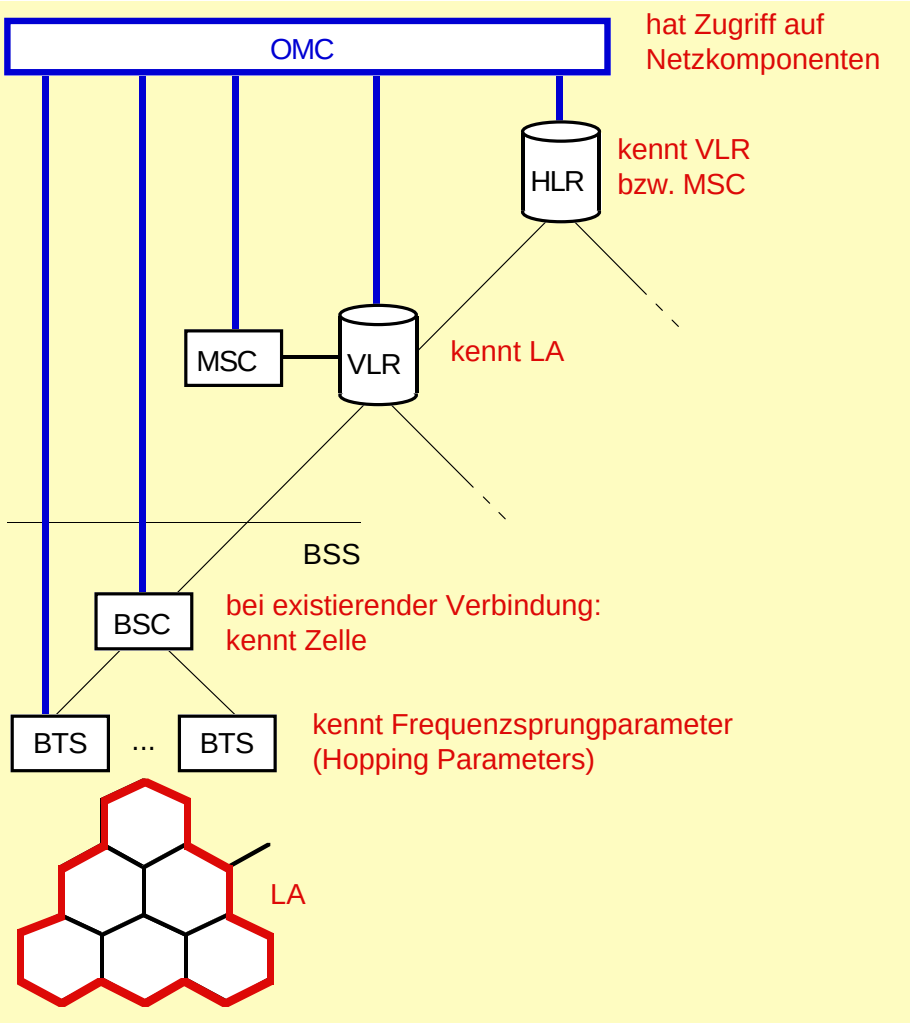

Bewegungs-profile im GSM

Möglich durch:

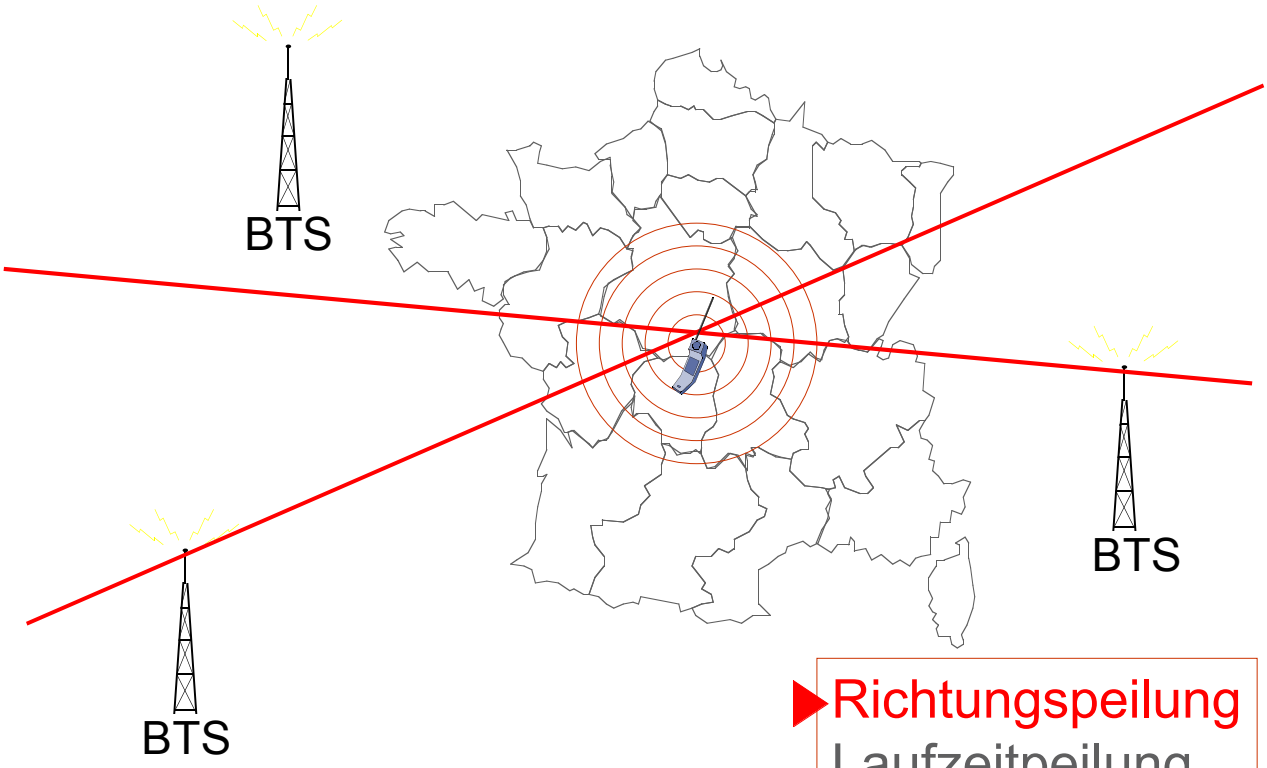
1. Abfrage der gespeicherten Daten (“Fernwartung”)
2. Peilung

Auswege:

1. Datenschutzfreund-liches Location Management
2. Direct Sequence Spread Spectrum

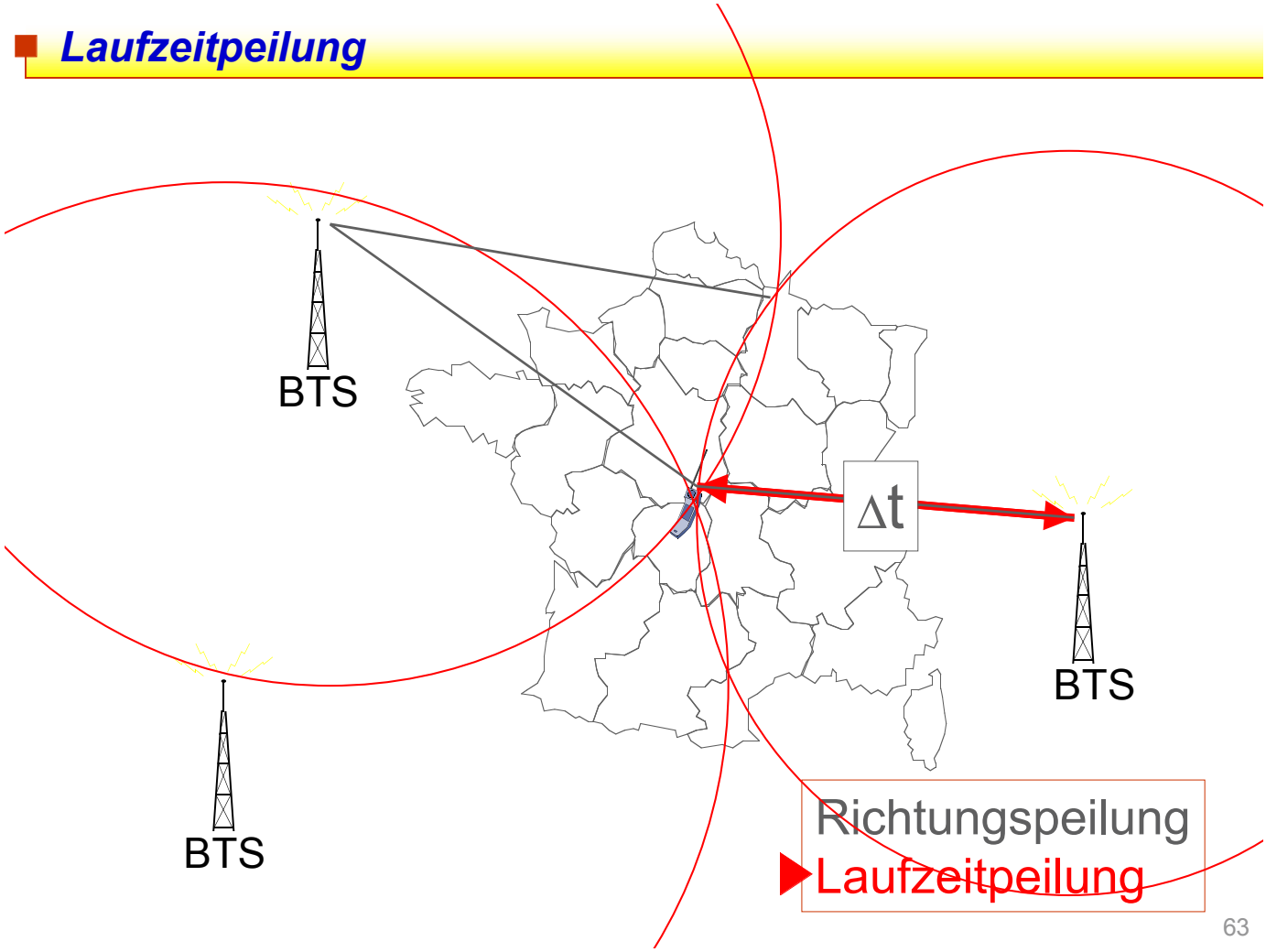


Richtungspeilung



Richtungspeilung
Laufzeitpeilung

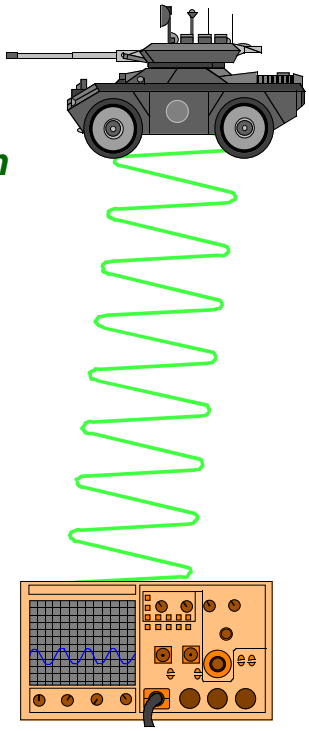
Laufzeitpeilung



Richtungspeilung
Laufzeitpeilung

Spread Spectrum Systems

- ***Exkurs:***
  - Funktechnik
  - insbesondere militärischer Bereich



- ***Funkkontakt zwischen verschiedenen militärischen Einheiten***
  - Sendung auf einer bestimmten Frequenz f_0 mit einer bestimmten Bandbreite B

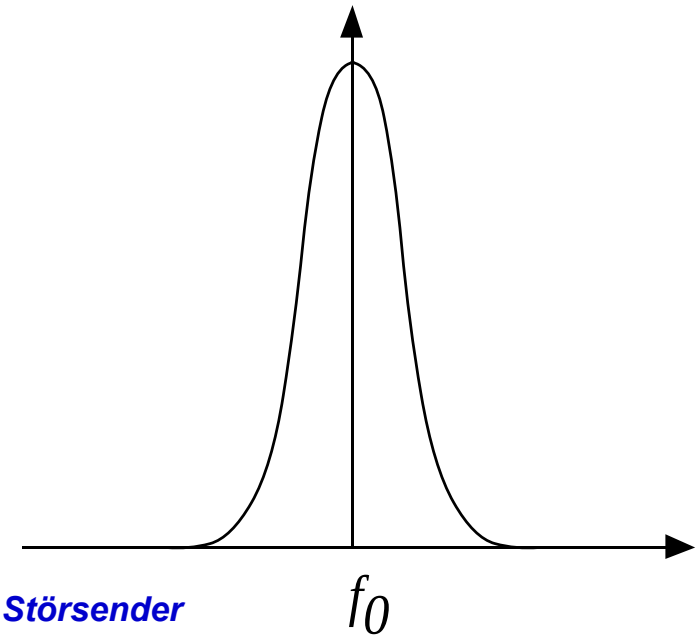
- ***Problem:***
  - deutliche Energiezunahme im Spektrum um f_0 herum

Schmalbandiges Senden

- ***Folgen:***

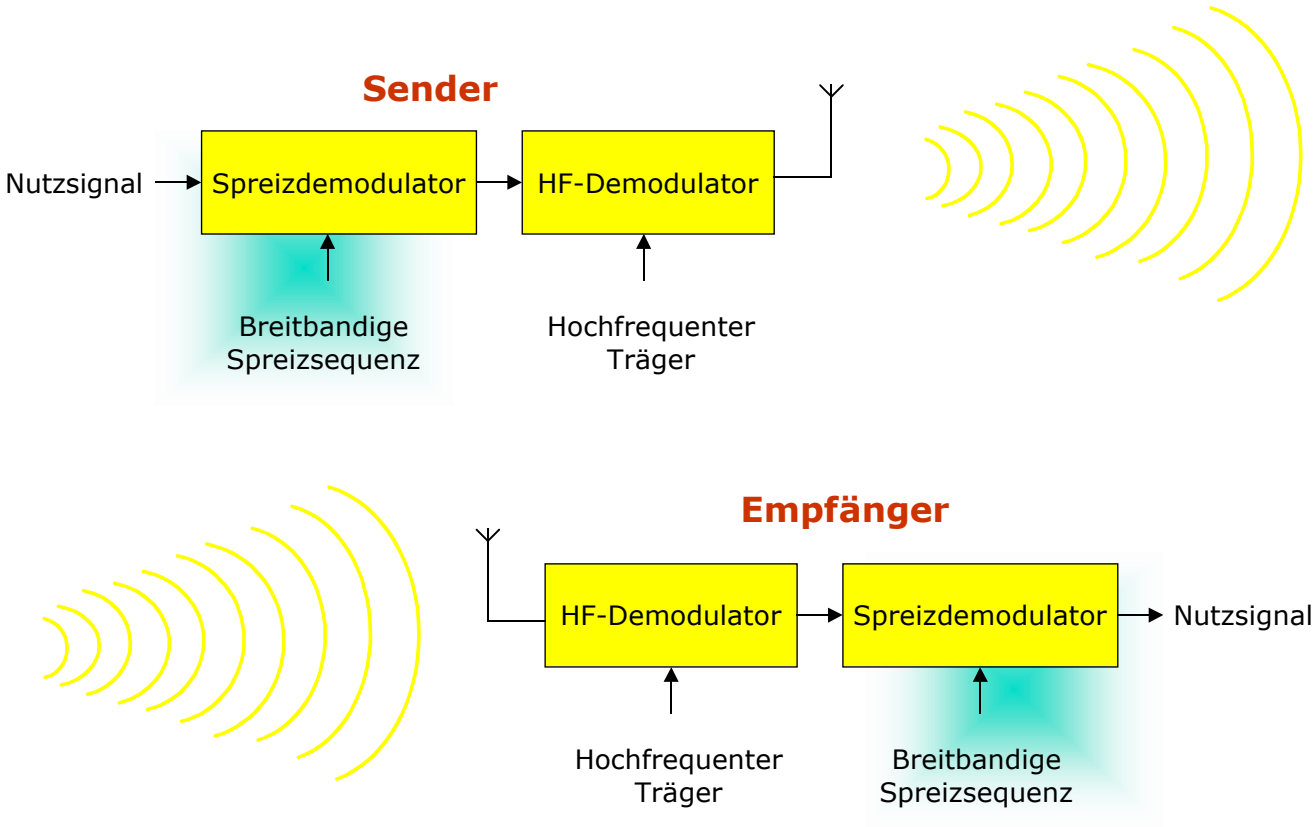
- ***Beobachtbarkeit des Sendens***
  - Spektrumanalysator registriert Energiezunahme

- ***Peilbarkeit des Senders***
  - da die elektromagnetischen Wellen Richtungsinformation in sich tragen

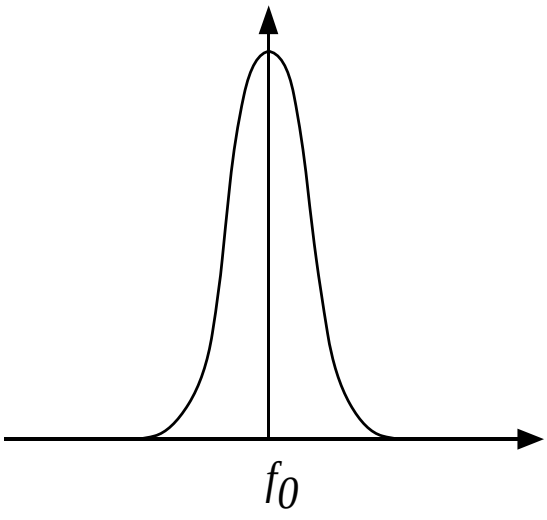


- ***Gegner kann Kommunikation mit Störsender verhindern***

Übertragungsmodell beim Bandspreizverfahren

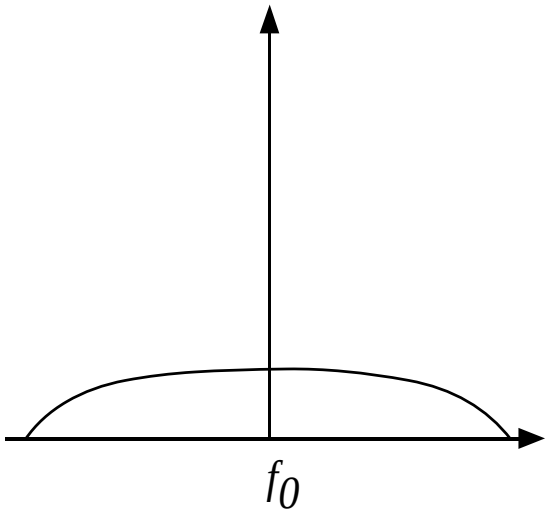


Spreizung



- ***Schmalbandiges Nutzsignal vor der Spreizung***
- ***Modulation mit breitbandiger Spreizsequenz:***
  - spezielle Funktionen (z.B. Walsh-Funktionen)
  - Pseudo-Noise-Sequence (PN-Code)

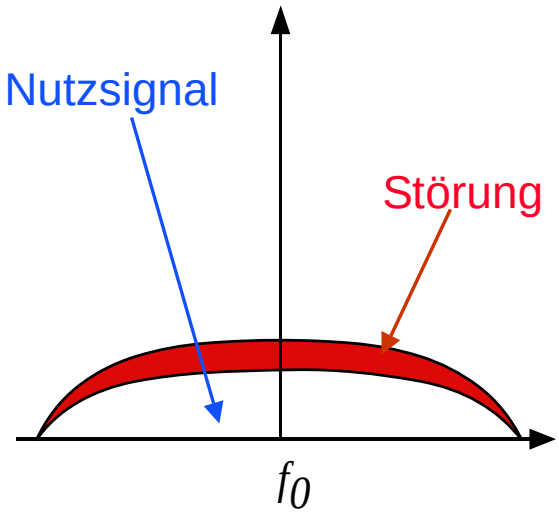
Spreizung



- *Schmalbandiges Nutzsignal vor der Spreizung*
- *Modulation mit breitbandiger Spreizsequenz:*
  - spezielle Funktionen (z.B. Walsh-Funktionen)
  - Pseudo-Noise-Sequence (PN-Code)
- ***Spektrale Spreizung***
- ***Verteilung der Energie auf ein großes Frequenzspektrum***

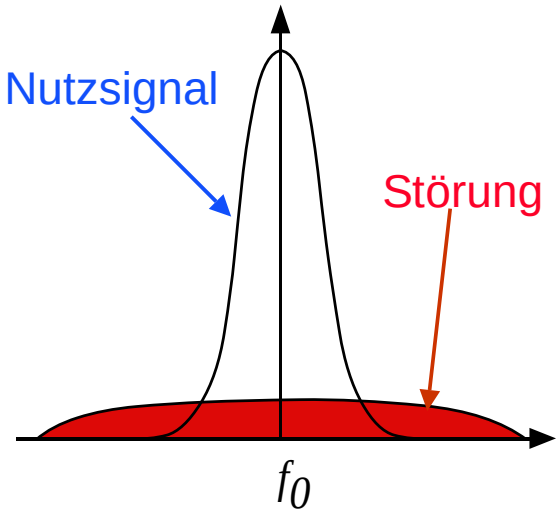
Despreizung

- ***gespreiztes Nutzsignal mit überlagerter Störung***



Despreizung

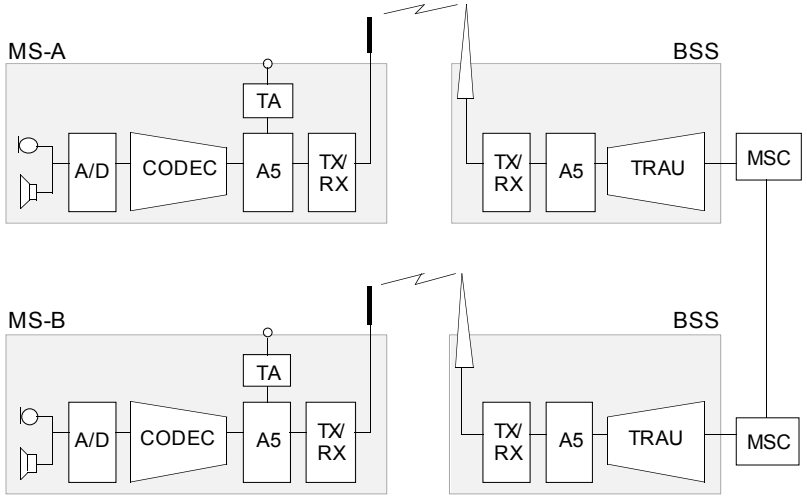
- *gespreiztes Nutzsignal mit überlagerter Störung*



- *Spektrale Spreizung der Störung*
- *despreiztes Nutzsignal*

Fehlende Ende-zu-Ende-Dienste

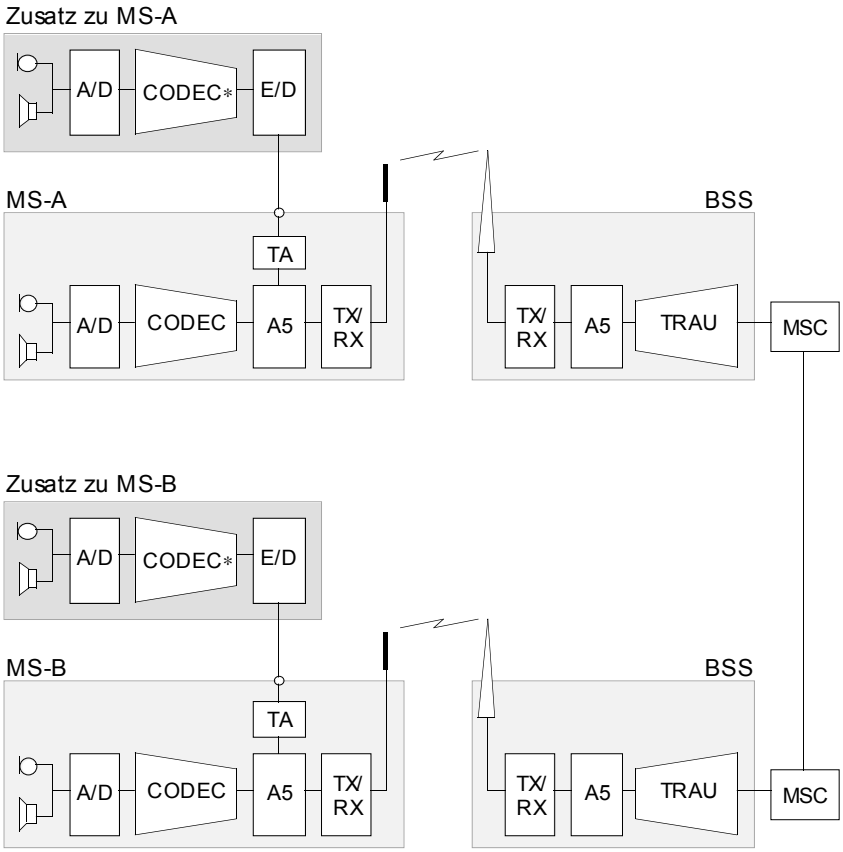
- *In GSM existieren keine bittransparenten Sprachkanäle*
  - Sprache wird vor Verschlüsselung verlustbehaftet komprimiert
  - Keine Ende-zu-Ende-Verschlüsselung realisierbar
- *Übertragungsweg im GSM (schematisch)*



MS	Mobile Station	A5	Verbindungsverschlüsselung
BSS	Base Station Subsystem	TX/RX	Transmitter/Receiver
A/D	Analog-Digital-Umsetzer	TRAU	Transcoder/Rate Adaption Unit
CODEC	Sprachcodierbaustein	MSC	Mobile Switching Centre
TA	Terminal Adaption		

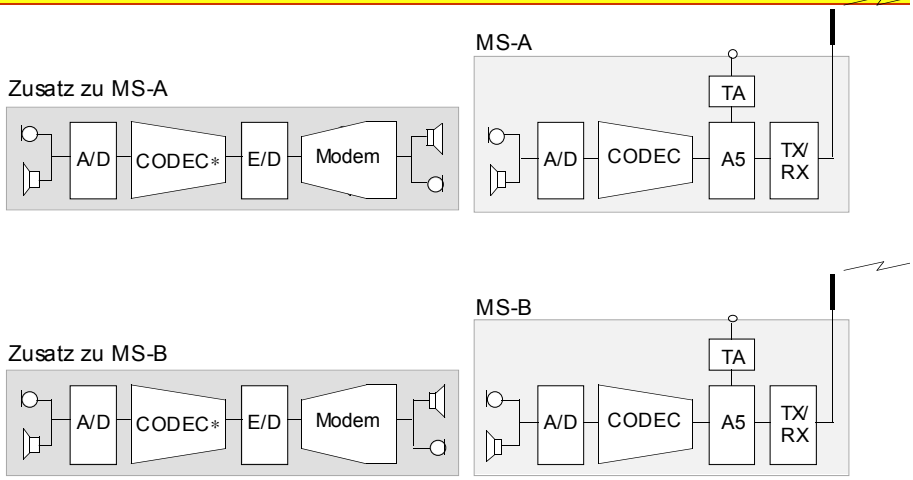
Optionen f.d. nachträgliche Realisierung von EzE-Diensten

- **Nutzung des bittransparenten Datenkanals**

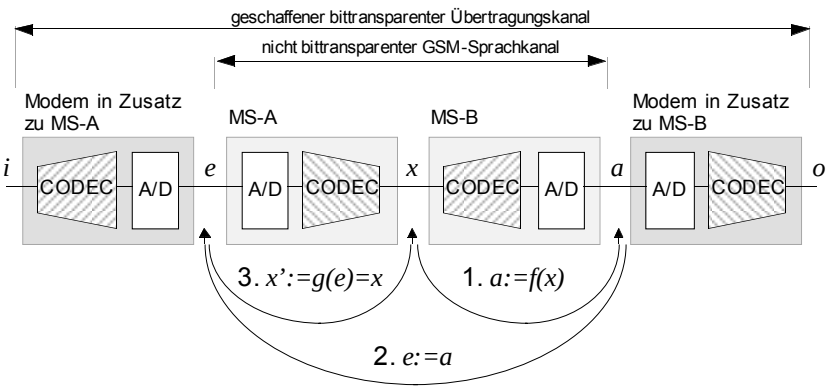


Optionen f.d. nachträgliche Realisierung von EzE-Diensten

- **Ergänzung des Signallaufs durch Modems**

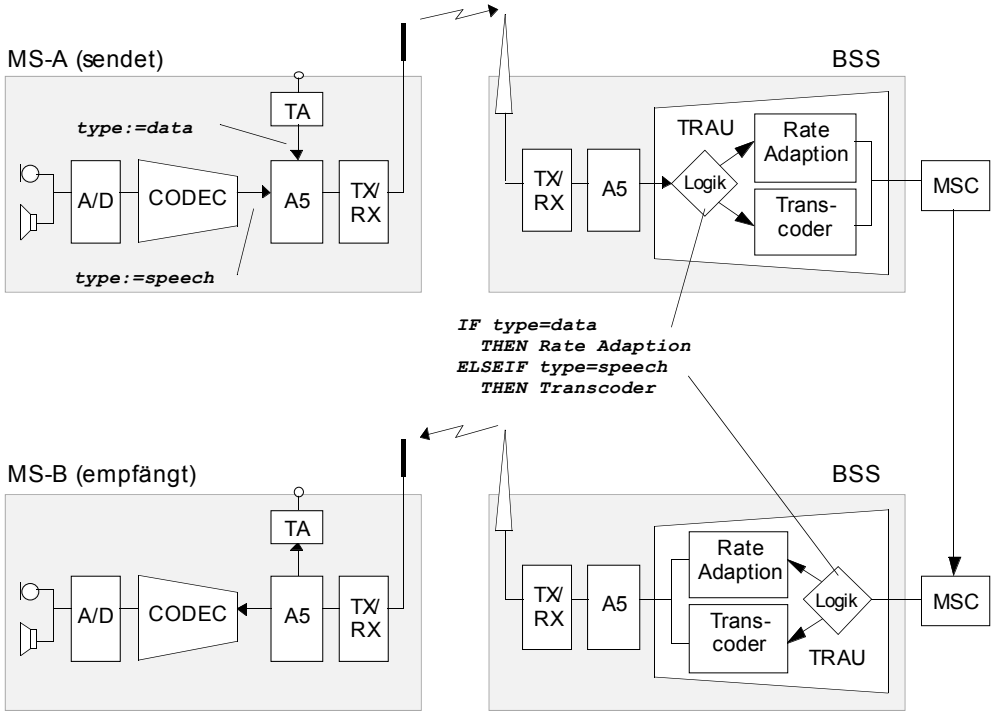


- **Kanalanpassung der Modems**



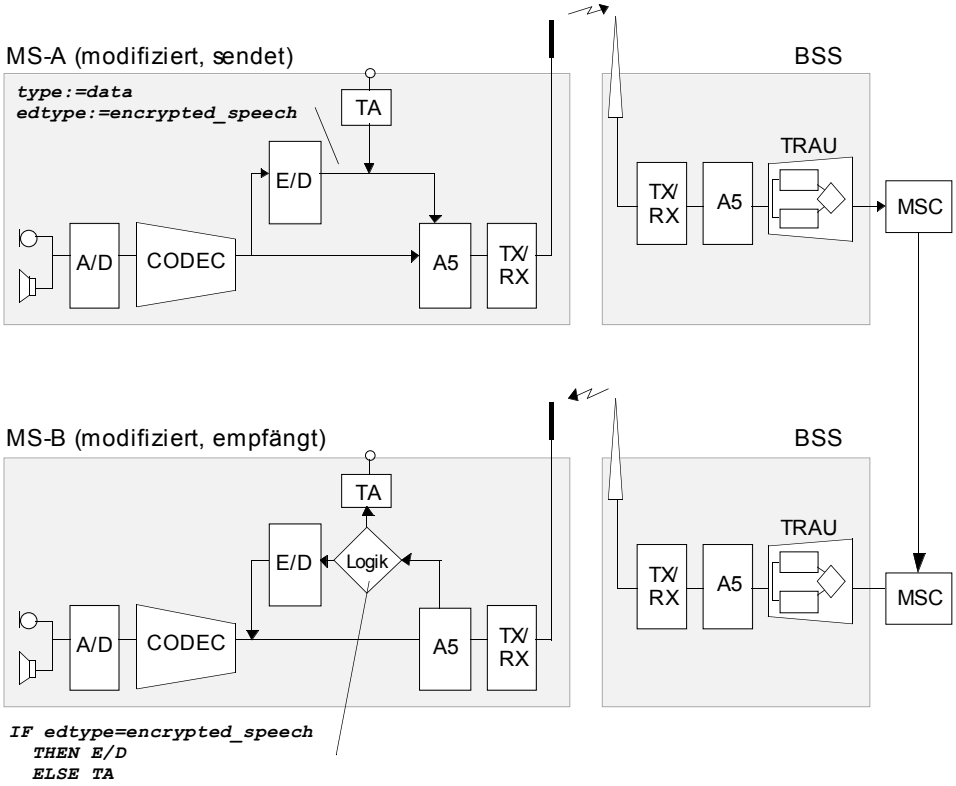
Optionen f.d. nachträgliche Realisierung von EzE-Diensten

- **Signalisierung des Datentyps (Sprache, Daten) im GSM (schematisch)**



Optionen f.d. nachträgliche Realisierung von EzE-Diensten

- **Sprachübertragung mit modifizierten Mobilstationen**



Zusammenfassung der Sicherheitsprobleme

- ***Krtitk an GSM (I)***
  - Vertraulichkeit des Ortes nur gegen Outsider und dort noch sehr schwach
  - Peilbarkeit von mobilen Stationen möglich
  - keine bittransparenten Sprachkanäle vorhanden, deshalb keine Ende-zu-Ende-Verschlüsselung möglich.
  - keine Ende-zu-Ende-Authentikation vorgesehen
  - keine gegenseitige Authentikation vorgesehen
  - Kryptoalgorithmen sind teilweise geheim gehalten
  - Kryptoalgorithmen sind ausschließlich symmetrisch
  - Schlüsselerzeugung und -verwaltung nicht unter Kontrolle der Teilnehmer

Zusammenfassung der Sicherheitsprobleme

- ***Krtitk an GSM (II)***
  - keine anonyme Netzbenutzung möglich
  - Vertrauen in korrekte Abrechnung ist nötig
  - keine Erreichbarkeitsmanagementfunktionen vorhanden
- ***Auswege***
  - Modifikation des Location Managements
  - Verhinderung von Peilung und Ortung durch funktechnische, informationstechnische und kryptographische Maßnahmen
  - Definition von Ende-zu-Ende-Diensten
  - Unterstützung asymmetrischer Kryptographie

Universal mobile telecommunication system (UMTS)

- ***Security functions of UMTS …***

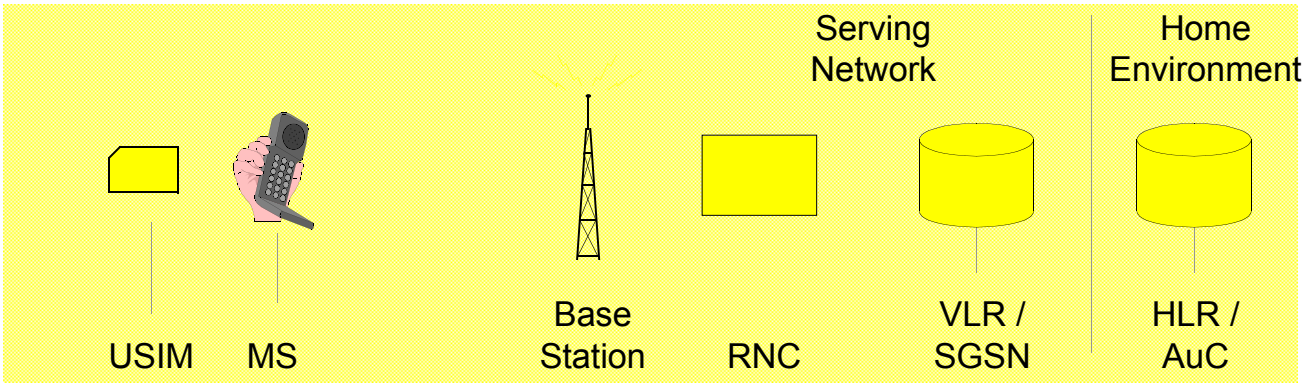
  … have been »inspired« by GSM security functions

- ***From GSM***
  - Subscriber identity confidentiality (TMSI)
  - Subscriber authentication
  - Radio interface encryption
  - SIM card (now called USIM)
  - Authentication of subscriber towards SIM by means of a PIN
  - Delegation of authentication to visited network
  - No need to adopt standardized authentication algorithms

- ***Additional UMTS security features***
  - Enhanced UMTS authentication and key agreement mechanism
  - Integrity protection of signaling information (prevents false-base-station attacks)
  - New ciphering / key agreement / integrity protection algorithms

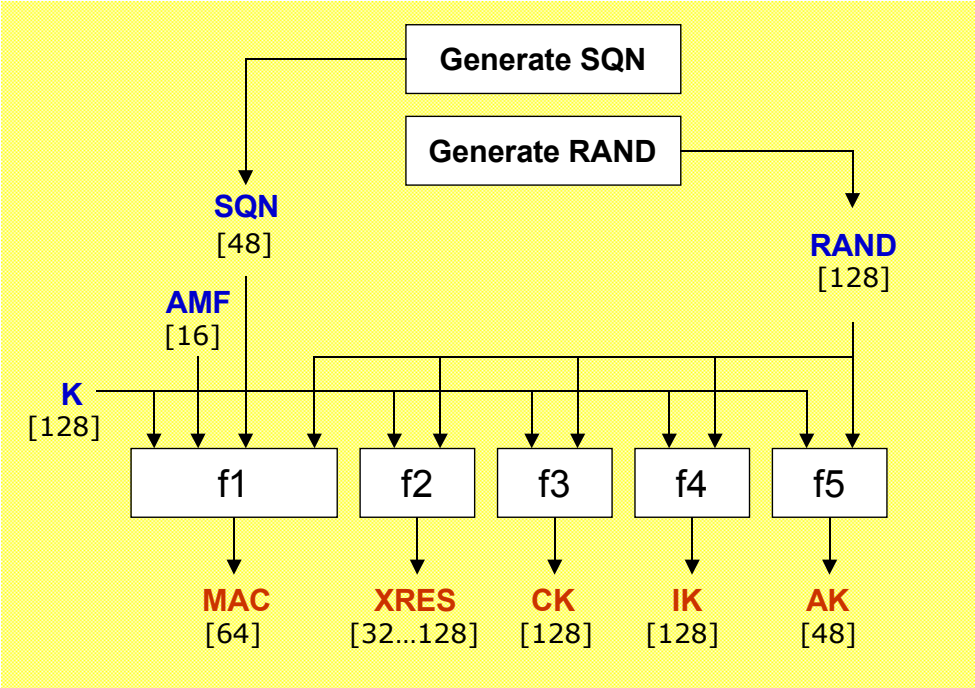
  … and a few minor features

UMTS Security Architecture



USIM	UMTS Subscriber Identity Module
MS	Mobile Station
RNC	Radio Network Controller
VLR	Visitor Location Reg.
SGSN	SG Serving Network
HLR	Home Location Register
AuC	Authentication Centre

Generation of authentication vectors

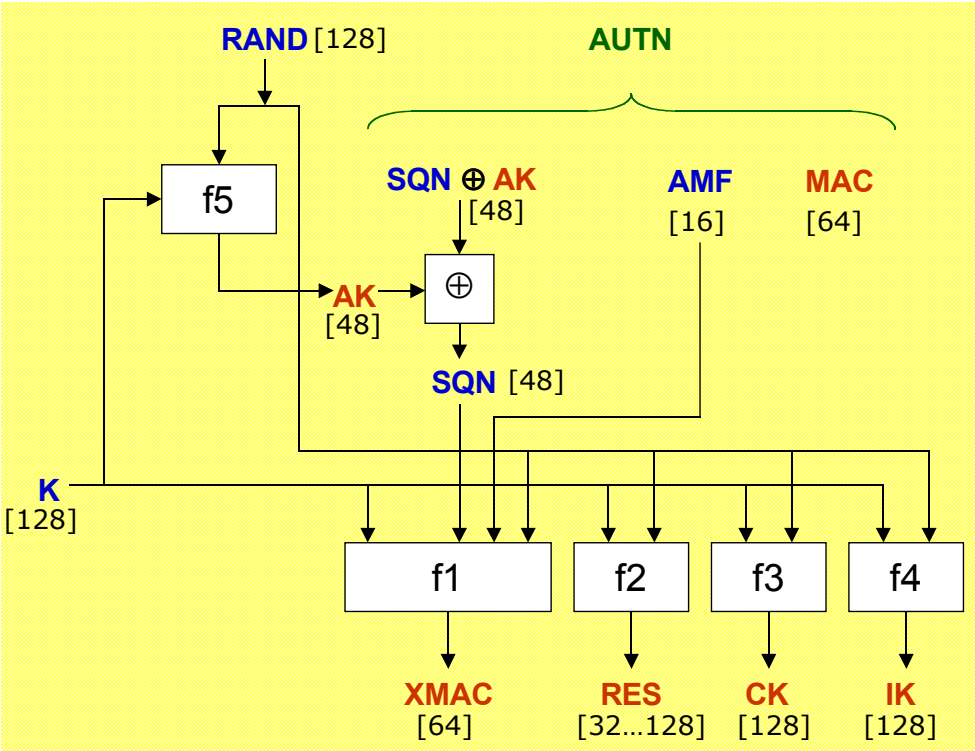


SQN	Sequence number
RAND	Random number
AMF	Authenticated Management Field
K	Secret Key
MAC	Message authentication code
XRES	Expected response
CK	Cipher key
IK	Integrity key
AK	Anonymity key
AUTN	Authentication token
AV	Authentication vector
[…]	# of bits

AUTN := SQN ⊕ AK || AMF || MAC

AV := RAND || XRES || CK || IK || AUTN

Authentication function in the USIM

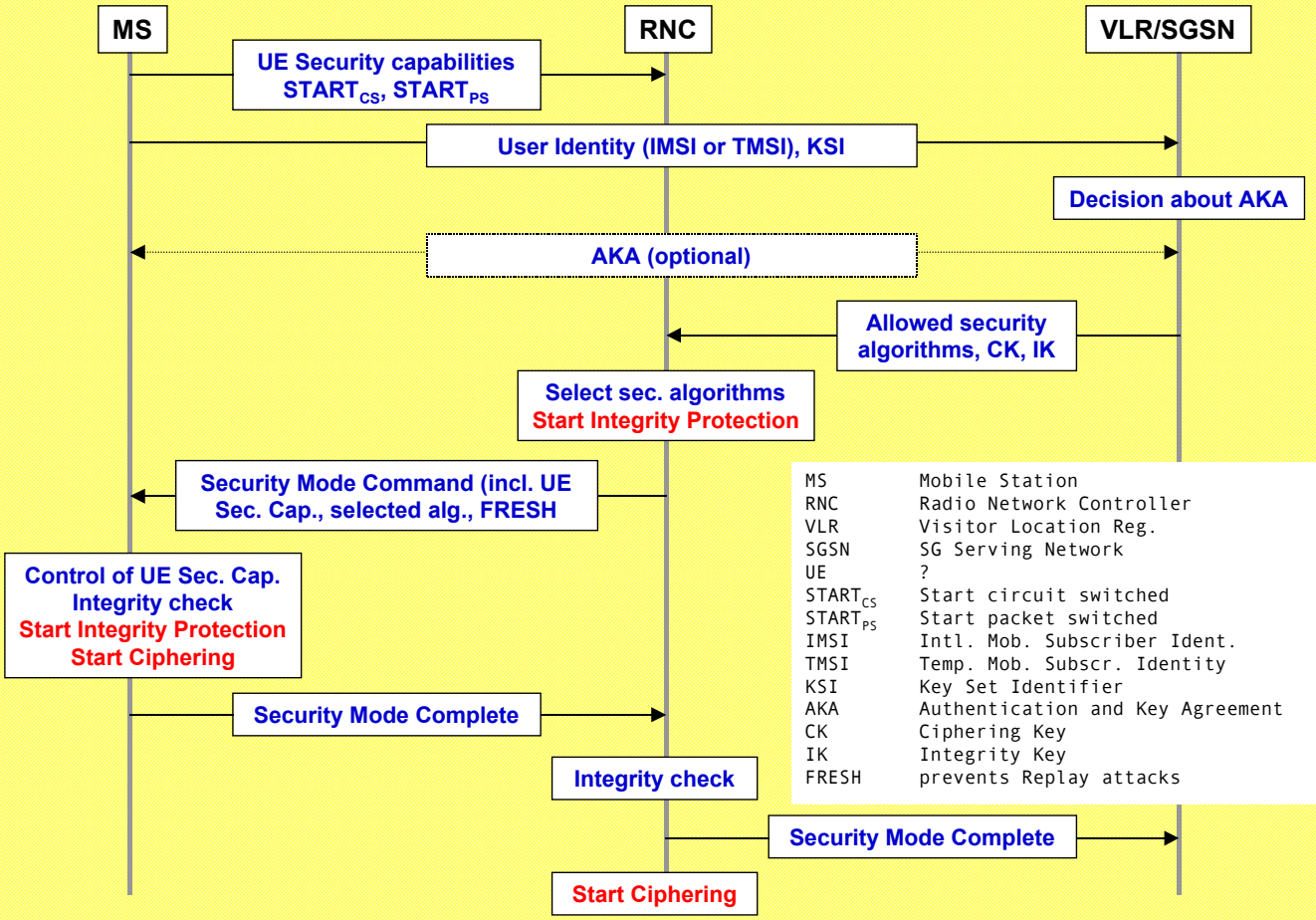


SQN	Sequence number
RAND	Random number
AMF	Authenticated Management Field
K	Secret Key
MAC	Message authentication code
XMAC	*Expected MAC*
RES	*Response*
CK	Cipher key
IK	Integrity key
AK	Anonymity key
AUTN	Authentication token
[…]	# of bits

Verify MAC == XMAC

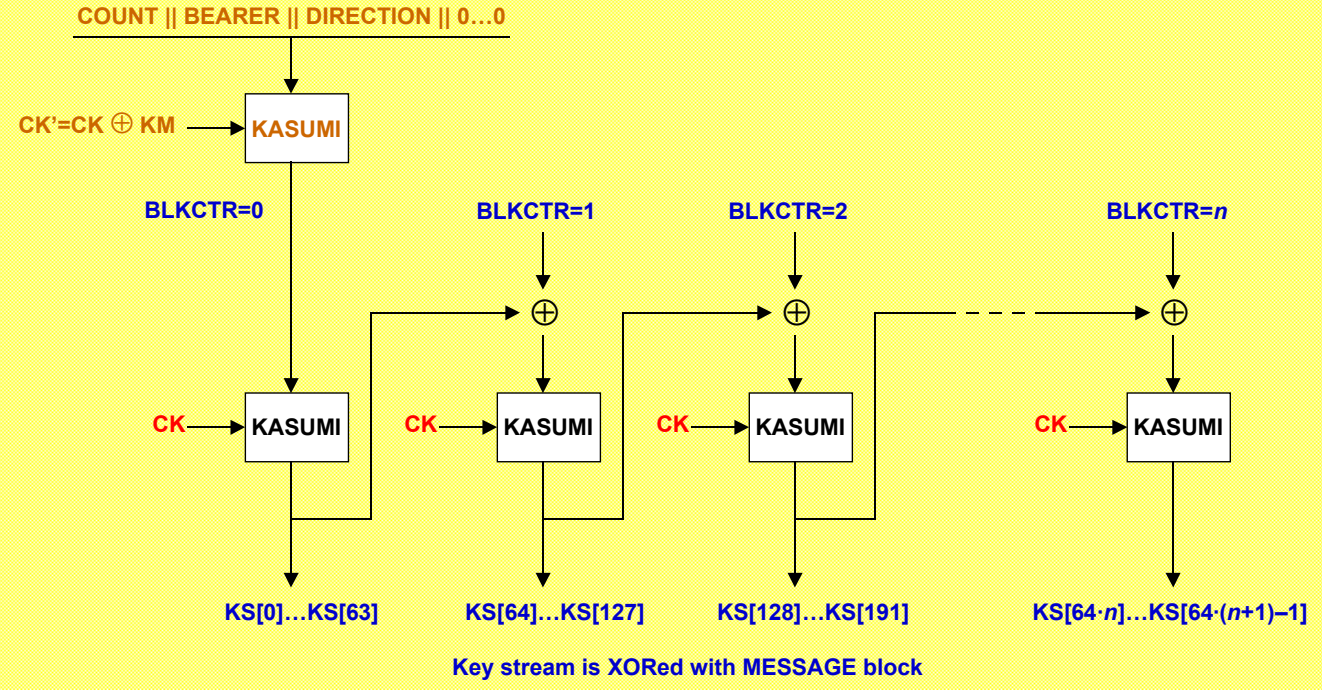
Verify that SQN is in the correct range

Security mode setup procedure



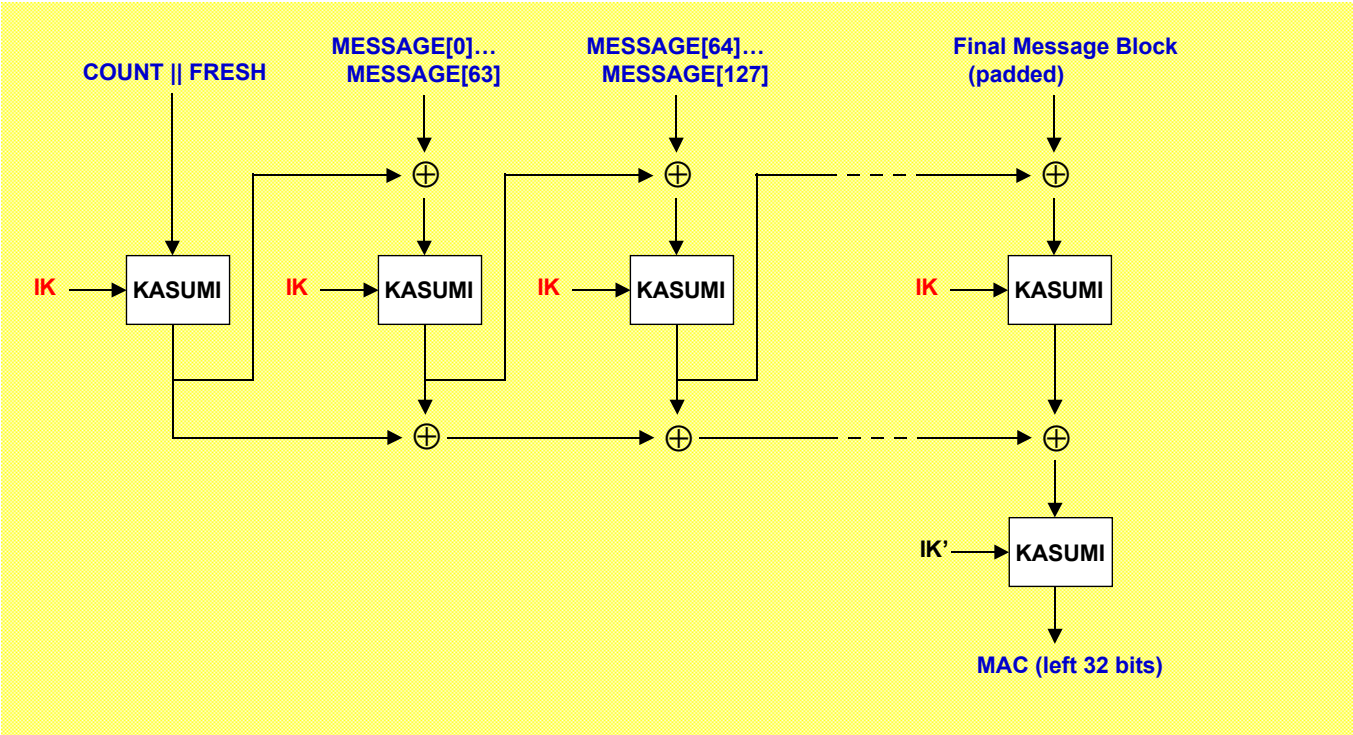
Cipher algorithm f8

- Combination of Output Feedback mode (OFB) and counter mode
- First encryption under CK' prevents chosen plaintext attacks (initialization vector is encrypted, KM: key modifier)



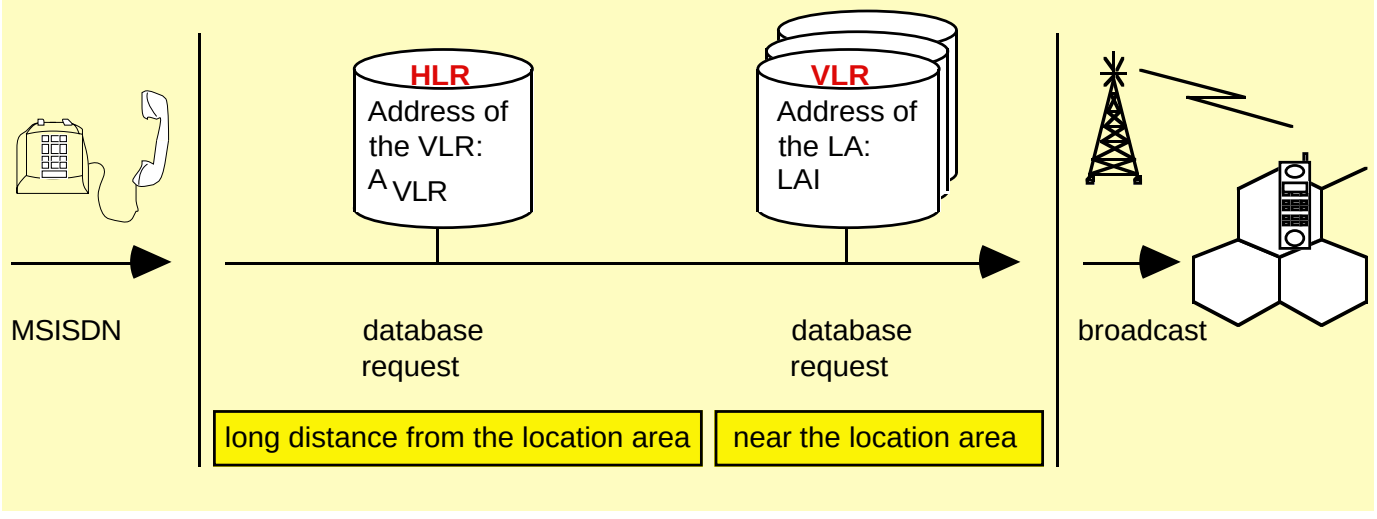
Integrity algorithm f9

- *ISO/IEC 9797-1 (MAC algorithm 2)*



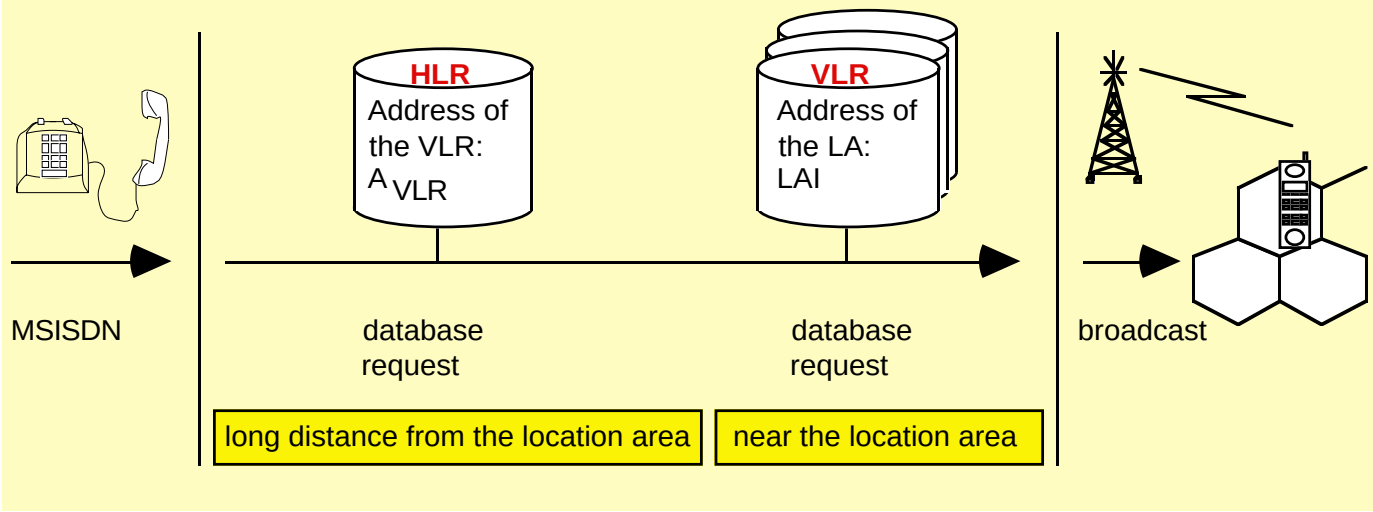
Protection of locations

- *Mobile user*
  - whishes to be reachable at his current location.
  - He won't be localizable by outsiders and the network operator unless the explicitly gives his permission
- *There is no mobile network that fulfills this demand.*



Protection of locations

- *GSM (Global System for Mobile Communication)*
  - Distributed storage at location registers
    - Home Location Register (HLR)
    - Visitor Location Register (VLR)
  - Network operator has global view on location information
- *Tracking of mobile users is possible*



Systematic: Protection of locations

A. Trust into the mobile station only

A.1 Broadcast method

A.2 Group pseudonyms

B. Additional trust into a private fixed station

B.1 Trusted address translation and broadcast

B.2 Reduction of broadcast areas

B.3 Explicit trustworthy storage of locations

B.4 Temporary pseudonyms (TP method)

C. Additional trust into a trusted third party

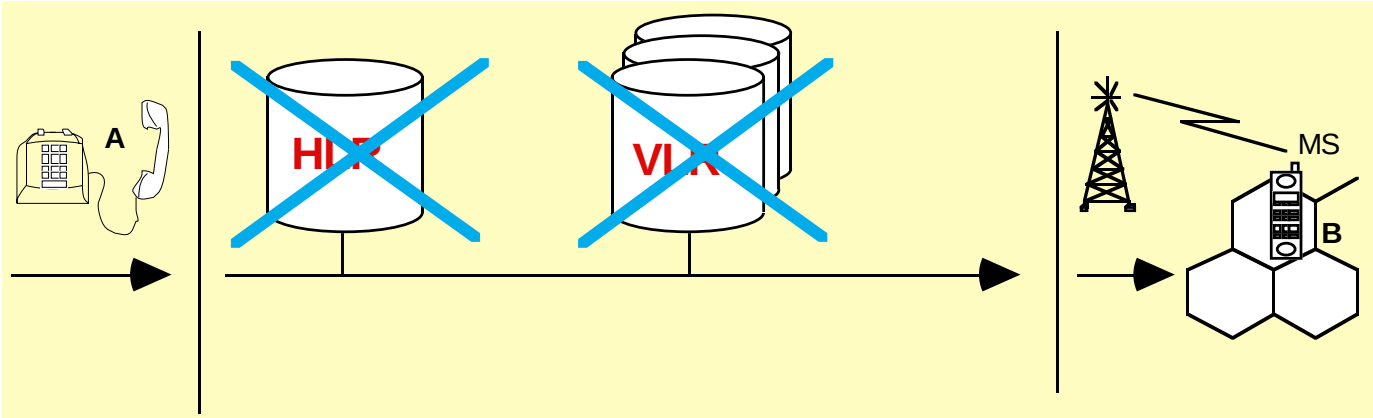
C.1 Trust Center

C.2 Co-operating chips

C.3 Mobile Communication-MIXing

Overview: Broadcast

- No storage of locations and global paging of mobile users

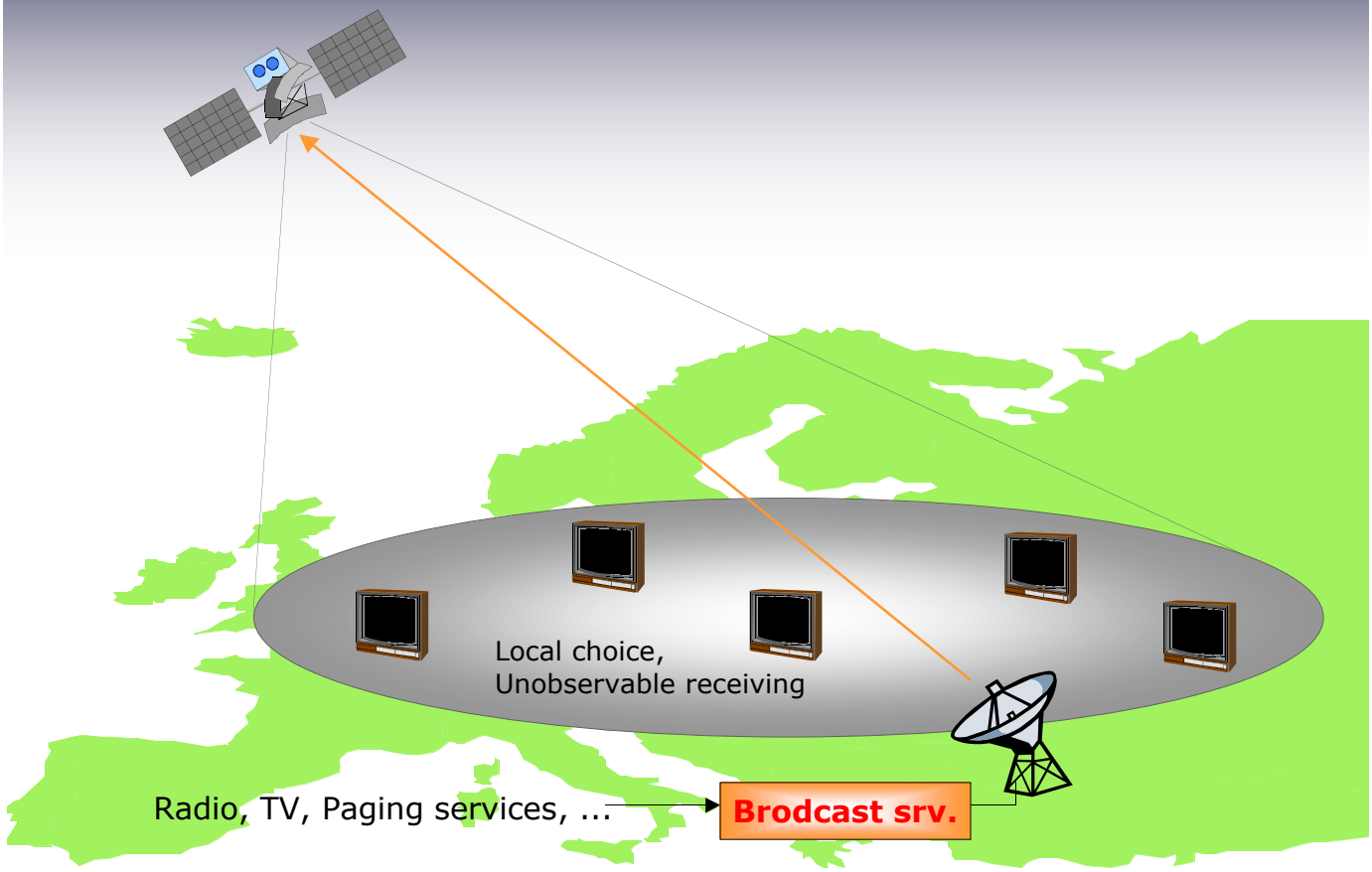


Overview: Broadcast

- No storage of locations and global paging of mobile users

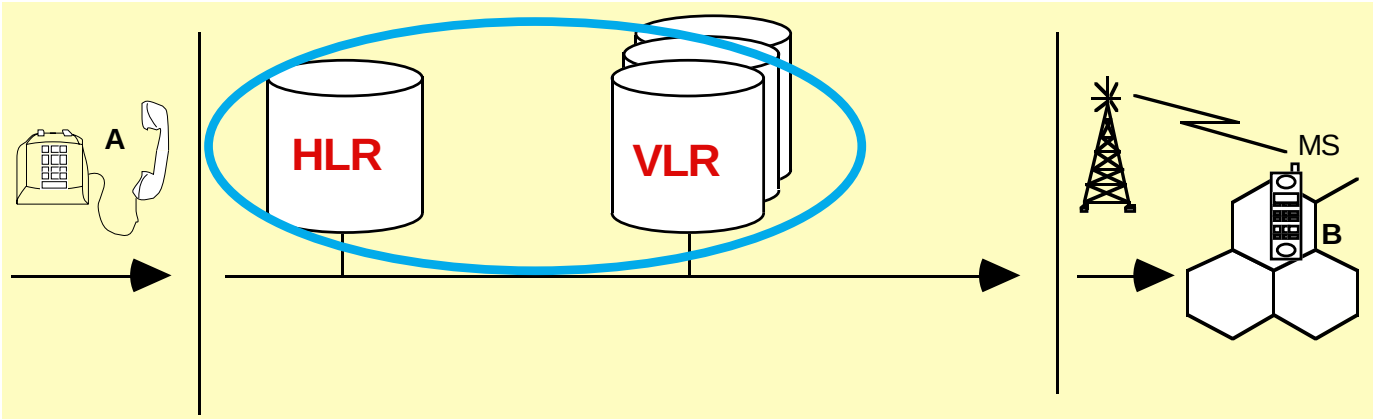
- Immense costs for bandwith …

Broadcast in general



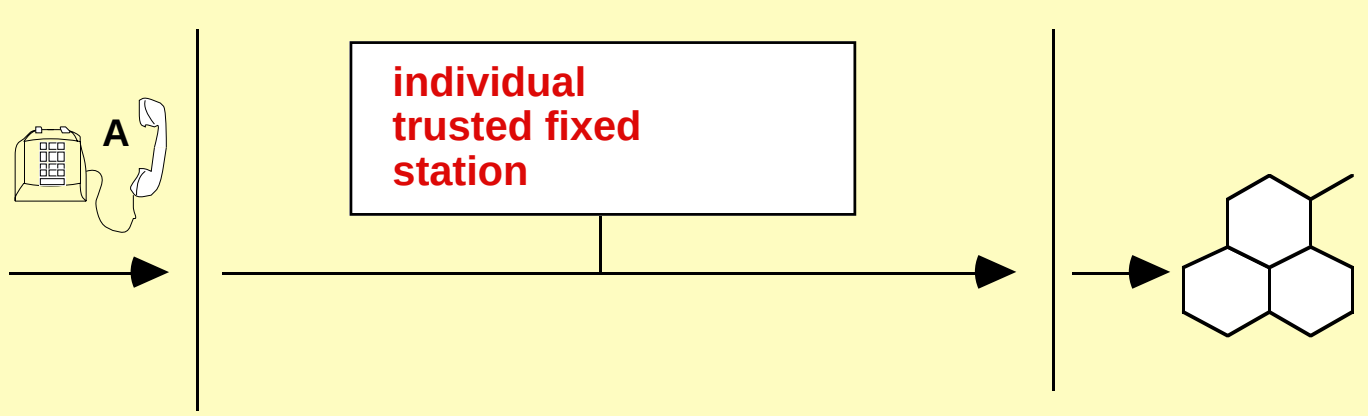
Overview : Trustworthy storage

- *Replace databases by trusted devices in the fixed network*



Overview : Trustworthy storage

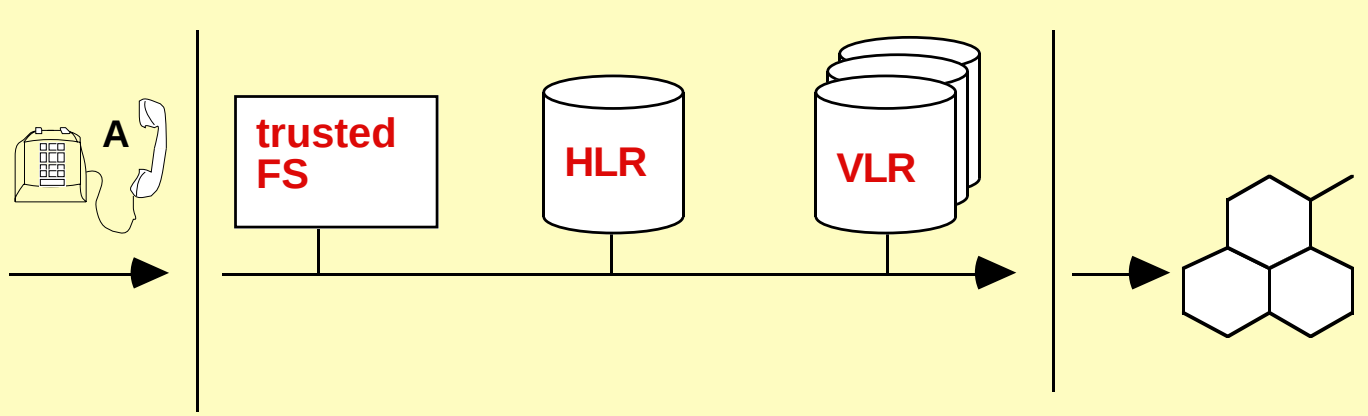
- *Replace databases by trusted devices in the fixed network*



- *Every location updating needs communication with trusted station.*
- *Question: How can we reduce cost of location updating?*

Overview : Trustworthy storage

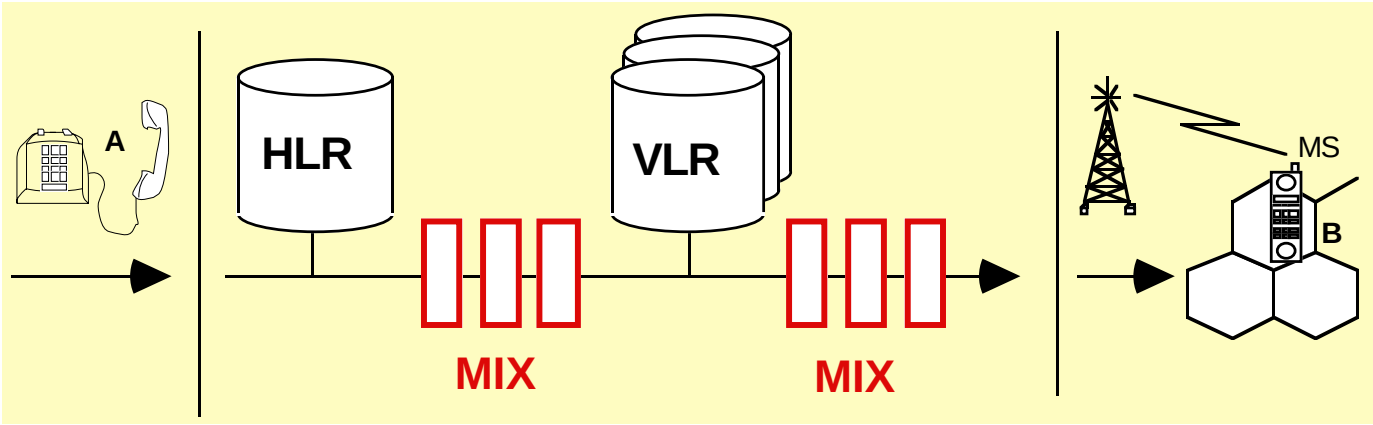
- *Tempory Pseudonyms (TP method)*



- *Can we do this without a trusted fixed station?*

Overview : Mobile Communication-MIXing

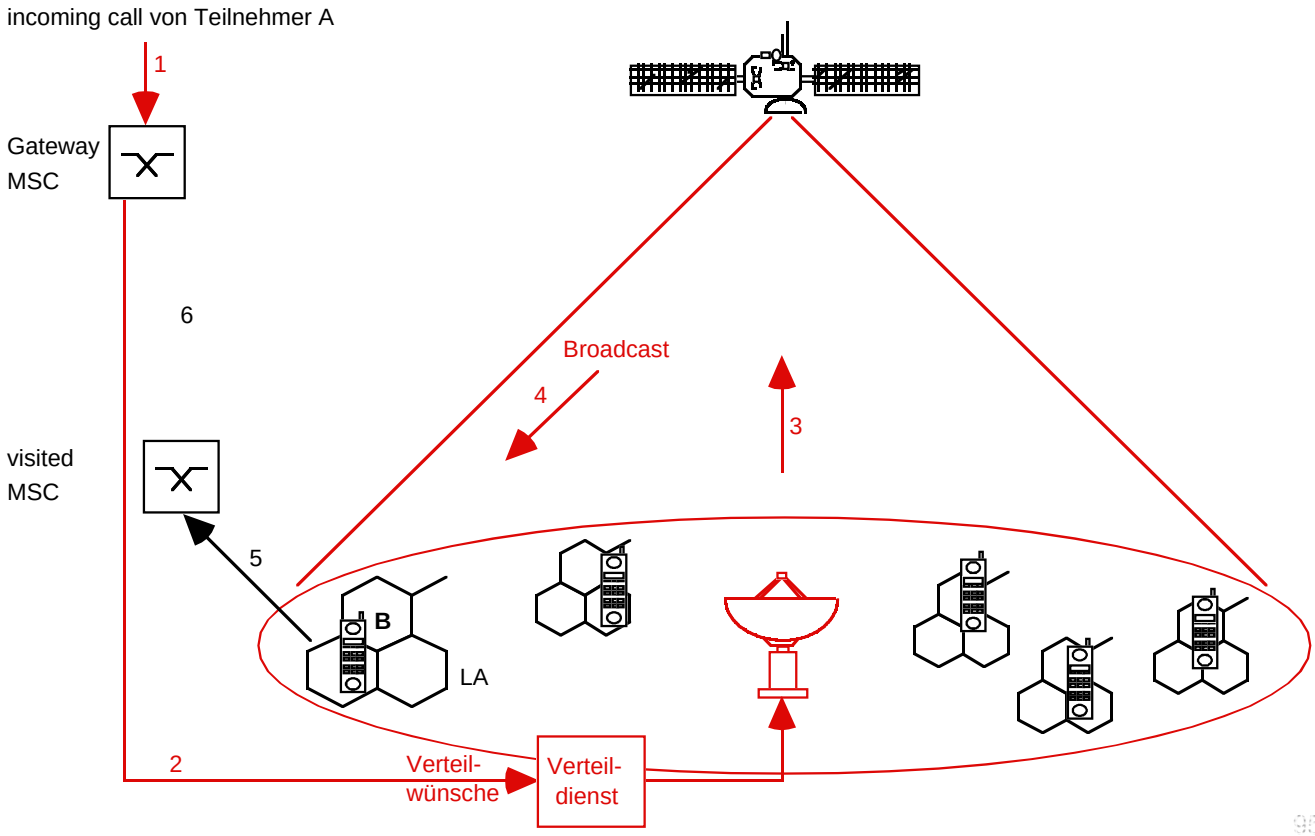
- *Covered storage of location information*



- *A MIX hides the communication relation between*
  - HLR and VLR
  - VLR and location area

Broadcast-Ansatz

- *Beispiel*



Schutz des Empfängers: Verteilung (Broadcast)

- ***Adressierung***
  - explizite Adressen: Routing
  - implizite Adressen: Merkmal für Station des Adressaten
    - verdeckt: asymm. Konzelationssystem
    - offen: Bsp. Zufallszahlengenerator
- ***Beispiel***
  - Paging von Verbindungswünschen zu mobilen Teilnehmern
  - Verzicht auf Speicherung von Aufenthaltsdaten

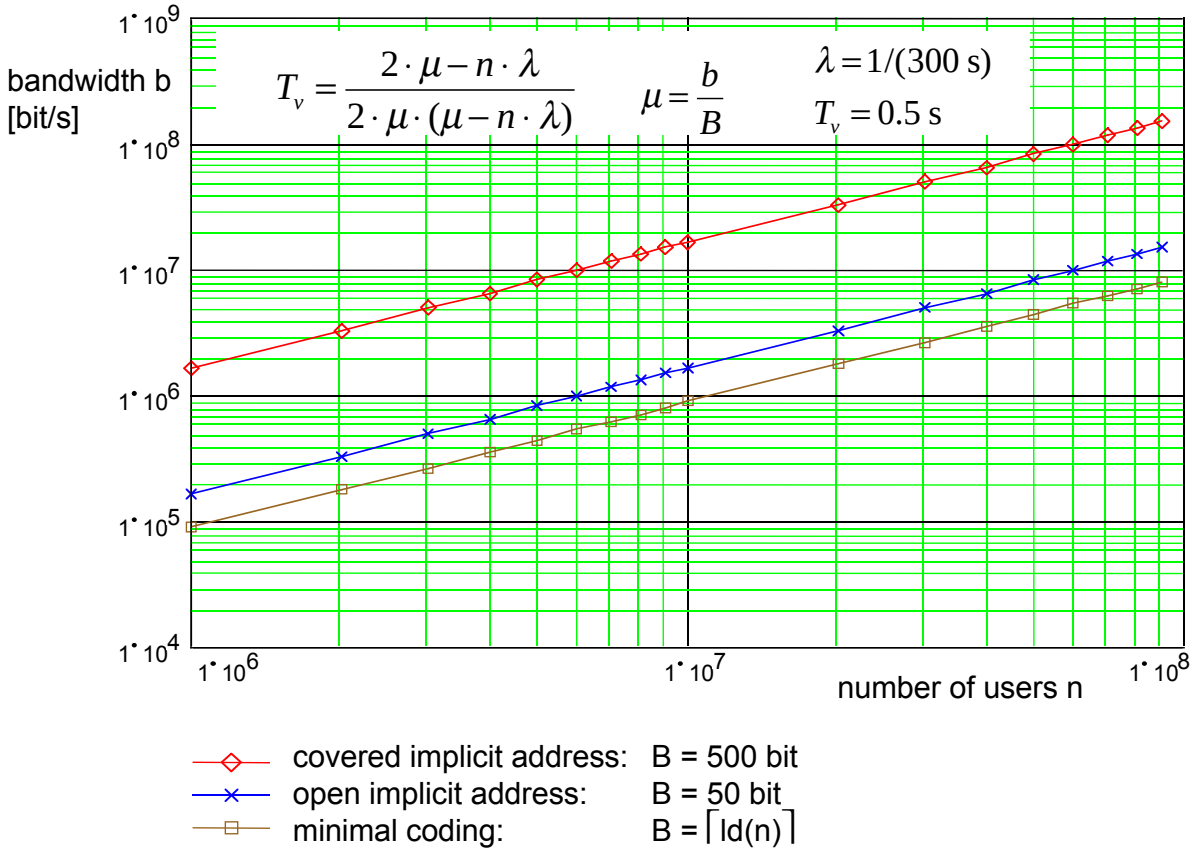
		Adreßverwaltung	
		öffentliche Adresse	private Adresse
implizite Adres-sierung	verdeckt	sehr aufwendig, für Kontaktaufnahme nötig	aufwendig
	offen	abzuraten	nach Kontaktaufnahme ständig wechseln

Implicit Addresses

- ***First contact: covered implicit address CIA***
  - Recipient publishes public encryption key **c**
  - Sender creates **CIA := c(R,S,M)**
    - Redundancy **R**
    - Seed **S** of a pseudo-random generator **PRG**
    - Message **M** (optional)
  - Recipient decrypts *all* received messages with private key **d**
    - Finds correct **R** for own messages only
- ***Following addressing: open implicit address OIA***
  - **OIA_{i+1} := PRG(i,seed)** (i = 0,1,2,…)
  - Sender :
    - calculates next **OIA**
    - encrypts message (optional) **M**
    - Sends **OIA, M**
  - Receiver: Associative memory of all valid **OIA**s to recognize own messages

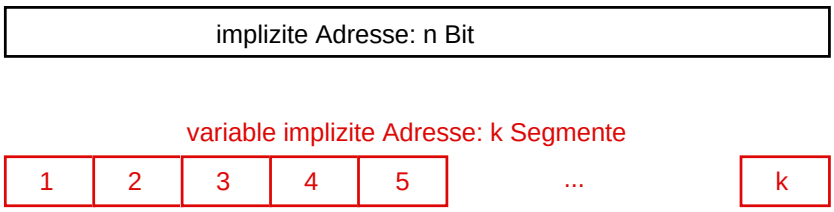
Broadcast method

- **Performance**



Variable implizite Adressierung

- **Ziel**
  - Bandbreiteaufwand gegenüber reinem Broadcast reduzieren



- **Vorgehen**
  - Implizite Adresse P wird nicht mehr als Ganzes gesendet
    - vorher: length(P) = n
  - Zerlegen von P in k Segmente
    - jetzt: length(P_i) = l_i mit (i=1..k) und sum(l_i, i=1, k)=n
  - Broadcast der Segmente Schritt für Schritt:

Variable implizite Adressierung

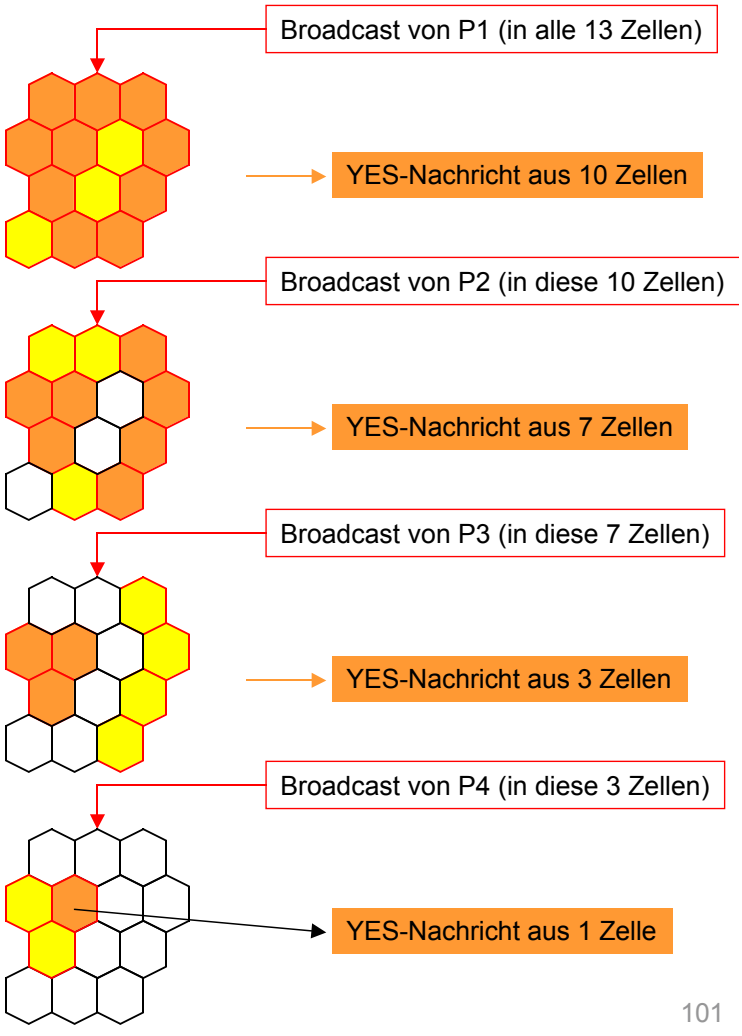
- ***Broadcast der Segmente Schritt für Schritt:***

```
10  LET C = alle Funkzellen des Versorgungsgebietes
        20  LET k = Anzahl der Adreßsegmente
        30  FOR i = 1 TO k DO
              Broadcaste P_i in alle Funkzellen in C
              IF (Mobilstation besitzt ausgestrahltes P_i AND
                 Mobilstation hat in allen vorangegangenen
                 Schritten geantwortet)
                  THEN sende "YES"
                  ELSE sende nichts
              LET C = alle Funkzellen mit mindestens einer
                 "YES"-Antwort
              IF number_of_elements(C) = 1 THEN GOTO 50
40  END FOR

// Zellseparation beendet
```

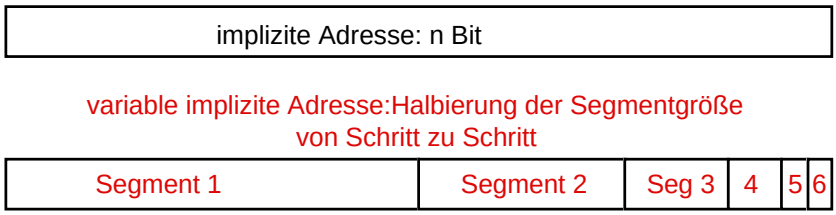

Variable implizite Adressierung

- ***Beispiel***



Variable implizite Adressierung

- **Zellseparation mit Verkleinerung der Segmente**
  - Reduzieren der Broadcastschritte auf log2(n)



Anzahl antwortender Stationen halbert sich im Mittel von Schritt zu Schritt

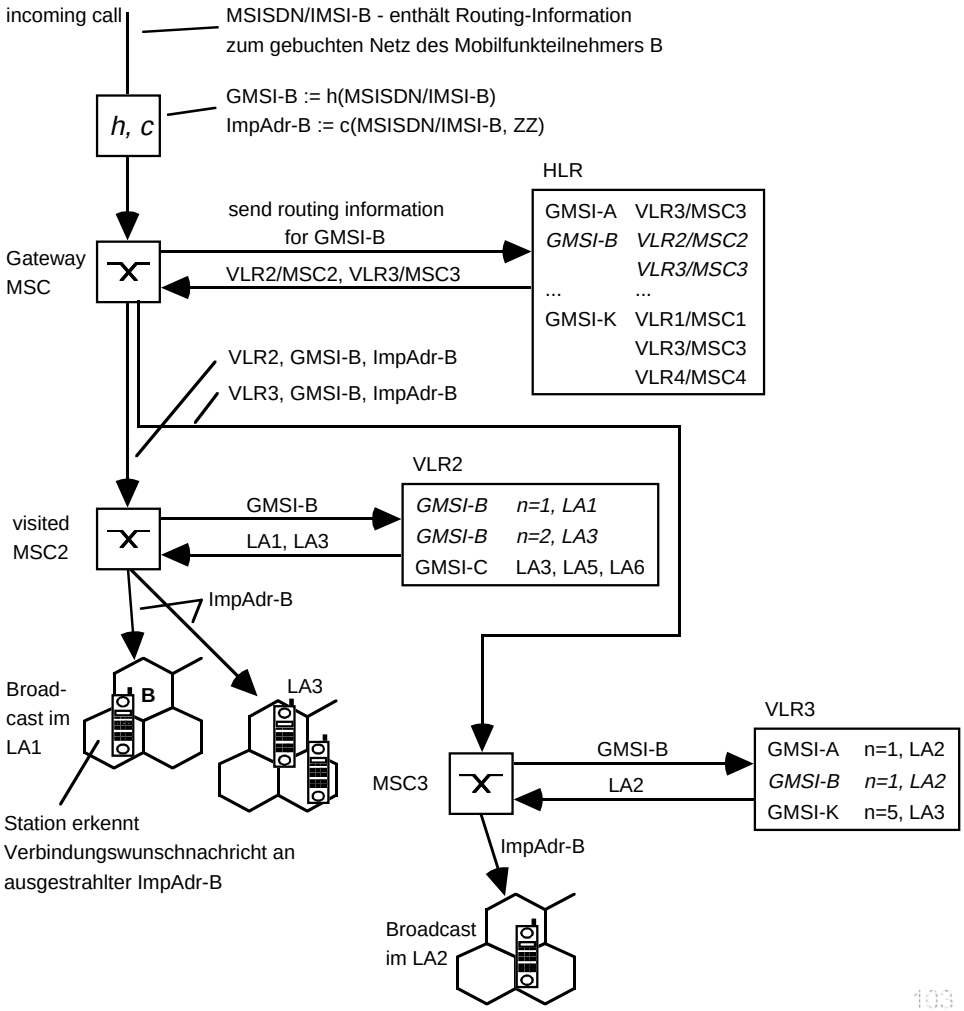
Banbreitenersparnis von 25% pro Funkzelle (bei geograph. Gleichverteilung der MS)

- **Algorithmus**

```
10   LET C = alle Funkzellen des Versorgungsgebietes
20   LET r = n
30   WHILE (r>1 AND number_of_elements(C)>1) DO
       Broadcaste die nächsten ceil(r/2) Bits von P in alle Funkzellen in C
       IF (Mobilstation besitzt ausgestrahlte Bits AND Mobilstation hat in allen vorangegangenen
           Schritten geantwortet) THEN sende "YES"
       LET C = alle Funkzellen mit mindestens einer "YES"-Antwort
       r := r - ceil(r/2)
40   END WHILE
50   Broadcaste die letzten r Bits von P
60   // Zellseparation beendet
```

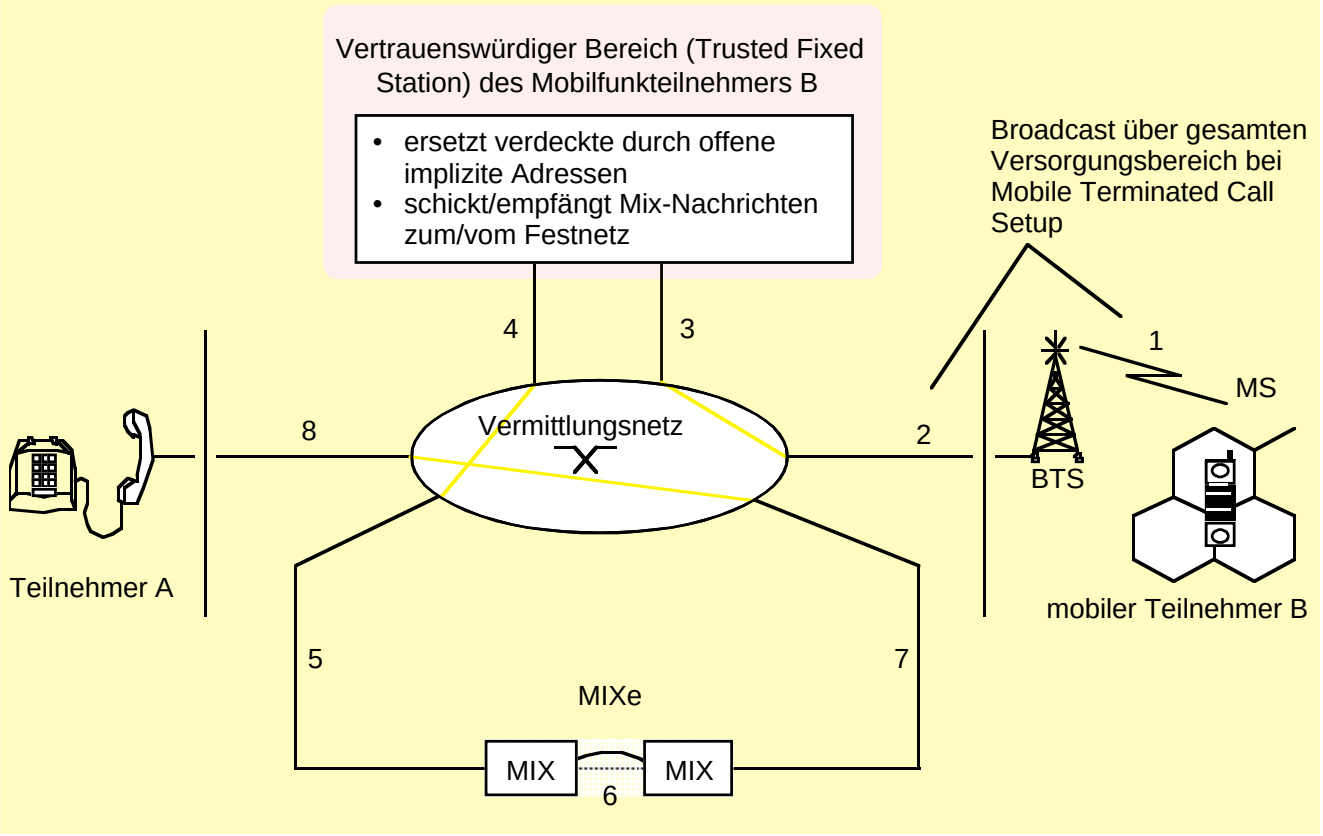

Methode der Gruppen-pseudonyme

- **Unschärfe („Überdeckung“) schafft Privacy**
- **starrer Zusammengang zwischen Gruppen-pseudonym und Identität**



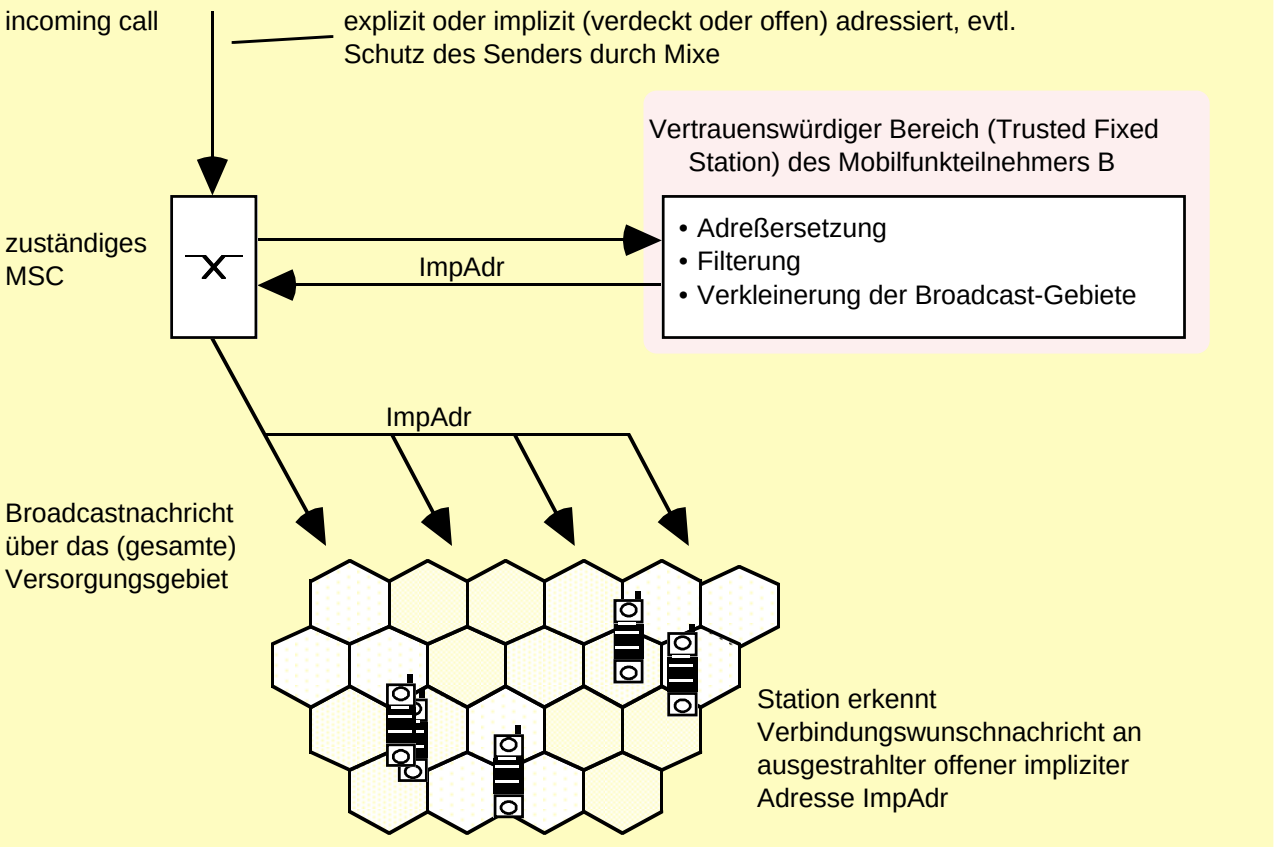
Verwendung eines vertrauenswürdigen Bereichs

- ... Adreßumsetzung und Verkleinerung der Broadcastgebiete



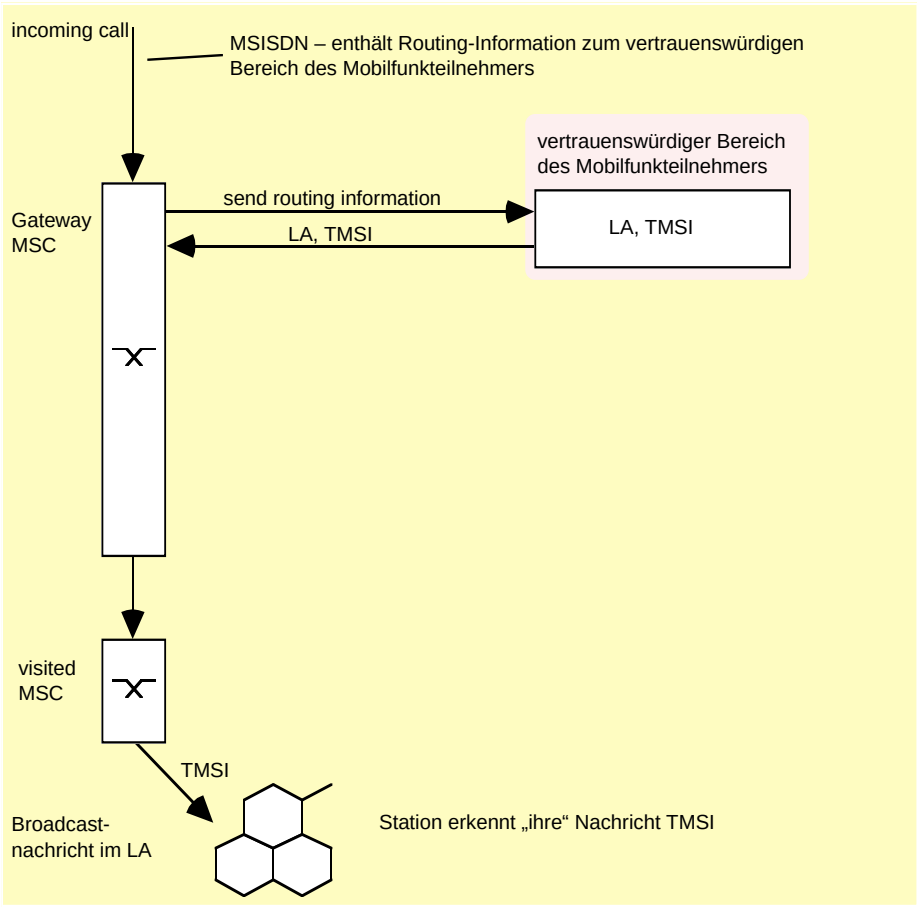
Verwendung eines vertrauenswürdigen Bereichs

- ... Adreßumsetzung und Verkleinerung der Broadcastgebiete (Forts.)



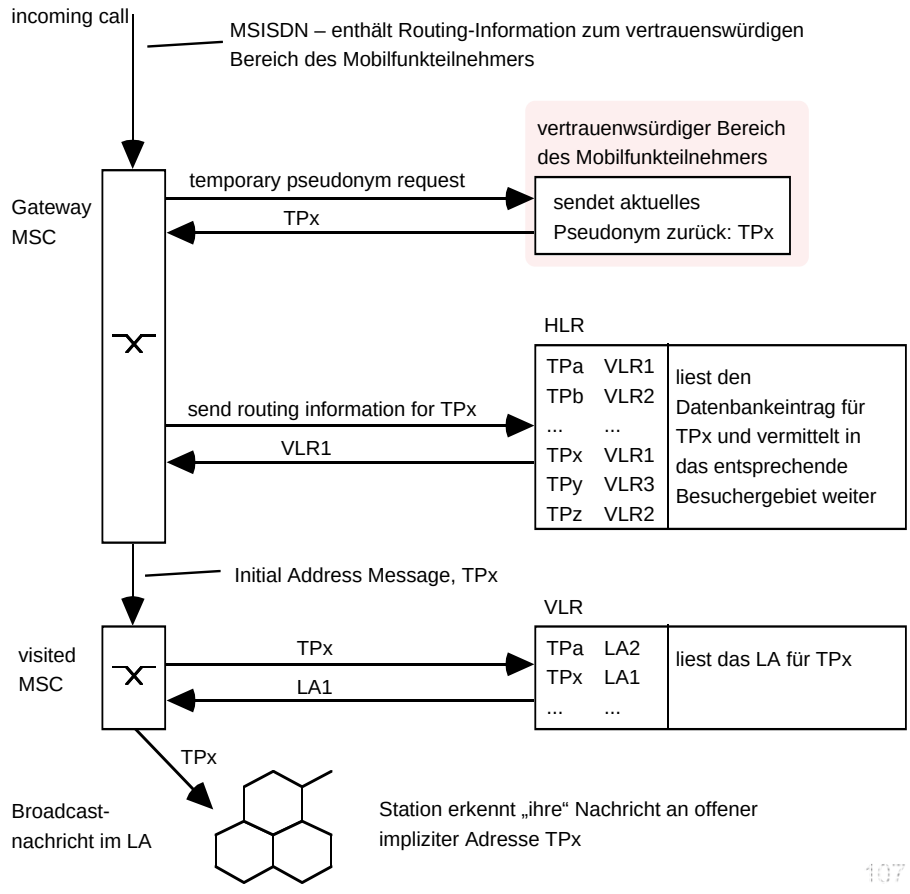
Verwendung eines vertrauenswürdigen Bereichs

- ***... zum Speichern der Lokalisierungsinformation***
  - Jede Aktualisierung erfordert Kommunikation mit dem vertrauenswürdigen Bereich
  - Vertrauenswürdiger Bereich übernimmt gesamtes netzseitiges Location Management



Verwendung eines vertrauenswürdigen Bereichs

- ***... zur Adreßumsetzung (Temporäre Pseudonyme)***
  - Location Management bleibt im Netz
  - Regelmäßiger Wechsel des Pseudonyms ist erforderlich
  - synchronisierte Uhren in MS und trusted FS
  - DB-Einträge verfallen nach bestimmter Zeit

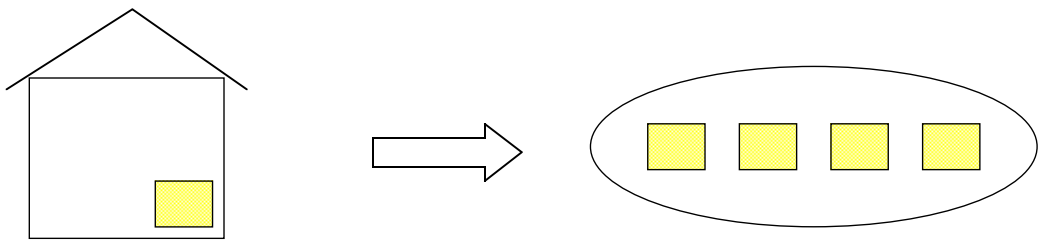


Sicherheitsbetrachtungen …

- ***Unberechtigte Abfrage der vertrauenswürdigen Umgebung***
  - führt zu Lokalisierung
  - Erstellung von Bewegungsprofilen mit Granularität der Anrufhäufigkeit
  - Ausweg: Logging der Zugriffe auf vertrauenswürdigen Bereich und Vergleich mit zugestellten Verbindungswünschen.
- ***Verwendung von Pseudonymen***
  - Funkschnittstelle: Implizite Adresse anstelle der TMSI
  - Datenbankeinträge: Unverkettbarkeit mit Identität
- ***Beobachtbarkeit der Kommunikationsbeziehungen***
  - Location Update explizite Speicherung: Kommunikationsbeziehung zwischen vertrauenswürdigem Bereich und MS führt zum Aufdecken des Orts
  - aber: Location Update TP-Methode: keine Kommunikation zwischen vertrauenswürdigem Bereich und MS notwendig

Vertrauen in einen fremden ortsfesten Bereich

- ***Vertrauen in eine Trusted Third Party***
  - Abwandlung der Methoden die einen eigenen vertrauenswürdigen Bereich voraussetzen
- ***Ersetze trusted FS durch TTPs***
  - unabhängige, frei wählbare vertrauenswürdige dritte Instanzen übernehmen Funktion
  - Dezentralisierung möglich (z.B. Distributed Temporary Pseudonyms).

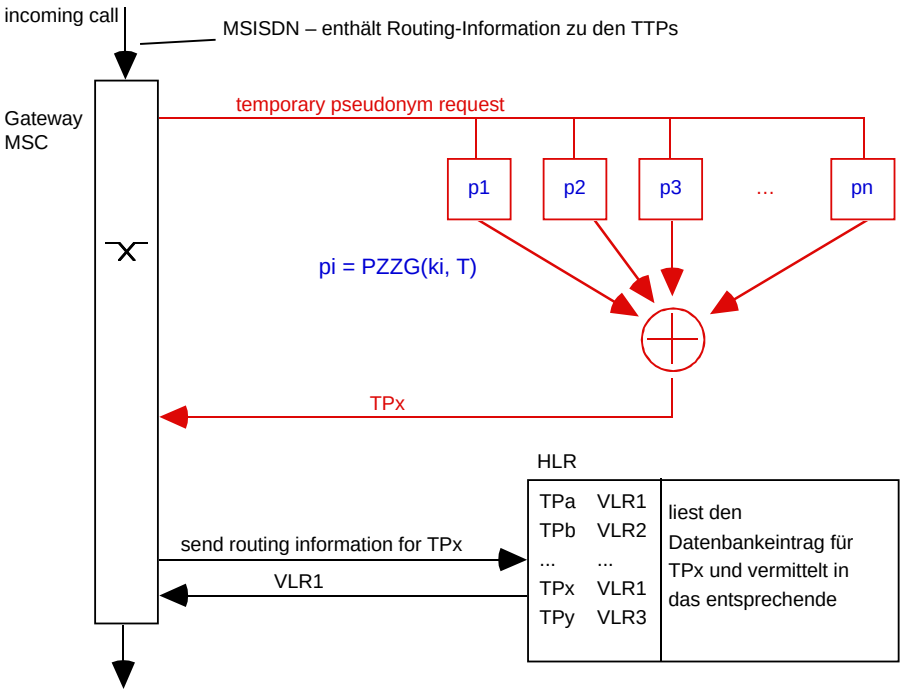


Trusted FS

Trusted Third Parties

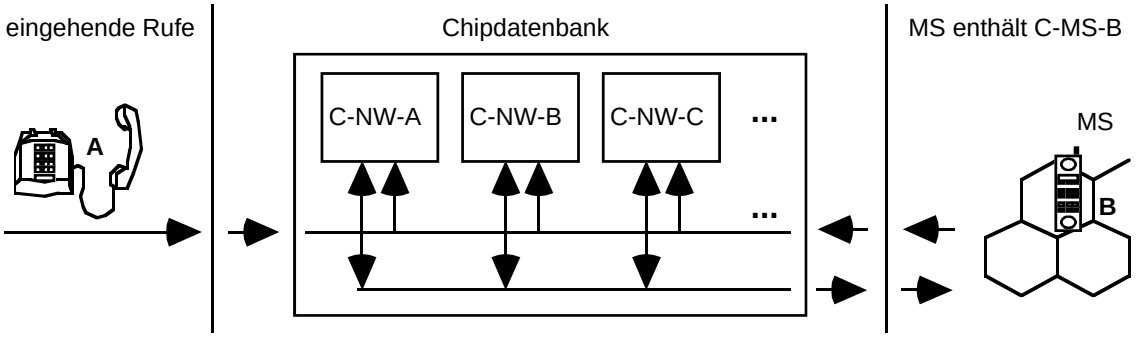
Vertrauen in einen fremden ortsfesten Bereich

- **Distributed Temporary Pseudonyms**
  - Teilnehmer tauscht mit n TTPs symmetrische Schlüssel aus



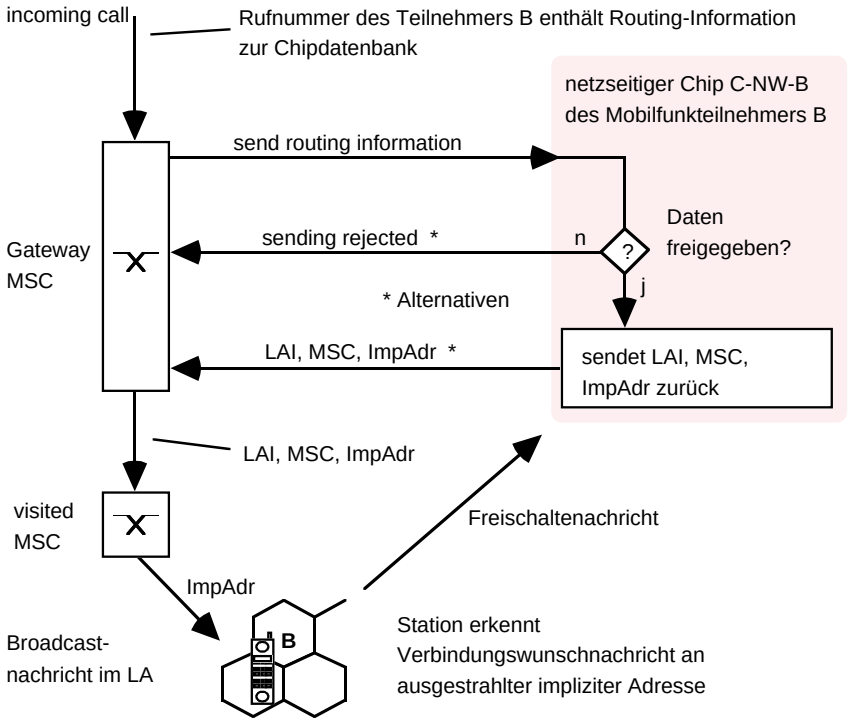
Methode der kooperierenden Chips

- **Architektur**
  - Vertrauen in physische Sicherheit der Chips
  - Anonymität durch Broadcast auf der Chipdatenbank



Methode der kooperierenden Chips

- **Call setup**
  - «Sperrmechanismus» — ein notwendiges Detail aller Verfahren mit vertrauenswürdiger Umgebung ?



Aufwands- und Leistungsbetrachtungen

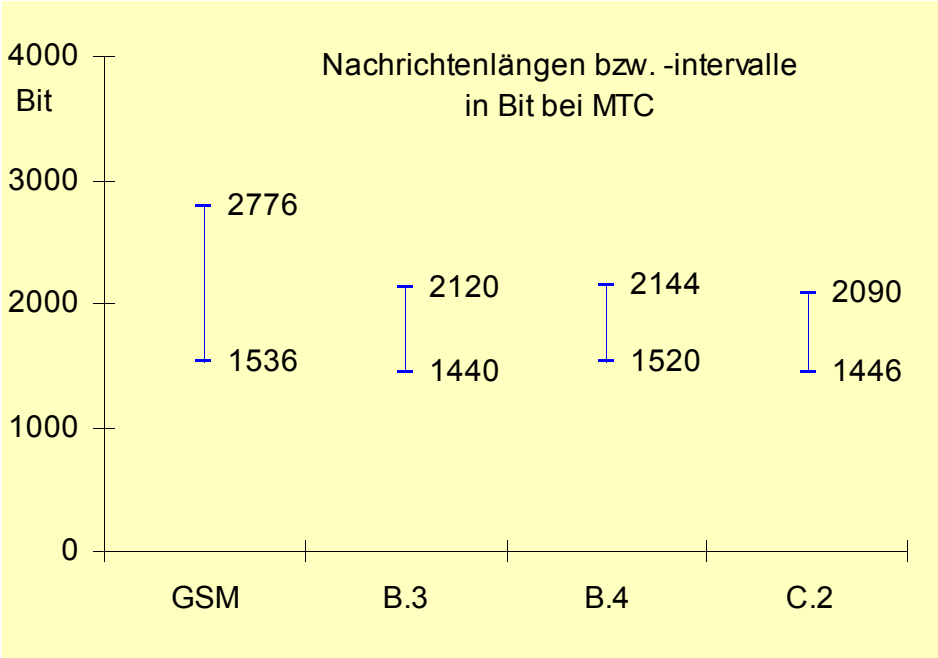
- **Typische Leistungsparameter**
  - Bandbreite
  - Verzögerungszeit
  - Durchsatz
  - Nachrichtenlängen
  - versorgbare Teilnehmerzahl
  - Kosten (LUP, Paging, …)
- **Was wird benötigt?**
  - Zahlen zum Verkehrsverhalten
  - Netzauslastung
  - Leistungsparameter der Netzkomponenten
  - Mobilitätsmodell

- **Verkehrskapazität MSC (typ.): Biala 94**
  - 300.000…600.000 Teilnehmer
  - 100.000 Busy Hour Call Attempts = 28 Vermittlungsversuche pro sek
- **Ankunftsraten: Fuhrmann, Brass 94**
  - MTC = 0,4 1/h (alle 2,5 h ein Anruf)
  - LUP = 1…5 1/h (LUP=3 1/h bei 3 Zellen pro LA, r=1 km, v=15 km/h)
- **Verzögerungszeiten:**
  - Call Setup ISDN: <= 0,5 s
  - Call Setup GSM: <= 40,0 s (Off Air Call Setup), typ. <2,5 s
  - LUP: <= 5 s (r = 1 km, 15 % Zellüberlappung (150 m), v <= 108 km/h)

Performance: Message lengths on the air interface

- **Mobile Terminated Calls**

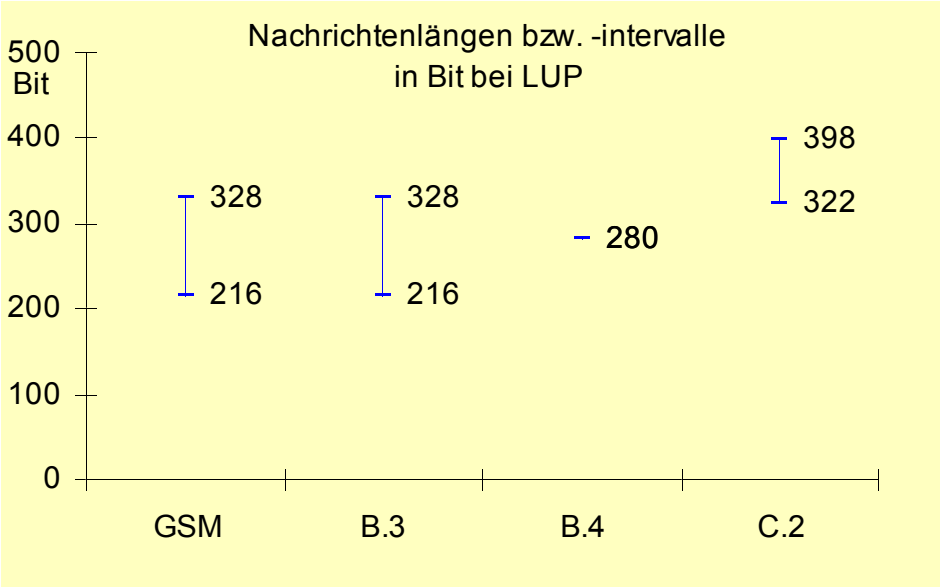
GSM reference
B.3 explicit trustworthy storage
B.4 TP method
C.2 cooperating chips



Performance: Message lengths on the air interface

- **Location Update**

GSM reference
B.3 explicit trustworthy storage
B.4 TP method
C.2 cooperating chips



Mobilkommunikationsmixe

- ***Verfahren leistet***
  - Schutz des Aufenthaltsortes
  - Unbeobachtbarkeit der Kommunikationsbeziehungen
- ***Angreifermodell***
  - Angreifer ist in der Lage, gesamte Kommunikation im Netz abzuhören
    - auf allen Leitungen und Funkstrecken
    - darf alle Datenbankeinträge kennen
- ***Idee***
  - Verzicht auf explizite Speicherung des Ortes in individuellem Vertrauensbereich
  - «verdeckte» Speicherung in Datenbanken
  - Verbergen der Kommunikationsbeziehung (Signalisierung) zwischen Datenbanken und Zielort durch Senden über Mixe

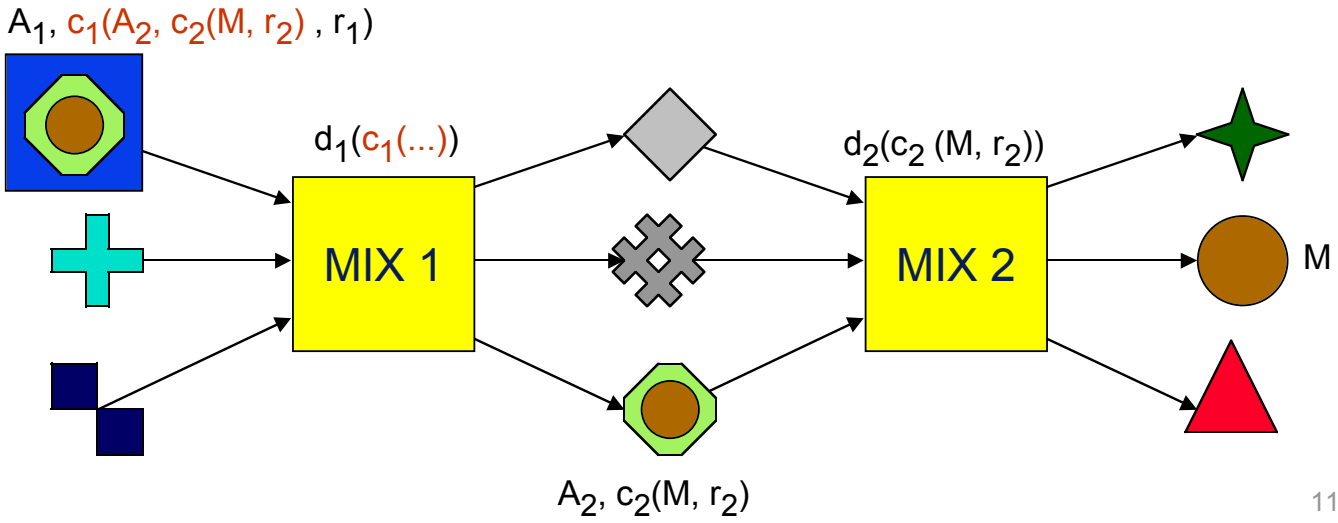
Mixe allgemein (Chaum 1981)

- ***Ziel***
  - Verkettbarkeit ein- und ausgehender Nachrichten verhindern
- ***Verkettungsmerkmale***
  - Zeitliche Relation zwischen Ein- und Ausgabe einer Nachricht
  - Kodierung der Nachrichten
- ***Aufbau eines Mix***
  - Umkodierung basiert auf asymmetrischer Kryptographie:

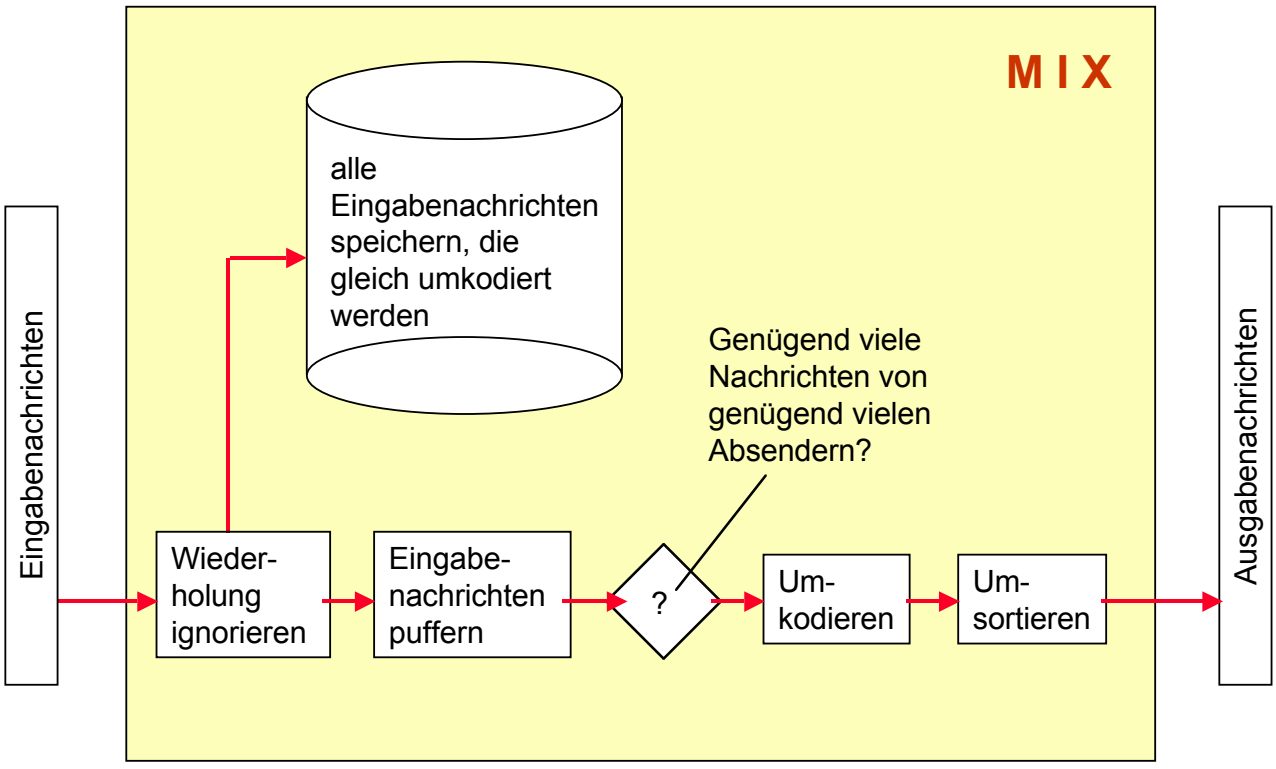
M_i	Mix i einer Kaskade
c_i	öffentlicher Verschlüsselungsschlüssel
d_i	privater Entschlüsselungsschlüssel (kennt nur M_i)

MIX (Chaum 1981)

- ***Functions of a MIX:***
  - sample messages (process more than one msg to provide unlinkability)
  - ignore duplicate messages (prevent uncovering of replayed messages)
  - change coding (basically remove a layer of encryption)
  - change order (out them out in a different order)
- ***A MIX hides the relation between incoming and outgoing message***



Mixe allgemein (Chaum 1981)



Mobilkommunikationsmixe zentralisiert

- **Aufenthaltsortsregistrierung**

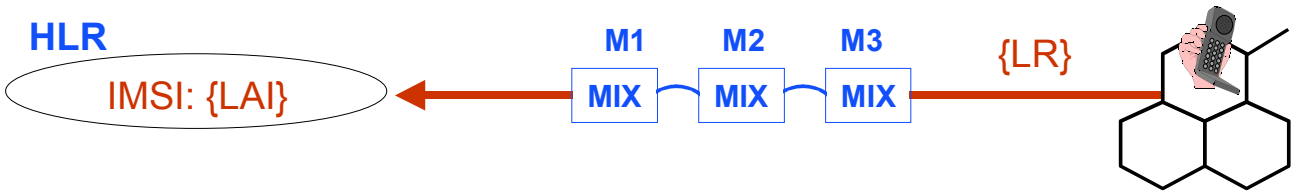
1. MS bildet «verdeckten» Aufenthaltsort

   $\{LAI\} := c_1 (k_1, c_2 (k_2, c_3 (k_3, ImpAdr)))$

2. MS sendet Aufenthaltsortsregistrierung (MS → Mixe → HLR)

   $\{LR\} := c_3 (c_2 (c_1 (IMSI, \{LAI\})))$

M_i	Mix i einer Kaskade
c_i	öffentlicher Verschlüsselungsschlüssel
d_i	privater Entschlüsselungsschlüssel (kennt nur M_i)



Mobilkommunikationsmixe zentralisiert

- **Rufaufbau zum mobilen Teilnehmer**

1. Lesen des HLR-Datenbankeintrages

   IMSI: $\{LAI\} = c_1 (k_1, c_2 (k_2, c_3 (k_3, ImpAdr)))$

2. Absetzen der Verbindungswunschnachricht

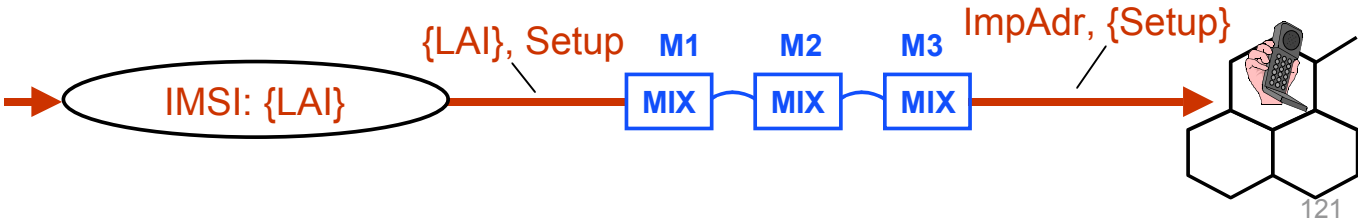
   {LAI}, Setup

3. In den Mixen wird {LAI} ent- und Setup verschlüsselt

   $\{Setup\} := k_3 (k_2 (k_1 (Setup)))$

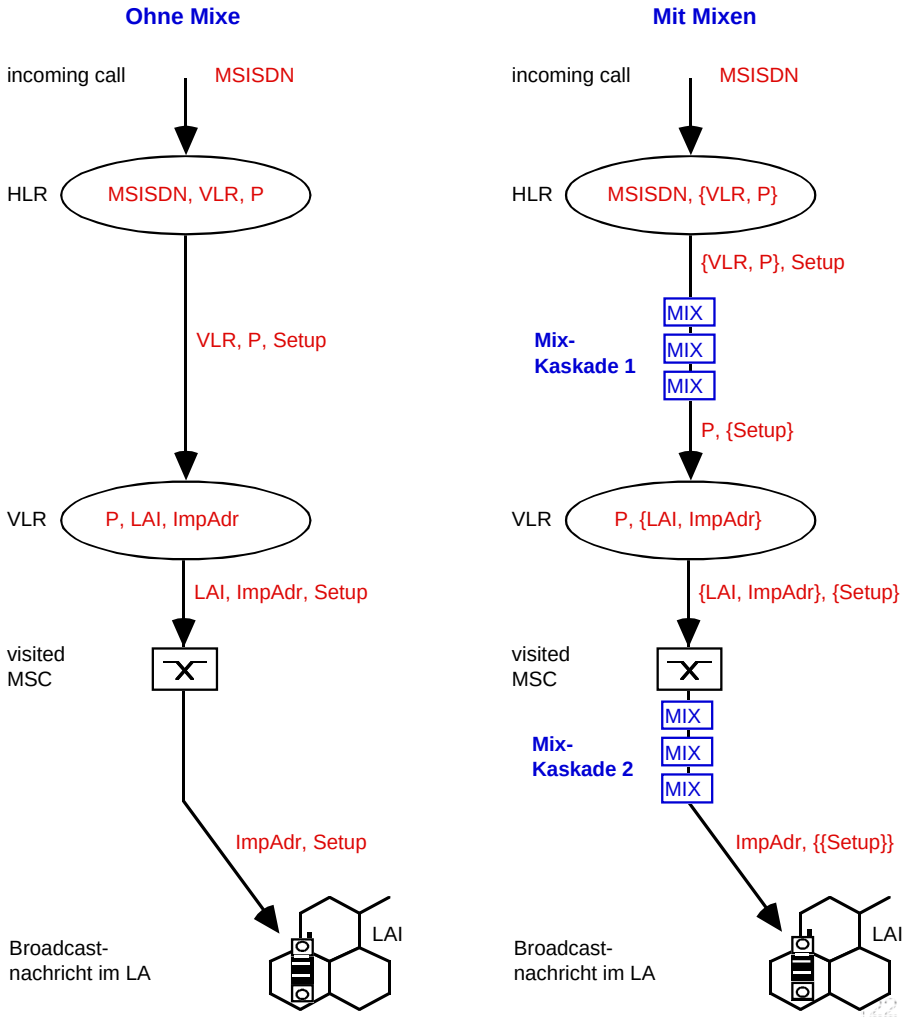
4. Im Aufenthaltsgebiet wird ausgestrahlt

   ImpAdr, {Setup}



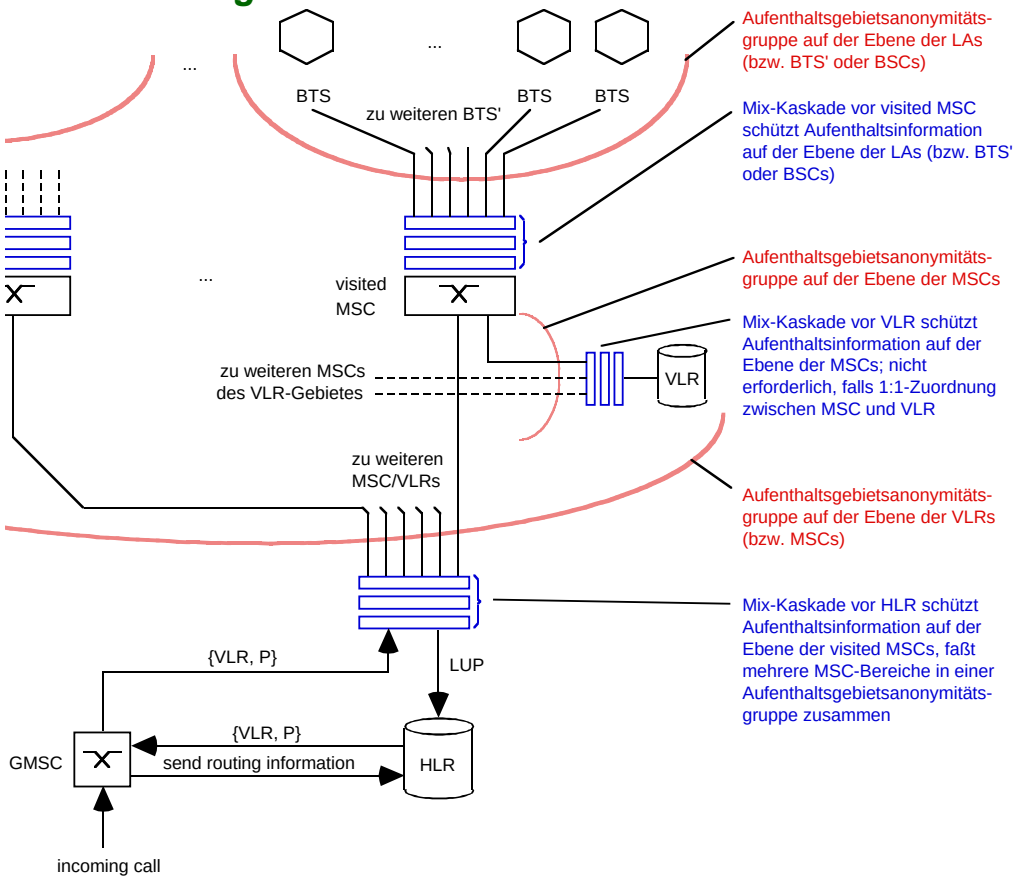
Mobilkommunikationsmixe dezentralisiert

- ***Grundidee pseudonymes Location Management***
  - Register: pseudonyme Speicherung
  - Mix-Netz: Unverkettbarkeit der pseudonym gespeicherten Information
  - Aufenthaltsgebietsgruppen: Zusammenfassung von Gebieten

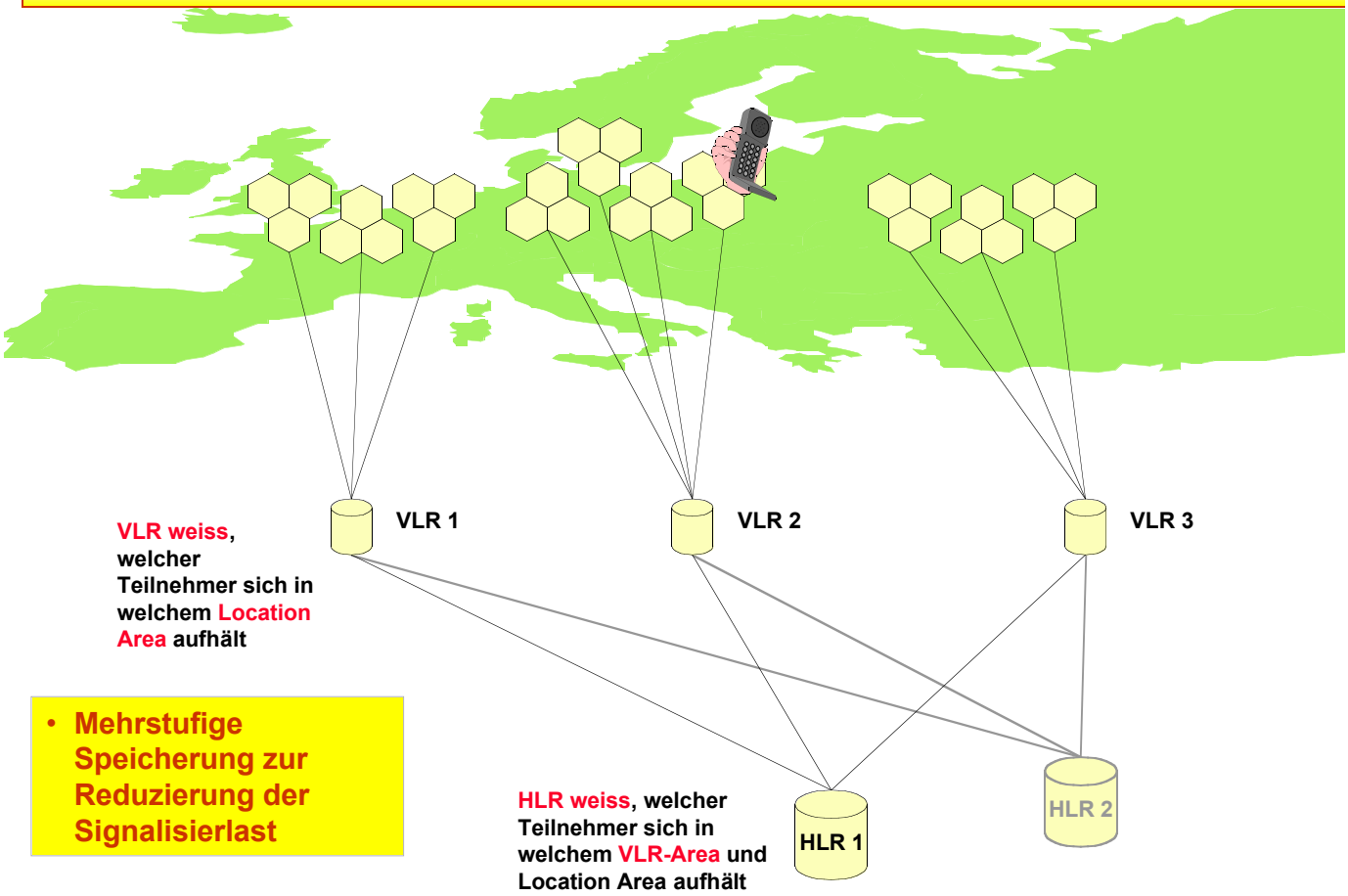


Aufenthaltsgebietsgruppen

- ***Zusammenfassung von Gebieten unterschiedlicher Granularität***

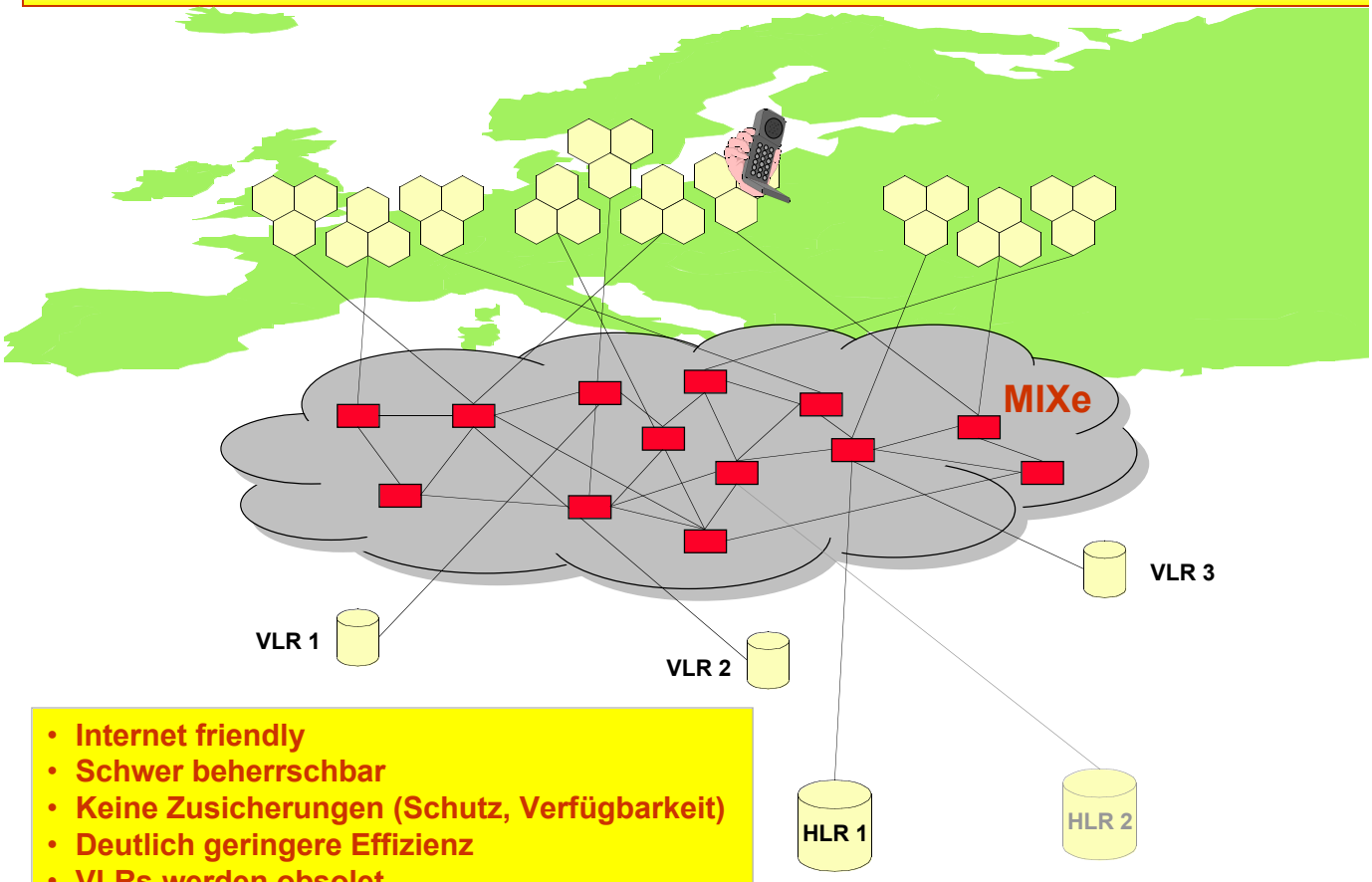


GSM



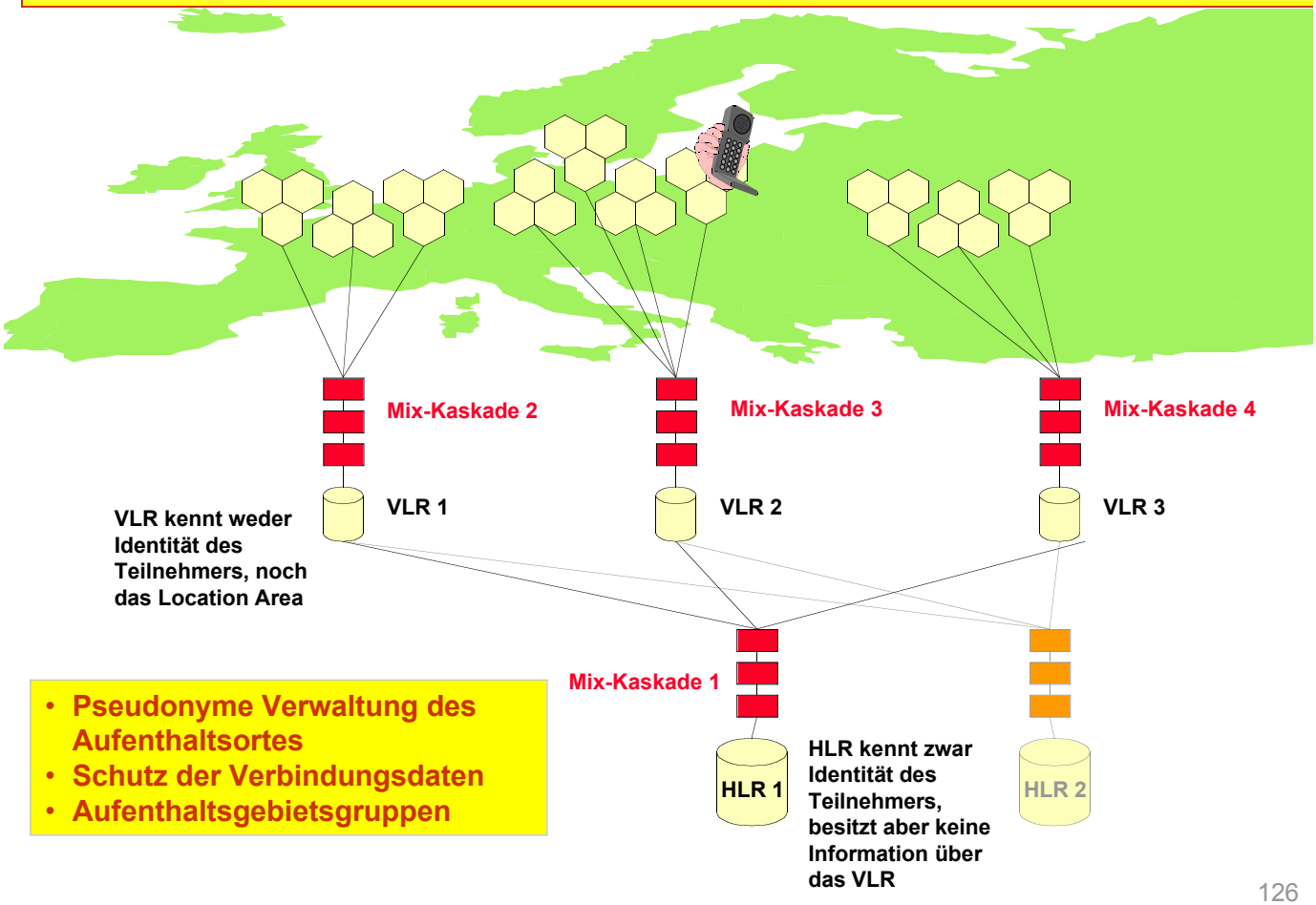
- Mehrstufige Speicherung zur Reduzierung der Signalisierlast

Mobilkommunikationsmixe: Variante 1: Anonymes Netz



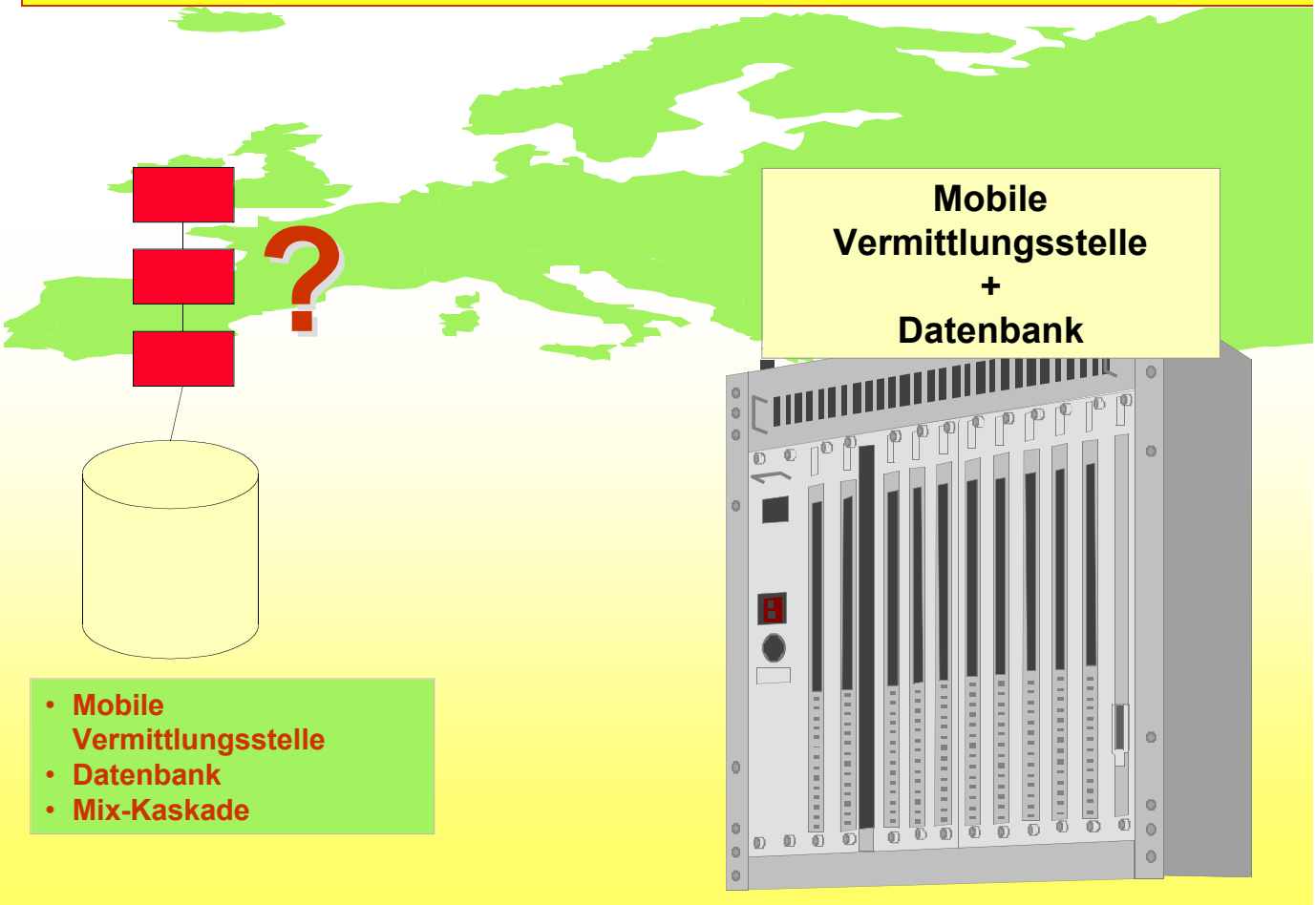
- Internet friendly
- Schwer beherrschbar
- Keine Zusicherungen (Schutz, Verfügbarkeit)
- Deutlich geringere Effizienz
- VLRs werden obsolet

Mobilkommunikationsmixe: Var. 2: Dedizierte Kaskaden



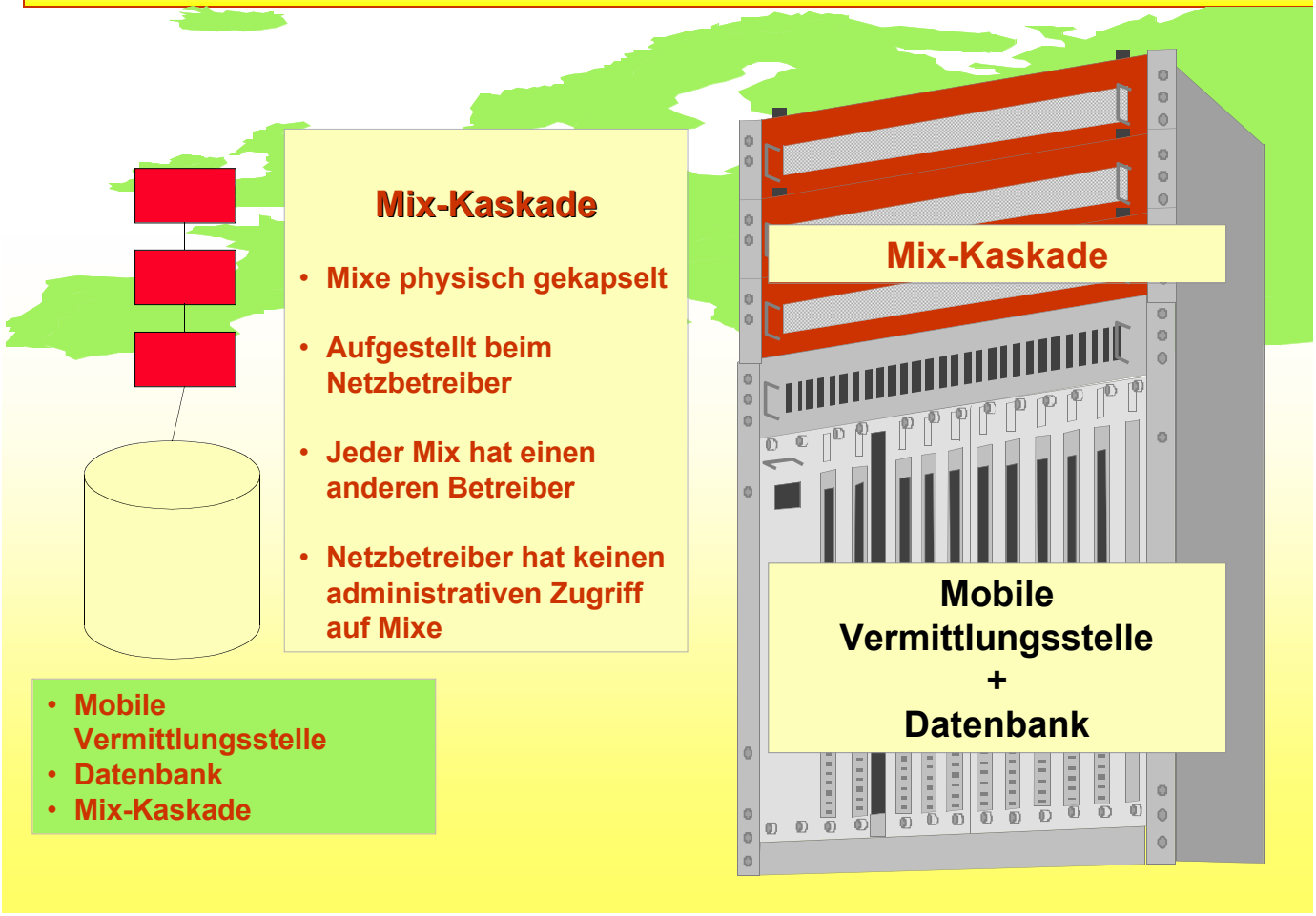
- Pseudonyme Verwaltung des Aufenthaltsortes
- Schutz der Verbindungsdaten
- Aufenthaltsgebietsgruppen

Mobilkommunikationsmixe: Dedizierte Kaskaden



- Mobile Vermittlungsstelle
- Datenbank
- Mix-Kaskade

Mobilkommunikationsmixe: Dedizierte Kaskaden



Authentisierung wie?

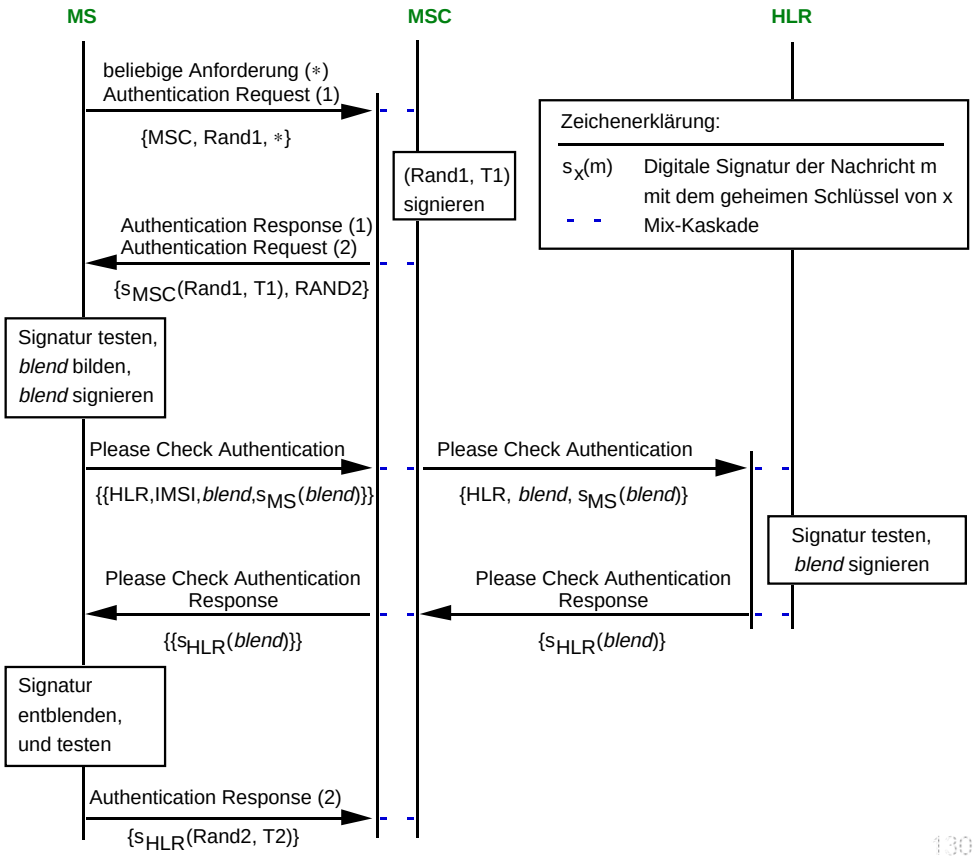
- ***Problem:***
  - Der besuchte Netzbetreiber soll feststellen können, daß ein Teilnehmer berechtigt ist, das Netz zu nutzen, ohne daß seine Identität aufgedeckt wird, denn das käme einer Lokalisierung gleich.
  - Der Teilnehmer soll feststellen können, daß er über einen echten Netzbetreiber kommuniziert.

VLR soll Berechtigung checken, darf aber Identiät von MS nicht erfahren. Blinde Signatur zur Auth. der MS

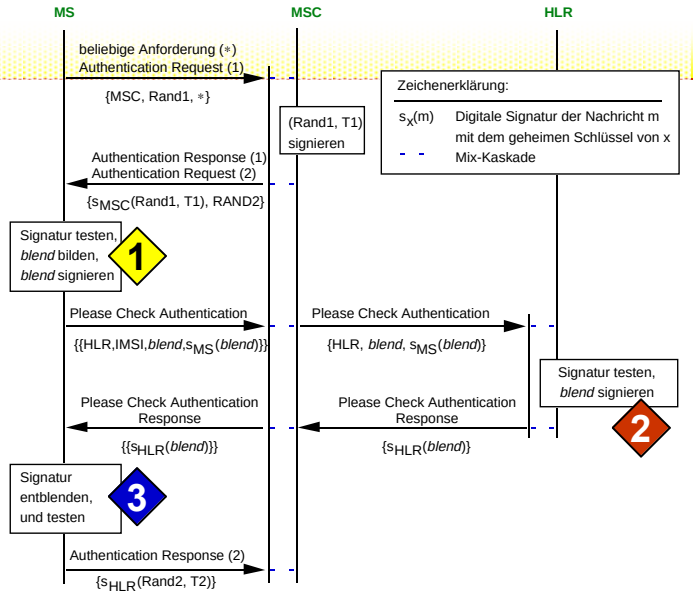
- ***Blindes Signaturverfahren***
  - Gegenseitige Authentikation
  - Verhinderung von Mißbrauch durch unberechtigte Teilnehmer, insbesondere damit der besuchte Netzbetreiber zu seinem Geld kommt
- ***Authentikation im GSM:***
  - Besuchter Netzbetreiber bekommt Auth.Triplet und prüft SRES von der Mobilstation auf Gleichheit.
  - Besuchter Netzbetreiber vertraut darauf, daß der Heimatnetzbetreiber vertrauenswürdig ist.

Protokoll für (gegenseitige) Authentikation

- **Problem: VLR soll Berechtigung checken, darf aber Identiät von MS nicht erfahren.**
- **Blinde Signatur zur Auth. der MS**



Blinde Signatur



1 Blenden:

$$blend := (Rand2, T2) \bullet z^{t_{HLR}} \bmod n$$

2 Signieren:

$$s_{HLR}(blend) = blend^{s_{HLR}} \bmod n$$

3 Es gilt:

$$s_{HLR}(blend) = \left((Rand2, T2) \bullet z^{t_{HLR}}\right)^{s_{HLR}} \bmod n$$

$$= (Rand2, T2)^{s_{HLR}} \bullet \left(z^{t_{HLR}}\right)^{s_{HLR}} \bmod n$$

$$= (Rand2, T2)^{s_{HLR}} \bullet z \bmod n$$

Entblenden:

$$s_{HLR}(blend) \bullet z^{-1} = (Rand2, T2)^{s_{HLR}} \bullet z \bullet z^{-1} \bmod n$$

$$s_{HLR}(Rand2, T2) = (Rand2, T2)^{s_{HLR}} \bmod n.$$

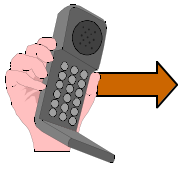
Abrechnung

- ***Heute:***
  - **Ankommende Anrufe** werden berechnet, wenn sich der mobile Teilnehmer im Ausland (bzw. einem Fremdnetz) aufhält.
  - Unterschiedliche Tarifierung für **abgehende Gespräche**:
    - lokale Gespräche (vergleichbar mit Ortsgespräch)
    - Gespräche innerhalb des eigenen Netzes
    - Gespräche in fremde Netze (Festnetz, Mobilnetze)

- ***Anwendbare Konzepte:***
  - ***Anonyme und unbeobachtbare digitale Zahlungssysteme*** (digitales Bargeld-Äquivalent)
  - Digitale Briefmarken (vorbezahlt), Micro-Payments, Tick-Payments

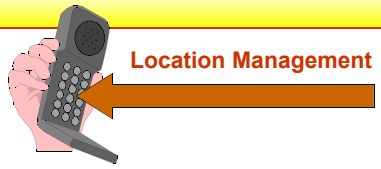
Abrechnung

- ***Abgehende Rufe (von der MS zu einem beliebigen Teilnehmer)***
  - Location Management Prozeduren sind nicht involviert
  - Trotzdem muß Aufenthaltsort geschützt bleiben
  - Vorausgesetzt wird ein vorhandenes anonymes Zahlungssystem
  - Teilnehmer T hat eine MS ohne ID und ein dig. Wallet



- ***Skizze:***
  - MS von T sucht ein Netz (passiver Vorgang)
  - MS meldet Verbindungswunsch an (→ Zielrufnummer)
  - Netz legt Kosten fest und meldet sie an T (← Kosten)
  - T bzw. MS entscheidet und übermittelt Geldbetrag (→ Geld)
  - Netz baut Verbindung zum Ziel auf
- ***Zu klären:***
  - Fehlertoleranz, fehlgeschlagene Verbindung (Ziel besetzt etc.)
  - Tarifierung in Abhängigkeit der Gesprächsdauer
  - Netz betrügt (kassiert Geld und verweigert Verbindungsaufbau)

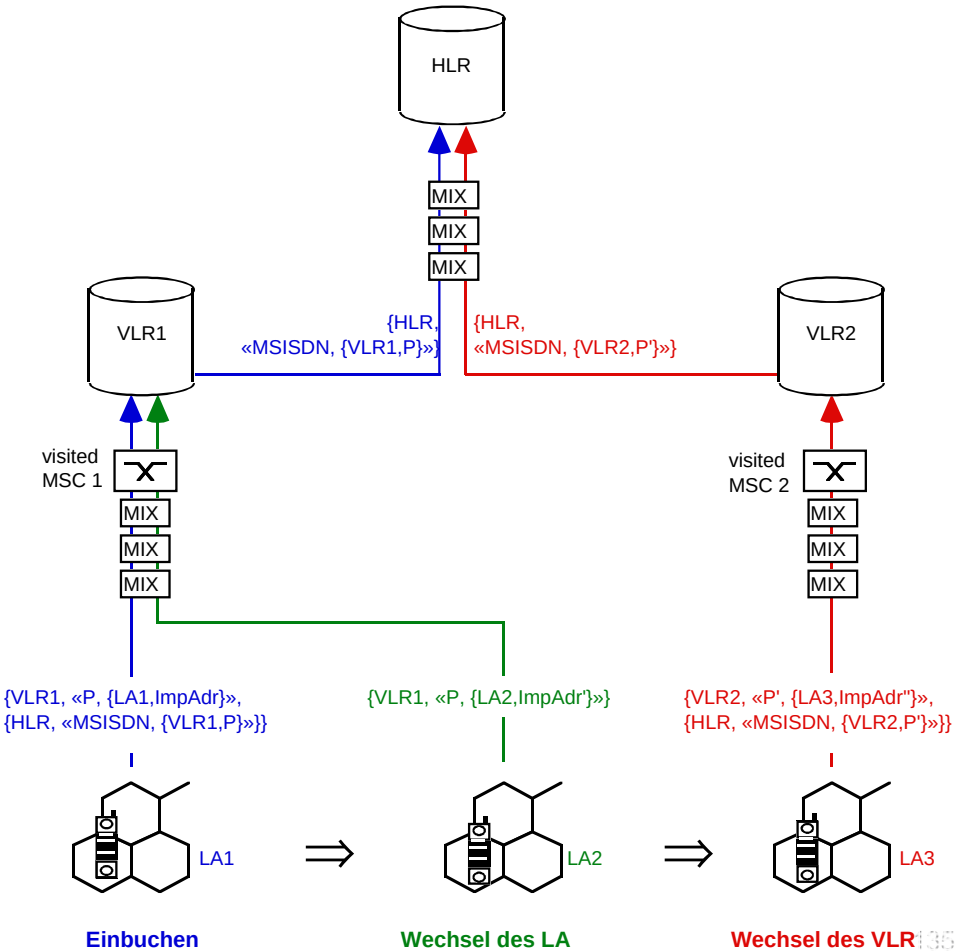
Abrechnung



- ***Ankommende Rufe (zur MS)***
  - Wer bekommt Geld?
  - Besuchter Netzbetreiber oder Heimatnetzbetreiber oder beide?
- ***Skizze (beide fordern Geld):***
  - Signalisierung zur MS
  - Empfangene Signalisiernachricht enthält Geldforderung von Heimatnetz
  - T erhält mit dem Authentication Request (2) die Forderung des besuchten Netzes
  - T schickt mit der Please Check Authentication Nachricht den vom Heimatnetz geforderten Geldbetrag
  - Heimatnetz antwortet mit Please Check Authentication Response nur bei Empfang des Geldes
  - T schickt mit der Authentication Response (2) den vom besuchten Netz geforderten Betrag

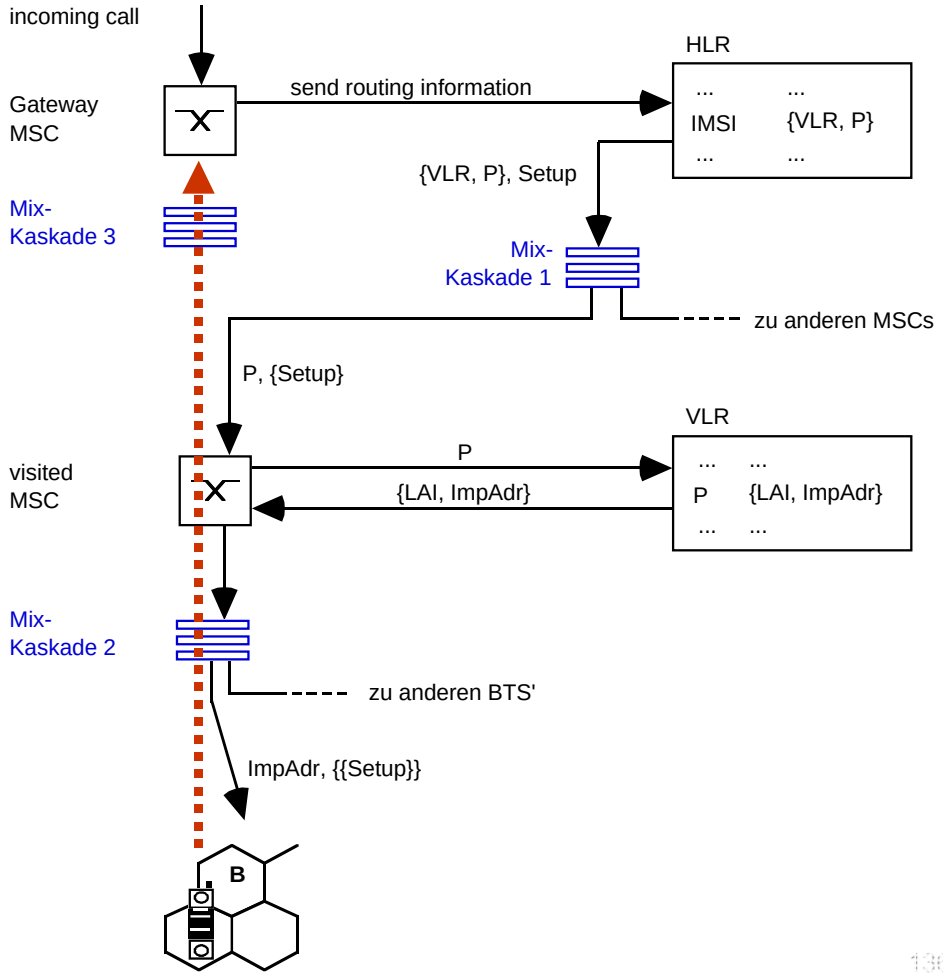
MK-Mixe dezentralisiert

- ***Location Registration und Location Update***



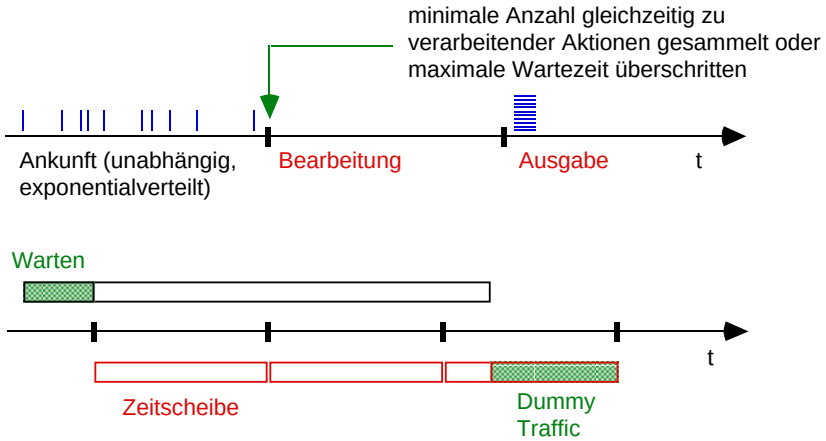
MK-Mixe dezentralisiert

- ***Dezentralisiertes Verfahren (Verbindungsaufbau)***
  - Eintrag im HLR unter Identität:
    IMSI: {VLR, P}
  - Eintrag im VLR unter Pseudonym P:
    P: {LAI, ImpAdr}



Mobilkommunikationsmixe

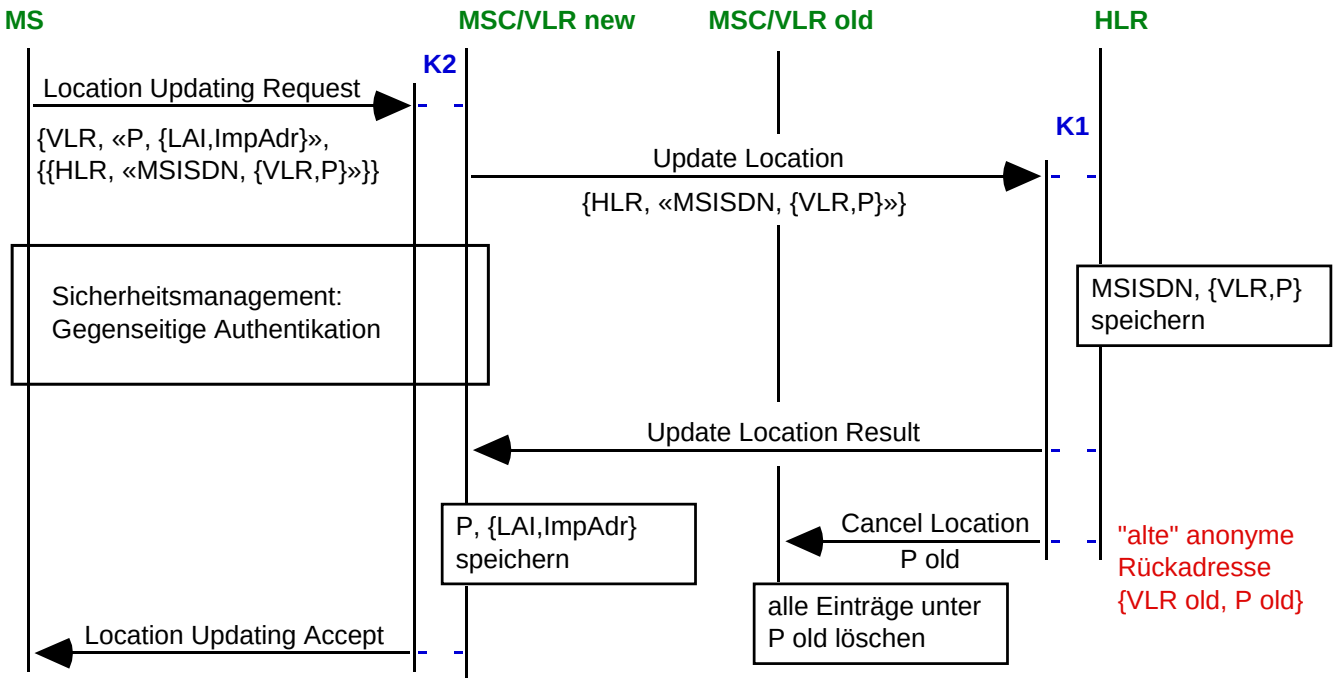
- ***Mixfunktion***
  - Verkettbarkeit über Kodierung der Nachrichten durch Umkodieren (Kryptographie) und Umsortieren verhindert
  - Verkettbarkeit über zeitliche Korrelationen durch Sammeln von Nachrichten und schubweise Ausgabe verhindert
- ***Taktung (Zeitscheiben) und Dummy Traffic:***
  - Zusammenfassung der Signalisiernachrichten mehrerer Teilnehmer



Mobilkommunikationsmixe

- **Grenzen**
  - Dummy Traffic nur eingeschränkt anwendbar
    - begrenzte Akkukapazität der Mobilstationen
  - Verkehrsaufkommen im Netz muß hoch genug sein, damit Schutz erreicht wird
    - einzelne, isolierte Aktion ist im Netz beobachtbar
    - Teilnehmer wartet zu lange auf Erbringen des Dienstes

Location Update Protokoll



Mobile Terminated Call Setup Protokoll

- **Communication Request geht ein beim HLR**
  - mit Schutz des Rufenden: $CR = A_{GMSC}, c_{MS}(KZ_{init}, k_{AB})$
  - ohne Schutz des Rufenden: $CR = A_{GMSC}$, ISDN-SN, $c_{MS}(k_{AB})$
- **Anonymous Communication Request**

$ACR = A_{25}, c_{25}(D_{25}, \ldots c_{21}(D_{21}, m_{K3})\ldots)$ mit

$m_{K3} = A_{35}, c_{35}(D_{35}, \ldots c_{31}(D_{31}, m_{Setup})\ldots)$ mit

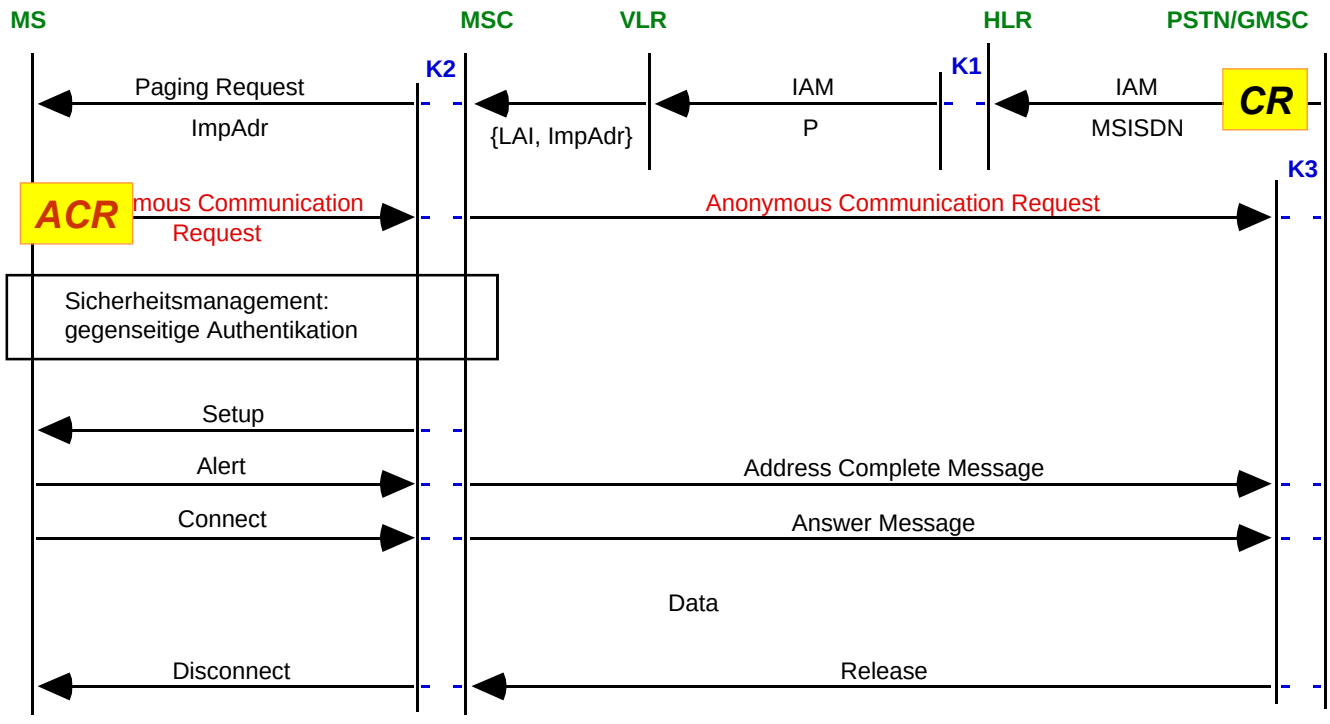
$m_{Setup} = A_{GMSC}$, ISDN-SN/KZ_T, Bv und

$D_{i,j} = T, k_{i,j}$ mit i=2…3, j=5…1, Zeitscheibe: T

- **Kanalkennzeichen**

$KZ_T = f(T, k_{AB})$ mit Ende-zu-Ende-Verschlüsselungsschlüssel: k_{AB}

Mobile Terminated Call Setup Protokoll



Mobile Originated Call Setup Protokoll

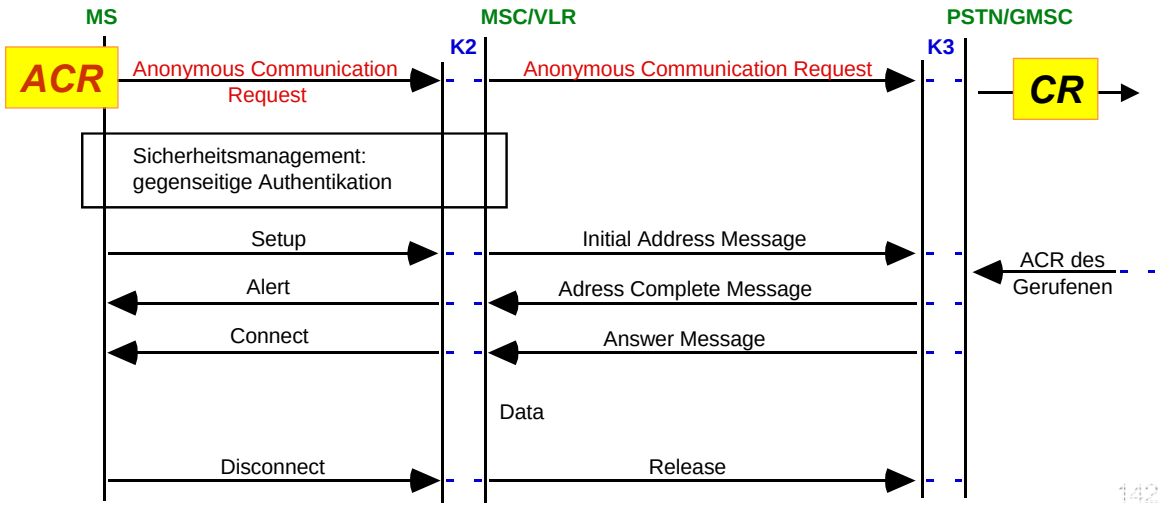
- $ACR = A_{25}, c_{25}(D_{25}, \ldots c_{21}(D_{21}, m_{K3})\ldots)$ mit

  $m_{K3} = A_{35}, c_{35}(D_{35}, \ldots c_{31}(D_{31}, m_{Setup})\ldots)$ mit

  $m_{Setup} = CR, KZ_T, Bv$ mit

  CR = ISDN-SN, $c_{ISDN\text{-}SN}(KZ_{init}, k_{AB})$ und

  $D_{i,j} = T, k_{i,j}$ mit i=2…3, j=5…1



Leistungsfähigkeit

- ***Verfahren leisten***
  - alle: Schutz des Aufenthaltsortes
  - teilweise: Unbeobachtbarkeit der Kommunikationsbeziehungen
    - gegenüber Kommunikationspartner und Netzbetreiber
    - lokale Angreifer (Datenbanken, Insider)
    - globale Angreifer (alle Kommunikation ist überwachbar)
- ***Hauptprobleme***
  - Kanalstruktur existierender Netze
    - Modifikation nötig, damit effizient realisierbar
  - Effizienzverlust zwischen 1 und 10 % je nach Verfahren:
    - Bei maximaler Auslastung ist die versorgbare Teilnehmerzahl maximal 10% geringer.

Mobilkommunikationsmixe

- **Nachrichtenlängen**

- Nachrichtenlängen wachsen mindestens um das 1,2-fache (Rufaufbau) und sogar um das 6,8-fache (Aufenthaltsaktualisierung)

	GSM	Mobilkommunikationsmixe
Rufaufbau	1728…2968	3624…8008
Aufenthaltsaktualisierung	216…328	2221…4502

- **Effizienz**
  - Effizienzmaß: Verhältnis der verfügbaren Verkehrskanäle bei den Mobilkommunikationsmixen und bei GSM
  - Mobilitätsverhalten der Teilnehmer beeinflußt die Effizienz
  - Effizienzverlust bezogen auf bedienbare Teilnehmerzahl ist ca. 10 % bei N_{LUP}=88 in 5 Sekunden (entspricht 20.000 Teilnehmern pro Zelle)

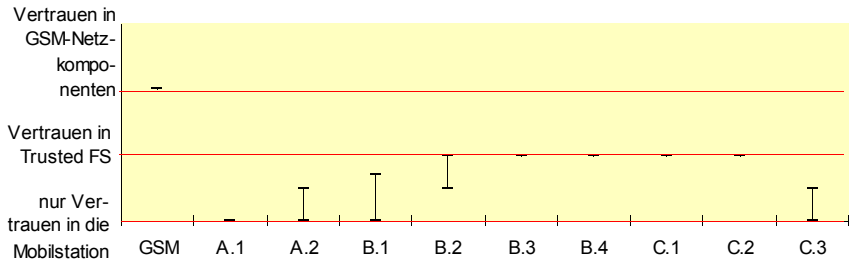
- **Problem: Kanalstruktur von GSM nicht flexibel genug**

Komponenten der MK-Mixe

Komponente	Bedeutung
Mixe	Schutz der Kommunikationsbeziehung zwischen Sender und Empfänger einer Nachricht
Anonyme Rückadressen	Unverkettbarkeit der Übermittlung der Verbindungswunschnachrichten zwischen Registern
Signatur der anonymen Rückadresse beim HLR	Überprüfbarkeit, daß in einem Schub Rückadressen von genügend vielen Teilnehmern bearbeitet werden, d.h. Verhindern eines (n-1)-Angriffs
Pseudonym *P*	Verkettbarkeit des Adreßkennzeichens mit dem Datenbankeintrag im Register (außer HLR, dort MSISDN)
Symmetrische Schlüssel $k_{i,j}$ in den anonymen Rückadressen	Effizientes Umkodieren der mitgelieferten Informationen, Etablieren eines symmetrischen Mix-Kanals bei Call Setup und Location Update; Verwendung einer nicht selbstsynchronisierenden Chiffre zur Verhinderung von Replay-Angriffen
Implizite Adresse *ImpAdr*	Adressierung der MS auf der Funkschnittstelle, Wiedererkennung der anonymen Rückadresse, um symmetrische Schlüssel $k_{i,j}$ zu rekonstruieren
Zeitstempel, Zeitscheibennummer *T*	Verhindern des Replay alter (Mix-Eingabe)-Nachrichten
Kennzeichen *Bv/Bl*	Kennzeichen für Empfänger einer Nachricht, um bedeutungsvolle von bedeutungslosen Nachrichten zu unterscheiden
Kanalkennzeichen KZ_T	Verbinden der unbeobachtbaren Mix-Kanäle von rufendem und gerufenem Teilnehmer
Funktion $f(T, k_{AB})$	Funktion zur Berechnung der Kanalkennzeichen
Symmetrischer Schlüssel k_{AB}	Symmetrischer Sitzungsschlüssel der kommunizierenden Teilnehmer, Parameter zur Berechnung der Kanalkennzeichen

Vergleich der Verfahren: Vertrauen (qualitativ)

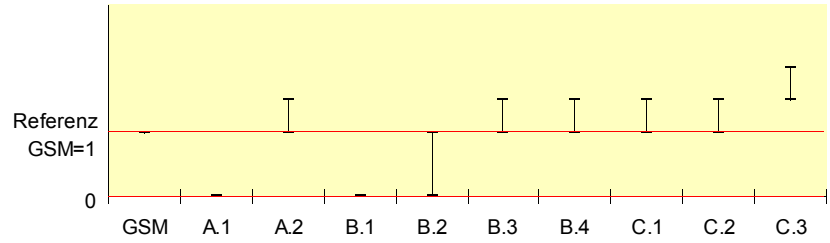
- *Nötiges Vertrauen in einzelne Netzkomponenten bzgl. Vertraulichkeit des Aufenthaltsorts*



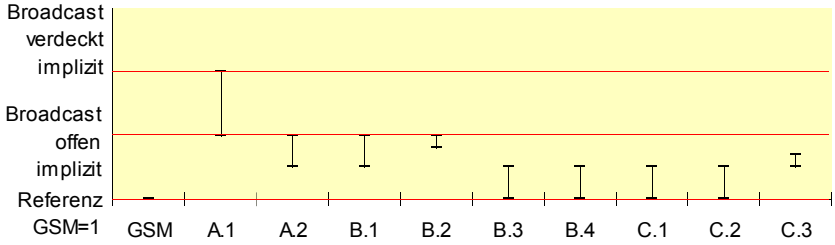
GSM	**Referenzwerte**	**B.3**	**explizite vertrauensw.Speicherung**
A.1	**Broadcast mit impliziter Adressierung**	**B.4**	**TP-Methode**
A.2	**Gruppenpseudonyme**	**C.1**	**Vertrauenswürdige Dritte**
B.1	**Adreßumsetzungsmethode**	**C.2**	**Methode der kooperierenden Chips**
B.2	**Verkl. der Broadcastgebiete**	**C.3**	**Mobilkommunikationsmixe**

Vergleich der Verfahren: Bandbreite (qualitativ)

- *Location Update*



- *Call Setup*



GSM	**Referenzwerte**	**B.3**	**explizite vertrauensw.Speicherung**
A.1	**Broadcast mit impliziter Adressierung**	**B.4**	**TP-Methode**
A.2	**Gruppenpseudonyme**	**C.1**	**Vertrauenswürdige Dritte**
B.1	**Adreßumsetzungsmethode**	**C.2**	**Methode der kooperierenden Chips**
B.2	**Verkl. der Broadcastgebiete**	**C.3**	**Mobilkommunikationsmixe**

Vergleich der Verfahren

	Referenz	A.1	A.2	B.1 – B.4 und C.1		C.2	C.3
	GSM	Broad-cast- Methode	Gruppen-pseudo- nyme	Vertrauenswürd. Speicherung in Trusted FS		Koope-rierende Chips	Mobil-komm.- Mixe
				explizit	TP-Meth.		

Nötiges Vertrauen

Vertrauen in die Mobilstation	nötig	nötig	nötig	nötig	nötig	nötig
Vertrauen in einen ortsfesten Bereich	–	nicht nötig	nicht nötig	zusätzlich nötig	nötig	nicht nötig
Vert. in ein Datenschutz garantierendes Kommunikationsnetz	–	nicht nötig	nicht nötig	nötig	nicht nötig	nötig
Vertrauen in Dritte (Trusted Third Party, TTP), entspricht C.1	nötig	nicht nötig	nicht nötig	möglich, entspricht dann C.1	nicht nötig	nicht nötig

Vergleich der Verfahren

	Referenz	A.1	A.2	B.1 – B.4 und C.1		C.2	C.3
	GSM	Broad-cast- Methode	Gruppen-pseudo- nyme	Vertrauenswürd. Speicherung in Trusted FS		Koope-rierende Chips	Mobil-komm.- Mixe
				explizit	TP-Meth.		

Signalisieraufwand

Funkschnitt-stelle MTC	Bezugs-punkt	sehr hoch	höher	etwa gleich	gering-füg. höher	etwa gleich	höher
Funkschnitt-stelle LUP	Bezugs-punkt	entfällt	höher	höher wg. Zen-tralität	gering-füg. höher	höher wg. Zen-tralität	höher
Bandbreiteauf-wand im Festnetz	Bezugs-punkt	geringer bzgl. Loc. Mgmt.	höher	hoch durch Zen-tralität	gering-füg. höher	hoch durch Zentr.	höher

Funktechnische Peilbarkeit und Ortbarkeit

Sendeverf. zum Schutz vor Pei-lung und Ortung	Fre-quency Hopping	nötig, z.B. über Direct Sequence Spread Spectrum

Vergleich der Verfahren

	Referenz	A.1	A.2	B.1 – B.4 und C.1		C.2	C.3
	GSM	Broad-cast- Methode	Gruppen-pseudo- nyme	Vertrauenswürd. Speicherung in Trusted FS explizit	TP-Meth.	Koope-rierende Chips	Mobil-komm.- Mixe

Anordnung der Sicherheitsbereiche

zentral	quasizen-tral	entfällt		zentral		Zentral	beides ist möglich
dezentral	wäre möglich		dezentral		dezentral		
Diversität der Komponenten	wäre möglich	bedeu-tungslos	nicht not-wendig	notwendig bei Trusted FS		notwen-dig	notwen-dig im Mix-Netz

Dynamisierbarkeit der Sicherheitsbereiche

nur statisch möglich	HLR	entfällt	HLR	Trusted FS	C-NW C-MS	HLR, Mix-Kas-kaden
dynamisch möglich	nicht vor-handen, wäre aber möglich		nicht vor-handen, wäre aber möglich	ausweichen auf TTPs, entspricht dann C.1	nicht sinnvoll, wäre aber möglich	frei wähl-bare Mixe wären möglich

Vergleich der Verfahren

	Referenz	A.1	A.2	B.1 – B.4 und C.1		C.2	C.3
	GSM	Broad-cast- Methode	Gruppen-pseudo- nyme	Vertrauenswürd. Speicherung in Trusted FS explizit	TP-Meth.	Koope-rierende Chips	Mobil-komm.- Mixe

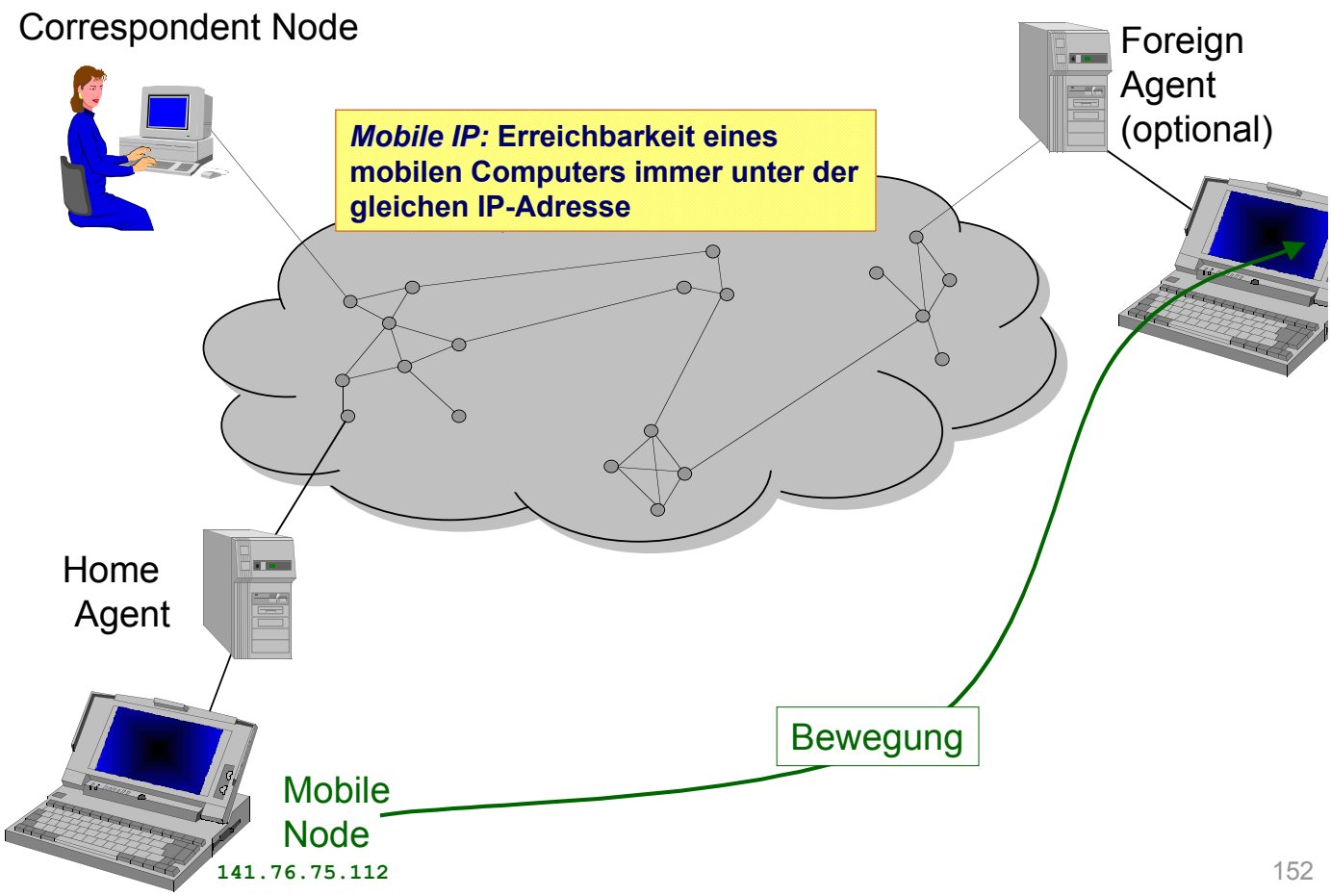
Mobilitätsmanagement

Schutz der Komm.-bez. beim Einbuchen	nicht vor-handen	entfällt	nicht nötig	zusätzlich nötig	nicht nötig	gewähr-leistet
Verkettung von Teilnehmer-aktionen	Teilneh-mer nicht anonym	nicht möglich	hoch	gering	gering	nicht möglich

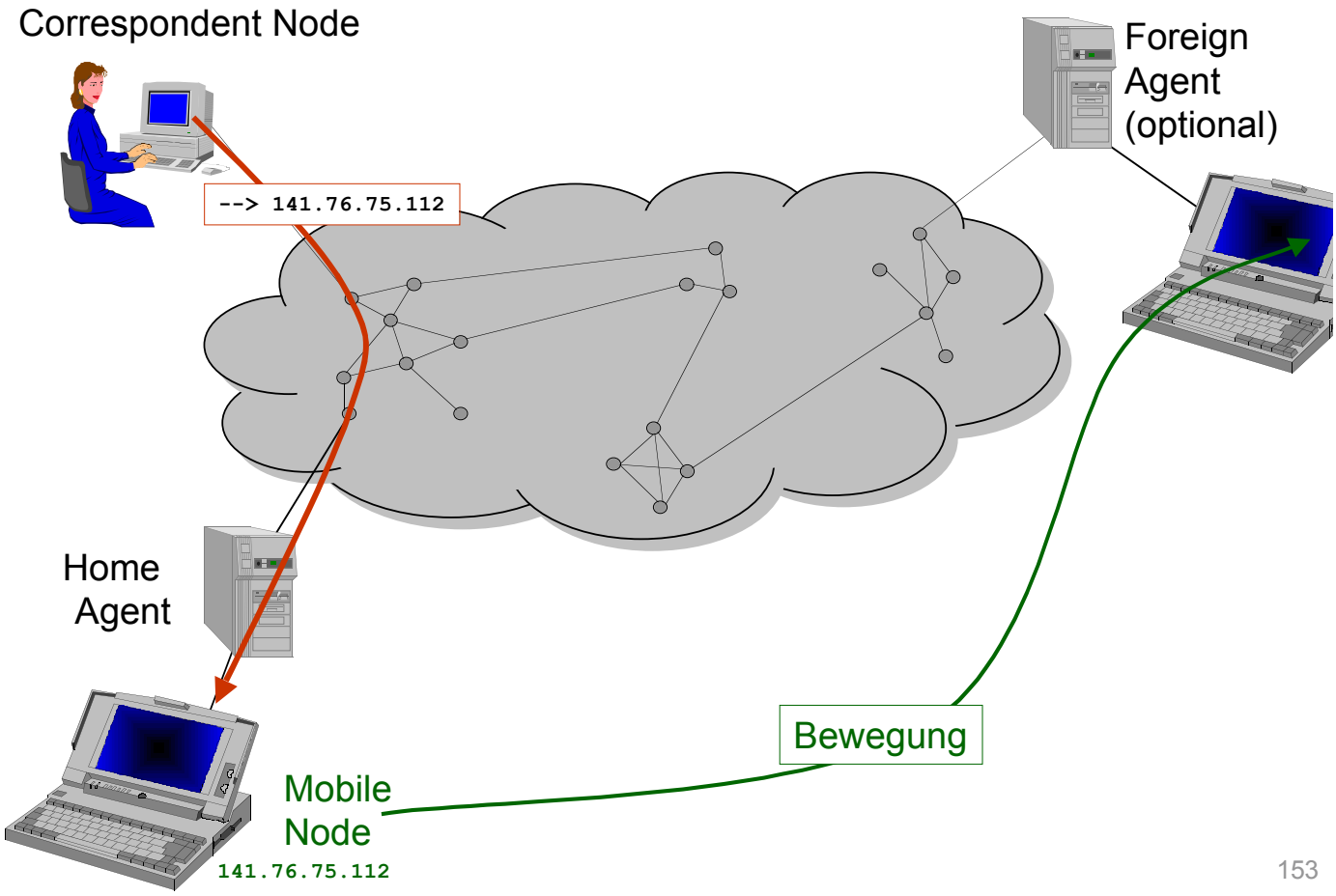
Verbindungsmanagement

Schutz der Komm.-bez. beim Signalisie-ren (Call Setup)	nicht vor-handen	nicht nötig	nicht nötig	zusätzlich nötig	zusätzlich nötig bis zum HLR	nötig	gewähr-leistet
Adressierungs-merkmal auf der Fu-schnittstelle	TMSI	implizite Adresse	implizite Adresse	TMSI o. implizite Adresse	PMSI, TMSI, i. Adr.	TMSI, PMSI, impl. Adr.	implizite Adresse
Schutz der Komm.-bez. während einer Verbindung	nicht vor-handen	nötig, z.B. über Mix-Netze					

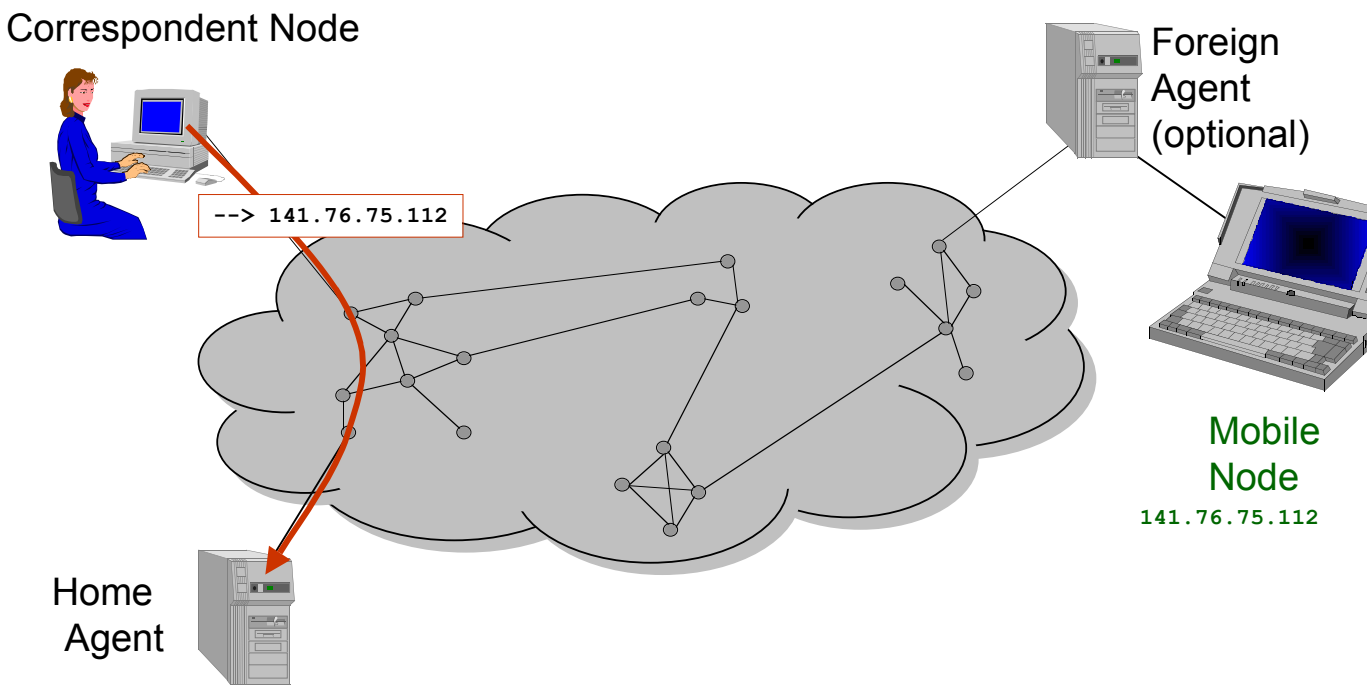
Mobile Internet Protocol: Prinzip 1/4



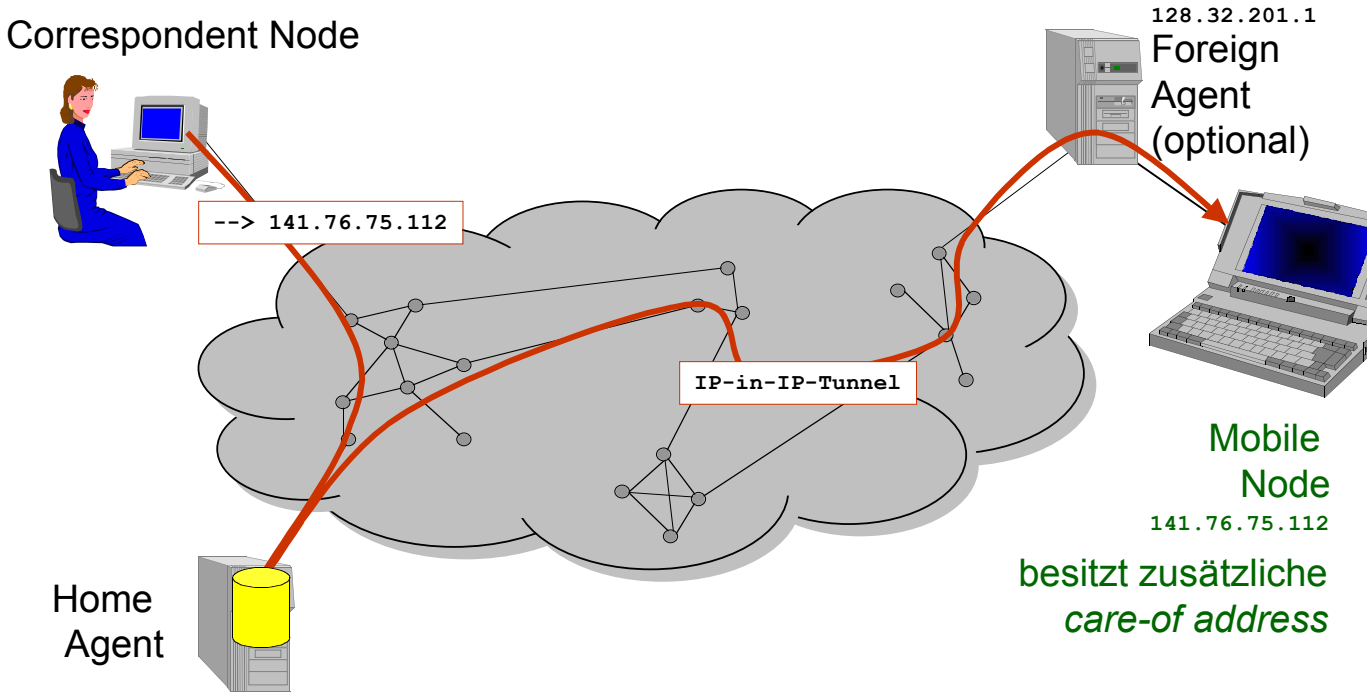
Mobile Internet Protocol: Prinzip 2/2



Mobile Internet Protocol: Prinzip 3/4



Mobile Internet Protocol: Prinzip 4/4

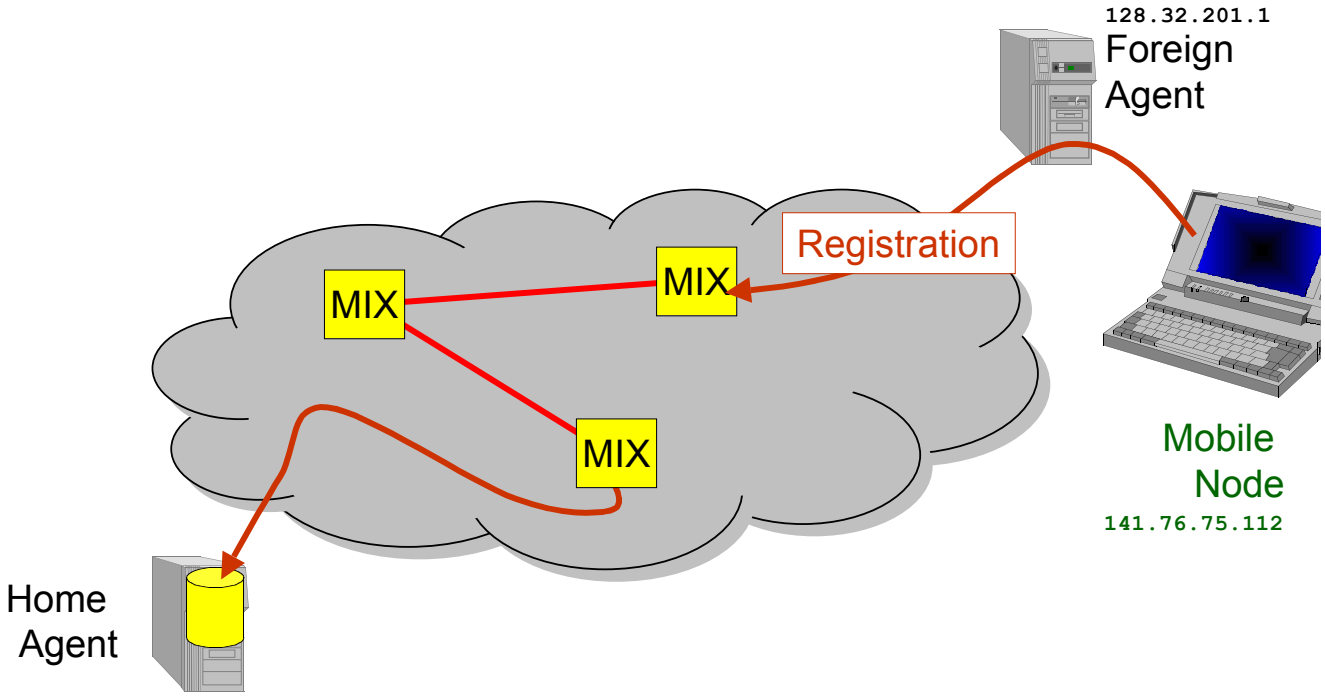


Binding:
141.76.75.112 --> 128.32.201.1

Mobile Internet Protocol: Sicherheitsfunktionen

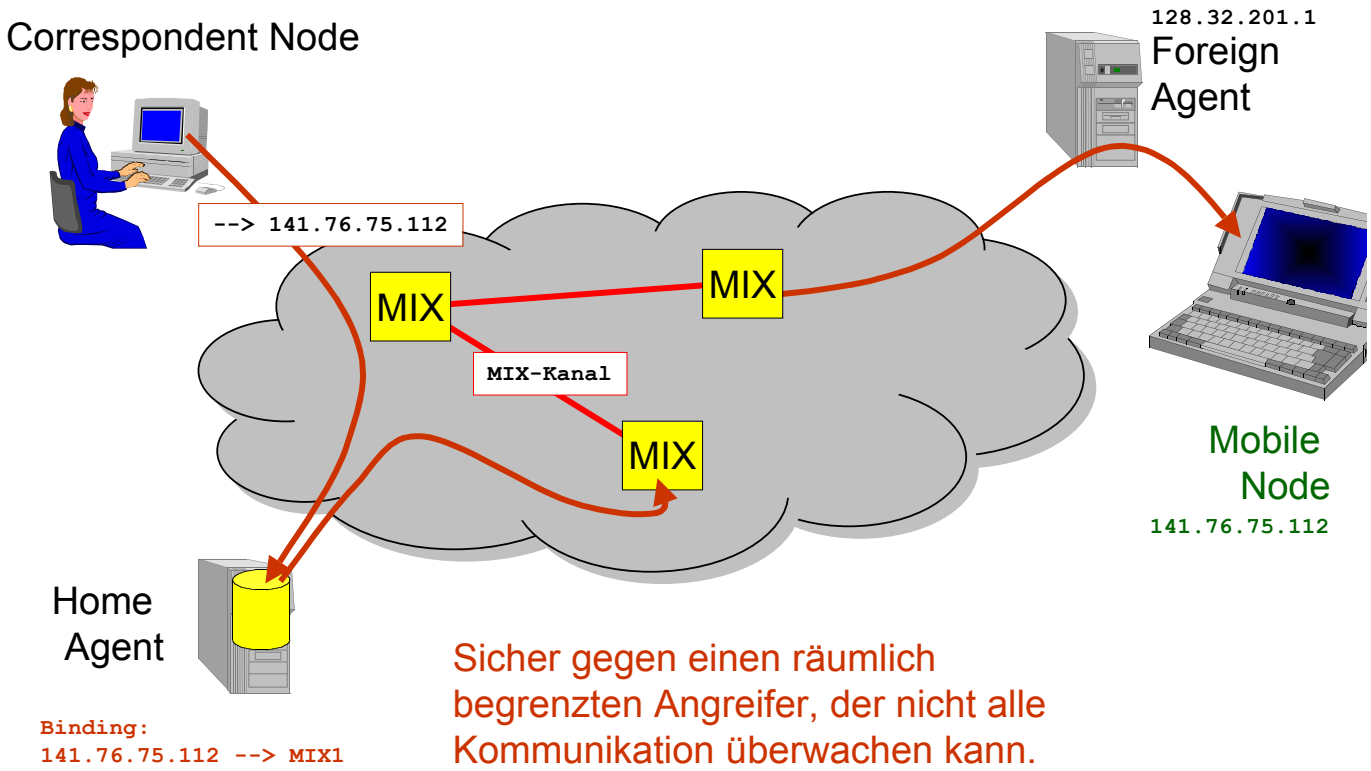
	Mobile IPv4	Mobile IPv6
Authentikation	√ shared secret zwischen Mobile Node und Home Agent MD 5 Fingerprint	√ IPSec/IPv6 Authentication Header (AH) MD 5, SHA-1
Verschlüsselung	∅	√ IPSec/IPv6 Encapsulated Security Payload (ESP) DES/CBC
Schutz vor Lokalisierung	∅	∅
	Mixed Mobile IP Non-Disclosure Method	

Mobile Internet Protocol: Schutz vor Lokalisierung



Mixed Mobile IP (MMIP)
Non-Disclosure Method

Mobile Internet Protocol: Schutz vor Lokalisierung



Sicher gegen einen räumlich begrenzten Angreifer, der nicht alle Kommunikation überwachen kann.

Mixed Mobile IP (MMIP)
Non-Disclosure Method

Politische Dimension solcher Konzepte

Freiheit	Regulierung
– Es gibt gesetzliche Grundlagen, die eine Bereitstellung pseudonymer und anonymer Dienstleistungen ausdrücklich erlauben und anregen. – Empfehlungscharakter – IuKDG (TDDSG § 4(1)) – Kein Zwang („soweit technisch möglich und zumutbar“)	– Derzeit von der Politik nicht gewünscht – TKG fordert die Speicherung der Kundendaten (Name, Adresse, ...), sogar bei vorbezahlten Systemen (Xtra-Card etc.) – Überwachungsschnittstellen (TKG § 88), die dem Bedarfsträger die unbeobachtbare Überwachung erlauben

Gesetzliche Grundlagen sind keineswegs konsolidiert.

Technische Möglichkeiten des Schutzes und der legalen Überwachungsmöglichkeiten ausloten, jedoch möglichst kein vorauseilender Gehorsam

Security of mobile communication

- **Conclusion**
  - Protection of locations can be technically realized
  - However, there is a demand for legal enforcement
- **More information**
  - http://www.inf.tu-dresden.de/~hf2/mobil/