Technischer Datenschutz in der Mobilkommunikation

Analyse von Sicherheitsproblemen in existierenden Netzen

Hannes Federrath

TU Dresden, Institut für Theoretische Informatik, 01062 Dresden
federrath@inf.tu-dresden.de

Oktober 1995 – März 1996

Dieses Papier wurde inhaltlich im Oktober 1995 fertiggestellt. Alle nachfolgenden Versionen weisen gegenüber der Version vom Oktober 1995 nur geringe Änderungen auf.

Dank

Für Zuarbeiten, insbesondere an den Abschnitten über *Location Update* und *Call Setup* danke ich Jan Müller. Weiterhin danke ich allen Studenten und Kollegen, die während des Forschungsseminars, in dem Teile dieses Papiers vorgestellt wurden, mit Anregungen und Verbesserungen zum Entstehen dieses Papiers beigetragen haben. Diese Arbeit wurde finanziell unterstützt von der Gottlieb-Daimler- und Karl-Benz-Stiftung Ladenburg.

Hannes Federrath

Inhaltsverzeichnis

1 Allgemeines zur Mobilkommunikation 5

1.1 Unterschiede zwischen Festnetz- und Mobilkommunikation 5
1.2 Einteilungsmöglichkeiten für mobile Netze 5
1.3 Beispiele für mobile Netze 6
1.3.1 C-Netz 6
1.3.2 AMPS (Advanced Mobile Phone Service) 6
1.3.3 CT (Cordless Telephone) 6
1.3.4 DECT (Digital European Cordless Telephone) 7
1.3.5 GSM 7
1.3.6 PCN, DCS 1800 7
1.3.7 ERMES (European Radio Messaging System) 7
1.3.8 DSRR (Digital Short Range Radio) 7
1.3.9 TFTS (Terrestrial Flight Telephone System) 7
1.3.10 MODACOM 8
1.3.11 Wireless Networks 8
1.3.12 Iridium von Motorola 8
1.3.13 GPS (Global Positioning System) 8
1.3.14 UMTS (Universal Mobile Telecommunication System) 9

2 Mobilkommunikationssysteme und Sicherheit 11

2.1 Technische Datenschutzforderungen 11
2.2 Die Sicherheitswelt der „anderen“ 12

3 Mobilkommunikation am Beispiel GSM 15

3.1 Allgemeines 15
3.1.1 Standardisierung von GSM 15
3.1.2 Leistungsmerkmale von GSM 15
3.1.3 GSM in Zahlen 16
3.2 Struktur von GSM 16
3.2.1 Architektur 16
3.2.2 Funktechnischer Aufbau 18
3.2.3 Mobilfunkgebiete im GSM 19
3.2.4 Subscriber Identity Module 19
3.3 Datenbanken des GSM 20
3.3.1 Home Location Register 20
3.3.2 Visitor Location Register 21
3.3.3 Equipment Identity Register 21
3.3.4 Authentication Center 21

4 Sicherheitsrelevante Prozeduren und Funktionen im GSM 23

4.1 Zugangskontrolle 23
4.2 Authentikation mittels Challenge-Response-Verfahren 23
4.3 Pseudonymisierung des Teilnehmers durch TMSI 24
4.4 Generierung des Chiffrierschlüssels Kc 26
4.5 Inhaltsdatenverschlüsselung auf der Luftschnittstelle 26
4.6 Ein Beispiel 27

5 Mobilitäts- und Verbindungsmanagement des GSM 29
5.1 Location Management 29
5.1.1 Altes VLR, altes MSC, neues LA 30
5.1.2 Altes VLR, neues MSC, neues LA 31
5.1.3 Neues VLR, neues MSC, neues LA 32
5.2 Rufaufbau (Call Setup) 32
5.2.1 Mobile Originated Call Setup 33
5.2.2 Mobile Terminated Call Setup 33

6 Sicherheitsprobleme beim GSM 35
6.1 Erstellbarkeit von Bewegungsprofilen 35
6.2 Entgeltabrechung 36
6.3 Registrierung der Gerätekennungen (EIR) 37
6.4 Zusammenfassung 37

7 Abkürzungsverzeichnis 39

8 Literaturverzeichnis 41

Abbildungen

Klassifikation der Öffentlichen Funknetze (in Anlehnung an [Bial_94, S.3]) 6
Prinzipschaltbild eines GPS-Empfängers für C/A-Code 9
Architekturschema des GSM nach [Keda_91] 17
Logischer Netzaufbau im GSM 18
Aufteilung der Bandbreite in Radiokanäle 18
Authentikationsprozedur 24
Neuvergabe einer TMSI bei bekannter alter TMSI 25
Neuvergabe einer TMSI bei unbekannter alter TMSI 25
Generierung von Kc 26
Verschlüsselung auf der Funkschnittstelle 27
Zusammenspiel von Sprachkodierung, Inhaltsdatenverschlüsselung und Kanalkodierung 27
Zusammenspiel der Sicherheitsfunktionen am Beispiel Location Update 28
Verschiedene Situationen für LUP und HOV 30
LUP: Altes VLR, altes MSC, neues LA (TMSI bekannt) 31
LUP: Altes VLR, neues MSC, neues LA (TMSI bekannt) 32
LUP: Neues VLR, neues MSC, neues LA (altes VLR erreichbar bzw. TMSI bekannt) 32
Mobile Originated Call Setup 33
Mobile Terminated Call Setup 34

1 Allgemeines zur Mobilkommunikation

Mobilkommunikation findet man inzwischen allerorts: Wo vor einigen Jahren noch Spezialanwendungen dominierten, hat sich der Massenmarkt durchgesetzt. Wer durch die größeren Städte Deutschlands (und Europas) schlendert, findet auf Häusern und Türmen oft neuen „Antennensalat“: Die Fernsehantennen sind verschwunden, die Mobilfunkantennen sind an ihre Stelle getreten.

Die Geschichte der Mobilkommunikation geht einige Jahre zurück:

Bereits Ende des vergangenen 19. Jahrhunderts gelang dem Ingenieur und Nobelpreisträger für Physik Marconi (1874 – 1937) der Nachweis der drahtlosen Nachrichtenübertragung.

Im Jahre 1918 wurden in Deutschland die ersten Mobilfunkversuche entlang der Eisenbahnstrecke Berlin – Zossen in fahrenden Zügen durchgeführt.

Im Jahre 1926 wurde ein öffentlicher Zugtelefondienst auf der Strecke Hamburg – Berlin eröffnet.

Die Mobilfunktechnik wurde jedoch erst in den 50er Jahren stark weiterentwickelt, nachdem man die Vorteile der UKW-Technik nutzen konnte. So entstanden handvermittelte Funktelefonnetze im 30-, 80- und später 160-MHz-Bereich. Diese Netze wurden 1958 in das sog. A-Netz integriert, das 1968 eine nationale Flächendeckung von etwa 80 % erreichte und von ca. 10 000 Teilnehmern genutzt werden konnte. Ab 1972 wurde das A-Netz dann durch die Netze B/B2 abgelöst, die 1986 etwa 27 000 Teilnehmer versorgten.

Ab 1985 begann der Betrieb des zellularen Funknetzes C, das als erstes nationales Netz die landesweite Auffindbarkeit und damit Erreichbarkeit unterstützte (sog. *Roaming*).

Mit dem D-Netz begann für den Massen-Mobilfunk Anfang der 90er Jahre das digitale Zeitalter. Dieses Netz wurde europaweit als sog. GSM-Netz (*Global System for Mobile Communication, Groupe Spéciale Mobile*) standardisiert. Das E-Netz ist prinzipiell ein GSM-Netz, wird aber oft als DCS 1800 (*Digital Cellular System*) oder PCN (*Personal Communication Network*) bezeichnet.

1.1 Unterschiede zwischen Festnetz- und Mobilkommunikation

Einige wesentliche Unterschiede zwischen Festnetz- und Mobilkommunikation sind:

Die Teilnehmer können sich größräumig bewegen.

Die Bandbreite auf der Luftschnittstelle ist knapp.

Die Luftschnittstelle ist störanfälliger als die Leitungen des festen Netzes.

Die Luftschnittstelle bietet neue Angriffsmöglichkeiten: z.B. Peilbarkeit und erleichterte Abhörmöglichkeit.

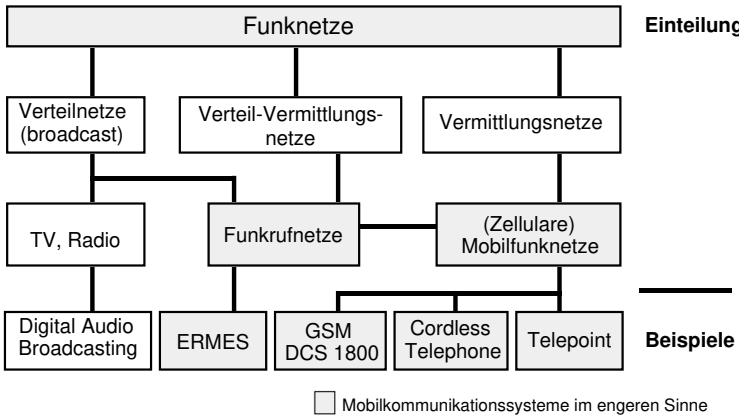
1.2 Einteilungsmöglichkeiten für mobile Netze

Mobile Netze verwenden den freien Raum als Übertragungsmedium. Entsprechend kann man mobile Netze nach der Wellenlänge bzw. Frequenz des Trägers im Übertragungsmedium unterscheiden: Hertzsche Wellen, auch **Funkwellen** genannt (f = 100 MHz bis mehrere GHz), **Lichtwellen** (infrarot) und Schallwellen (bisher ungebräuchlich).

Da Bandbreite im Mobilfunk knapp ist, nutzt man die mit zunehmender Frequenz abnehmende Ausbreitungsfähigkeit der Wellen aus und verwendet die zugewiesenen Frequenzbänder mehrfach. Hierzu ist eine Einteilung des zu versorgenden Gebietes in Bereiche, sog. Zellen, notwendig. Entsprechend der Zellgröße können wir **Pikozellen** (d < 100 m), **Mikrozellen** (d < 1 km) [Evci_92] sowie **Makrozellen** (d < 20 km), **Hyperzellen** (d < 60 km) und sog. Overlay-Zellen (d < 400 km) [Bial_94, S.6] unterscheiden.

Weitere Unterscheidungsmerkmale könnten z.B. öffentliche oder nichtöffentliche, terrestrische oder satellitengestützte, analoge oder digitale mobile Netze sein.

Öffentliche Funknetze an sich lassen sich z.B. in folgender Weise klassifizieren:



Klassifikation der Öffentlichen Funknetze (in Anlehnung an [Bial_94, S.3])

1.3 Beispiele für mobile Netze

Die folgende Zusammenstellung ist größtenteils aus [Silb_92] entnommen. Durch den sich schnell verändernden Markt ist damit zu rechnen, daß in kürzester Zeit neue Services entstehen werden.

Außer Satellitennetzen arbeiten die meisten Funknetze im UHF-Band (300 MHz–3 GHz).

Bei der Darstellung wird bereits auf einige Sicherheitsmerkmale eingegangen.

1.3.1 C-Netz

Das C-Netz – ein deutsches Netz – arbeitet auf den (unverschlüsselten, aber verschleierten) Sprachkanälen als *analoges zellulares Funknetz*. Die Signalisierung wurde hier jedoch bereits digitalisiert und unterstützt *Roaming*. Als Arbeitsfrequenz wurde ein Bereich um 450 MHz festgelegt.

1.3.2 AMPS (Advanced Mobile Phone Service)

AMPS ist ein amerikanischer *analoger Mobilfunk-Standard*, ähnlich dem deutschen C-Netz.

1.3.3 CT (Cordless Telephone)

Cordless Telephone entwickelte sich in mehreren Etappen (CT-0,-1,-2,-3, neuerdings DECT) (nach [Bial_94, S.12f]):

Zunächst wurde **CT-1** von der CEPT realisiert. Reserviert wurden dafür europaweit die Frequenzen 914 MHz und 958 MHz. Später wurden diese Frequenzbereiche an das GSM vergeben. CT-1 arbeitet analog. Sprache wird unverschlüsselt übertragen.

CT-2/(CAIS: *Common Air Interface Standard*) ist in Großbritannien auch unter dem Namen **Telepoint** bekannt geworden. Es ermöglicht in städtischen Gebieten das Führen eines Telefongesprächs, jedoch nicht das Entgegennehmen. Damit wurde auf das aufwendige Lokalisierungsmanagement verzichtet. Bei CT-2 wird die Sprache verschleiert (invertiert) übertragen.

CT-3 wurde parallel zu DECT entwickelt und unterstützt pikozellulare Mehrzellenstrukturen.

1.3.4 DECT (Digital European Cordless Telephone)

DECT wurde von der ETSI 1992 genormt. Ihm wurde europaweit der Frequenzbereich 1880 bis 1900 MHz zugeteilt. Mit einer Datenrate von 32 kbit/s soll DECT kompatibel zu PSTN (herkömmliches Telefonnetz) und UMTS (*Universal Mobile Telecommunication System*) sein. Es ist ein pikozellulares Funknetz mit Mehrzellenkonfiguration, die über eine hierarchische Gruppierung erreicht wird. So unterstützt es verschiedene Zielnetze mit unterschiedlichen Zellgrößen und Anwendungen. Dadurch soll eine gute Verwendbarkeit als lokaler (inhouse), aber auch globaler Kommunikationsstandard gegeben sein. DECT unterstützt dadurch auch das Streben nach einer persönlichen und stets einheitlichen Kommunikationsumgebung, wie sie von der PCN-Initiative gefordert wird.

1.3.5 GSM

GSM ist ein zellulares Funknetz der zweiten Generation, das *Roaming* unterstützt. In den weiteren Abschnitten wird auf GSM näher eingegangen.

1.3.6 PCN, DCS 1800

PCN wurde Ende 1988 auf Initiative des britischen Ministeriums für Handel und Industrie (DTI) ins Leben gerufen. Ziel von PCN ist die Weiterentwicklung zellularer Mobilfunkdienste auf der Basis von GSM. Dabei soll es

- eine höhere Kapazität und Dienstqualität als GSM bieten,
- sowohl geschäftliche als auch private Kunden (Heimbedarf) als Zielgruppe erreichen,
- auch mit Festnetz-Diensten in Wettbewerb treten.

PCN, auch DCS 1800 genannt, ist ein direkter Nachkömmling des GSM und unterscheidet sich im wesentlichen in seiner Funkfrequenz, die höher liegt als die von GSM. Dadurch werden kleinere Zellen und somit wiederum sparsamere und leichtere mobile Geräte möglich. Die Zellengröße ist kleiner als bei GSM.

PCN bietet wie DECT gute Ansätze auf dem Weg zu einem weltumspannenden Mobilkommunikationssystem, dem UMTS. Ein deutliches Zeichen sind z.B. Bestrebungen, ein Interworking zwischen beiden Standards (PCN und DECT) bei der Rufnummernidentifizierung, der Aufenthaltsregistrierung und Datenverschlüsselung auf der Funkschnittstelle zu erreichen.

1.3.7 ERMES (European Radio Messaging System)

ERMES ist ein Beispiel für einen Pager-Dienst. Als Ergänzung zu den zellularen GSM-Diensten soll es einen europaweiten, flächendeckenden Funkrufdienst bereitstellen.

1.3.8 DSRR (Digital Short Range Radio)

DSRR ermöglicht ausschließlich Verbindungen zwischen mobilen Teilnehmern. Dabei werden Verbindungen auch über Relaisstationen geschaltet. Zielgruppe dieses Systems sind vor allem kleinere Betriebe und Transportunternehmen, aber auch Personen, die bisher Teile ihrer Kommunikation über CB-Funk abgewickelt haben.

DSRR wurde von der ETSI standardisiert und hat die Frequenzbereiche 880-890 MHz und 933-935 MHz.

1.3.9 TFTS (Terrestrial Flight Telephone System)

TFTS ist ein terrestrisches Flugtelefonsystem, dessen Normung durch die ETSI und SITA im Dezember 1991 begann. Es sollte 1993 eingeführt werden. TFTS ist für den europäischen Luftverkehr bestimmt und arbeitet in zwei 5-MHz-Bändern bei 1,7 und 1,8 GHz.

1.3.10 MODACOM

Modacom ist ein Produkt der Deutschen Telekom AG und soll in den deutschen Ballungsgebieten als paketorientierter Datendienst mit 9,6 kbit/s zur Verfügung stehen. Sprache wird nicht unterstützt. Durch Mailbox-Dienste wird die ständige Erreichbarkeit der Endgeräte gesichert. Es unterstützt Datenbank-Abfrage-Dienste und Paketvermittlung (X.25) und soll darüber hinaus als Außendienst- und Fahrzeugsteuerungssystem dienen.

1.3.11 Wireless Networks

Der Name ist eigentlich irreführend, da es sich bei den hier behandelten Netzen ausschließlich um „schnurlose“ Netze, Dienste oder Geräte handelt. Wireless Networks finden meist Anwendung als sog. Inhouse Networks. Sie arbeiten oft auf Infrarot- Basis, z.B. im medizinischen Bereich, um die dort ohnehin schon hohe (elektromagnetische) Strahlenbelastung gering zu halten. Meist werden sie zur Datenkommunikation eingesetzt.

1.3.12 Iridium von Motorola

Iridium ist ein Satelliten-Kommunikationsdienst, der von Motorola ins Leben gerufen wurde. Satelliten-Kommunikationsdienste sind als Ergänzung zu den terrestrischen Mobilkommunikationssystemen zu verstehen.

Iridium arbeitet mit 77 auf einer niedrigen Umlaufbahn (*Low Earth Orbit*, LEO) kreisenden Satelliten. Technisch verwendet Iridium ein ähnliches Konzept wie GSM. Durch die großen Zellgebiete lassen sich die Handover-Prozesse, die durch die Relativbewegung Satellit/Erdoberfläche vorgenommen werden müssen, bedeutend einfacher als im GSM lösen, da die vergleichsweise geringe Bewegung des mobilen Teilnehmers vernachlässigt werden kann. Als Frequenzbereich wurde die Frequenzen 1,61 und 1,6255 GHz reserviert. Die Funkkanäle sind ähnlich dem GSM in TDMA-Frames (*Time Division Multiplex Access*) geteilt.

Der große Vorteil der Satellitenkommunikation ist die überall gegebene potentielle Erreichbarkeit des mobilen Teilnehmers. Das ermöglicht neue Dienste wie weltweites Paging und Personensuchsysteme.

Ein weiteres, in der Normung befindliches Satelliten-Kommunikationssystem ist Inmarsat *(International Maritime Satellite).*

1.3.13 GPS *(Global Positioning System)*

GPS wurde von der US-Verteidigungsbehörde ab 1970 aufgebaut und ist seit 1993 verfügbar. Es ermöglicht die absolute Standortermittlung (in 3 Ebenen) auf (fast) jedem Punkt der Erde mit einer Genauigkeit von wenigen Metern. Es liefert dabei kontinuierliche Angaben über Position und Geschwindigkeit von Objekten sowie hochgenaue Zeitangaben.

GPS ist also eigentlich kein Mobilkommunikationssystem im engeren Sinne, sondern ein Navigationssystem.

Ein Vorteil von GPS gegenüber anderen Navigationssystemen ist seine Wetterunabhängigkeit. Offizieller Name ist Navastar GPS (*Navigation System with Timing and Ranging*).

Das System besteht aus den drei Systemanteilen Raumsegment, Kontrollsegment und Nutzsegment (nach [Grab_89]).

Das **Raumsegment** besteht aus 18 Satelliten[1] auf 6 Umlaufbahnen in 20178 km Höhe mit einer Umlaufzeit von 11 Stunden 57 Minuten. Zu jedem Zeitpunkt können so auf jedem Punkt der Erde mindestens 4 Satelliten gleichzeitig empfangen werden.

---

1 Andere Angaben sprechen auch von 24 Satelliten, von denen nur 21 benötigt werden [With_95].

Jeder Satellit hat einen Empfänger und Sender und sendet auf zwei sog. L-Band Trägerfrequenzen (L1=1575,42 MHz und L2=1227,60 MHz) einen zivilen (*C/A-Code, Clear* oder *Coarse Acquisition Code*) und einen militärischen Code (*P-Code, Precision* oder *Pseudorandom Code*). Übermittelt werden:

- die Identität des sendenden Satelliten,
- seine Position,
- die Uhrzeit,
- weitere Informationen.

Das P-Code-Signal wird verschlüsselt übertragen, hat eine Bandbreite von 20 MHz und ist Spread Spectrum (PN)-moduliert. Das C/A-Code-Signal hat dagegen nur eine Bandbreite von etwa 2 MHz.

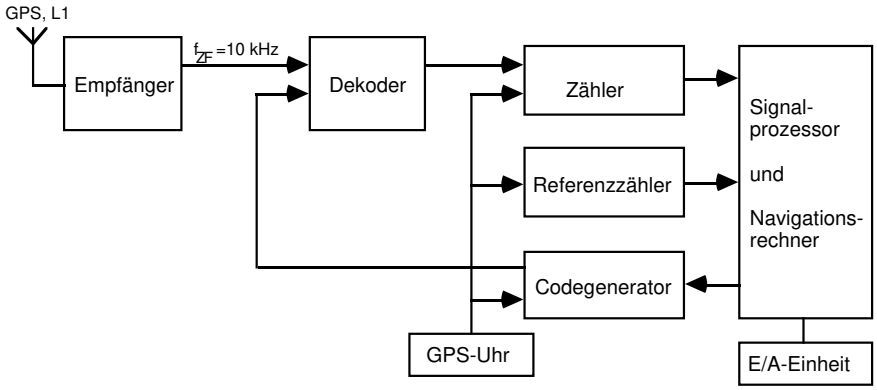
Das **Kontrollsegment** besteht aus mehreren Bodenstationen, welche die Flugbahnen der Satelliten vermessen und ggf. Korrekturdaten übermitteln. Die Bodenstationen dokumentieren außerdem, ob die von den Satelliten gesendeten Daten richtig sind.

Das **Nutzsegment** wird durch die sog. GPS-Empfänger gebildet. Der GPS-Empfänger auf der Erde empfängt zur gleichen Zeit die Signale von 4 Satelliten, wobei nur 3 Signale für eine dreidimensionale Standortbestimmung nötig sind. Der vierte Satellit dient zur Synchronisation der Empfängeruhr mit der Atomuhr des Satelliten. Durch die Auswertung der Phasenverschiebung der Satellitensignale (Doppler-Effekt) kann der Empfänger die eigene Geschwindigkeit und Beschleunigung ermitteln.

Die Genauigkeit von GPS beim C/A-Code beträgt ca. 30-100 m, die Geschwindigkeit kann auf 0,1m/s ermittelt werden und die Zeitgenauigkeit beträgt 100 µs. Leider sieht das System vor, daß der Betreiber die Ungenauigkeit bewußt auf 200 m erhöhen kann. Für zivile Anwendungen wird nur eine Frequenz ausgewertet.

Die Genauigkeit von GPS beim P-Code soll 15 m betragen. Die Geschwindigkeitsmessung wird ebenfalls mit 0,1m/s angegeben und die Zeitgenauigkeit mit 100 ns.

Die Genauigkeit von GPS kann durch das sog. Differenzortungsverfahren (*Differential GPS*) weiter verbessert werden. Hierzu wird ein GPS-Empfänger an einem exakt vermessenen Standort stationär eingesetzt. Dessen bekannte Position wird mit den von GPS gelieferten Daten verglichen und die Korrekturdaten an alle lokalen GPS-Empfänger weitergeleitet.



Prinzipschaltbild eines GPS-Empfängers für C/A-Code

1.3.14 UMTS (Universal Mobile Telecommunication System)

UMTS wird als das allgemeine Mobilkommunikationssystem der Zukunft (3. Generation) bezeichnet. In UMTS ist die Schaffung einer gemeinsamen Plattform für existierende Systeme der 2. Generation, beispielsweise Mobilkommunikationssysteme der Standards GSM, DECT, DCS 1800, ERMES usw., sowie die Integration neuer Systeme geplant.

Merkmale von UMTS sind:

- **Weltweite Nutzbarkeit:** Das bedeutet, daß UMTS einer internationalen Normung unterzogen werden muß. Deshalb soll eine weltweite Standardisierung unter dem Namen *Future Public Land Mobile Telecommunication System* (FPLMTS) erfolgen.
- **Integration aller Mobilfunkdienste:**
  - schnurlose: CT2, z.B. das britische Telepoint, und DECT,
  - zellulare: GSM, DCS 1800, PCN,
  - Satellitenkommunikation, z.B. Iridium von Motorola,
  - weitere: z.B. Pager-Dienste wie ERMES.
- **Unterstützung von Mobilität in Festnetzen** (z.B. *Personal Mobility*).
- **Nutzung neuer Frequenzbereiche:** Für FPLMTS wurden bereits Frequenzbänder zwischen 1,7 und 2,69 GHz reserviert. Ebenso soll ein Bereich bei 20 GHz für Satellitennetze belegt werden.
- **Kleinere Funkzellen**, um noch mehr Teilnehmer pro Fläche versorgern zu können. UMTS will mindestens 50 % der Bevölkerung erreichen, also ein Massendienst werden.

Im Zusammenhang mit UMTS und FPLMTS tauchen oft auch die Begriffe *Universal Personal Telecommunications* (UPT) und *Personal Communication Services* (PCS) auf. UPT/PCS bezeichnen als Basis der Kommunikationssysteme der 3. Generation

- ***Terminal Mobility***: Jeder Teilnehmer kann beliebige Terminals als aktuelle Endgeräte verwenden.
- ***Personal Mobility***: Ein Teilnehmer ist stets unter *einer* Rufnummer erreichbar. Hierbei existieren sogar Überlegungen, einem Teilnehmer eine von Geburt an gültige „Kommunikationsnummer“ zuzuweisen.
- universelle drahtlose Kommunikationsmöglichkeiten,
- **Bereitstellung nutzerspezifischer Dienstprofile**, z.B. Anruf-Management-Dienste (*call management*, Erreichbarkeitsmanagement).

Um die Vielfältigkeit der angebotenen Dienste, Frequenzen und Übertragungstechniken überhaupt effizient nutzen zu können, ist für UMTS/FPLMTS die Entwicklung eines multifunktionalen persönlichen Kommunikationsendgerätes (***Personal Communicator***), das alle mobilen Möglichkeiten in sich vereint nötig. Außerdem wird es sicher in Zukunft an vielen (öffentlichen) Stellen multifunktionale Endgeräte und Kommunikationsdosen geben, über die UPT/PCS-Dienste genutzt werden können.

Eine Untersuchung zu sicherheitsrelevanten Arbeiten an UMTS ist in [Römh_95] zu finden.

2 Mobilkommunikationssysteme und Sicherheit

Hier soll insbesondere Sicherheit in Mobilkommunikationssystemen betrachtet werden. Deshalb werden in den folgenden Abschnitten einige Bemerkungen zur Beschreibung von Sicherheitsanforderungen gemacht. Diese sind teilweise ableitbar aus (bzw. identisch mit) denen herkömmlicher Kommunikationsnetze [Pfit_89]. Jedoch bringt der Mobilitätsaspekt neue oder speziellere Forderungen an technischen Datenschutz hervor.

2.1 Technische Datenschutzforderungen

Eine Möglichkeit, Schutzziele zu formulieren, sind die folgenden **technischen Datenschutzforderungen** [Pfit_93]:

Vertraulichkeit (*confidentiality*)

c1 *Nachrichteninhalte* sollen vor allen Instanzen außer dem Kommunikationspartner vertraulich bleiben.

c2 *Sender* und/oder *Empfänger* von Nachrichten sollen voreinander *anonym* bleiben können, und *Unbeteiligte* (inkl. Netzbetreiber) sollen *nicht in der Lage* sein, sie *zu beobachten*.

c3 Weder potentielle Kommunikationspartner noch Unbeteiligte (inkl. Netzbetreiber) sollen ohne Einwilligung den *momentanen Ort* einer mobilen Teilnehmerstation bzw. des sie benutzenden Teilnehmers ermitteln können.

Integrität (*integrity*)

i1 Fälschungen von *Nachrichteninhalten* (inkl. des *Absenders*) sollen erkannt werden.

i2 Gegenüber einem Dritten soll der Empfänger *nachweisen* können, daß Instanz *x* die Nachricht *y gesendet hat*.

i3 Der Absender soll das *Absenden* einer Nachricht mit korrektem Inhalt *beweisen* können, möglichst sogar den Empfang der Nachricht.

i4 Niemand kann dem Netzbetreiber *Entgelte* für erbrachte Dienstleistungen vorenthalten. Umgekehrt kann der Netzbetreiber nur für korrekt erbrachte Dienstleistungen Entgelte fordern.

Verfügbarkeit (*availability*)

a1 Das Netz ermöglicht Kommunikation zwischen allen Partnern, die dies *wünschen* (und denen es nicht verboten ist).

Diese Datenschutzforderungen sind die bisher wohl umfassendsten und stärksten formulierten. Die Dreiteilung nach Vertraulichkeit, Integrität und Verfügbarkeit mit ihren Unterteilungen (**c1 – c3**, **i1 – i4** und **a1**) hat den Vorteil, sehr übersichtlich zu sein. Allerdings fällt auf, daß die Begriffe teilweise weit gefaßt wurden: So könnte man **i1** als **Integrität der Nachrichteninhalte** bezeichnen, wogegen **i2 – i4** unter dem Oberbegriff **Zurechenbarkeit** (*accountability*) eingeordnet werden können. Ähnlich verhält es sich mit **c2**, das häufig einfach unter **Anonymität** läuft. Die Forderung **c3** stellt ein Spezifikum für die Mobilkommunikation dar.

Die technischen Datenschutzanforderungen sind recht umfassend und gut geordnet. Sie dienen daher als Basis der hier vorgenommenen Sicherheitsbetrachtungen. Nicht alle Forderungen werden jedoch für alle Teilnehmer eines Kommunikationsnetzes gleich stark gelten. Vielmehr stellen die Forderungen eine Art „Maximaldatenschutz“ dar. Das bedeutet, daß für den Teilnehmer, der dies wünscht, die Forderungen zumindest von technischer Seite her erfüllt werden können.

Da bei den Betrachtungen nicht mehr nur die Sicherheit eines Netzbetreibers oder Dienstanbieters eine Rolle spielt, sondern ebenfalls die Sicherheit des Nutzers, betreffen die genannten Schutzziele die Interessen mehrerer Instanzen. Deshalb kann nach Erreichen der Schutzziele von **mehrseitiger Sicherheit** gesprochen werden.

2.2 Die Sicherheitswelt der „anderen“

Bei der Analyse verschiedener Literaturquellen unter dem Gesichtspunkt Datensicherheit zeigt sich, daß die Autoren unterschiedliche Anforderungen an die Sicherheit in Mobilfunknetzen stellen. Ein wesentlicher Grund dafür sind voneinander abweichende Vorstellungen von schützenswerten Informationen oder Komponenten eines Mobilfunknetzes.

In [CoBr_92] werden vier Forderungen an ein Funknetz in Bezug auf Datenschutz erhoben:

Anf. 1.1 Schutz der Inhaltsdaten (*protection of user data*),

Anf. 1.2 Schutz der Verbindungsdaten (*protection of signalling information*), inkl. Ort des Teilnehmers,

Anf. 1.3 Benutzer- und Geräteauthentifikation (*user authentication, equipment verification*),

Anf. 1.4 korrekte Abrechnung durch Netzbenutzer und Netzbetreiber (*fraud prevention*).

Eine weitere Zusammenstellung von Sicherheitsanforderungen ist in [GrWo_92] zu finden:

Anf. 2.1 Gegenseitige Identifikation und Authentikation zwischen den Knoten aller Netzwerkverbindungen,

Anf. 2.2 Schutz von Informationen, welche die Identität und den Aufenthaltsort des Nutzers betreffen,

Anf. 2.3 Schutz der Nutzer- und Signalisierungsdaten, um ein Abhören dieser Daten zu verhindern und damit eine Lokalisierung oder Identifizierung eines Nutzers zu unterbinden,

Anf. 2.4 Nichtabstreitbare Abrechnung der Gebühren – es muß möglich sein, unabhängig die Richtigkeit von Gebührenabrechnungen eines Dienstanbieters für einen Nutzer zu überprüfen.

In [Frey_94] werden ebenfalls vier Sicherheitsanforderungen für UMTS formuliert:

Anf. 3.1 Die Menge der geheimen Daten im System sollte so klein wie möglich sein. Die geheimen Informationen zur Authentikation müssen an gut geschützten Orten verwahrt und dürfen nicht übertragen werden. Ein geheimer Schlüssel zur Authentikation sollte beim Nutzer aufbewahrt werden.

Anf. 3.2 Korrekte Rechnungen sind im Interesse aller beteiligten Parteien. Eine eingeschränkte Vertrauensbeziehung wird durch einen sicheren Rechnungsdienst, zur Überprüfung im Falle einer Meinungsverschiedenheit, kompensiert.

Anf. 3.3 Geheime Informationen zur Authentikation, zum Beispiel GSM-Tripel (*Authentication Sets*), sollten nicht ohne Restriktionen zwischen den einzelnen UMTS-Teilnetzen übertragen werden.

Anf. 3.4 Der Austausch von geheimen Schlüsseln zwischen Teilnehmern und Stationen, welche im voraus keine Möglichkeit hatten, über einen sicheren Kanal ein Geheimnis zu teilen, muß möglich sein.

Gemäß den „Technischen Datenschutzforderungen“ ensprechen die in [CoBr_92] formulierten den Forderungen **c1**, **c2**, **i1** und **i4**. Dabei enthält **Anf. 1.2** den Schutz des Aufenthaltsortes von Benutzern entsprechend **c3**, wenn der Netzbetreiber mit eingeschlossen ist. Entsprechendes gilt für **Anf. 1.4**.

Die aus [Frey_94] entnommenen Sicherheitsanforderungen stellen die Interessen der Netzwerkbetreiber stark in den Vordergrund. Dem Schutz des Netzwerkes vor unberechtigter Nutzung durch Dritte dienen **Anf. 3.1** und **Anf. 3.3**, die Ausstellung von korrekten Rechnungen (entspricht **Anf. 3.2**) genügt den Bedürfnissen aller beteiligten Parteien. Die Verhinderung des Ermittelns des momentanen Aufenthaltsortes

eines Nutzers, wie es zum Beispiel **Anf. 2.2**, **Anf. 2.3** und **c3** zum Ziel haben, wird bei [Frey_94] gar nicht berücksichtigt.

Die Anforderungen von [GrWo_92] tangieren die wichtigsten Aspekte des Datenschutzes in Mobilfunknetzen, obgleich sie relativ allgemein formuliert sind. Es fehlen hier nur die Punkte Nutzeranonymität, Empfangsbestätigung, Absendebestätigung und Netzverfügbarkeit, welche bei den „Technischen Datenschutzforderungen“ vorhanden sind.

3 Mobilkommunikation am Beispiel GSM

GSM dürfte das weltweit bisher erfolgreichste digitale zellulare Mobilfunknetz sein. Die folgenden Abschnitte widmen sich diesem Funknetz etwas genauer.

3.1 Allgemeines

3.1.1 Standardisierung von GSM

GSM ist heute die gebräuchliche Abkürzung für *Global System for Mobile Communication*. Dabei war es ursprünglich die Kurzbezeichnung für *Groupe Spéciale Mobile*, einer Arbeitsgruppe der ETSI. Somit ist GSM eigentlich keine *globale* Norm, sondern eine europäische.

Die Arbeit an der Standardisierung wurde 1982 (noch innerhalb des CEPT) begonnen. Den Abschluß der ersten Phase der Spezifikation bildeten die ETSI/GSM-Recommendations Serien 01.xx bis 12.xx:

01. Allgemeines	07. Terminaladapter (Anpassungseinheit der MS)
02. Dienstaspekte	08. Schnittstellen BTS-BSC, BSC-MSC
03. Netzaspekte	09. Anschluß an Fremdnetze, Signalisierung
04. Schnittstelle MS-BSS	10. Anschluß an Fremdnetze, Verkehrsdaten
05. Übertragung auf dem Funkweg (HF-Aspekte)	11. Typprüfverfahren der MS und Spezifikation der MF-Entitäten
06. Sprachkodierung	12. Netzmanagement (Betrieb und Wartung des GSM-PLMN-Systems)

Die Standardisierungsphase 2 widmete sich weniger den technischen Details als neuen Diensten. Im Final Release soll der Übergang zu höheren Frequenzen und geringerer Sendeleistung geschafft werden, was mit DCS 1800 auch gelungen ist. Die Verbesserung der Sprachkodierung hin zur sog. Halbraten-Kodierung soll erfolgen.

3.1.2 Leistungsmerkmale von GSM

Es sollen als die wichtigsten Leistungsmerkmale des GSM genannt werden:

- 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,
- eingebaute Sicherheitsmerkmale:
  - Zugangskontrolldienste (PIN, Chipkarte),
  - Authentikations- und Identifikationsdienste,

  - Unterstützung von temporären Identifizierungsdaten (Pseudonymen),
  - Abhörsicherheit für Outsider auf der Funkschnittstelle,
- relativ niedriges Kostenniveau,
- flexible Dienstgestaltung,
  - Dienstevielfalt,
  - Entwicklungsfähigkeit,
- priorisierter Notrufdienst,
- Ressourcenökonomie auf der Funkschnittstelle durch FDMA (*Frequency Division Multiplex Access*), TDMA (*Time Division Multiplex Access*), Sprachkodierung, Warteschlangentechniken etc.

3.1.3 GSM in Zahlen

Es wird geschätzt, daß im Jahre 2000 etwa 3,4 Millionen Teilnehmer die GSM-Netze Deutschlands

- D1-Netz der Deutschen Telekom AG,
- D2-Netz der Mannesmann Mobilfunk AG,
- E-Netz eines neu gebildeten Konsortiums, eigentlich ein DCS 1800-Netz

nutzen werden. Für jedes einzelne D-Netz bedeutet das weit über 2 000 installierte BTS' und über 40 MSCs. Die Anzahl der BTS' im E-Netz dürfte noch bedeutend größer sein.

Die folgenden Angaben stammen aus [Bial_94, S.138]:

Eine GSM-Vermittlungsstelle (MSC) ist in der Lage, 300 000 bis 600 000 Teilnehmer zu bedienen. Die typische Verkehrskapazität eines MSCs liegt unterhalb von 100 000 *Busy Hour Call Attempts*.

Für Europa sollen die GSM-Netze die Anforderungen bis zum Jahr 2000 erfüllen können:

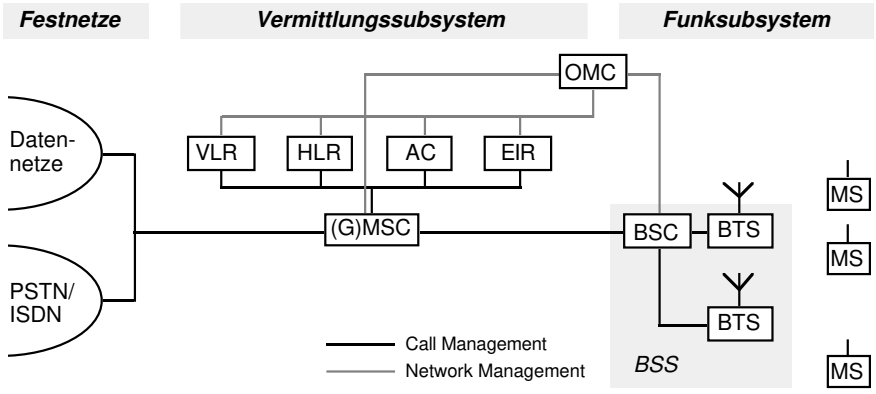
- GSM im 900 MHz-Bereich: 20 Millionen Teilnehmer,
- DCS 1800: 40 Millionen Teilnehmer.

Bei Zugriff auf weitere Ressourcen (z.B. schmalere *Traffic Channels,* TCH) soll sich die Teilnehmerzahl sogar auf 60 Millionen erhöhen lassen.

3.2 Struktur von GSM

3.2.1 Architektur

Das GSM-Netz ist ein auf Sprachübertragung optimiertes Netz. Es soll den Mobilfunkteilnehmern Zugang zu den öffentlichen Festnetzen – *Integrated Services Digital Network* (ISDN) und *Public Switched Telephone Network* (PSTN) – bieten und umgekehrt. Weiterhin sind auch Möglichkeiten zur Datenkommunikation (z.B. *Mobile Computing*) vorgesehen.



AC	Authentication Register	MS	Mobile Station
BSS	Base Station Subsystem	(G)MSC	(Gateway) Mobile Switching Center
BSC	Base Station Controller	OMC	Operation and Maintenance Center
BTS	Base Transceiver Station	PSTN	Public Switched Telephone Network
EIR	Equipment Identity Register	VLR	Visitor Location Register
HLR	Home Location Register	ISDN	Integrated Services Digital Network

Architekturschema des GSM nach [Keda_91]

Das *Operation and Maintenance Center* (OMC) nimmt eine zentrale Stellung ein. Ihm untergeordnet sind die Mobilfunkdatenbanken *Home Location Register* (HLR) und *Visitor Location Register* (VLR). Weiterhin existieren noch das *Authentication Center* (AC) und das *Equipment Identity Register* (EIR). Diese enthalten Daten und Funktioen für die Zugangskontrolle zum Netz.

Über die Mobilvermittlungsstellen MSC *(Mobile Switching Center)*, die funktechnischen Einrichtungen BSS *(Base Station Subsystem)* mit Steuereinrichtung BSC *(Base Station Controller)* und Funktürme BTS *(Base Transceiver Station)* erfolgt der Nachrichtenfluß der Inhaltsdaten im mobilen Netz.

Die mobilen Geräte (*Mobile Station*, MS) können im GSM durch das Versorgungsgebiet bewegt werden, ohne daß der Funkkontakt abreißt (*Roaming*).

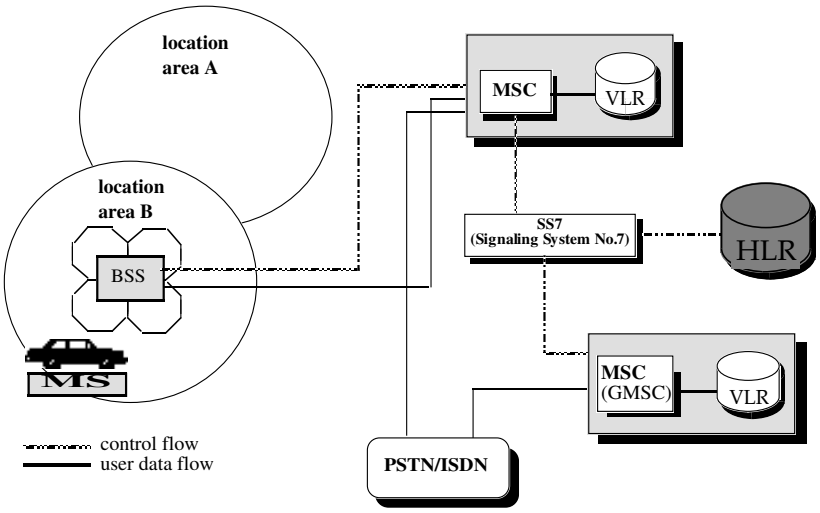
Damit ein Übergang zum herkömmlichen Telefonnetz (PSTN/ISDN) möglich wird, existieren im Funknetz spezielle Vermittlungsstellen mit *Gateway*-Funktionalität, sog. *Gateway-MSCs* (GMSC).

Auf der logischen Ebene sind das HLR, das AC und EIR zentral. Diese Bestandteile müssen aber deshalb nicht physisch zentral angeordnet sein.

Die Trennung von Vermittungsfunktionen (MSC, BSC, BTS) und Speicherfunktionen (HLR, VLR, EIR, AC) unterstreichen das modulare Konzept von GSM, wordurch die Komplexität des Gesamtsystems auf überschaubare Funktionsblöcke reduziert wird.

Das AC übernimmt netzseitig wichtige Funktionen bei der Abwicklung der Authentikationsprozedur. Hier werden die teilnehmerindividuellen symmetrischen Schlüssel Ki gespeichert und Rechenoperationen für die Authentikationsprozedur und Generierung der Chiffrierschlüssel für die Verschlüsselung auf der Luftschnittstelle durchgeführt. Das AC bildet das Gegenstück zum SIM (*Subscriber Identity Module*), der Chipkarte, die jeder Teilnehmer erhält.

Das EIR ist eine Datenbank, die die Gerätekennungen von zugelassenen, fehlerhaften und gesperrten Geräten (MS) enthält.



Logischer Netzaufbau im GSM

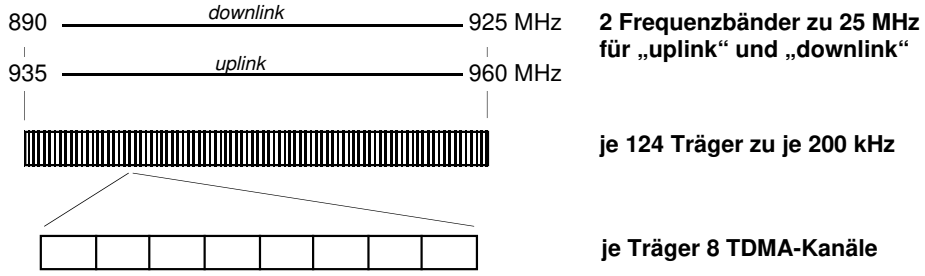
3.2.2 Funktechnischer Aufbau

Das GSM-System arbeitet im Frequenzbereich (*Primary Band*) von 890-915 und 935-960 MHz mit einem Duplex-Abstand von 45 MHz. Diese Frequenzbereiche wurden europaweit für GSM reserviert. Sie bilden 124 Radiofrequenzkanäle mit einer Kanalbreite von 200 kHz, die im FDMA-Verfahren verwendet werden. Einschließlich Fehlerschutzmaßnahmen entspricht das einer Bitrate von 271 kbit/s (nach [Keda_91]). Die Frequenzplanformel für das Primary Band lautet nach [Bial_94] (mit n=1..124):

$F_{uplink}(n) = 890{,}2 \text{ MHz} + (n\text{-}1) \cdot 0{,}2 \text{ MHz}$

$F_{downlink}(n) = F_{uplink}(n) + 45 \text{ MHz}$

Jeder Radiokanal enthält 8 Zeitschlitz-Kanäle (mit einer Verweildauer von $8 \cdot 0{,}577 \text{ ms} \approx 4{,}615 \text{ ms}$), die im TDMA-Verfahren verwendet werden. Als Modulationsverfahren wird GMSK (*Gaussian Minimum Shift Keying*) verwendet. Als Medienzugriffsverfahren kommt *Slotted Aloha Random Access* zum Einsatz.



Aufteilung der Bandbreite in Radiokanäle

Ein TDMA-Kanal teilt sich in die logischen Verkehrskanäle (*Traffic Channels*, TCH)

- Dm (*Data mobile*): Steuerkanal ähnlich dem D-Kanal des ISDN) und
- Bm (*Bearer mobile*): Nutzkanal für Sprache und Daten

sowie einen Low-Rate-Verkehrskanal Lm (*Low mobile*).

Der Signalisierungskanal Dm wird grob eingeteilt in 3 logische Kanäle:

- Broadcast Control Channel (BCCH),
- Common Control Channel (CCCH),

- Dedicated Control Channel (DCCH).

Diese Kanäle werden noch weiter unterteilt. In [Bial_94, S.77] ist eine Übersicht zu finden.

Da die Bandbreite auf der Funkschnittstelle knapp ist, wurden Warteschlangentechniken bei der Kanalvergabe implementiert. Eine besondere Stellung nimmt dabei das sog. *Off Air Call Setup* (OACSU) ein: Nach einem Wählvorgang beim *Call Setup* wird nicht sofort ein Funkkanal reserviert, sondern erst, wenn der gerufene Teinehmer abgenommen hat. (Zwischen Rufen und Abheben können bis zu 40 Sekunden vergehen.) In der Zwischenzeit kommt der Ruf in eine Warteschlange. Durch OACSU wird eine effizientere Auslastung der Frequenzen erreicht. Allerdings kann dann u.U. der Fall eintreten, daß zum Zeitpunkt des Abnehmens gerade kein Kanal frei ist. Dann wird der Teilnehmer durch eine Ansage gebeten zu warten.

Ein Ergänzungssystem zum GSM-Mobilfunk ist das DCS 1800 (Digital Communication System im 1800 MHz-Band). Es unterscheidet sich vom GSM durch höhere Trägerfrequenzlage (1710-1880 MHz), durch breitere Bänder (75 MHz) und durch einen höheren Duplex-Abstand (95 MHz). Durch die höhere Frequenz werden kleinere und leichtere Geräte möglich, da die Sendeleistung der Mobilstation geringer ist. Die Zellgrößen werden kleiner. In der Signalisierung existieren nur minimale Unterschiede zu GSM.

3.2.3 Mobilfunkgebiete im GSM

Ein **Location Area** (LA) ist die kleinste geographisch adressierbare Einheit des Funknetzes. Ein LA kann aus mehreren *Base Station Areas* bestehen, d.h. mehrere Funkzellen können in einer LA zusammengefaßt sein. Durch die LAI (*Location Area Identification*), die über einen speziellen Signalisierungskanal ausgestrahlt wird, ist jede LA eindeutig bestimmt.

Ein **VLR-Area** wird aus einem oder mehreren LAs zusammengesetzt und von einer Besucherdatei *Visitor Location Register* (VLR) verwaltet.

Ein **MSC-Area** entspricht einem geographischen Bereich. Gewöhnlich wird *einem MSC-Area genau ein VLR zugeordnet*.

Eine **Funkzelle** ist der kleinste geographische Versorgungsbereich eines Funknetzes. Die Funkzelle wird über eine BTS versorgt. Jede BTS hat einen *Base Transceiver Station Identity Code* (BSIC), der für die Aufenthaltsaktualisierung, sog. *Location Update* (LUP) verwendet wird. Die Funkzelle besitzt eine sog. *Cell Identity* (CI), aus der auch die zuständige MSC-Adresse ermittel werden kann.

Ob und wie das Lokalisierungsmanagement auf Zellebene realisiert wird, ist unabhängig von der Struktur des Lokalisierungsmanagements auf LA-Basis.

Durch die physikalische Teilung des Versorgungsgebietes in Funkzellen wird die Begrenzung der Bandbreite auf der Funkschnittstelle durch Mehrfachnutzung von Frequenzbändern in nicht angrenzenden Zellen erreicht. Die Folge ist eine effiziente Ausnutzung der Bandbreite, die jedoch mit einer detaillierten Frequenzplanung vor Inbetriebnahme des Netzes erkauft wird. Außerdem bildet die Dämpfung der Funkwellen eine natürliche Begrenzung für die Größe der Funkzellen. Die Dämpfung ist bei konstanter Sendeleistung z.B. abhängig von der Sendefrequenz und den örtlichen Gegebenheiten (Funkschatten, Mehrwegeausbreitung).

Die logische Teilung in LAs ist zunächst unabhängig von der Teilung in Funkzellen. Die Größe und Anordnung eines LA wird durch die Anzahl zu versorgender Teilnehmer, ihrem Verkehrsverhalten und ihrer Mobilität bestimmt. Durch geschickte Zuordnung der Zellen zu einem LA (z.B. entlang eines Straßenzugs) werden Location Update- und Handover-Prozesse minimiert.

3.2.4 Subscriber Identity Module

Das SIM (*Subscriber Identity Module*) ist eine Chipkarte (*Smart Card*). Sie wird auch als *Circuit Card* bezeichnet und ist standardisiert nach ISO IS-7816. Mit der SIM-Karte wird eine MS „personalisiert“.

Die wichtigsten **permanenten Daten und Prozeduren** auf der SIM sind:

- IMSI (*International Mobile Subscriber Identity*),
- teilnehmerspezifischer symmetrischer Schlüssel *Ki,*
- Algorithmus A3 für *Challenge-Response*-Authentikationsverfahren,
- Algorithmus A8 zur Generierung des Schlüssels *Kc* zur Inhaltsdatenverschlüsselung,
- PIN (*Personal Identification Number*) für Zugangskontrolle.

Die wichtigsten **temporären Daten** sind:

- TMSI (*Temporary Mobile Subscriber Identity*),
- LAI,
- Chiffrierschlüssel *Kc*,
- CKSN (*Ciphering Key Sequence Number*).

3.3 Datenbanken des GSM

3.3.1 Home Location Register

Das HLR (*Home Location Register*) enthält semipermanente und temporäre Daten über die Funkteilnehmer, die einem HLR-Bereich zugeordnet sind. Jeder Verbindungsaufbau wird über das HLR abgewickelt.

Die wichtigsten **semipermanenten Daten** sind:

- International gültige Rufnummern des mobilen Teilnehmers:

  MSISDN (*Mobile Subscriber International ISDN Number*) – eine 15-stellige Nummer, beinhaltet

  - das Land (CC, *Country Code*), für Deutschland die 49,
  - das gebuchte Netz des Landes (NDC, *National Destination Code*), für das deutsche D1-Netz die 171, für D2 die 172,
  - die Nummer des HLR und die Teilnehmerkennung.

  Die MSISDN ist weltweit und netzübergreifend eindeutig.

  IMSI – eine 15-stellige Nummer, besteht aus

  - Landeskennzahl (MCC, *Mobile Country Code*, für Deutschland die 262),
  - nationaler Netzkennzahl (MNC, *Mobile Network Code*, für das deutsche D1-Netz die 01, für D2 die 02) und
  - einer teilnehmerspezifischen Nummer.

  Nach [MaMo_91] ist die IMSI für jeden GSM-Teilnehmer europaweit eindeutig. Die IMSI ist dem Mobilfunkteilnehmer nicht bekannt [Bial_94, S.84].

- Bestandsdaten über den *Subscriber*: Name/Firma, Anschrift, Zahlungsart, je nach Zahlungsart Bankverbindung oder Daten der Kreditkarte,
- gebuchtes Dienstprofil: Prioritäten, Anrufweiterleitung, Dienstrestriktionen, z.B. *Roaming*-Einschränkungen.

Die wichtigsten **temporären Daten** dienen größtenteils dem *Location Management*:

- Umbuchungs- oder Aufenthaltsnummer: MSRN (*Mobile Subscriber Roaming Number*) – beinhaltet das Land, das gebuchte Netz (PLMN) des Landes, das MSC des aktuellen LAs,
- LMSI (*Local MS Identity*) – wird vom VLR zugewiesen und dient zusammen mit der IMSI der beschleunigten Suche von HLR-Daten,
- VLR-Adresse, MSC-Adresse,

- eine Anzahl von *Authentication Sets* vom AC: *RAND, SRES, Kc* (siehe spätere Bemerkungen),
- Daten für den SMS-Dienst (*Short Message Service*),
- Gebührendaten für die Weiterleitung an die *Billing-Centers.*

3.3.2 Visitor Location Register

Das VLR (*Visitor Location Register*) ist eine lokale Datenbank, die vor allem dazu dient, den Verbindungsaufbau effizient durchführen zu können. Meist ist einem MSC auch ein VLR zugeordnet. Das VLR enthält Kopien von Daten aus dem HLR und spezifische VLR-Daten:

Die wichtigsten dort gespeicherten **temporären Daten** sind:

- IMSI, MSISDN,
- Daten zum gebuchten Dienstprofil: Prioritäten, Anrufweiterleitung, Dienstrestriktionen,
- Gebührendaten für die Weiterleitung an die *Billing-Centers.*

Die wichtigsten dort gespeicherten **transienten Daten** sind:

- TMSI – ein Pseudonym, das innerhalb eines VLR-Areas die Unverkettbarkeit von Teilnehmeraktionen gegenüber *Outsidern* auf der Funkschnittstelle gewährleisten soll,
- MSRN, LAI,
- MSC-Adresse, HLR-Adresse,
- Statusinformationen, Routinginformationen.

3.3.3 Equipment Identity Register

Das EIR (*Equipment Identity Register*) enthält semipermanent die Gerätekennungen (15 Ziffern) IMEI *(International Mobile Station Equipment Identity)* und zugehörigen Nutzungsberechtigungen aller zugelassenen Mobilfunkendgeräte. Die Gerätekennungen werden in sog.

- *white-lists* (zugelassene Endgeräte, verkürzte IMEI gespeichert),
- *grey-lists* (fehlerhafte Endgeräte, die *beobachtet* werden, volle IMEI gespeichert) und
- *black-lists* (technisch mangelhafte oder *gestohlene* Geräte, die gesperrt sind, volle IMEI gespeichert)

eingetragen. Es ist eine Lokalisierung der Geräte möglich!

Bei jeder Aufenthaltsregistrierung (*Location Registration*) ist auch eine Überprüfung der IMEI vorgesehen [Bath_92].

3.3.4 Authentication Center

In der Reihe der Mobilfunkdatenbanken nimmt das AC eine Sonderstellung ein. Im AC sind folgende Daten **permanent** gespeichert:

- IMSI,
- teilnehmerspezifischer symmetrischer Schlüssel *Ki.*

Weiterhin werden für die *Challenge-Response*-Authentikationsprozedur und die Schlüsselgenerierung zur Inhaltsdatenverschlüsselung sog. ***Authentication Sets*** gebildet. Sie bestehen IMSI-spezifisch aus:

- *RAND* (128 Bit) als Zufallszahl (*Challenge*) für die Authentikationsprozedur. Dieser Wert wird über die Funkschnittstelle an die MS gesendet.
- *SRES* (32 Bit) als korrekter Vergleichswert (*Signed Response*) für die Authentikationsprozedur,
- *Kc* (64 Bit) für Inhaltsdatensentschlüsselung in der BSC.

Netzwerkseitig besitzt nur das AC die Algorithmen A3 und A8 zur Bildung von *SRES* und *Kc* aus *RAND* und *Ki*.

In gewisser Hinsicht bildet das AC das netzseitige Äquivalent zum SIM. Allerdings ist es – trotz der Trennung zum HLR – von seiner Struktur her ungeeignet, den Mehrseitigkeitsaspekt von Sicherheit zu unterstützen, da es für den Teilnehmer nicht zwangsläufig eine vertrauenswürdige Stellung einnimmt. Das auf symmetrischer Kryptographie basierende Verfahren zur Authentikation (und Inhaltsdatenverschlüsselung auf der Luftschnittstelle) zwingt die Teilnehmer allerdings zu Vertrauen in AC.

Aus reinen Effizienzgründen hätte man die AC-Funktionalität komplett dem HLR zuordnen können. Dem Autor ist nicht bekannt, ob dies in praktischen Realisierungen des GSM etwa sogar der Fall ist. Immerhin erfolgt die Speicherung des Tupels (IMSI, *Ki*) in der Datenbank des AC in verschlüsselter Form.

Die folgende Übersicht zeigt, wo welche sicherheitsrelevanten Algorithmen und Daten verwendet werden:

HLR	Sets of RAND/SRES/Kc zu jeder IMSI
VLR	Sets of RAND/SRES/Kc zu jeder IMSI, CKSN, TMSI, LAI zu jedem Kc
MSC/BSS	A5, temporär anrufbezogen Kc, CKSN, TMSI, IMSI, Kc
AuC	A3, A8, Ki, Kc, IMSI, RAND, SRES
EIR	IMEI
ME	A5, IMEI
SIM	A3, A8, IMSI, Ki, Kc, PIN, Super-PIN, Personal Unblocking Key, RAND, SRES, CKSN, TMSI, LAI, SIM-Status

4 Sicherheitsrelevante Prozeduren und Funktionen im GSM

In GSM wurden eine Reihe sicherheitsrelevanter Prozeduren und Funktionen integriert, von denen die wichtigsten hier erläutert werden.

4.1 Zugangskontrolle

Die Zugangskontrolle zum Netz erfolgt mittels *Token* (Chipkarte, SIM), die über eine PIN geschützt wird. Diese geheime Identifikationsnummer muß vom Teilnehmer nach dem Einlegen der SIM-Karte oder nach dem Einschalten der MS eingegeben werden, damit eine Personalisierung erfolgen kann. Die PIN ist auf der Karte als vier- bis achtstellige Zahl gespeichert und kann nach dem Einbuchungsvorgang geändert werden (MS interne Funktion).

Für Zusatzdienste kann weiterhin ein zusätzlicher Passwort-Schutz erfolgen.

Beim Einbuchen ins Netz wird eine Authentikationsprozedur gestartet.

Um Mißbrauch durch Diebstahl zu verhindern und zusätzlich technisch fehlerhafte oder mangelhafte Geräte zu beobachten bzw. zu sperren, wird eine Abfrage der IMEI vorgenommen.

4.2 Authentikation mittels Challenge-Response-Verfahren

Bevor die Authentikationsprozedur beginnt, muß sich der Teilnehmer mit seiner IMSI beim Netz anmelden. Dies geschieht mindestens beim allerersten Einbuchen eines neuen Teilnehmers. Danach ist gewöhnlich eine Anmeldung mit der TMSI möglich. Daraufhin wird die Authentikationsprozedur gestartet.

Weitere Authentikationsprozeduren können netzseitig beliebig oft initiiert werden. Mindestens bei

- Aufenthaltsregistrierung (*Location Registration*),
- *Call Setup* (in beiden Richtungen),
- verbindungsloser Aktivierung von Zusatzdiensten,
- Kurznachrichtendienst SMS (*Short Message Service*),
- LUP mit VLR-Wechsel

wird die Authentikationsprozedur angestoßen.

Dazu wird der MS eine Zufallszahl *RAND* (*Challenge*, 128 Bit) gesendet. Im SIM der Mobilstation wird in einem Algorithmus A3 eine Verknüpfung von *Ki* und *RAND* vorgenommen und als *SRES'* (Response, 32 Bit) an das Netz zurückgegeben. Im VLR werden *SRES* (vom *Authentication Set*) und *SRES'* auf Gleichheit getestet. Bei *SRES=SRES'* ist die Authentikation erfolgreich verlaufen.

Die zur MS übertragene Zufallszahl *RAND* wird weiterhin zur Generierung des Schlüssels *Kc* verwendet (siehe nachfolgende Abschnitte).

Um nicht bei jeder Authentikationsprozedur die Daten vom (u.U. weit entfernten) AC holen zu müssen, werden zu einem Zeitpunkt aus Effizienzgründen mehrere *Authentication Sets* berechnet und an das HLR zur Speicherung gegeben. Jedes *Authentication Set* wird nur einmal benutzt. Zu diesen Bemerkungen siehe auch [CoBr_92].

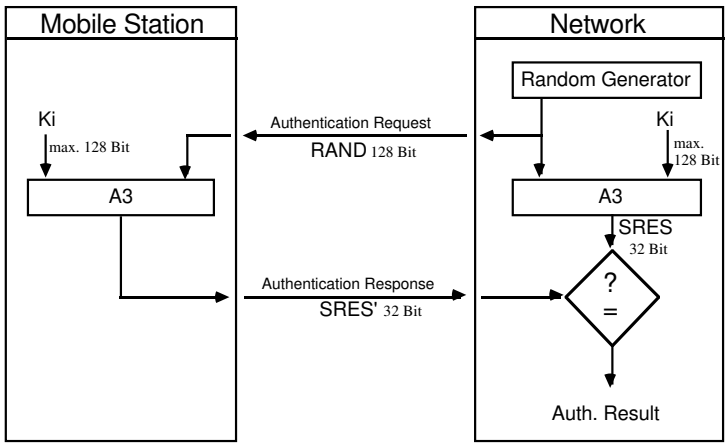
Der kryptographisch relevante **Algorithmus A3** ist

- auf dem SIM untergebracht,

- eine mit *Ki* parametrisierte Einwegfunktion,
- nicht (europaweit, weltweit) standardisiert, sondern kann vom Netzbetreiber festgelegt werden. Die Schnittstellen sind jedoch standardisiert.

Über die kryptographischen Eigenschaften von A3 ist praktisch nichts bekannt.

Es wurde *keine gegenseitige Authentikation* vorgesehen: Lediglich der Nutzer authentisiert sich vor dem Netz.



Authentikationsprozedur

4.3 Pseudonymisierung des Teilnehmers durch TMSI

Die TMSI (*Temporary Mobile Subscriber Identity*) stellt ein Pseudonym dar, das Anonymität und Unverkettbarkeit von Teilnehmeraktionen innerhalb des VLR-Area gegenüber *Outsidern* des Kommunikationsnetzes auf der Funkschnittstelle gewährleisten soll, da Signalisierungsdaten teilweise unverschlüsselt übertragen werden. Sie wird z.B. nach erfolgreicher Authentikation vom VLR vergeben und ist zusammen mit der LAI an die IMSI gebunden [Bial_94, S.84].

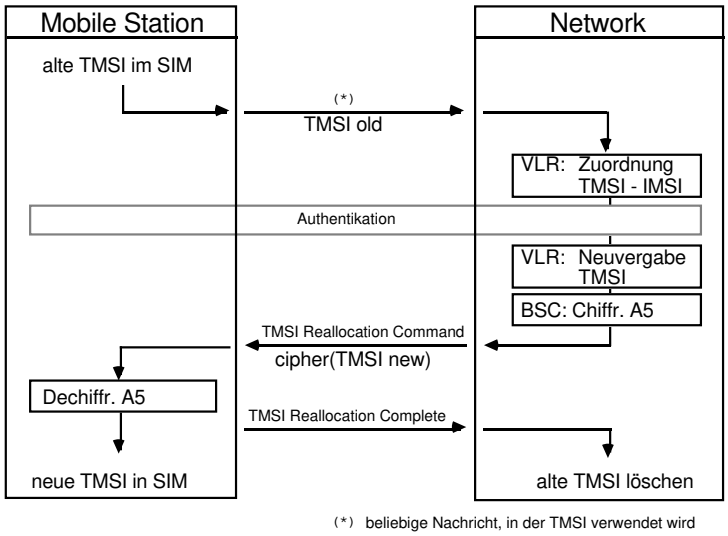
Da eine Mobilstation bei der allerersten Kontaktaufnahme (erstes Einbuchen) bzw. nach technischen Störungen im regulären Ablauf zunächst keine TMSI besitzt, muß sie sich mit ihrer IMSI melden. Die IMSI ist eine dem Teilnehmer unbekannte explizite Adresse, die ein gewöhnlich öffentliches Pendant besitzt: die MSISDN.

Ihr wird dann vom Netz eine TMSI zugewiesen. Nach einem Ausbuchen bleibt die aktuelle TMSI zusammen mit der LAI sowohl im Netz als auch in der SIM des Teilnehmers gespeichert. Das nächste Einbuchen kann dann pseudonym erfolgen.

Wann und wie oft die TMSI geändert werden soll, legt der Netzbetreiber fest. Der mobile Teilnehmer hat darauf keinen unmittelbaren Einfluß (Es sei denn, er bucht sich regelmäßig aus und wieder ein…). In [GSM_03.20, S.12] wird jedoch angegeben, daß zumindest bei jedem LUP eine Änderung der TMSI erfolgen muß. Laut [CoBr_92] wird bei jeder Gelegenheit, bei der eine Authentikation durchgeführt wird, auch die TMSI neu vergeben.

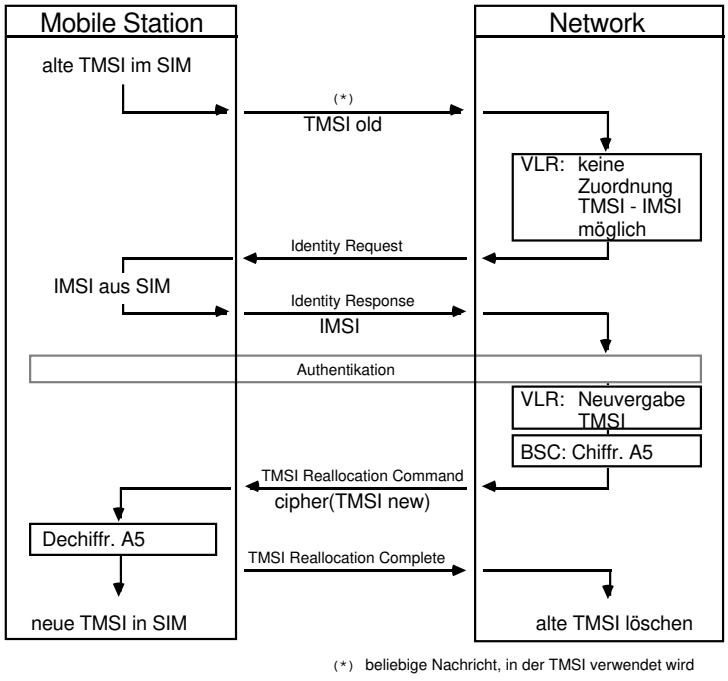
Der TMSI-Vergabe geht stets eine erfolgreich verlaufene Authentikationsprozedur voraus.

Weiterhin sind keine Details über den Algorithmus, nach dem eine TMSI generiert wird, bekannt [CoBr_92].



Neuvergabe einer TMSI bei bekannter alter TMSI

Falls im Netz Fehlfunktionen auftreten, z.B. wenn das alte VLR bei einem LUP nicht erreichbar ist, Daten verloren gegangen sind oder die übermittelte TMSI im VLR unbekannt ist, darf das Netzwerk die IMSI von der MS jederzeit anfordern. Es wird jedoch bereits in [GSM_03.20, S.12] darauf hingewiesen, daß dies eine Verletzung der Dienstqualität ist und nur angewendet werden soll, wenn nötig.



Neuvergabe einer TMSI bei unbekannter alter TMSI

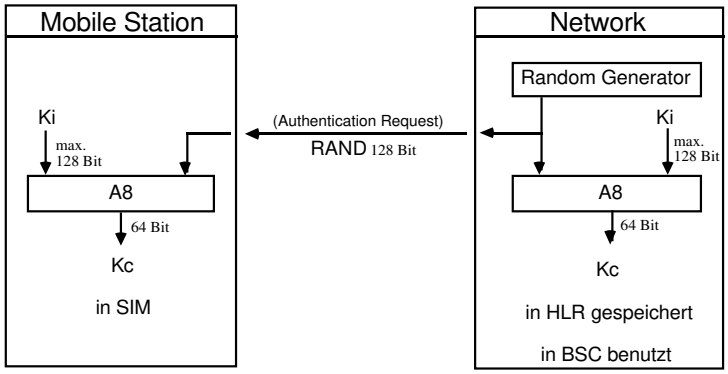
Die Verschlüsselung der TMSI auf der Luftschnittstelle erfolgt mit demselben Algorithmus A5 wie die Verschlüsselung der Inhaltsdaten. Da es jedoch Situationen geben kann, wo keine Verschlüsselung auf der Funkschnittstelle stattfindet (z.B. bei Inkompatibilität mit Algorithmen im Ausland), ist die Anonymisierung mittels TMSI nicht mehr möglich, da jetzt die unverschlüsselten TMSIs miteinander verkettet werden können.

4.4 Generierung des Chiffrierschlüssels Kc

Bevor die Inhaltsdatenverschlüsselung auf der Luftschnittstelle vorgenommen werden kann, muß ein Chiffrierschlüssel *Kc* generiert werden.

Auch dieser Prozedur geht ein Authentikationsprozeß voraus. Mit jeder Authentikation ändert sich auch *Kc*, der über den **Algorithmus A8** aus dem bei der Authentikation verwendeten *RAND* generiert wird. Für A8 gelten dieselben Eigenschaften wie für A3.

Da die Algorithmen A3 und A8 stets gleichzeitig verwendet werden, bietet sich ein kombinierter Algorithmus A3/A8 an, der beide Werte – natürlich unterschiedlich – berechnet.



Generierung von Kc

4.5 Inhaltsdatenverschlüsselung auf der Luftschnittstelle

Der Klartextstrom wird mit einem pseudozufälligen Bitstrom chiffriert.

Der verwendete **Algorithmus A5** ist europa- bzw. weltweit (Algorithmus A5X) standardisiert. Über seine kryptographischen Mechanismen ist nichts bekannt. Er ist *in der mobilen Station untergebracht*.

Der Algorithmus generiert alle 4,615 ms (das ist die Länge eines TDMA-Frames) eine Folge von 114 pseudozufälligen Bits. Die Frame-Nummer dient der Synchronisation zwischen Mobilstation und BSC, wo netzseitig der Algorithmus angewendet wird.

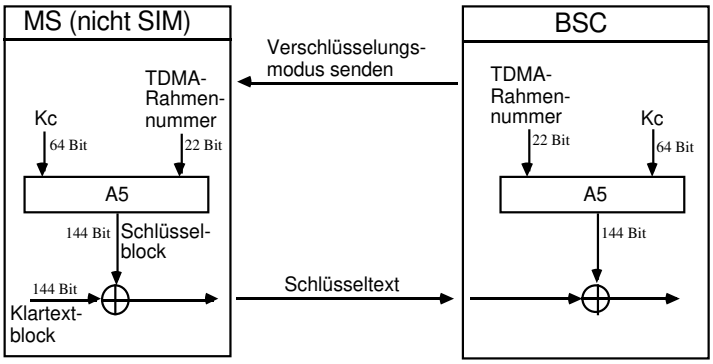
Über die Stärke des Algorithmus ist bekannt, daß sich der pseudozufällige Bitstrom erst nach ca. 209 Minuten wiederholt.

Um den Import- und Exportbestimmungen einiger Länder gerecht zu werden, wurde ein kryptographisch schwächerer **Algorithmus A5*** (oder **A5/2**) definiert, der in diesen Ländern zur Anwendung kommt. Deshalb sind alle neueren Mobilfunkgeräte mit beiden Algorithmen ausgestattet.

Das Netzwerk teilt der mobilen Station vorher mit, welchen Verschlüsselungsalgorithmus sie verwenden soll. Dem Autor ist nicht bekannt, ob das hierzu verwendete *Ciphering Mode Command* auch den Modus „keine Verschlüsselung“ zuläßt. Man muß aber annehmen, daß dieser Modus vorhanden ist.

Um sicherzustellen, daß sowohl im BSC als auch in der MS ein gültiger Schlüssel Kc verwendet wird, existiert eine sog. *Ciphering Key Sequence Number* (CKSN). Wie die CKSN gebildet wird, ist dem Autor nicht bekannt.

Die Chiffrierung wird vom Netzwerk mit einem *Ciphering Mode Command* initiiert, um zu signalisieren, daß mit Verschlüsselung auf TCH und DCCH angefangen werden soll. Mit *Ciphering Mode Complete* der MS erfolgt die Bestätigung und zugleich die Synchronisation für die MS. Die Verschlüsselung kann auch mit dem ersten chiffrierten Rahmen bestätigt werden.

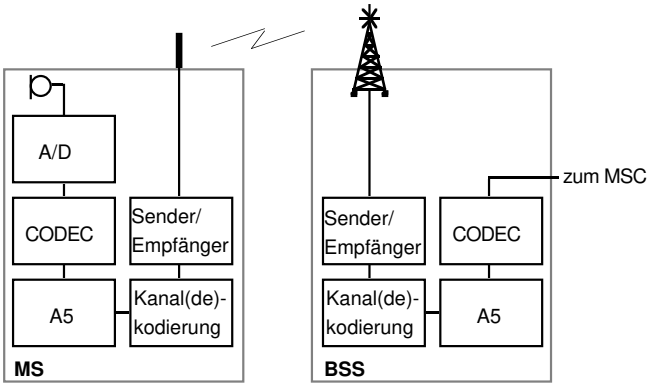


Verschlüsselung auf der Funkschnittstelle

Die Vertraulichkeit der Signalisierungsdaten auf der Funkschnittstelle (*Signalling Information Element Confidentiality*) wird ebenfalls durch Verschlüsselung erreicht.

Insbesondere werden IMEI, IMSI, sonstige Teilnehmeridentitäten, Rufnummer des Anrufers (beim *Mobile Terminating Call,* MTC) und die Rufnummer des Gerufenen (beim *Mobile Originating Call,* MOC) vertraulich behandelt [Bial_94, S.188].

Das folgende Bild zeigt das Zusammenspiel von Sprachkodierung im sog. CODEC-Baustein, der Inhaltsdatenverschlüsselung mit A5 und der Kanalkodierung:



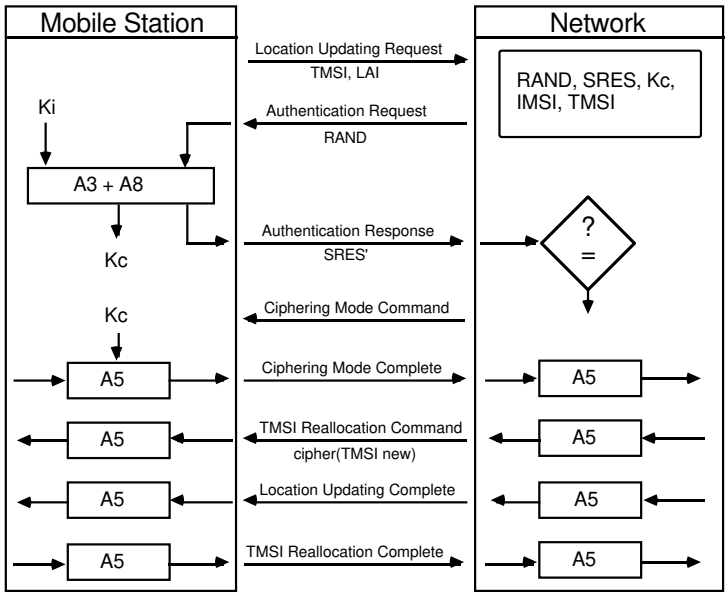
Zusammenspiel von Sprachkodierung, Inhaltsdatenverschlüsselung und Kanalkodierung

4.6 Ein Beispiel

Das folgende Beispiel soll das Zusammenwirken von Authentikation und Verschlüsseln an einem etwas umfassenderen Beispiel für *Location Update* demonstrieren:

Durch die MS wird ein *Location Updating Request* abgesetzt. Daraufhin fordert das Netz die MS auf, sich zu authentisieren. Nach erfolgreich verlaufener Authentikation wird der MS der Verschlüsselungsmodus mitgeteilt und von der MS bestätigt. Danach wird ihr die neue TMSI mitgeteilt und eine *Location Updating Complete*-Nachricht geschickt. Die MS bestätigt den Empfang der neuen TMSI mit *TMSI Reallocation Complete.*

Das Bild verdeutlicht, daß die Signalisierungsdaten verschlüsselt (Algorithmus A5) über die Luft übertragen werden.



Zusammenspiel der Sicherheitsfunktionen am Beispiel Location Update

5 Mobilitäts- und Verbindungsmanagement des GSM

5.1 Location Management

Wie bereits beschrieben, ist das Versorgungsgebiet eines GSM-Netzes eingeteilt in *Location Areas* (LA), wobei ein LA mehrere Funkzellen umfassen kann. Über einen speziellen Signalisierungskanal strahlen die Basisstationen eine *Location Area Identification* (LAI) aus.

Zum **Einbuchen** in das Netz empfängt die Mobilstation (MS) zunächst die LAI und meldet sich bei der zuständigen *Base Transceiver Station* (BTS) unter einer dem Netz bekannten Identität an.[2] Die BTS ist einem *Mobile Switching Center* (MSC) mit *Visitor Location Register* (VLR) zugeordnet. Durch die BTS wird der Aufenthaltswunsch der MS an das MSC/VLR weitergeleitet. Nach erfolgreicher Authentizitätsprüfung wird im VLR ein Dateieintrag mit der gemeldeten LAI des Teilnehmers angelegt. Außerdem wird beim gebuchten Netzbetreiber des Teilnehmers[3] im *Home Location Register* (HLR) ein Verweis auf das aktuelle MSC/VLR angelegt.

Damit die MS bei Bewegung stets erreichbar ist, muß sie den Wechsel eines Versorgungsbereiches (LA oder MSC/VLR-Bereich) erkennen und dem Netz melden. Die hierfür nötigen ***Location Update***-Prozeduren (LUP) werden von der MS ausgelöst.

Handover (HOV) ist das Umschalten einer Kommunikationsverbindung, z.B. eines Gesprächs, auf einen anderen Funkweg. Je nach System sind verschiedene Verbindungsüberwachungsfunktionen und aktive Maßnahmen implementiert. Im GSM wird diese Aufgabe vom Netz übernommen. Das PLMN verfügt über eine globale Übersicht der Verkehrssituation und der vorhandenen Ressourcen und kann in den meisten Fällen diese Aufgabe gut erfüllen (vgl. [MoPa_92, S.399]).

Beim Zellenwechsel innerhalb eines LA bedarf es keines LUPs. Bei einer existierenden Gesprächsverbindung ist allerdings ein HOV erforderlich.

Beim Wechsel eines LA im selben MSC/VLR-Bereich bedarf es nur einer Aktualisierung des VLR-Eintrages.

Bei einem Wechsel in einen neuen MSC/VLR-Bereich muß dort ein neuer VLR-Eintrag angelegt werden, der Eintrag im HLR auf das neue MSC/VLR aktualisiert und der Eintrag im alten VLR gelöscht werden.

Da einem VLR mehrere MSCs zugeordnet sein können, gibt es noch den LUP-Fall „neues MSC, aber altes VLR“.

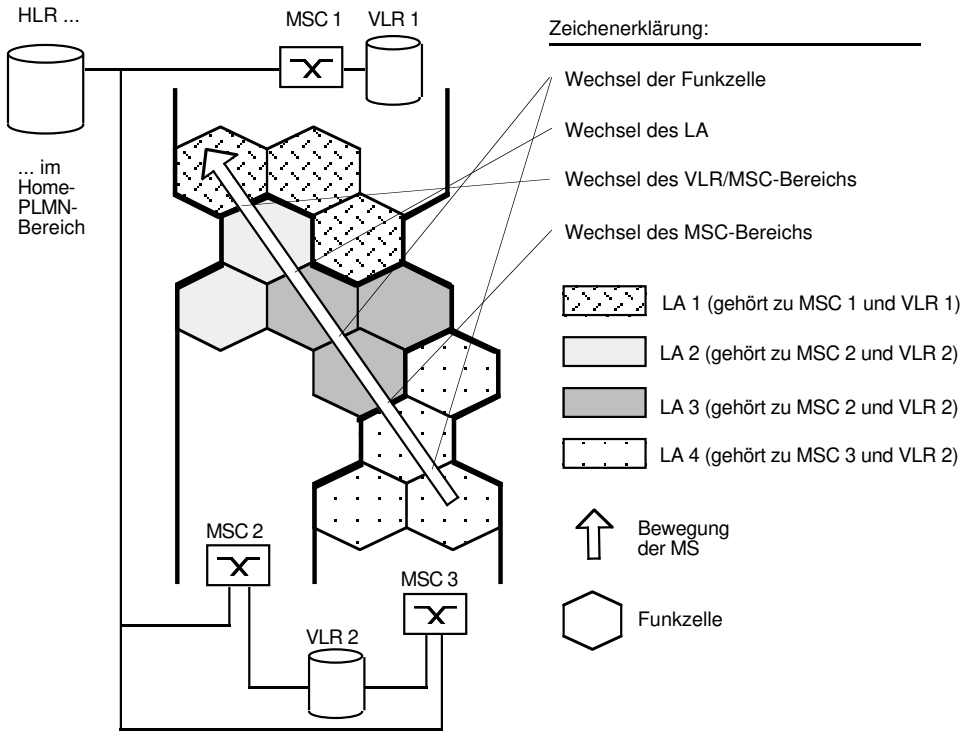
mögliche LUP-Situationen:

LA	MSC	VLR
neu	alt	alt
"	neu	alt
"	"	neu

[2] Beim ersten Einbuchen ist das die *International Mobile Subscriber Identity* (IMSI). Bei jedem weiteren Einbuchen ist das ein Pseudonym, die sog. *Temorary Mobile Subscriber Identity* (TMSI), die zusammen mit der LAI, in dem die MS angemeldet war, die Verkettbarkeit zur IMSI für das Netz ermöglicht. Die TMSI wird im GSM verwendet, um die häufige Übertragung der IMSI über die Funkschnittstelle zu vermeiden. Es soll dadurch für Outsider verborgen werden, wer sich wo im Netz aufhält.

[3] häufig *Home Public Land Mobile Netzwork* (Home-PLMN) genannt

Durch das beschriebene Location Management wird erreicht, daß ein **ankommender Anruf** (*Mobile Terminated Call*, MTC) für den mobilen Teilnehmer in den aktuellen Aufenthaltsbereich der MS vermittelbar ist. Hierzu wird durch Abfrage des HLR-Eintrages das zuständige MSC/VLR ermittelt und der ankommende Ruf dorthin weiter vermittelt. Im zuständigen VLR wird das LA ermittelt und über die zuständigen BTS' eine Verbindungswunschnachricht im LA ausgestrahlt.

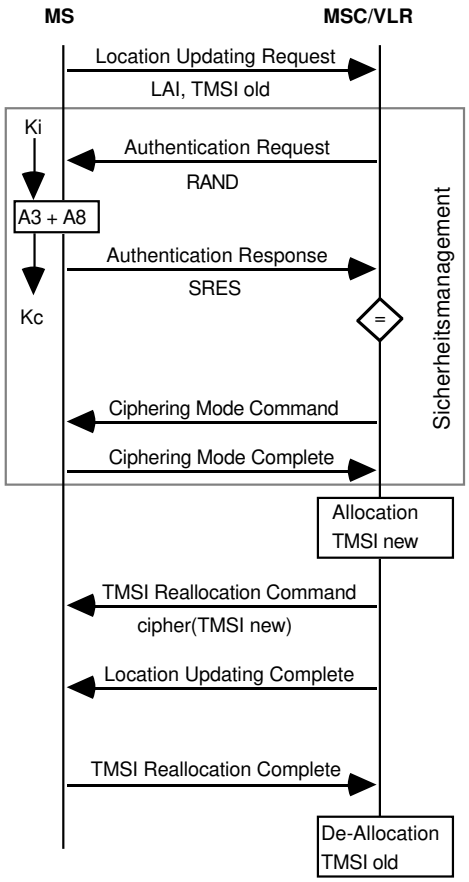


Verschiedene Situationen für LUP und HOV

5.1.1 Altes VLR, altes MSC, neues LA

Im folgenden Bild wird das Protokoll für ein LUP zwischen zwei LAs dargestellt, die zum selben VLR- und MSC-Bereich gehören. Die Randbedingungen dabei sind, daß das alte VLR erreichbar ist und dort die alte TMSI bekannt ist. Sollte das nicht der Fall sein, dann wird über eine *Identity Request*-Nachricht die IMSI angefordert (siehe auch Vergabe der TMSI). Die restlichen Protokollschritte bleiben erhalten.

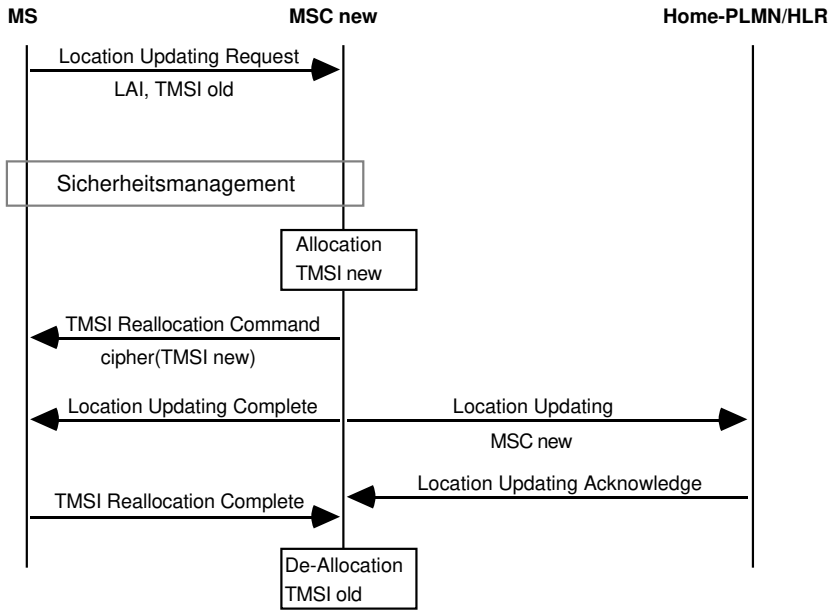
Um das Zusammenspiel von LUP-Prozessen und Sicherheitsmanagement noch einmal deutlich zu machen, wurden die Protokollschritte für Authentikation, Chiffrierschlüsselgenerierung und Verschlüsselungsmodus-Auswahl in dieses Bild hinzugenommen. Aus Gründen der Übersichtlichkeit wird bei den weiteren Bildern darauf verzichtet.



LUP: Altes VLR, altes MSC, neues LA (TMSI bekannt)

5.1.2 Altes VLR, neues MSC, neues LA

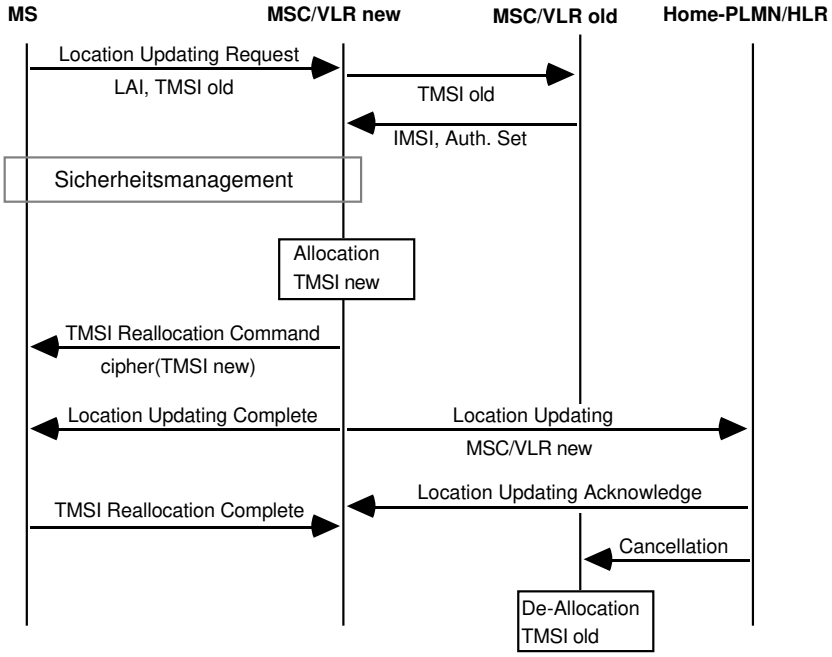
Diese LUP-Prozedur wird ausgeführt, wenn das alte LA und das neue LA zu verschiedenen MSCs gehören, aber zum selben VLR. Die Anfragen an das VLR wurden weggelassen.



LUP: Altes VLR, neues MSC, neues LA (TMSI bekannt)

5.1.3 Neues VLR, neues MSC, neues LA

Diese LUP-Prozedur wird ausgeführt, wenn das alte LA und das neue LA zu verschiedenen VLRs gehören.



LUP: Neues VLR, neues MSC, neues LA (altes VLR erreichbar bzw. TMSI bekannt)

5.2 Rufaufbau (Call Setup)

Man unterscheidet je nach Initiierung und Ziel vier verschiedene Rufaufbau-Typen:

- *Mobile Originated Call* (MOC),

- *Mobile Terminated Call* (MTC),
- *Mobile-Mobile Call* (MMC),
- *Transit Call*.

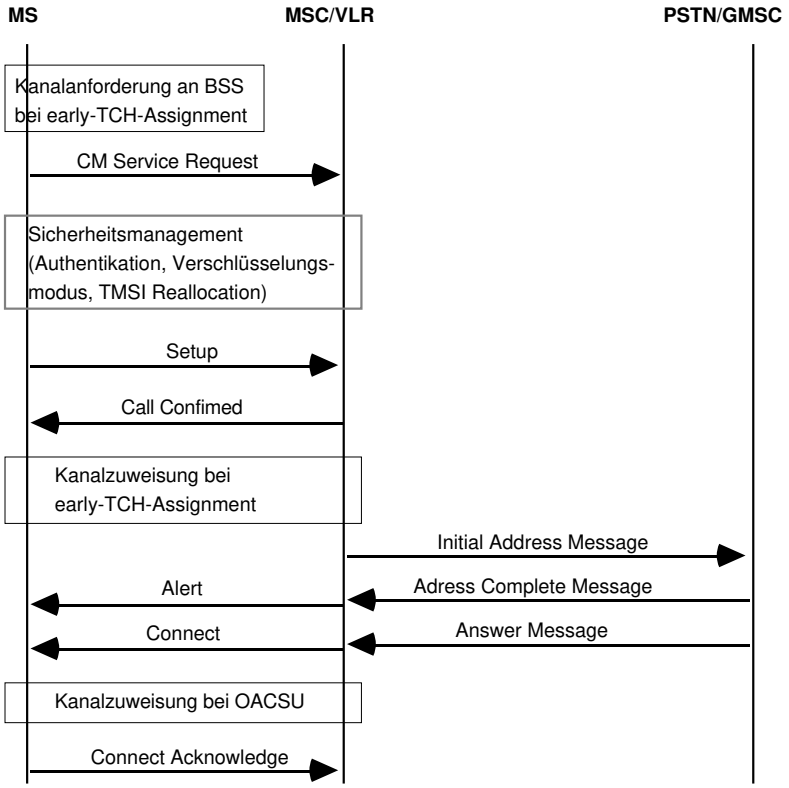
Im folgenden sollen jedoch nur MOC- und MTC-*Setup* behandelt werden.

Bei einem Verbindungsaufbau kann es sich abhängig vom Aufenthaltsort der MS um einen Prozeß handeln, der über mehrere verschiedene nationale und/oder internationale Netze (ISDN/PSTN/PDN/PLMN) verläuft.

Es wird zwischen *Call Setup* mit *early*-TCH-*Assignment* und „funkfreiem“ Rufaufbau (*Off Air Call Setup*, OACSU) unterschieden. Man spricht von einem OACSU, wenn ein TCH zwischen MS und Netz erst nach *Call Confimed* zugeordnet wird.

5.2.1 Mobile Originated Call Setup

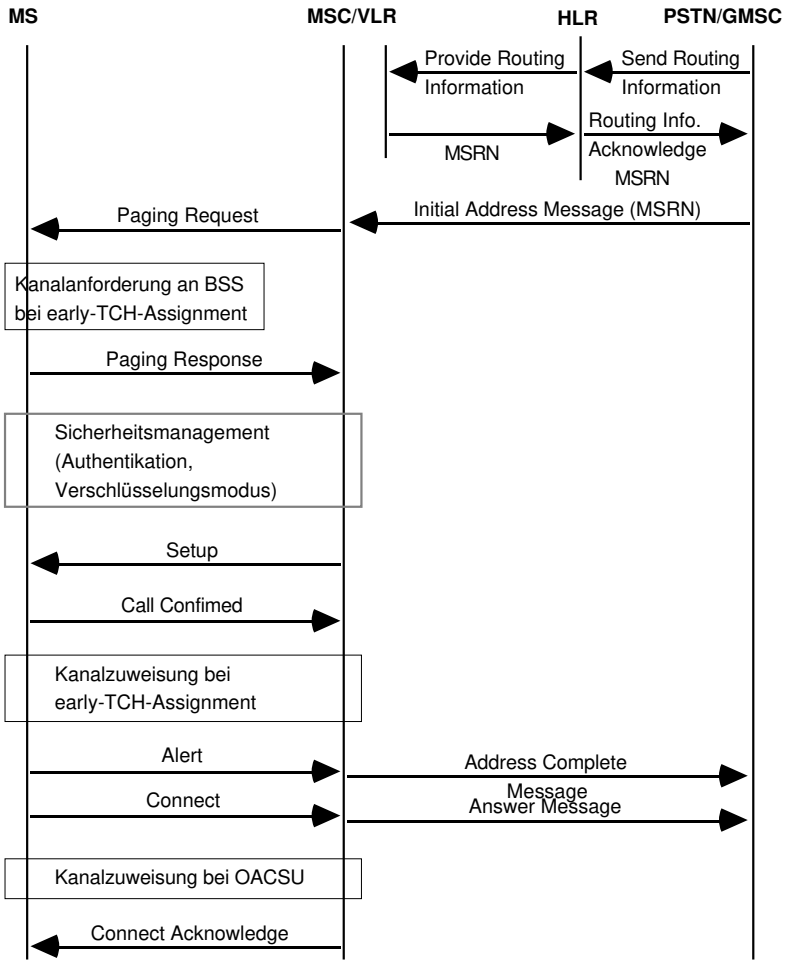
Ein MOC ist ein von der MS ausgehender Anruf.



Mobile Originated Call Setup

5.2.2 Mobile Terminated Call Setup

Ein MTC ist ein zur MS kommender Anruf. Beim MTC unterscheidet man mehrere Varianten je nach Aufenthaltsort des Teilnehmers und der zur Verfügung stehenden *Routing*-Informationen und Leitwege. An dieser Stelle wird ein vom Fremdnetz kommender (*Network Initiated*) MTC beschrieben, bei dem das aktuelle GMSC bereits gefunden wurde.



Mobile Terminated Call Setup

6 Sicherheitsprobleme beim GSM

Dieser Abschnitt geht detaillierter auf einige gravierende Sicherheitsprobleme (bezogen auf die formulierten technischen Datenschutzforderungen) ein. Die erkannten Sicherheitsmängel werden abschließend noch einmal zusammengefaßt.

6.1 Erstellbarkeit von Bewegungsprofilen

Da das Mobilfunknetz jederzeit in der Lage ist, einen Teilnehmer zu erreichen, d.h. seinen aktuellen Aufenthaltsort kennt, ist bei kontinuierlicher Akkumulation von Lokalisierugsinformation die Aufzeichnung eines Bewegungsprofils eines Teilnehmers (genauer: des SIM-Moduls) möglich. Dies verstößt gegen die Datenschutzforderung **c3**.

Auf den verschiedenen Ebenen des Netzes existieren folglich verschiedene Möglichkeiten zur Erstellung von Bewegungsprofilen:

Ebene HLR: Für jede IMSI wird die aktuelle VLR/MSC-Adresse, die LMSI sowie zusätzliche Routinginformation gespeichert. Eine Erstellung von *Bewegungsprofilen mit VLR-Genauigkeit* ist möglich. Es erfolgt keine Verknüpfung der IMSI mit den Bestandsdaten [Bath_92].

Ebene VLR/MSC: Für jeden Teilnehmer, der sich im VLR/MSC-Bereich aufhält, wird die LAI gespeichert und ständig aktualisiert. Nach [Bath_92] ist im VLR der Grad der *Informationsgenauigkeit bis zur BSC* gegeben. Das legt den Schluß nahe, daß ein LA (eindeutig bestimmt durch seine LAI) einem BSC-Bereich entspricht. Im Standard ist dies nicht explizit ausgeführt, für eine effiziente Implementierung des GSM-Standards ist diese Annahme jedoch durchaus sinnvoll. Ähnliches gilt auch für die Zuordnung VLR–MSC: Es ist nicht eindeutig beschrieben, ob jedem MSC genau ein VLR zugeordnet ist und umgekehrt. Für die technische Realisierung ist diese 1:1-Zuordnung aber sinnvoll. In der Literatur wird deshalb häufig von einem MSC/VLR-Bereich gesprochen.

Verläßt ein Teilnehmer den zuständigen MSC/VLR-Bereich, werden die Lokalisierungsdaten gelöscht. Im VLR erfolgt *keine* Sortierung der Daten nach Teilnehmern [Bath_92].

Ebene BSS: Für die Realisierung des Lokalisierungsmanagements auf Zellebene sind im BSS (genauer im BSC) entsprechende Funktionen realisiert. Man kann also davon ausgehen, daß, solange sich ein Teilnehmer im zuständigen BSS aufhält, *Lokalisierungsinformationen bis auf Zellgenauigkeit* vorhanden sind. Diese Informationen sind für das Interworking von GSM-Netzen und deren Bestandteilen (verschiedener Hersteller, Betreiber und/oder Nationen) nicht erforderlich. Gründe hierfür könnten sein:

- Das BSC ist eine in sich geschlossene Einheit ohne Schnittstellen, über die Zellinformationen übertragen werden müssen. Das BSC als Steuereinheit auf Funkebene steuert die BTS' über Port- oder Funkadapteradressen direkt. Für das GSM-Netz ist also eine Funkzelle keine geographische Einheit im eigentlichen Sinn. Die BTS selbst ist nur eine funktechnische Einrichtung ohne Rechenkapazität.
- Für die Abrechnung der Dienstbenutzung sind im GSM nur Lokalisierungsinformationen mit BSC-Genauigkeit bzw. LAI-Genauigkeit erforderlich ([Bath_92], siehe auch obige Bemerkungen), nicht jedoch mit Zellgenauigkeit.

Funktechnische Ebene, Peil- und Ortbarkeit: Da elektromagnetische Wellen Richtungsinformation enthalten, ist eine Peilung und Ortung von Sendern gewöhnlich möglich. Dies gilt auch für die Sendeeinrichtungen der Mobilstationen der Teilnehmer. Im GSM (Phase 2) wird das Sendeverfahren *Frequency Hopping* (FH) angewendet, das die Peilbarkeit für Außenstehende zwar erschwert, jedoch nicht verhindert [Thee_94]. Der Netzbetreiber ist jedoch sehr gut in der Lage, über bestimmte Peilverfahren (z.B. Laufzeitpeilung) selbst innerhalb der Funkzelle den Aufenthaltsort eines Teilnehmers festzustellen. Theoretisch sind also Bewegungsprofile auf wenige Meter genau möglich. Solche Peilungsverfahren sind allerdings

bisher nicht implementiert. Es könnte aber durchaus sein, daß ein Netzbetreiber zu gegebener Zeit einen Ortungsdienst anbietet, z.B. als Notfalldienst. Technische Überlegungen hierzu fanden sich z.B. in [Kenn_95].

6.2 Entgeltabrechung

Zur Abrechnung der Dienstnutzung werden Verbindungsdaten, sog. Anrufdatensätze (*Call-, Billing-Records*), vom HLR und VLR an **Abrechnungszentralen** (sog. *Billing-Centers*) übermittelt, nach Teilnehmern sortiert und mit den Bestandsdaten verknüpft. Da die Verbindungsdaten auch die BSC bzw. LAI einer Verbindung enthalten, sind die Billing-Centers in der Lage, Bewegungsprofile mit der Genauigkeit der LAI und Abrechnungsrecord-Periode zu erstellen.

Die Felder eines **Anrufdatensatzes** können beinhalten (nach [MaMo_91]):

- die MSISDN und IMSI des rufenden Teilnehmers (bei einem *Mobile Originated Call*),
- die IMEI des benutzten Gerätes,
- die gerufene Nummer,
- die gewählten Ziffern: normalerweise identisch mit der gerufenen Nummer, jedoch wichtig bei Kurzwahlnummern und Anrufweiter- bzw. -umleitung,
- die Standortinformation bestehend aus
  - MSC-Bereich: ähnlich aufgebaut wie die Rufnummer (15 Ziffern): CC, NDC, 2 Ziffern für MSC-Kennung, weitere für Abrechnung bedeutungslose Ziffern,
  - LAI und CI,
  - Funkkanalkennung – nicht für die Abrechnung nötig,
- die sog. *Trunk-Group*, d.h. die Verbindungsleitung, auf der das MSC die Verbindung weiterschaltet; – nicht für Gebührenabrechnung mit dem Kunden relevant, evtl. aber für Abrechnung mit anderen (Festnetz)betreibern,
- benutzte Zusatzdienste,
- Typ der Mobilstation (*Mobile Station Classmark*): enthält Daten zur Sendeleistung und ob es sich um ein Handy, tragbares Gerät oder Einbaugerät handelt,
- Zeitmarkierungen (*Time Stamps*): Beginn, Ende, Dauer des Gesprächs (Uhrzeit und Datum),
- OACSU-Indikator: zeigt an, ob ein Gespräch mit *Off Air Call Setup* aufgebaut wurde,
- *Fullrate/Halfrate*-Indikator: gibt an, ob die Verbindung auf einem *Fullrate*- oder *Halfrate*-Kanal ablief,
- Grund für die Beendigung des Gesprächs (*Cause for Termination*): gibt an, ob normales Ende, Funkstörung, gestohlenes Gerät oder Ausfall einer Netzkomponente,
- Datenvolumen (bei Datendiensten ausgewertet),
- eine laufende Nummer (*Call Reference*).

Da LUPs des mobilen Teilnehmers einen z.T. hohen Signalisierungsaufwand zur Folge haben können, ist auch die Erstellung eines ***Location Update Records*** zur Entgeltabrechnung möglich [MaMo_91]. Er enthält dann:

- die IMSI,
- den alten und neuen Standort des Teilnehmers,
- den Typ der Mobilstation (*Mobile Station Classmark*),
- Zeitmarkierungen (*Time Stamps*) für die LUP-Ausführung und
- *Cause for Termination.*

Hat ein Teilnehmer einen **Einzelentgeltnachweis** gebucht, werden einige Daten der Billing-Records an den Diensteanbieter (soweit vorhanden) und an den *Subscriber* (derjenige, der den Dienst gebucht hat) weitergereicht. Ob die Standortkennungen an den Diensteanbieter weitergereicht werden, hängt im wesentlichen vom gebuchten Dienstprofil des Teilnehmers ab. Gewöhnlich werden sie jedoch nicht weitergereicht. An den Subscriber werden *keine* Standortkennungen weitergereicht. Der Einzelentgeltnachweis soll nach [Bath_92] folgende Daten enthalten:

- eine laufende Nummer,
- *Time Stamps*: Datum und Uhrzeit eines Gesprächs, Gesprächsdauer,
- Nummer des angerufenen Teilnehmers (voll oder verkürzt),
- Tarif des Gesprächs (Haupt-/Nebenzeit),
- Entgelteinheiten und Preis.

Die **Netzbenutzung mit vorbezahlten Wertkarten** ist derzeit nicht möglich. Ob ein solcher Dienst in die GSM-Netze implementiert werden soll, ist nicht bekannt. Einige Voraussetzungen hierfür sind mit dem Entgeltzusatzdienst *Advice of Charge* (AoC) aber bereits geschaffen. Bei aktiviertem AoC werden die während eines Rufs angefallenen Gebühreneinheiten *nach* dem Gespräch dem Teilnehmer übermittelt und angezeigt. Nach der GSM Rec. 02.24 kann allerdings eine Differenz von maximal einer Einheit zwischen den tatsächlich angefallenen und den übermittelten Gebühren auftreten. Als Grund wird die Zeitsynchronisation zwischen Mobilstation und Netz angegeben.

Der AoC-Dienst war zur Einführungsphase des GSM leider noch nicht verfügbar. Dem Autor ist nicht bekannt, ob er inzwischen implementiert ist.

Für die Netze der dritten Generation wird die Netzbenutzung mit vorbezahlten Wertkarten aber ausdrücklich gefordert.

Leider sind im GSM keinerlei Funktionen implementiert, die dem Nutzer garantieren, daß die **Rechnungsstellung** korrekt verlaufen ist, d.h. nur das in Rechnung gestellt wurde, was tatsächlich genutzt wurde. Es sind keine anonymen digitalen Zahlungssysteme implementiert.

6.3 Registrierung der Gerätekennungen (EIR)

Wie bereits erläutert, existieren im GSM sog. Gerätekennungsdatenbanken (EIR). Jedes GSM-Mobilfunkgerät besitzt eine entsprechende IMEI, die abgefragt werden kann. Die Erstellung von Bewegungsprofilen eines Gerätes auf der grauen (und schwarzen) Liste ist explizit vorgesehen.

Ursprünglich war im EIR nur die Speicherung der IMEI geplant. Es gab aber bei einigen Betreibern (z.B. D2) Überlegungen, die IMEI zusammen mit den Bestandsdaten (z.B. wer das Gerät erworben hatte) zu speichern! Ziel war es, dem Besitzer Hinweise auf aktuellere Software u.ä. zu geben, sowie eine Verfolgung der das Netz störenden Geräte zu ermöglichen (siehe [Bath_92]).

6.4 Zusammenfassung

Zusammenfassend lassen sich also **bezüglich der Sicherheitsaspekte** folgende Punkte an GSM kritisieren:

- Es existieren keine Maßnahmen für die Vertraulichkeit des Aufenthaltsorts.
- Die Peilbarkeit von mobilen Stationen ist möglich.
- Es ist keine Ende-zu-Ende-Authentikation möglich.
- Es ist keine Ende-zu-Ende-Konzelation möglich.
- Die verwendeten Kryptoalgorithmen (A3, A5, A5*, A8) sind teilweise geheim gehalten.
- Die Verschlüsselungsverfahren sind symmetrisch.
- Die Schlüsselerzeugung erfolgt nicht unter der Kontrolle der Teilnehmer.

- Keine gegenseitige Authentikation, d.h. des Teilnehmers vor dem Netz *und* Netzes vor dem Teilnehmer.
- Vertrauen in die korrekte Abrechnung ist wie bei den bisherigen Netzen erforderlich.
- Es ist keine anonyme Netzbenutzung möglich.
- GSM unterstützt bisher keine vorbezahlten Wertkarten.

Fazit: GSM ist zwar ein funktionierendes mobiles Netz *mit* Sicherheitsfeatures, erfüllt jedoch *nicht* alle „Technischen Datenschutzanforderungen". Insbesondere der *Mehrseitigkeitsaspekt* von Sicherheit wurde nicht berücksichtigt.

Als **weitere Kritikpunkte** können formuliert werden:

- Es existieren keine bittransparenten Kanäle, die eine Verlängerung der transparenten 64 kbit/s-ISDN-Kanäle zum GSM erlauben.
- Durch die erhöhte technische Erreichbarkeit folgt eine erhöhte persönliche Erreichbarkeit, was neue Erreichbarkeitsmanagement-Dienste erforderlich machen wird.
- Die elektromagnetische Verträglichkeit der Funkwellen durch den menschlichen Organismus ist bis heute nicht vollständig geklärt.
- Durch die hohe Komplexität von GSM ist eine überschaubare Kontrolle des Gesamtsystems schwer möglich[4].

Mögliche **Auswege** zu einem sichereren Netz könnten sein:

- Modifikation des *Location Managements*,
- Verhinderung von Peilung und Ortung durch funktechnische, informationstechnische und kryptographische Maßnahmen,
- Definition von Ende-zu-Ende-Diensten,
- Unterstützung von asymmetrischen Kryptoalgorithmen (*Public Key Cryptography*),
- Implementation von Erreichbarkeitsmanagementfunktionen, die Privatheit unterstützen,
- Modifikation der Abrechnungsfunktionen, Ermöglichen der Netzbenutzung mit vorbezahlten Wertkarten.
- ferner: Geschickte Ausnutzung von Trends bei Neukonzeption von Netzen (z.B. Zellüberlappungen).

Die digitalen Mobilkommunikationssysteme haben mit GSM ihren ersten Vertreter für den Massenmarkt in Europa und die Entwicklung neuer Systeme schreitet natürlich voran. Dies und die teilweise noch unbefriedigenden Sicherheitsmerkmale der vorhandenen Netze sind genug Motivation, mit neuen Vorschlägen zum datenschutzgerechteren Design künftiger Netze beizutragen. Ein solches künftiges Netz ist UMTS (*Universal Mobile Telecommunication System*). Außerdem mag es – in gewissen Grenzen – stets Möglichkeiten geben, die vorhandenen und bereits standardisierten Netze an geeigneter Stelle zu modifizieren oder um entsprechende Zusatzdienste zu erweitern, um sie datenschutzgerechter zu gestalten.

4 GSM: *Great Signalling Monster*.

7 Abkürzungsverzeichnis

A3	kryprographischer Algorithmus zur Authentikation
A5	kryptographischer Algorithmus zur Inhaltsdatenverschlüsselung auf der Luftschnittstelle
A8	kryptographischer Algorithmus zur Generierung von Kc
AC	Authentication Center
AoC	Advice of Charge
BCCH	Broadcast Control Channel
Bm	Bearer mobile (Channel)
BSC	Base Station Controller
BSIC	Base Transceiver Station Identity Code
BSS	Base Station Subsystem
BTS	Base Transceiver Station
CAIS	Common Air Interface Standard
CC	Country Code
CCCH	Common Control Channel
CEPT	Conference Europeenne des Administrations des Postes et des Telecommunications, Konferenz der Europäischen Post- und Fernmeldeverwaltungen
CI	Cell Identity
CKSN	Ciphering Key Sequence Number
CM	Connection Management
CMR	Cellular Mobile Radio
CODEC	Kunstwort für (Sprach)kodierer/-dekodierer
CT	Cordless Telephone
DCCH	Dedicated Control Channel
DCS 1800	Digital Cellular System 1800
DECT	Digital European Cordless Telephone
Dm	Data mobile (Channel)
DSRR	Digital Short Range Radio
DTI	Department of Trade and Industry, britisches Ministerium für Handel und Industrie
EIR	Equipment Identity Register
ERMES	European Radio Messaging System
ETSI	European Telecommunications Standards Institute, Europäisches Institut für Telekommunikationsnormen
FDMA	Frequency Division Multiplex Access
FH	Frequency Hopping
FPLMTS	Future Public Land Mobile Telecommunication System
GMSK	Gaussian Minimum Shift Keying
GPS	Global Positioning System
GSM	Global System for Mobile Communication, Groupe Spéciale Mobile
HLR	Home Location Register
HOV	Handover

IMEI	International Mobile Station Equipment Identity
IMSI	International Mobile Subscriber Identity
IN	Intelligent Network
Inmarsat	International Maritime Satellite
ISDN	Integrated Services Digital Network
IT	Informationstechnik, informationstechnisch-
Kc	Cipher Key, temporär gültig
Ki	Individueller geheimer Schlüssel eines Teilnehmers
LA	Location Area
LAI	Location Area Identification
LEO	Low Earth Orbit
Lm	Low mobile (Channel)
LMSI	Local MS Identity
LUP	Location Update
MCC	Mobile Country Code
MNC	Mobile Network Code
MOC	Mobile Originated Call
MS	Mobile Station
MSC	Mobile Switching Center
MSISDN	Mobile Subscriber International ISDN Number
MSRN	Mobile Subscriber Roaming Number
MTC	Mobile Terminated Call
NDC	National Destination Code
OACSU	Off Air Call Setup
OMC	Operation and Maintenance Center
PCN	Personal Communication Network
PCS	Personal Communication Services
PDN	Public Data Network
PIN	Personal Identification Number
PLMN	Public Land Mobile Network
PSTN	Public Switched Telephone Network
RAND	Zufallszahl für Authentikation
SIM	Subscriber Identity Module
SITA	Internationale Luftverkehrsgesellschaft
SMS	Short Message Service
SRES	Signed Response, Antwort auf den RAND-Wert der Authentikationsprozedur
TCH	Traffic Channel
TDMA	Time Division Multiplex Access
TMSI	Temporary Mobile Subscriber Identity
UMTS	Universal Mobile Telecommunication System
UPT	Universal Personal Telecommunications
VLR	Visitor Location Register
W-LAN	Wireless Local Area Network
W-PBX	Wireless Private Branch Exchanges

8 Literaturverzeichnis

Bath_92 Beate Bathe-Peters: Lösungsansätze für Datenschutzprobleme beim Mobiltelefon; Dokumentation des ITG-Forums „Gestaltungsfelder beim Mobiltelefon“, 12. Mai 1992, Frankfurt am Main, 93-96.

Bial_94 Jacek Biala: Mobilfunk und intelligente Netze; Vieweg, Braunschweig/Wiesbaden, 1994.

CoBr_92 J. C. Cooke, R. L. Brewster: Cryptographic Security Techniques for Digital Mobile Telephones; IEE 2nd Int. Conf. on Private Switching Systems and Networks, London, GB, 23. - 25. Juni 1992, 123-130.

Evci_92 Evci, C. Cengiz : Race-UMTS for third generation wireless communications; ANN. TÉLÉCOMMUN., 47, Nr. 7-8, 1992.

FKPS_94 Hannes Federrath, Dogan Kesdogan, Andreas Pfitzmann, Otto Spaniol: Erreichbarkeitsmanagement und Notrufdienst auf der Basis datensparsamer Adressierung; Arbeitspapier zum Kolleg „Sicherheit in der Kommunikationstechnik" der Gottlieb Daimler - und Karl Benz - Stiftung Ladenburg, April 1994.

Frey_94 L. Frey: The Possible Use of Public Key Cryptosystems for UMTS; Mobile Telecommunication Workshop (1994) 364-368.

Grab_89 Grabau, Rudolf: Technische Aufklärung: Sensoren, Systeme und Verfahren. entdecken-klassifizieren-identifizieren-orten-auswerten; Franckh-Verlag, Stuttgart 1989.

GrWo_92 Jos Grond, Wiliam Wolfowicz: Security Issues for Universal Mobile Telecommunication System; Proceedings of 11th International Conference on Computer Communication, Geneva, Italy, 1992, 613-616.

GSM_03.20 ETSI: ETSI/TC GSM: 03.20 European digital cellular telecommunications system (Phase 2); Security related network funktions (GSM 03.20). Version 4.2.2, October 1993.

GSM_93 ETSI: GSM Recommendations: GSM 01.02 - 12.21; February 1993, Release 92.

Keda_91 J. Kedaj: Mobilfunkdienste der Deutschen Bundespost TELEKOM; Unterrichtsblätter der Deutschen Bundespost TELEKOM, Jg. 44, 1991, 424-434.

Kenn_95 Orlik Kennemann: Mobile Location in Cellular Radio Systems Based on Pattern Tecognition Techniques Using a Learning and Adaptive Data Base; Proc. of the IFIP TC 6 International Workshop on Personal Wireless Communications, Verlag der Augustinus Buchhandlung Aachen, 1995, 63-71.

MaMo_91 Mannesmann Mobilfunk: Anrufdatensätze; Ergänzung zur Dokumentation des ITG-Forums „Gestaltungsfelder beim Mobiltelefon“, 12. Mai 1992, Frankfurt am Main.

Mich_91 Uwe Michel: Sicherheitsfunktionen im paneuropäischen Mobilfunknetz; Proc. Verläßliche Informationssysteme (VIS'91), März 1991, Darmstadt, Informatik-Fachberichte 271, Springer-Verlag, Heidelberg 1991, 133-145.

MoPa_92 Mouly, Michel; Pautet, Marie-Bernardette: The GSM System for Mobile Communications. Michel MOULY & Marie-Bernadette PAUTET 1992.

Pfit_89 Andreas Pfitzmann: Diensteintegrierende Kommunikationsnetze mit teilnehmerüberprüfbarem Datenschutz; Universität Karlsruhe, Fakultät für Informatik, Dissertation, Feb. 1989, IFB 234, Springer-Verlag, Heidelberg 1990.

Pfit_93 Andreas Pfitzmann: Technischer Datenschutz in öffentlichen Funknetzen; Datenschutz und Datensicherung DuD 17/8 (1993) 451-463.

Römh_95 Dirk Römhild: Das Universal Mobile Telecommunication System (UMTS) aus der Sicht des Technischen Datenschutzes; Großer Beleg, TU Dresden, Institut für Theoretische Informatik, September 1995

Silb_92 Armin Silberhorn: Stand der europäischen Normung im Mobilfunkbereich – Behindern technische Standards den Datenschutz?; Symposium „Datenschutz: Komfort und Freiheit des Kunden in der Telekommunikation“, 2. Sept. 1991, Materialien zum Datenschutz 15, Herausgeber: Berliner Datenschutzbeauftragter, Mai 1992, 104-125.

Thee_94 Jürgen Thees: Konkretisierung der Methoden zum Schutz von Verkehrsdaten in Funknetzen; Diplomarbeit am Institut Theoretische Informatik der TU Dresden, Juni 1994.

Whit_95 Christine White: On-Road, On-Time, and On-Line; Byte 20/4 (1995) 60-66.