GSM spezifische Abläufe

KURZFASSUNG

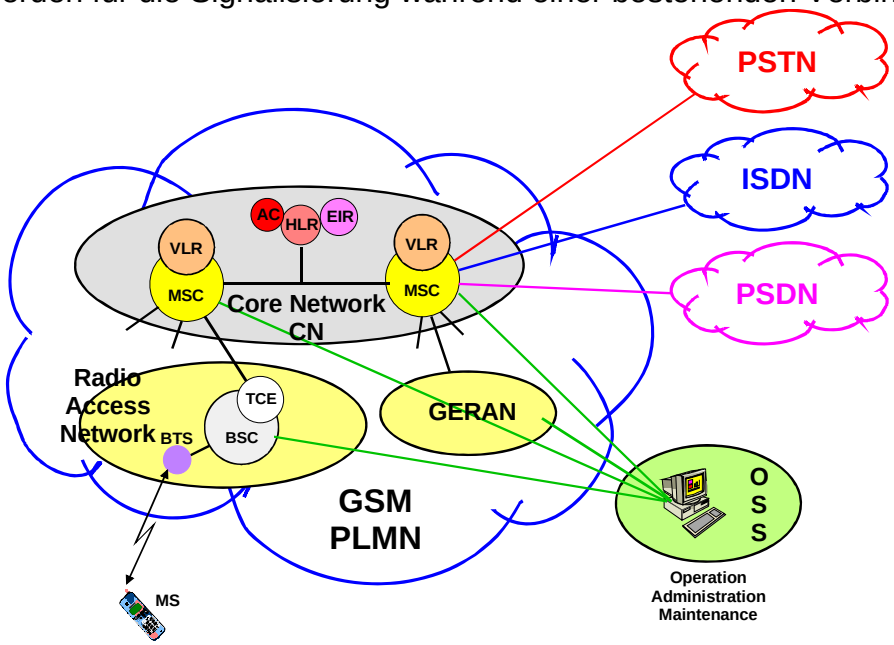
31 Seiten

INHALT

1 Übersicht

Sobald ein Mobilteilnehmer sein Endgerät einschaltet laufen vor der Einbuchung ins Netz zunächst gerätespezifische Prüfsequenzen ab und anschließend die netzbezogenen Vorgänge, von denen die Authentication die wichtigste Aktivität ist, da sie außer bei der Inbetriebnahme (Einschalten) auch vor jedem Gesprächsaufbau durchgeführt wird.
Neben der Authentication, die bei einem Festnetzanschluss nicht erforderlich ist da das Teilnehmer-Endgerät nicht mobil an das Netz angeschlossen ist, sind in einem GSM-Netz noch die den Standortwechsel des Endgerätes betreffenden Abläufe des im eingeschaltetem aber Gesprächslosen Zustand – sog. Location Update – bzw. während des Gesprächszustandes – sog. Handover – systemspezifisch.
Um diese systemspezifischen Abläufe optimal abwickeln zu können wurden im GSM folgende spezifischen Gruppen von Signalisierungskanälen vorgesehen:

- Im Zeitschlitz 0 eines TDMA-Rahmens
  - BCH Broadcast Channel, nur Downlink für zellenspezifische Informationen, Synchronisation, Frequenzkorrektur, ...
  - CCCH Common Control Channel, Uplink und Downlink, können von allen MSs z.B. zur Anforderung von Diensten benützt werden
  - DCCH Dedicated Control Channel, Uplink und Downlink, wird einer MS zur Abwicklung eines bestimmten Dienstes, z.B. Verbindungsaufbau zugeteilt.
- Im Speech Channel
  - ACCH Associated Signalling Channels, sind Teil des Speech Channels und werden für die Signalisierung während einer bestehenden Verbindung benützt.



GERAN	GSM Radio Access NW	CN	GSM Core Network	OSS	Operation and Maintenance Subsystem
AC	Authentication Center	HLR	Home Location Register	EIR	Equipment Identification Reg.
MSC	Mobile Switching Center	VLR	Visitor Location Register	BSC	Base Station Controller
BTS	Base Transceiver Station	MS	Mobile Station	PLMN	Public Land Mobile Network
PSDN	Public Switched Data Network	PSTN	Public Switched Telephone Network		
TCE	Transcoding Equipment				

Bild 1 GSM - Netzstruktur

Schlüsselwörter

Physikalische Kanäle, logische Kanäle, Burst, Steuerkanal, IMSI Attach, IMSI Detach, Location Update, Handover, Authentication, Interrogation, Paging.

2 Kanalstrukturen auf der Funkschnittstelle

2.1 Physikalische Kanalstruktur

Die physikalischen Kanäle auf der Luftschnittstelle U_m sind durch ihre Trägerfrequenz und die zur Verfügung stehenden, alle 4,615 ms wiederkehrenden Zeitschlitze charakterisiert.

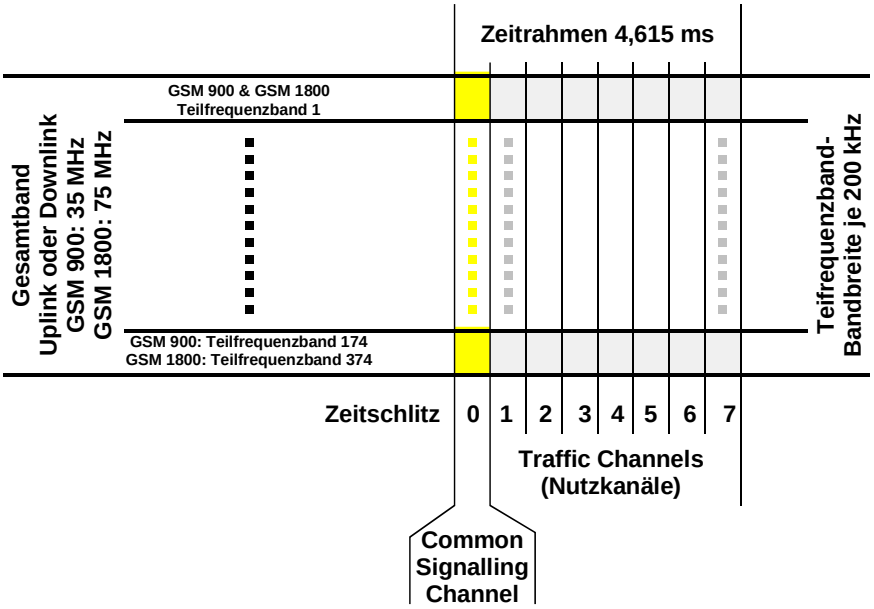


Bild 2 Die physikalische Rahmenstruktur auf der Luftschnittstelle U_m

Eigenschaften eines physikalischen Kanals

(1) Entsprechend den zur Verfügung stehenden GSM-Frequenzbändern wird mittels Frequenzmultiplex eine bestimmte Anzahl von Radio Frequency Channels RFC gebildet, welche mittels Zeitmultiplex in jeweils 8 Slots unterteilt werden:

- bei GSM 900 124 RFC,
- bei extended GSM 900[1] 124 + 50 = 174 RFC und
- bei GSM 1800 374 RFC

Jeder Slot – Zeitschlitz - besitzt eine Länge entsprechend der Dauer von 156,25 bit bzw. 0,577 ms (15/26 ms). Diese Länge ergibt sich aus der Übertragungsrate des Modulationsverfahrens (1625/6 kbit/s) und der Anzahl an Bits, die man in einem Slot überträgt. Damit die Mobilstationen nicht gleichzeitig senden und empfangen müssen, wird Uplink mit einer Verzögerung von drei Slots gesendet.
Genutzt wird ein Slot durch Bursts mit einer Länge von 148 Bit, die, um Überlappungen mit anderen Bursts zu vermeiden, um die Guard Period, entsprechend der Dauer von 8,25 Bit, kürzer als die Slots sind. Wenn Nachrichten länger als ein Burst sind, werden sie auf mehrere Bursts aufgeteilt und dann übertragen.

Burst-Strukturen

(2) Insgesamt existieren fünf verschiedene Strukturen von Bursts, die sich durch Funktion und Inhalt unterscheiden. Die in allen Bursts vorkommenden Tail-Bits überbrücken die Zeitperiode, in welcher die Sendeleistung am Beginn und Ende eines Bursts hoch- bzw. herun-

[1] In Österreich nicht verwendet

tergetastet wird und für eine korrekte Datenübertragung nicht benützt werden kann; sie haben immer die im Standard festgelegte Wertigkeit „logisch Null“.

Normal Burst

TB 3	Encrypted Bits 57	1	Trainings-sequence 26	1	Encrypted Bits 57	TB 3	Guard 8,25

stealing flag

Frequency Correction Burst

TB 3	Fixed Bitpattern 142	TB 3	Guard 8,25

Synchronization Burst

TB 3	Encrypted Bits 39	Extended Trainingssequence 64	Encrypted Bits 39	TB 3	Guard 8,25

Dummy Burst

TB 3	Fixed Bitpattern 58	Trainings-sequence 26	Fixed Bitpattern 58	TB 3	Guard 8,25

Access Burst

Ext. TB 8	Sync. Sequence 41	Encrypted Bits 36	TB 3	Guard Intervall 68,25

Bild 3 Burststrukturen

- **Normal Burst:** dient der Informationsübertragung in Traffic und Control Channels, wobei die Stealing-Flags angeben ob der Burst Nutzdaten oder Signalisierungsinformationen beinhaltet.
  Die 26 Bit Trainings-Sequenz besteht aus vordefinierten Bitmustern, die für die Kanalschätzung und Synchronisation verwendet werden. Mit dieser Sequenz kann z.B. die Intersymbolinterferrenz, bedingt durch die Laufunterschiede bei der Mehrwegausbreitung, eliminiert werden. Es sind 8 verschiedene Trainings-Sequenzen definiert, mit denen bis zu 16µs ausgeglichen werden können.
- **Synchronization Burst:** dient zur Synchronisation und überträgt die laufende Nummer des TDMA-Rahmens und den BSIC (Basic Station Identity Code). Wird der Synchronization Burst wiederholt ausgestrahlt, so spricht man vom SCH (Synchronization Channel).
- **Frequency Correction Burst:** wird von der Feststation periodisch auf dem BCH (Broadcast Channel) ausgestrahlt und dient sowohl zeitlich als auch im Frequenzbereich zur Synchronisation der MS mit der BTS, um mögliche Störungen benachbarter Frequenzen zu vermeiden. Wird der Frequency Correction Burst wiederholt ausgestrahlt, so spricht man vom FCCH (Frequency Correction Channel).
- **Dummy Burst:** wird, falls keine Daten vorliegen, von der BTS in einem freien Slot gesendet.
  Dieser Frequenzkanal entspricht dem, auf dem der BCCH ausgestrahlt wird, der es der MS erlaubt, Leistungsmessungen durchzuführen. Wie man aus dem Bild oben erkennen kann, besteht der DB im Inneren aus einer 26-Bit Trainings-Sequenz.
- **Access Burst:** dient der Verbindungsaufnahme einer MS mit einer BTS und wird für einen wahlfreien Vielfachzugriff auf dem RACH (Random Access Channel) verwendet. Dieser Burst ist kürzer als die anderen, weil er nicht voraussetzt, dass die MS voll synchron zur BTS ist.
  Um Kollisionen auf dem RACH durch nicht synchronisierte MSs zu verringern hat der Access Burst eine viel größere Guard Period als die übrigen Bursts (68,25 Bit gegen-

über 8,25 Bits),. Wodurch sich eine Schutzzeit von mindestens 200µs bei einem maximalen Zellenradius von 35 km ergibt. Die Trainingssequenz ist der BTS bekannt und ermöglicht ihr dadurch das Entdecken des Access Bursts. Die Datenbits enthalten ausschließlich Informationen der MS.

2.2 Logische Kanalstruktur

Die physikalischen Kanäle – Slots - werden, sobald sie für Sprach- oder Signalisierungsverbindungen, benützt werden als logische Kanäle bezeichnet. In der Regel entspricht ein physikalischer Kanal einem logischen Kanal, in Abhängigkeit von der notwendigen Übertragungskapazität ist es jedoch auch möglich mehrere logische Aktivitäten über einen physikalischen Kanal abzuwickeln oder aber mehrere physikalische Kanäle für die Aufgaben eines logischen Kanals zu benützen.
Auf der Frequenzebene erfolgt die Abbildung der logischen Kanäle auf physikalische durch die Radio Frequency Channels die in bestimmten geografischen Bereichen für den Informationsaustausch vorhanden sind.
(3) Auf der Zeitebene erfolgt die Abbildung von logischen auf physikalische Kanäle mit Hilfe immer wieder (zyklisch) durchlaufener Multiframe-Muster auf die sich die MS mittels des Synchronization Channel SCH synchronisiert. Die Multiframe-Struktur beginnt mit den TDMA-Rahmen, welche acht Zeitschlitze zur Übertragung der verschiedenen Bursts enthalten. Mehrere TDMA-Rahmen werden zu sog. Mehrfachrahmen (Multiframes) und diese wieder zu Superframes und weiter zu Hyperframes zusammengefasst.
Man unterscheidet zwei verschieden lange Mehrfachrahmen:

- 26er Multiframes für Traffic Channels
  In ihnen werden die Bursts der Verkehrskanäle (TCH) und der ihnen zugeordneten SACCHs und FACCHs übertragen.
  Die SACCHs werden im TDMA-Rahmen 12 bzw. 25 übertragen.
  Der FACCHs verwendet bei Bedarf Zeitschlitze des TCHs und kennzeichnet die entsprechenden Bursts durch Setzen des „stealing flags“.
- 51er Multiframes für Control Channels
  In ihnen werden die Bursts der restlichen Control Channels übertragen. Innerhalb eines 51er Multiframes können mehrere Kombinationen der zu übertragenden Signalisierungskanäle realisiert werden.

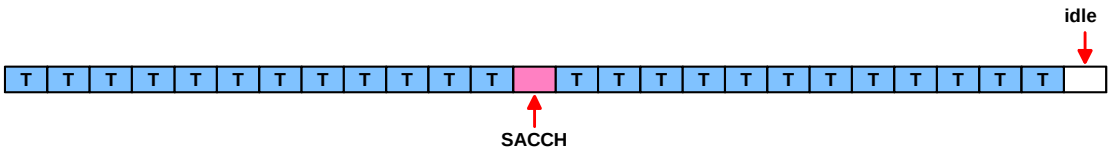


Bild 4 26er Mehrfachrahmens für full rate speech

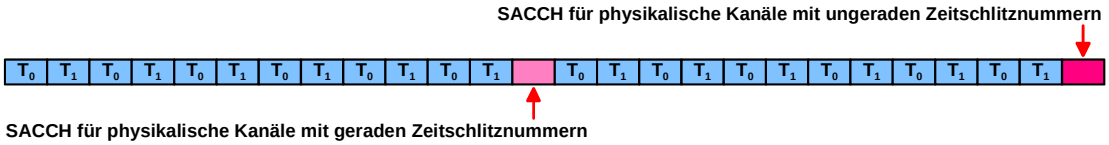


Bild 5 26er Mehrfachrahmens für half rate speech

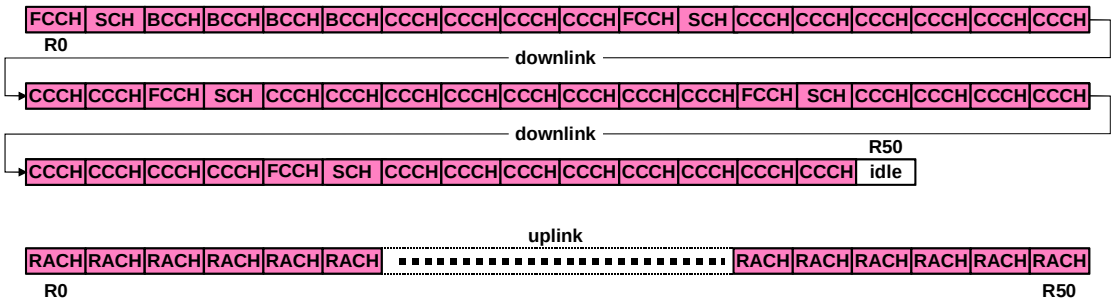


Bild 6 Mögliche Struktur eines 51er Mehrfachrahmens

51 der 26er Mehrfachrahmen und 26 der 51er Mehrfachrahmen werden zu einem Superrahmen (Superframe) zusammengefasst. 2048 Superrahmen ergeben einen Hyperrahmen (Hyperframe). Zur Übertragung eines solchen Hyperrahmens werden nahezu 3,5 Stunden gebraucht.

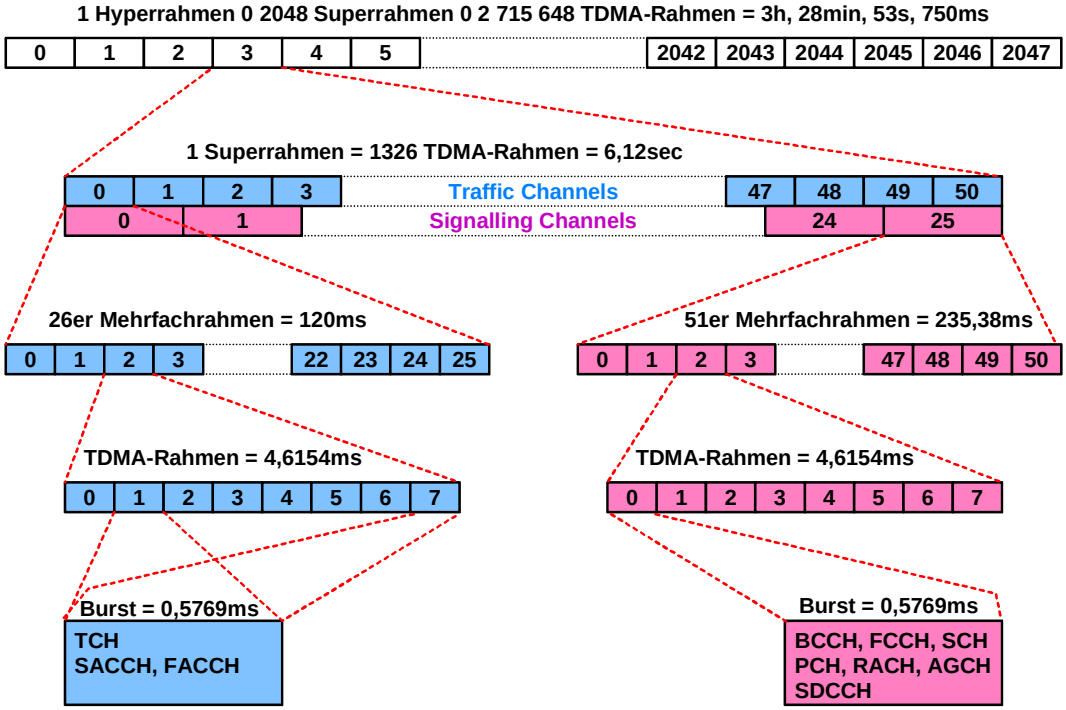


Bild 7 Hierarchie der Rahmenstrukturen

Bei logischen Kanälen kann man zwischen solchen für Nutzdatenaustausch – Traffic Channels – und solchen für den Austausch von Signalisierungsnachrichten unterscheiden.
In Slot 0 – Common Signalling Channel - sind, entsprechend den vielfältigen Anforderungen drei Gruppen von Signalisierungskanälen untergebracht, die ihrerseits wie folgt weiter unterteilt sind:

- BCH Broadcast Channels
  - o BCCH Broadcast Control Channel (Downlink)
  - o FCCH Frequency Correction Channel (Downlink)
  - o SCH Synchronisation Channel (Downlink)
- CCCH Common Control Channels (kann unterschiedlich kombiniert sein)
  - o PCH Paging Channel (Downlink)
  - o RACH Random Access Channel (Uplink)
  - o AGCH Access Grant Channel (Downlink)
- DCCH Dedicated Control Channels
  - o SDCCH Stand-Alone Dedicated Control Channel (up- und Downlink)

In den Slots 1 bis 7 sind untergebracht:

- TCH Traffic Channels (Up- und Downlink)
- SACCH Slow Associated Control Channels (up- und Downlink)
- FACCH Fast Associated Control Channels (up- und Downlink)

(4) Broadcast Channels, (BCH) Diese Bezeichnung ist ein Oberbegriff für Punkt-zu-Mehrpunkt-Verbindungen über welche im Simplex-Modus Nachrichten von der Feststation zur Mobilstation übertragen werden.

- **Broadcast Control Channel, (BCCH):** Über diesen Kanal werden Informationen über das Netz zur Mobilstationen übertragen. Dazu gehören z.B. Kennzeichnung des Netzes, Verfügbarkeit bestimmter Optionen wie Frequency Hopping, Voice Activity Detection sowie die von der Feststation und benachbarten Feststationen verwendeten Frequenzen.
- **Frequency Correction Channel (FCCH):** Über diesen Kanal wird der Frequency Correction Burst übertragen wodurch sich die MS auf die Frequenz der BTS synchronisieren kann.
- **Synchronisation Channel (SCH):** Über diesen Kanal werden Synchronisation Bursts zur Mobilstation übertragen damit sie sich auf den Hyperrahmen synchronisieren kann.

Common Control Channels, (CCCH) Diese Bezeichnung ist ein Oberbegriff für Steuerkanäle, über die die Verbindungsaufnahmen zwischen Netz und Mobilgerät abgewickelt werden. Zu den CCCH-Kanälen gehören:

- **Paging Channel (PCH):** Dieser Kanal existiert nur in Downlink-Richtung und wird zur selektiven Adressierung eines gerufenen Mobilgerätes bei einem Verbindungswunsch aus dem Netz (eingehender Ruf) aktiviert.
- **Random Access Channel (RACH):** Dieser Zugriffskanal kommt nur in Uplink-Richtung vor und ermöglicht der Mobilstation über ein S-ALOHA Zugriffsverfahren, bei der Feststation Kanalkapazität für einen Verbindungswunsch anzufordern.
- **Access Grant Channel (AGCH):** Auf diesem logischen Kanal antwortet die Feststation der Mobilstation auf eine über den RACH eingetroffene Nachricht. Über den AGCH, der nur in Downlink-Richtung existiert, wird der Mobilstation entsprechend dem vom Netzbetreiber gewählten Verbindungsaufbaumechanismus, ein SDCCH oder ein TCH zugewiesen.

Dedicated Control Channels, (DCCH) Diese Bezeichnung ist ein Oberbegriff für drei bidirektionale Punkt-zu-Punkt Steuerkanäle, über die mit unterschiedlichen Bitraten Signalisierungsnachrichten zur Verbindungssteuerung übertragen werden. Man kann zwischen folgenden DCCH-Kanälen unterscheiden:

- **Stand-Alone Dedicated Control Channel (SDCCH):** Dieser Kanal wird immer dann betrieben, wenn der Verkehrskanal nicht zugewiesen ist und wird der Mobilstation zugeordnet, solange nur Steuerinformation übertragen wird. Die vom SDCCH benötigte Kanalkapazität ist mit 782 bit/s geringer als die des TCH. Steuerinformation des SDCCH betrifft z. B. Registrierung, Authentifizierung, Aufenthalts-Koordinierung und Daten zur Verbindungseinrichtung.

Traffic Channel (TCH): Dieser Kanal wird zur Übertragung von Full-Rate- oder Half-Rate-Sprache oder zur Übertragung von Nutzdaten mit bis zu 14,4 kbit/s verwendet.

Slow Associated Dedicated Control Channel (SACCH): Dieser Kanal wird immer gemeinsam mit dem TCH zugeordnet. Über den SACCH werden mit einer Datenrate von 950 bit/s Systeminformationen vom Netz zur Mobilstation und Messdaten über Pegel- und Empfangsqualität von der MS an das Netz übertragen.

Achtung: der Slow Associated Control Channel ist nicht im Kanal 0 eines TDMA-Rahmens untergebracht, sondern im Rahmen 13 bzw. 26 eines 26er TDMA-Rahmens.

Fast Associated Dedicated Control Channel (FACCH): Dieser Kanal wird kurzfristig nur dann eingerichtet, wenn ein Verkehrskanal existiert und benutzt dabei dessen Zeitschlitze. Das bedeutet, dass der FACCH in einer Kanalkombinationsstruktur die Zeitschlitze belegt, die sonst für den TCH reserviert sind. Ein FACCH wird z. B. für einen bevorstehenden Handover eingerichtet, wobei die dafür benötigten Steuerdaten über den FACCH übertragen werden. Dieser Kanal erlaubt u. a. Bitraten von 4600 bit/s bzw. 9200 bit/s.

Achtung: der Fast Associated Control Channel ist nicht im Kanal 0 eines TDMA-Rahmens untergebracht, sondern benützt bei Bedarf den Zeitschlitz eines Traffic Channels.

3 Signalisierungsabläufe

In Mobilfunknetzen sind die Signalisierungsabläufe wesentlich komplexer als im Festnetz, da Mobilstationen nicht nur abgeschaltet sein, sondern sich auch im Netz frei bewegen können. Aus diesem Grund sind in Mobilnetzen nicht nur Prozeduren zum Verbindungsaufbau und –abbau erforderlich sondern z.B. auch solche zur Überprüfung der Netz-Zugangsberechtigung und der Bestimmung des Aufenthaltsortes.

3.1 Adressen und Kennungen

Struktur und Einsatz der im GSM verwendeten Adressen und Kennungen

MSISDN - Mobile Subscriber ISDN Number

Die MSISDN ist die Teilnehmerrufnummer, unter welcher der Mobilteilnehmer erreichbar ist. Sie entspricht dem Rufnummern-Schema der ITU-T-Empfehlung E.164 und besteht aus max.15 Ziffern.

CC (2/3)	NSN (13/12)		
CC (2/3)	NDC (3)	HLRID (2)	RN (max. 8)

- CC Landeskennzahl/Country Code, 2- oder 3-stellig
- NSN nationale Rufnummer/National Significant Number bestehend aus
  - NDC Bereichskennzahl/Network Destination Code, 3-stellig
  - HLRID HLR Identifier, 2-stellig
  - RN Teilnehmerrufnummer, max. 8-stellig

IMSI - International Mobile Subscriber Identity

(5) Die internationale Mobilfunk-Teilnehmerkennung ist eine netzinterne Kennung, die u.a. auf der SIM-Karte vermerkt ist und zur Identifizierung einer Mobilstation im Mobilnetz dient. Sie ist dem Teilnehmer nicht bekannt.

MCC (3)	MNC (2)	HLRID (2)	IN (max 8)

- MCC Mobilnetz-Landeskennzahl/Mobile Country Code, 3-stellig
- MNC Mobilnetz-Kennzahl/Mobile Network Code, 2-stellig, dient zur Unterscheidung der Mobilnetze innerhalb eines Landes
- HLRID HLR Identifier, 2-stellig
- IN Subscriber Identification Number, ist nicht mit der Teilnehmerrufnummer identisch, max. 8-stellig

TMSI - Temporary Mobile Subscriber Identity

Die TMSI ist eine aus 32 Bit bestehende temporäre Nummer, die zur Signalisierung auf der U_m-Funkschnittstelle dient und einen Teilnehmer ausschließlich im aktuellen VLR identifiziert. Sie wird vom VLR vergeben und hat nur begrenzte Gültigkeitsdauer. Die TMSI-Nummer wird im VLR und auf der SIM-Karte gespeichert.

32 Bit

MSRN - Mobile Station Roaming Number

Die MSRN-Nummer wird benötigt um eine Nutzkanalverbindung zwischen der rufenden MSC und der gerufenen MSC aufzubauen. Sie wird im Rahmen der Interrogation auf Anforderung der rufenden MSC vom HLR bzw. VLR_B zugewiesen

VCC (3)	VNDC (3)	VMSCID (2)	VSN (7)

- VCC Landeskennzahl des besuchten GSM-Netzes/Visitor Country Code,
- VNDC Visitor National Destination Code, entspricht der Bereichskennzahl
- VMSCID Visited Mobile Switching Center kennzeichnet das aktuelle MSC
- VSN Visitor Subscriber Number ergänzt die Stellenzahl der MSRN entsprechend ITU-T E.164, entspricht jedoch keiner Teilnehmerrufnummer sondern der Vermittlungsstellen-Kennzahl.

LAI - Location Area Identity

(6) Die LAI gibt jene Zellengruppe an, in der sich der Mobilteilnehmer aufhält, die Zelle selbst ist nicht bekannt. Mit Hilfe der LAI kann der Mobilteilnehmer beim Aussenden eines Paging-Rufes (Passivgespräch) gefunden werden.

MCC (3)	MNC (2)	LAC (2Byte)

- MCC Mobilnetz-Landeskennzahl/Mobile Country Code, 3-stellig
- MNC Mobilnetz-Kennzahl/Mobile Network Code, 2-stellig, dient zur Unterscheidung der Mobilnetze innerhalb eines Landes
- LAC Location Area Code, kennzeichnet eine Gruppe von Zellen innerhalb eines Mobilnetzes (= 2 Byte)

VLR-ID – Visitor Location Register Number (**ZGV7-Signalling-Point)**
Sie dient zur Lokalisierung aktiver (eingeloggter) GSM-Teilnehmer und entspricht der Adresse eines ZGV7-Signalling-Points.

CC (2/3)	NDC (2)	VMSCID (2)

- CC – Country Code
- NDC – Network Destination Code
- MSCID – Mobile Services Switching Center Nr, kennzeichnet das besuchte MSC.

HLR-ID – Home Location Register Number (**ZGV7-Signalling-Point)**
Sie dient zur Kennzeichnung des HLR in welchem ein Mobilteilnehmer registriert ist. Sie ist Bestandteil der MSISDN und besteht aus:

CC (2/3)	NDC (3)	HLRID (2)

- CC Landeskennzahl/Country Code, 2- oder 3-stellig
- NSN nationaler Rufnummer/National Significant Number bestehend aus
  - NDC Bereichskennzahl/Network Destination Code, 3-stellig
  - HLRID HLR Identifier, 2-stellig

GT – Global Title (ZGV7-Signalling-Point)
Unter Global Title versteht man eine weltweit eindeutige (Signalisierungsadresse) Adresse, die ein weltweites Routing von Zeichengabeinformationen ermöglicht.

- Der MGT wird durch eine Global Title Translation (GTT) aus der Teilnehmerrufnummer errechnet.
- Der GTT befreit die ursprünglichen Signalisierungspunkte von der Last, jeden potentiellen Bestimmungsort kennen zu müssen, zu dem sie eventuell eine Nachricht weiterleiten müssen.

Beim Durchführen einer GTT, braucht der STP den genauen Bestimmungsort der Nachricht nicht zu kennen, da auch eine vorläufige GTT vorgenommen werden kann, bei der Tabellen verwendet werden um einen anderen STP entlang der Route zum Bestimmungsort zu finden. Dieser STP kann eine endgültige GTT durchführen, um die Meldung zu ihrem endgültigen Bestimmungsort weiterzuleiten.
Die vorläufige GTT (Global Title Translation) minimiert die Notwendigkeit der STPs umfangreiche Informationen über Netzknoten zu pflegen, die weit entfernt von ihnen, z.B.: in anderen Staaten eingesetzt werden.

IMEI – International Mobile Equipment Identity
Die IMEI-Nummer entspricht der Geräteseriennummer des Mobile Equipments (Handy ohne SIM-Karte) und besteht aus vier Kennfeldern, die insgesamt 15 Zeichen ergeben:

TAC (6)	FAC (2)	SNR (6)	Reserve

- TAC - Type Approval Code (6 Zeichen) – Hersteller und Gerätetyp
- FAC - Final Assembly Code (2 Zeichen) - Endmontageland
- SNR - Serial Number (6 Zeichen)

Ursprünglich bestand die Idee alle IMEI-Nummern in einer eigenen Datenbank, dem EIR - Equipment Identity Register, zu speichern, wobei das EIR aus drei Listen besteht: Die weiße, die graue und die schwarze Liste. Es gibt aber so gut wie keinen GSM-Netzbetreiber der das EIR in seiner Netzarchitektur realisiert hat, da die IMEI-Nummern sehr leicht manipulierbar sind und somit der Sinn des EIR verloren geht.

3.2 Authentifizierung

Unter der Bezeichnung „Authentifizierung“ (engl.: Authentication) werden die Vorgänge zur Überprüfung der Zugangsberechtigung und der Verschlüsselung der Funkschnittstelle verstanden.

Aufgaben der Authentifizierung und der daran beteiligten Einrichtungen
Eine Authentication wird durch das VLR durchgeführt und hat folgende Aufgaben:

- Überprüfung der Zugangsberechtigung einer SIM-Karte zum Netz und
- Bereitstellung eines Verschlüsselungscodes für den zu benützenden Funkkanal

An einer Authentication sind folgende Einrichtungen beteiligt:

- Subscriber Identity Module SIM im Mobile Equipment,
- Authentication Center – AC,
- Home Location Register HLR und
- Visitor Location Register VLR

Subscriber Identity Module - SIM

(7) auf ihr sind folgende Daten gespeichert:

- Permanente Daten
  - IMSI (International Mobile Subscriber Identity),
  - Ki (individuelle Teilnehmerschlüssel),
  - Algorithmen A_3, A_5 und A_8 (netzbetreiberindividuell) und
  - PUK (Personal unblocking Key)
- Temporäre Daten
  - LAI (Local Area Identity) und
  - TMSI (Temporary Mobile Subscriber Identity),
- Semipermanente Daten
  - PIN Code (Personal Identification Number)

Authentication Center – AC

(8) Aufgabe des Authentifizierungszentrums (Authentication Center – AC) ist die Erzeugung teilnehmerindividueller Parametersätze, sog. Triples, die über das HLR an die VLRs zur Authentifizierung von Teilnehmern beim Aufbau einer Aktiv- oder Passivverbindung so wie für eine Location Registration weitergegeben.
Die Parametersätze bestehen aus :

- RAND (random number): Zufallszahl
- SRES (signed response): Referenzwert für die Authentication
- Kc (cipher key): Code zur Verwendung für die Funkkanalverschlüsselung

Das AC generiert bei jeder Anforderung immer mehrere – in der Regel drei – Triples pro Mobilteilnehmer und übergibt sie auf Anforderung über das HLR an das VLR. Bei einer weiteren Authentication verwendet das VLR das nächste Triple. Sind keine Triples mehr vorhanden, wird vom HLR ein neuer Satz angefordert.
Das Erzeugen der Triples erfolgt, wie Bild 8 zeigt, im AC aufgrund

- einer Anforderung durch das VLR
- einer im AC erzeugten Zufallszahl RAND.
- teilnehmerindividueller Daten die auf der SIM Karte und im HLR gespeichert sind und auf Grund der Update Request – Nachricht dem AC gemeldet werden,
- den auf SIM Karte und im AC gespeicherten netzspezifischen Algorithmen A3 und A8 und

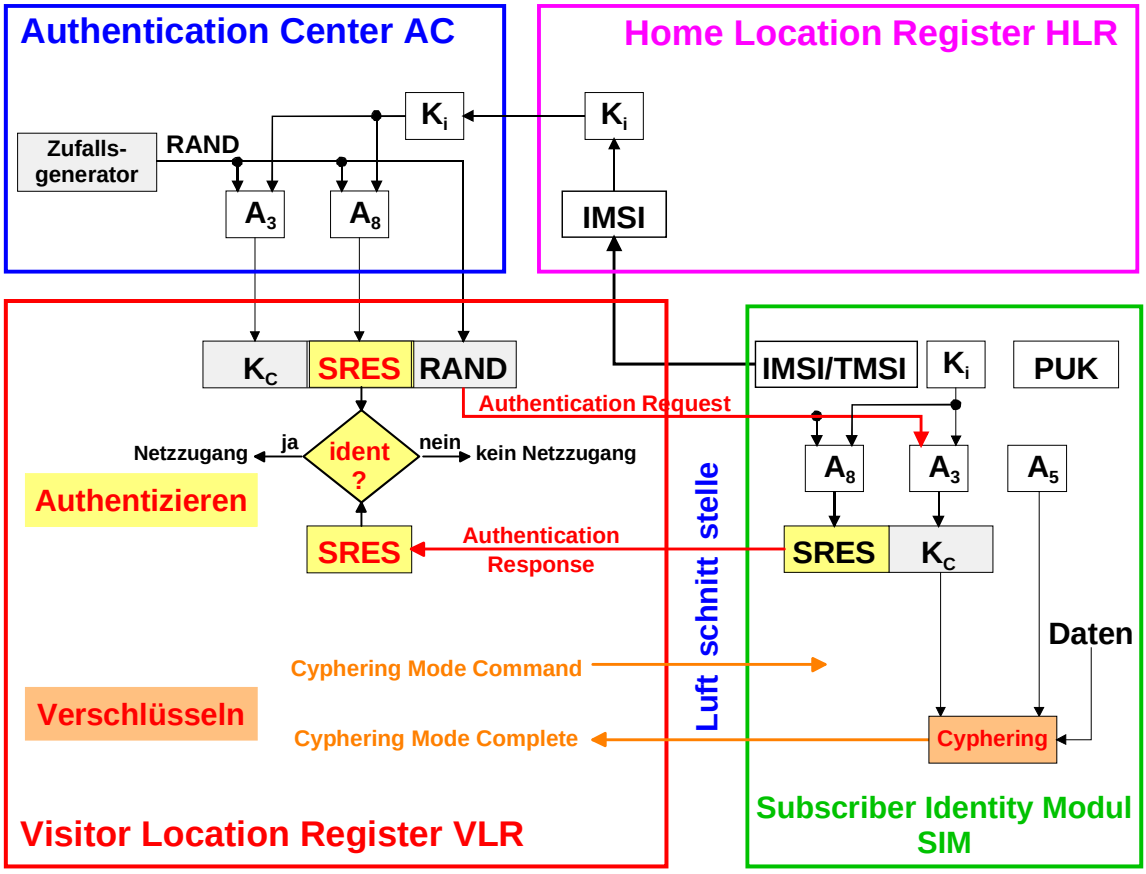


Bild 8 Erzeugen der Triples im AC und der MS

Home Location Register - HLR

(9) Das HLR dient zur Speicherung Daten aller in einem GSM-Netz registrierten Teilnehmer. Logisch ist nur ein Home Location Register je Netz erforderlich. Aus organisatorischen und strukturellen Gründen sind jedoch immer mehrere HLR vorhanden. Die ersten beiden Ziffern der MSISDN geben den HLR-Bereich an.
Im Heimatregister HLR werden z.B.: folgende Teilnehmerdaten gespeichert:

- International Mobile Subscriber Identity (IMSI)
- internationale GSM Rufnummer des Teilnehmers (MSISDN = Mobile Subscriber ISDN Number oder Rufnummer des Teilnehmers im öffentlichen Netz)
- Parameter A_3, A_5 und A_8 zur Authentifizierung und Verschlüsselung
- zugelassene Zusatzdienste
- temporäre Teilnehmerdaten, wie z B.

- Adresse des VLR (VLR-ID) bzw. die MSRN des MSC in dessen Aufenthaltsbereich sich die MS im Augenblick befindet
- oder im Falle einer Anrufweiterleitung die Telefonnummer, zu der die Anrufe weitergeleitet werden.

Visitor Location Register – VLR

(10) Das Besucherregister VLR dient zur Speicherung der Daten aller sich im Bereich des zugehörigen MSC aufhaltenden Mobilstationen. Die permanenten Teilnehmer-Daten sind dieselben wie im HLR, die temporären unterscheiden sich jedoch. So enthält das VLR zusätzlich die

- TMSI, Temporary Mobile Subscriber Identity, eine zeitlich begrenzte Identität der Mobilstation um die permanente IMSI nicht über die Luftschnittstelle senden zu müssen, sowie die
- LAI, Local Area Identity, identifiziert den aktuellen Aufenthaltsbereich der Mobilstation. Sie ist die genaueste Information über den aktuellen Aufenthaltsort des Mobilteilnehmers im VLR – die Zelle selbst ist nicht bekannt.

Auslösen einer Authentifizierung

Eine Authentication wird bei folgenden Vorgängen durch einen Service Request an das VLR eingeleitet:

- Einbuchen (IMSI Attach)
  das ME sendet über die Funkschnittstelle die IMSI bzw. TMSI an das VLR.
- Location Update
  das ME sendet über die Funkschnittstelle einen Update Request an das VLR sobald sich die auf der SIM gespeicherte LAI von der über die Luftschnittstelle empfangenen unterscheidet.
- Aktivgespräch
  das ME fordert das Connection Management Service des Systems beim BSC und damit beim VLR an
- Passivgespräch
  das ME meldet sich mit einer Paging Response beim BSC und damit beim VLR

Phasen einer Authentifizierung

- VLR erhält einen Service Request und leitet die Authentifizierung ein
- bei einer Location Registration fordert das VLR eine Garnitur Triples an, bei allen anderen Vorgängen wird eine für diesen Teilnehmer reserviertes Triple verwendet
- Prüfen der Netzzugangsberechtigung
- Anfordern der Teilnehmerdaten vom HLR (z.B.: MSISDN, Diensteberechtigungen, …..)
- Funkkanalverschlüsselung durchführen

Ablauf der Authentifizierung

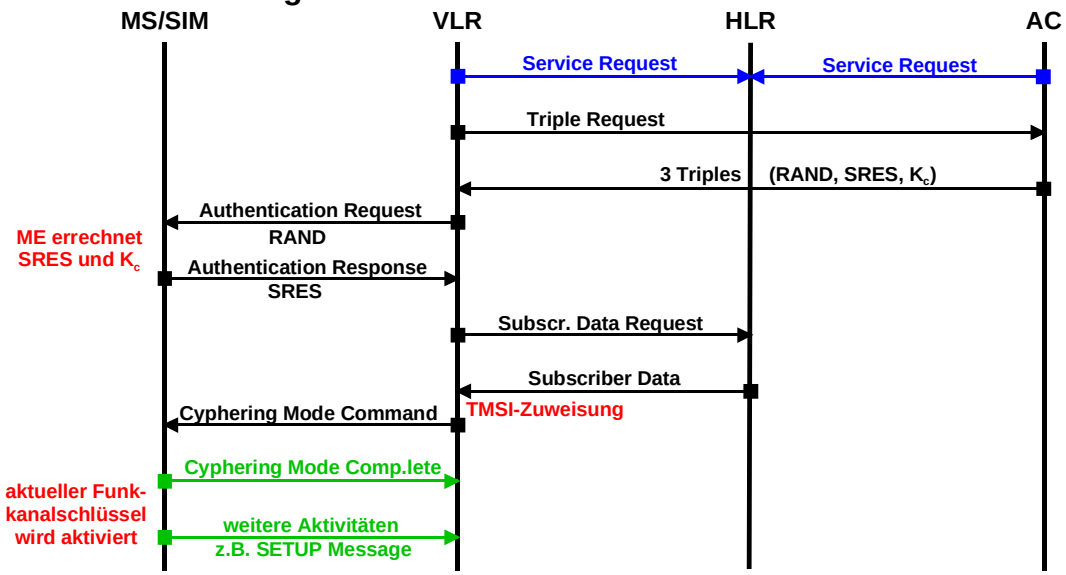


Bild 9 Ablauf einer Authentifizierung

(11) Je nach Aktivität des Teilnehmers sind entweder die Überprüfung der Zugangsberechtigung – ME einschalten – oder die Bereitstellung eines Funkkanalschlüssels – z.B. bei einer Gesprächsverbindung – die gewünschten Ergebnisse.

- Eine Authentication wird über einen von der MS oder dem HLR kommenden Service Request[2] an das VLR ausgelöst.
- Sind für diese MS im VLR keine Triples vorhanden, fordert das VLR mit einem Triple Request vom AC die Erstellung teilnehmerindividueller Triples und veranlasst die Übertragung des teilnehmerindividuellen Codes Ki vom HLR in das AC
- Nach Erhalt dreier Triple Sets verwendet das VLR eines davon für die Authentifizierung und sendet dessen RAND im Authentication Request über die Luftschnittstelle zur SIM, Diese errechnet mittels der permanent gespeicherten Daten Ki, A3 und A8 sowohl die SRES als auch den Cypher Key.
- Die von der SIM errechnete SRES wird in der Authentication Response über die Luftschnittstelle zum VLR übertragen und von diesem mit jener des AC verglichen. Bei Übereinstimmung der beiden ist die SIM berechtigt das Netz zu benützen.
- Nach erfolgreicher Authentication fordert das VLR mit einem Subscriber Data Request vom HLR die Daten dieses Mobilteilnehmers an und übermittelt dem HLR gleichzeitig entweder seine VLR-ID[3] oder die MSRN so wie die dem Teilnehmer temporär zugeordnete Temporary Mobile Subscriber Identity[4] (TMSI).
- Das HLR speichert sowohl VLR-Nummer/MSRN und TMSI ab und sendet die angeforderten Teilnehmerdaten an das VLR.
- Diese wird mit dem Verschlüsselungsbefehl zur MS gesendet und dort zusammen mit der neuen LAI auf der SIM-Karte abgespeichert.
- Nach Abschluss dieser Signalisierungsaktivitäten ist die MS im Netz eingebucht und der Teilnehmer kann seine GSM- Dienste nutzen.

[2] bei einem Wechsel des Aufenthaltsbereiches z.B. fordert die SIM dessen Aktualisierung beim VLR an wobei sie die TMSI über die Luftschnittstelle zum VLR sendet

[3] Die VLR-ID ist die internationale Signalisierungsadresse des VLR. Sie kennzeichnet nach einem Location Update das aktuelle VLR des Mobilteilnehmers im HLR und wird vor allem dann benutzt, wenn der Mobilteilnehmer angerufen wird, d.h. für einen Mobile Terminated Call (MTC)

[4] Die Temporary Mobile Subscriber Identity (TMSI) ist die Adresse der Teilnehmerdaten im VLR und ermöglicht einen schnelleren Zugriff auf diese Daten. Das ist vor allem bei einem Mobile Terminated Call (MTC) wichtig.

3.3 Location Management (Verwalten der Aufenthaltsinformation)

(12) Dem Location Management werden folgende Aufgaben zugeordnet:

- Ein- und Ausbuchen der MS (IMSI –Attach und IMSI-Detach)
  Beim Abschalten der MS wird ein Flag (Detach Flag) im VLR gesetzt. das z.B. für ein Weiterleiten ankommender Verbindungswünsche bei Abwesenheit des mobilen Benutzers verwendet werden kann. Beim Einbuchen oder durch eine beliebige andere Aktivität des mobilen Benutzers wird dieses Flag wieder zurückgesetzt.
- periodische Aktualisierung des Aufenthaltsortes
  Das Netz kann eine personalisierte MS auffordern, sich innerhalb einer vorgegebenen Registrierungsperiode (BCCH-Systeminformation, Intervall 6 min...24 h) beim Netz zu melden (Periodic Registration), sofern sie in dieser Zeitspanne keine anderweitige Signalisierungsaktivität getätigt hat.
  Bei jeder Aktivität mit dem Netz wird die Überwachungszeit für die Registrierungsperiode in der MS zurückgesetzt. Die periodische Registrierung kann zur Pflege der temporären Daten im VLR und HLR benutzt werden.
- Aktualisierung des Aufenthaltsortes im verbindungslosen Zustand (siehe Location Update)
  Die MS führt im IDLE_MODE fortlaufend die Zellauswahl durch. Sobald sie dabei in einen neuen Aufenthaltsbereich wechselt, aktualisiert sie mit einer Registrierungsprozedur die entsprechende Aufenthaltsinformation im Netz. Bei der Registrierung der Aufenthaltsinformation werden zwei Fälle unterschieden
  - Die MS kann in einen neuen Aufenthaltsbereich wechseln, der zum selben VLR-Bereich gehört (Intra-VLR Location-Updating). Dann ist nur eine Aktualisierung der Aufenthaltsinformation im VLR erforderlich.
  - Wechselt die MS gleichzeitig in einen neuen VLR-Bereich (Inter-VLR Location-Updating), so ist gleichzeitig eine Aktualisierung der Aufenthaltsinformation in den beteiligten VLRs und im HLR erforderlich.
- Aktualisierung des Aufenthaltsortes während einer bestehenden Verbindung (siehe Handover)

3.3.1 Location Update

(13) Wie oben angeführt erfolgt ein Location Update wenn das Handy eingeschaltet ist aber keine Nachrichtenverbindung besteht. Man unterscheidet in diesem Fall zwischen

- der Variante „Location Registration“ und
- „Location Update“

Der Vorgang der Location Registration geschieht beim erstmaligen Einbuchen in ein Mobilfunknetz bzw. beim Einschalten des Handys, falls dieses schon länger nicht mehr eingeschaltet war (mehrere Tage). Entscheiden für diese Prozedur ist, dass bei längerem Fernbleiben vom Mobilfunknetz die Daten aus dem VLR ausgetragen werden und im HLR vorübergehend abgelegt werden. Es existieren also noch keinerlei Daten im VLR, die für die Diensterbringung im zuständigen geographischen Bereich notwendig sind. Sollten das Fernbleiben so kurz gewesen sein, dass die Daten noch nicht ausgetragen worden sind, so wir die etwas verkürzte Prozedur des "Location Update" verwendet.

Bei der Location Registration schickt die MS ihre IMSI-Nummer und die LAI ihrer Aufenthaltszelle an das MSC, bzw. VLR, um den Teilnehmer im VLR zu registrieren. Hier muss die IMSI-Nummer verwendet werden, da zurzeit keine gültige TMSI-Nummer vorhanden ist - diese wurde ja aus dem VLR ausgetragen. Für eine korrekte Registrierung muss der Teilnehmer authentifiziert werden, wofür über das HLR vom AUC (AUtentication Center) diverse Sicherheitsparameter (Kc, RAND, SRES) angefordert werden und anschließend im VLR abgespeichert werden. War die Authentifizierung erfolgreich, so wird dem Teilnehmer eine neue MSRN zugewiesen, die zusammen mit der LAI im HLR gespeichert werden, und eine neue TMSI reserviert. Ebenso erfolgt die Prozedur für die Nutzdatenverschlüsselung und sobald diese erfolgreich war, wird dem Teilnehmer die TMSI verschlüsselt geschickt, womit auch die erfolgreiche "Location Registration" im Mobilfunknetz bestätigt wird. Letztlich wird auch noch von der MS der korrekte Empfang der TMSI bestätigt.
Die Location Update Prozedur unterscheidet sich von der Location Registration Prozedur dadurch, dass der MS bereits eine TMSI zugewiesen wurde, die ebenso im VLR noch gültig abgelegt ist. Diese TMSI ist nur mit einer LAI verknüpft eindeutig, sodass beide im SIM zusammen mit der TMSI gespeichert werden müssen. Im Rahmen der Aufenthaltsaktualisierung wird der MS eine neue TMSI zugewiesen. Hat sich im Zuge des Location Updates der Zuständigkeitsbereich des VLR geändert, so muss das neue VLR die Identifikations- und Sicherheitsdaten der MS vom alten VLR anfordern und lokal speichern.

Auslösen eines Location Update
Ein Location Update wird ausgelöst, wenn das „Handy“ eingeschaltet ist und dabei ohne bestehender Gesprächsverbindung seinen Aufenthaltsort wechselt. Damit ein möglichst geringer Signalisierungsaufwand für diese Aktivität erforderlich ist wird durch das Zusammenfassen mehrerer Zellen zu einer Zellengruppe eine gröbere Netzstruktur geschaffen und dadurch die Anzahl der Vorgänge reduziert. Der Update-Vorgang wird ausgelöst sobald die auf der SIM-Karte gespeicherte LAI (Location Area Identity = Zellengruppe) von der über den aktuellen Broadcast Control Channel BCCH) empfangenen LAI abweicht.

Aufgaben des Location Update
Die Aufgabe des Location Updates ist die Aktualisierung der Aufenthaltsdaten einer MS im VLR bzw. HLR um die MS im Falle einer Passivverbindung finden und rufen zu können.
Es werden zwei Fälle unterschieden:
Wechsel in einen Aufenthaltsbereich der zum selben VLR-Bereich gehört und
Wechsel in einen Aufenthaltsbereich (LAI) der zu einem anderen VLR-Bereich gehört

Phasen eines Location Update Ablaufes
1. Erkennen und Anfordern eines location update
2. Authentifizieren der MS
3. Eintragen der „neuen“ MSRN bzw. VLRid ins HLR
4. Starten der Verschlüsselung auf der Luftschnittstelle
5. Generieren einer neuen TMSI und übertragen zur MS
6. Anfordern neuer Triples wenn beim location update das letzte verbraucht wurde

Ablauf eines Location Update

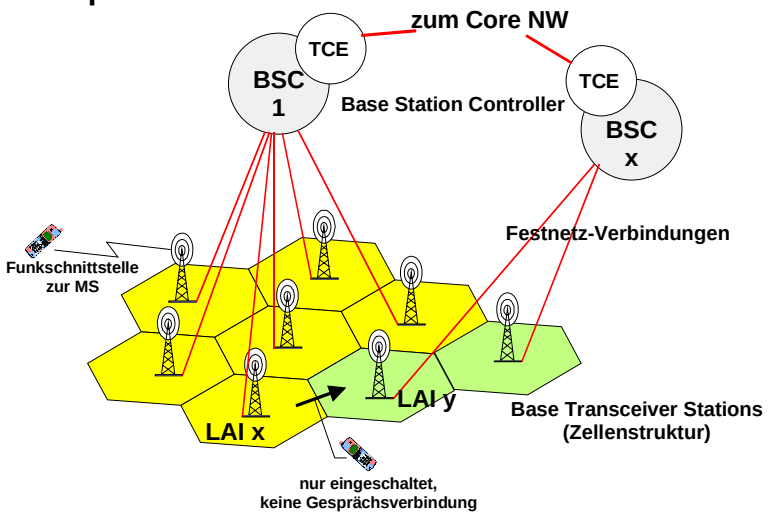


Bild 10 Location Update - beteiligte Netzkomponenten

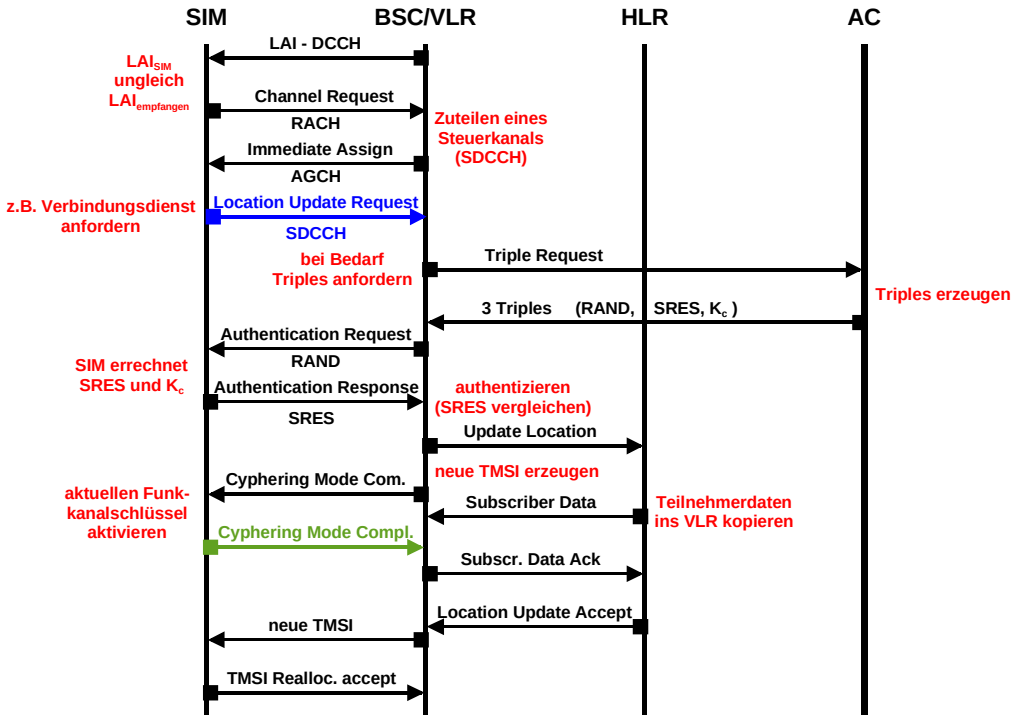


Bild 11 Location Update – gleicher VLR-Bereich

Jede eingeschaltete MS empfängt laufend über den aktuellen Broadcast Control Channel BCCH) die aktuelle LAI.
Besteht keine Gesprächsverbindung und weicht die auf der SIM-Karte gespeicherte LAI (Location Area Identity = Zellengruppe) von der über den aktuellen Broadcast Control Channel (BCCH) empfangenen ab, korrigiert die MS zunächst die LAI auf der SIM-Karte und fordert in Folge über den allgemein zugänglichen Common Control Channel (CCCH), die Zuordnung eines Dedicated Control Channels (DCCH) zur Abwicklung des Location Update vom BSC an.
Der Base Station Controller (BSC) führt die entsprechende Kanalzuweisung durch und meldet sie über den DCCH an die MS.
Über den DCCH sendet die MS eine Location Update Request – Nachricht an das zuständige VLR und teilt diesem ihre International Mobile Subscriber Identity (IMSI) so wie die „neue“ LAI mit.

Das VLR führt mit einem für diese IMSI im VLR gespeicherten Triple die Authentifizierung der MS durch und überträgt die für dieses VLR /MSC gültige VLRid/MSRN ins HLR damit der Teilnehmer bei einer Passivverbindung gesucht werden kann.
Anschließend ermittelt das VLR für diese MS eine neue TMSI, kopiert die Teilnehmerdaten vom HLR ins VLR (Aktivverbindung) und startet die Verschlüsselung auf der Funkschnittstelle.
Über die nun verschlüsselte Funkschnittstelle wird die „neue“ TMSI zu MS übertragen und auf der SIM-Karte gespeichert.
Quittungsmeldungen von der MS zum VLR schließen den Update-Prozess ab.
Sind für diese IMSI keine Triples mehr im VLR gespeichert, fordert das VLR einen neuen Satz Triples bei Authentication Center an.

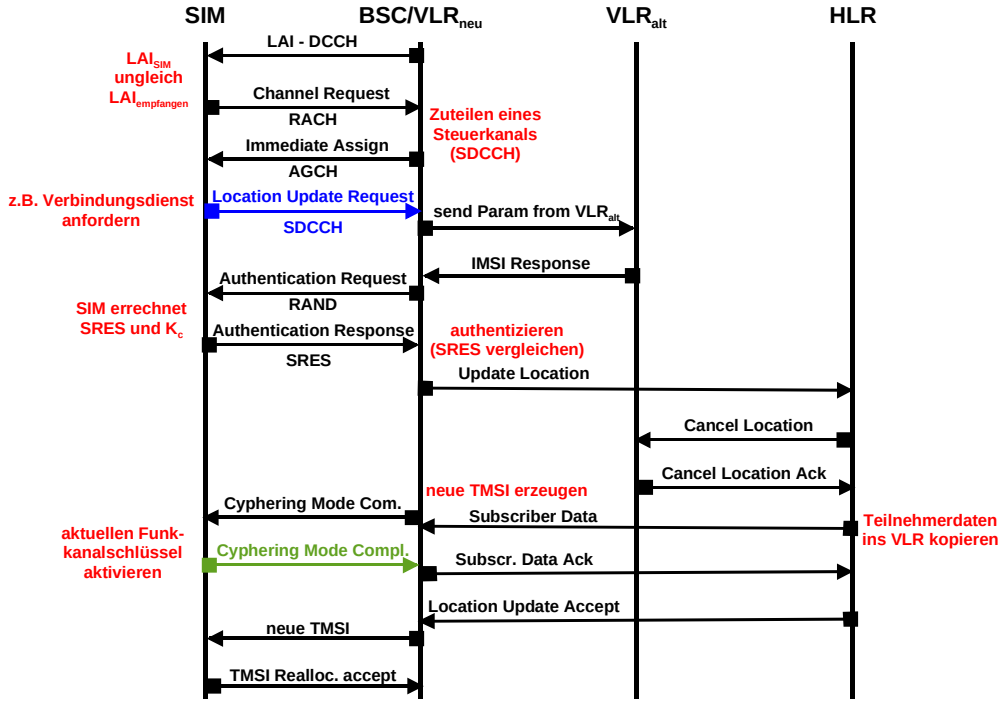


Bild 12 Location Update – unterschiedlicher VLR-Bereich

3.3.2 Handover

Unterschied zwischen Location Update und Handover

Location Update - LAI-Wechsel	Handover - Zellenwechsel
• ME ist eingeschaltet, d.h. im Netz eingeloggt. • Es besteht **keine** Nachrichtenverbindung	• ME ist eingeschaltet, d.h. im Netz eingeloggt. • Es besteht **eine** Nachrichtenverbindung
• ME vergleicht die auf der SIM gespeicherte LAI mit der auf dem „besten“ Kanal empfangenen	• ME misst die Empfangspegel der umliegender BTSs und meldet diese an den BSC
• bei Unterschied erfolgt ein Update Request des ME an das System	• bietet eine andere Zelle bessere Empfangsbedingungen als die aktuelle und ist in der neuen Zelle ein Speech Channel verfügbar, wird vom BSC der Handover durchgeführt

Tabelle 1 Unterschied zwischen Location Update und Handover

Aufgabe des Handover

(14) Ein Handover erfolgt während einer Gesprächsverbindung und ist erforderlich um den Abbruch dieser Verbindung zu verhindern. Bei einem Handover übernimmt die BTS der neuen Zelle die Funkversorgung der MS ohne Unterbrechung der Verbindung. Ein Handover wird vom Base Station Controller ausgelöst sobald dieser erkennen kann, dass der Empfangspegel einer anderen BTS besser ist als jener der aktuellen. Die Empfangspegel der aktuellen Zelle und der angrenzenden werden dem BSC über den Common Signalling Channel von der MS gemeldet.

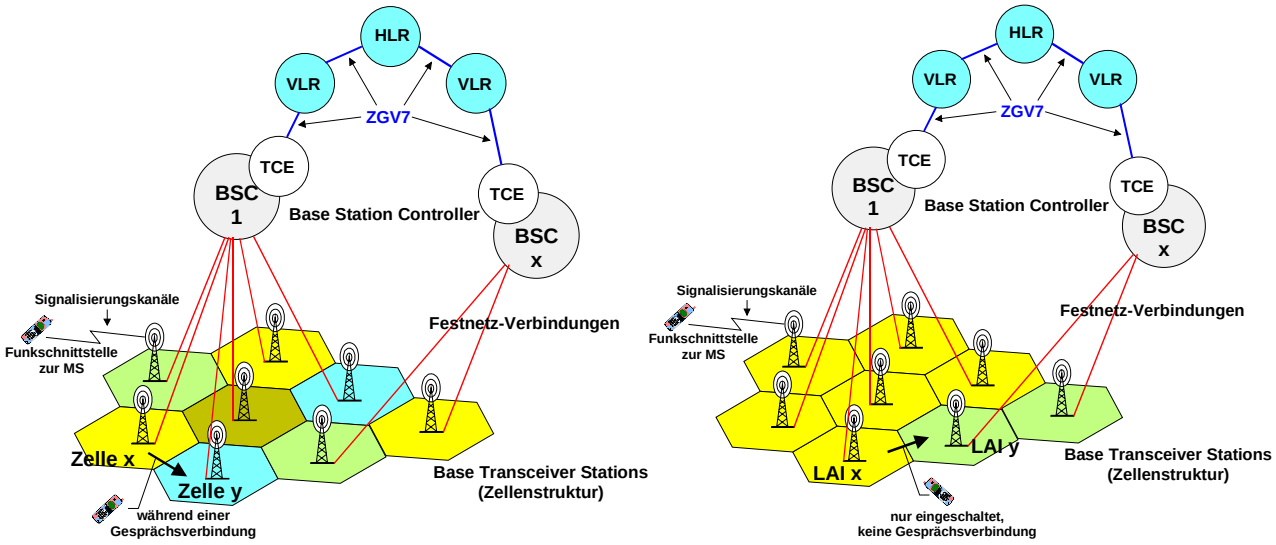


Bild 13 Handover – beteiligte Netzkomponenten

Handover-Varianten

(15) Es gibt vier Varianten von Handover:

- Intra-BTS Handover: (auch als Intracell-Handover bezeichnet) wird nicht beim Wechsel einer Zelle angewandt, sondern dann, wenn Störungen auf einem bestimmten physikalischen Kanal ein Umschalten zu einem anderen notwendig machen oder bei Einsatz des Frequency-Hopping-Verfahrens.
- Inter-BSC Handover: (auch als Intercell-Handover bezeichnet) wird zwischen den BTSs eines BSC durchgeführt
- Intra-MSC Handover: wird zwischen den BSCs einer MSC durchgeführt
- Inter-MSC Handover: wird zwischen zwei MSC durchgeführt

Handover-Schritte

Ein Handover besteht grundsätzlich aus vier Schritten:

- Schritt 1: die BSC entscheidet, dass ein Handover notwendig ist.
- Schritt 2: zur bestehenden Verbindung wird eine zweite parallel aufgebaut.
- Schritt 3: die MS schaltet zur neuen Verbindung um.
- Schritt 4: die ursprüngliche Verbindung wird ausgelöst.

Ablauf eines Intra-MSC-Handover

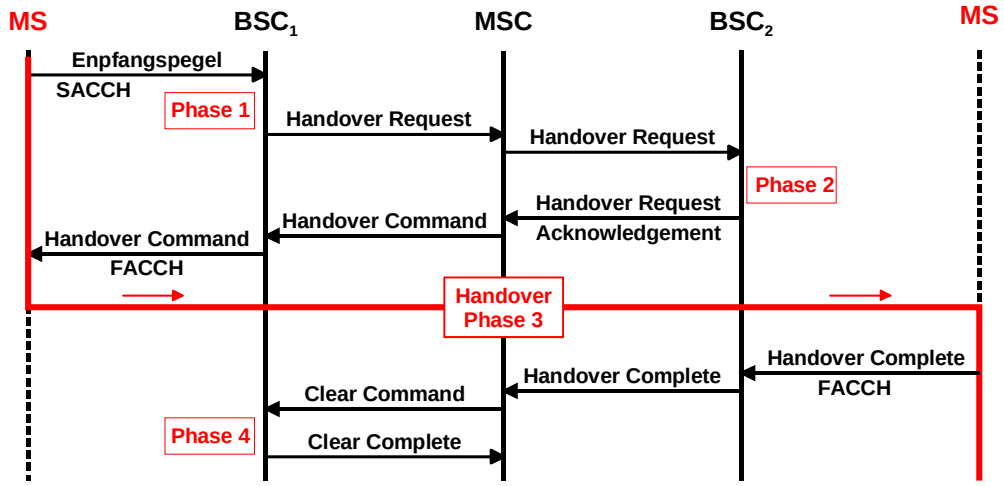


Bild 14 Ablauf eines Intra-MSC Handover

(16) Während einer bestehenden Verbindung misst die MS permanent den Empfangspegel und die Empfangsqualität der eigenen Zelle und die Empfangspegel der umliegenden Zellen. Die Resultate werden der BSC übermittelt, die einen Handover anstößt, wenn eine andere Zelle eine bessere Übertragungsqualität bietet.
Ein Mobilteilnehmer führt ein Gespräch in der Zelle A und fährt in die Zelle B. Die BSC erkennt, dass ein MSC-gesteuerter Handover erforderlich ist und meldet dies der MSC1.
Die MSC1 fordert von der MSC2 eine Handover Number (HON) und informiert die MSC2 über die Zelle B.
Die MSC2 fordert vom VLR eine HON an und von der BSC die Bereitstellung von Funkkanälen. Die Funkkanaldaten und die HON werden zur MSC1 zurückgesendet.
Die Handover Number (HON) wird nur beim Inter-MSC Handover benutzt- Sie dient dem MSC1 zum Aufbau der Nutzkanalverbindung zum MSC2. Die Struktur der HON entspricht der einer MSRN (CC, NDC und individueller Nummer) und wird ebenfalls vom ”neuen" VLR bereitgestellt.
Das MSC1 baut mit der HON die Nutzkanalverbindung zur MSC2 auf. Die Verbindung wird bis zur BTS komplettiert. MSC1 informiert jetzt die MS über den neuen Funkkanal und fordert sie zum Umschalten auf.
Die Verbindung zur alten BTS wird ausgelöst.

Ablauf eines Intracell Handovers

Ein Intracell-Handover (auch als Intra-BTS-Handover bekannt) wird dann durchgeführt, falls der Teilnehmer die Zelle nicht wechselt und die Kommunikationsqualität sich dermaßen verschlechtert hat, dass auf einen anderen Frequenzkanal oder auch Zeitschlitz in der Zelle umgeschaltet werden muss.
Das Intra-BTS-Handover wird vom BSC durchgeführt. Als Entscheidungskriterium für die Durchführung dieses Handovers dienen zwei Messwerte:

- der RXQUAL-Wert und
- der RXLEV-Wert.

Der RXQUAL-Wert ist das Maß für die Bitfehlerrate bei der Übertragung auf der Funkschnittstelle, und wird sowohl von BTS als auch MS gemessen. Die Bitfehlerrate lässt sich mit Hilfe der Trainingssequenz der Übertragungsbursts eruieren. Ist der RXQUAL-Wert bei der Funkübertragung schlecht, obwohl der RXLEV-Wert gute Werte aufweist, so kann auf Interferenzstörungen geschlossen werden.

Der RXLEV-Wert ist der Messwert des Empfangpegels auf der Funkschnittstelle und wird sowohl von BTS als auch MS gemessen

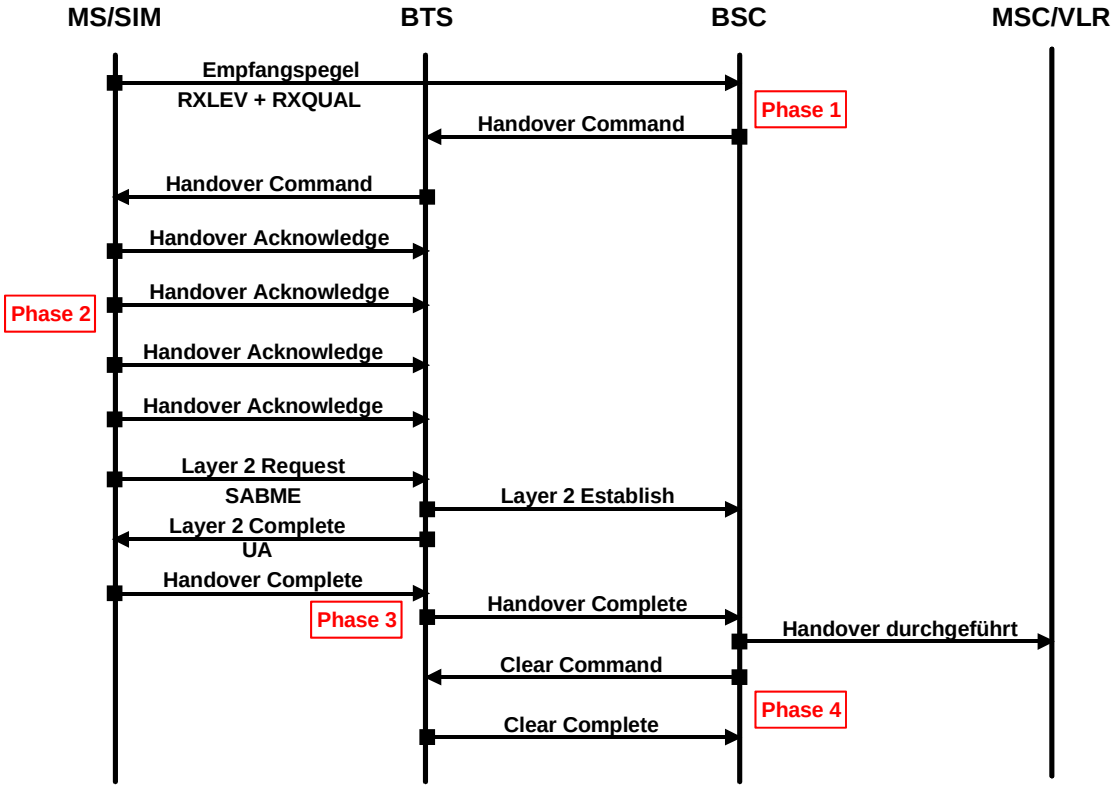


Bild 15 Ablauf eines Intracell Handover

- der BSC entscheidet an Hand der Werte RXLEV und RXQUAL, dass ein Intra-BTS-Handover durchzuführen ist und verifiziert dass der betreffende Kanal noch aktiv ist.
- Der BSC sendet je nach Netzkonfiguration entweder eine Handover- oder Assignment-Nachricht, mit der bekannt gegeben wird, auf welcher Frequenz und auf welchem Zeitschlitz der neue Kanal aufgebaut werden soll, und wie sich die MS auf dem neuen Kanal identifizieren soll.
- Empfängt die MS eine Handover -Nachricht, so überträgt sie beim synchronen Handover zur BTS maximal 4 Handover Acknowledge-Nachrichten, die aus einer temporären MS-Identifizierung bestehten.
  Empfängt sie dagegen eine Assignment -Nachricht, so werden keine Handover Acknowledge-Nachrichten gesendet.
- Anschließend sendet die MS SABME-Rahmen (Set Asynchronous Balanced Mode Extended) zur BTS solange gesendet werden bis der Aufbau einer Schicht2-Verbindung durch den Empfang eines UA-Rahmens (Unnumbered Acknowledgement) bestätigt wird
- Der Empfang des SABME-Rahmens von der BTS wird an den BSC mit der Establish-Nachricht weitergeleitet.
- Den erfolgreichen Handover bestätigt die MS durch das Senden einer Handover Complete- bzw. Assignment Complete-Nachricht.
- Anschließend wird die MSC durch die Handover durchgeführt-Nachricht vom Handover informiert.
- Abschließend wird die BTS vom BSC aufgefordert, die alte Verbindung freizugeben.

3.4 Verbindungsaufbau und -abbau

3.4.1 Aktivverbindung

Phasen beim Aufbau einer Aktivverbindung (Mobile Originated Call – MOC)
Hat der Mobilteilnehmer an seinem Endgerät eine Teilnehmernummer gewählt und abgeschickt sind folgende Ablaufschritte erforderlich:

- Channel Request
  über den Common Control Channel CCCH
  Anfordern und Zuteilen eines dedicated signalling channels um den Verbindungsaufbau durchführen zu können
- Authentification
  Überprüfen der Netz-Zugangsberechtigung des A-Teilnehmers
- Cyphering
  Verschlüsseln des Funkkanal des A-Teilnehmers
- TMSI reallocation
  dem A-Teilnehmer eine neue TMSI zuteilen
- Übertragen der B-Rufnummer zum MSC

Aufgaben von VLR und HLR im Rahmen einer Aktivverbindung
Zum Aufbau einer Aktivverbindung wird nur das VLR benötigt, da es im Rahmen der TMSI-Zuteilung alle nicht in der MS (auf der SIM-Karte) gespeicherten Daten wie z.B. vereinbarte Teilnehmerdienste vom HLR kopiert um den Verbindungsaufbau durch den ständigen Datenaustausch mit dem HLR nicht zu verzögern.

Ablauf einer Aktivverbindung (Mobile Originated Call)

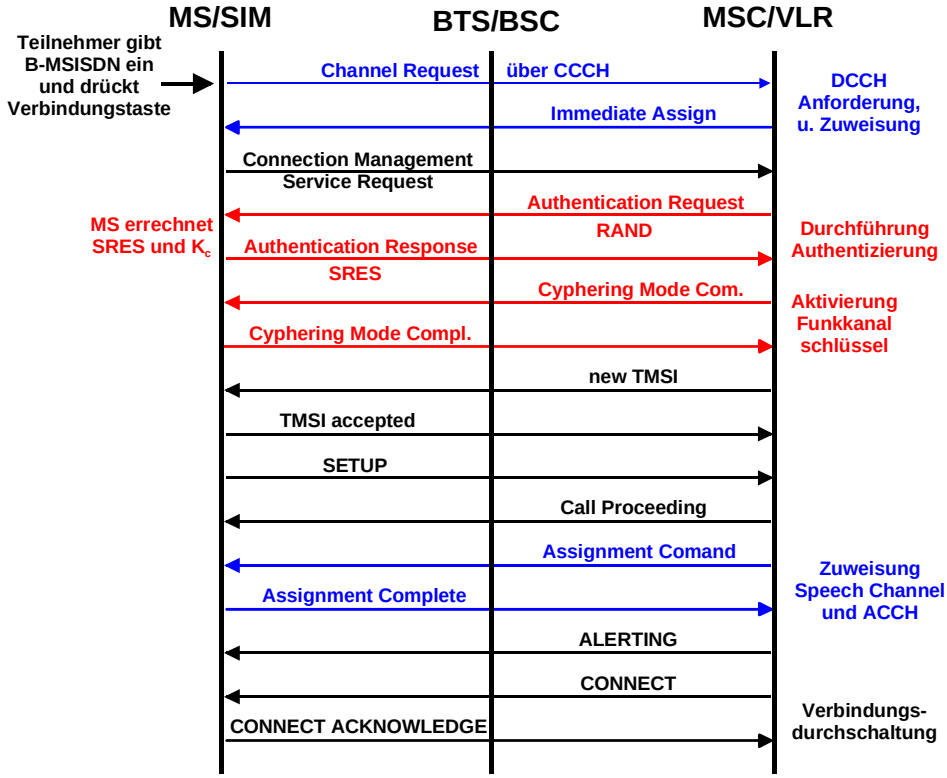


Bild 16 Ablauf einer Aktivverbindung

- **(17)** Nach Drücken der Verbindungstaste fordert die Mobilstation mit einer „Channel Request–Meldung“ im Common Control Channel CCCH die Zuteilung eines Dedicated Control Channel DCCH an, um die bereits gewählte B-Rufnummer absenden zu können.
- Die BSC ermittelt einen verfügbaren DCCH und weist diesen mit einer „Immediate Assignment-Meldung“ der MS zu.
- Über diesen DCCH fordert die Mobilstation beim BSC die Dienste der Vermittlungsschicht, also ein Connection Management Service an.
  Vor Aktivierung der Vermittlungsschicht wird jedoch eine Authentication, gefolgt von der Zuteilung einer neuen temporären Kennung TMSI durchgeführt.
- Die Authentication beginnt mit einer „Authentication Request“ – Meldung vom VLR, welche die RAND eines sog Triples enthält. Der Prozessor auf der SIM-Karte errechnet aus der RAND mit Hilfe der fest gespeicherten Algorithmen A3 und A8, so wie dem individuellen Schlüssel Ki den Wert SRES (Signed Response), der über den DCCH mit der Meldung „Authentication Response“ zurückgeschickt und im VLR mit der im AC errechneten SRES verglichen wird. Sind die vom AC zur Verfügung gestellte SRES und jene von der MS übertragene ident, ist die Authentifizierung positiv, d.h. der Teilnehmer berechtigt das Mobilnetz zu benützen.
- Die positiv durchgeführte Authentication wird vom MSC mit der Nachricht „Ciphering Mode Command“ über den DCCH beantwortet, welches die Mobilstation mit der Meldung „Cyphering Mode Complete“ beantwortet. Ab diesem Zeitpunkt erfolgt der Datenaustausch über die Luftschnittstelle verschlüsselt.
- Da die „alte“ TMSI über die noch nicht verschlüsselte Luftschnittstellen übertragen wurde, kann der MS vom VLR eine neu generierte TMSI zugewiesen und über die bereits verschlüsselte Luftschnittstelle übertragen werden.
- In der nun folgenden „Setup“ – Meldung teilt die Mobilstation über den DCCH dem MSC/VLR den gewünschten Basisdienst und die B-Rufnummer mit und erhält als Quittung, dass mit dem Verbindungsaufbau begonnen wurde die Meldung „Call Proceeding“ zurück.
- Anschließend an die Meldung „Call Proceeding“ erfolgt die Zuteilung eines Traffic Channels (Gesprächskanals) die der MS mit dem „Assignment Command“ mitgeteilt wird. Im Traffic Channel ist der für Signalisierungsaktivitäten während einer Verbindung benötigte Signalisierungskanal ACCH enthalten.
- Die Quittung der Mobilstation „Assignment Complete“ wird bereits über den ACCH gesendet, der bisher benützte DCCH wird freigegeben und steht wieder für andere Verbindungen zu Verfügung.
- Sobald es beim angerufenen Teilnehmer läutet, erhält die Mobilstation die Nachricht „Alert“ von der VSt des B-Teilnehmers über den ACCH. Die Mobilstation erzeugt ihrerseits den Rufton um dem A-Teilnehmer den aktuellen Verbindungszustand mitzuteilen.
- Nimmt der gerufene Teilnehmer den Anruf an, d.h. hebt er ab, schickt die VSt des B-Teilnehmers die „Connect“ – Meldung über den ACCH zur Mobilstation. Die Mobilstation quittiert mit „Connect Acknowledge“, worauf der Nutzkanal in den Netzelementen durchgeschaltet wird und zum Informationsaustausch zur Verfügung steht.

3.4.2 Passivverbindung

Phasen einer Passivverbindung (Mobile Terminated Call - MTC)

(18) Für die Durchschaltung eines Mobile Terminated Calls sind nach Eintreffen der MSISDN des B-Teilnehmers im (Gateway-) MSC folgende Ablaufschritte erforderlich:

- Interrogation
  Abfragen der MSRN („RN" des MSC des B-Teilnehmers) zum Aufbau einer Nutz- und Signalisierungsverbindung zwischen MSC_A und MSC_B
- Paging
  Ermitteln des Aufenthaltsbereiches des B-Teilnehmers, der sog. LAI und Suchen des B-Teilnehmers in seinem Aufenthaltsbereich.
- Authentification
  Authentifizieren des B-Teilnehmers – Überprüfen der Netz-Zugangsberechtigung
- Cyphering
  Funkkanal des B-Teilnehmers verschlüsseln
- TMSI reallocation
  dem B-Teilnehmer eine neue TMSI zuteilen
- Verbindungsdurchschaltung zum B-Teilnehmer

Interrogation

(19) Sobald die MSISDN von einem z.B. PSTN-Teilnehmer gewählt wird, führt die Ziffernbewertung im PSTN zum Aufbau einer Nutzkanalverbindung von der Ursprungs-VSt zum Gateway-MSC des gewählten Mobilnetzes welches die Interrogation durchführt. Wird die MSISDN von einem Mobil-Teilnehmer desselben Netzes gewählt, wird die Interrogation vom MSC des A-Teilnehmers durchgeführt.
Um zum Mobilteilnehmer verbinden zu können, egal wo sich dieser gerade aufhält, besitzt das GSM-Vermittlungsnetz zwei Datenbanken, die für die Mobilitätsverwaltung der Teilnehmer verantwortlich sind. Diese Datenbanken sind das zentral aufgestellte HLR (Home Location Register) und das jeweils einem geographischen Gebiet zugeordneten VLR (Visitor Location Register). Durch den Vorgang der Interrogation wird der Aufenthaltsbereich – VLR / MSC[5] - des B-Teilnehmers ermittelt.
Bei einem kommenden Gespräch identifiziert die Rufnummer des B-Teilnehmers (MSISIDN, z.B.: +436642012345), den HLR-Speicherbereich des B-Teilnehmers, in dem bzw. mit dessen Hilfe die Mobile Station Roaming Number (MSRN) ermittelt werden kann um sowohl eine Nutzkanalverbindung als auch eine Signalisierungsverbindung zum MSC des B-Teilnehmers durchschalten zu können.
Die Mobile Station Roaming Number (MSRN) ist eine Ziffernkombination, die in ihrer Struktur einer MSISDN entspricht, d.h. sie besteht aus CC, NDC und einer individuellen Nummer, kennzeichnet jedoch weder ein HLR noch einen Teilnehmer. Sie wird vom VLR des B-Teilnehmers auf Anfrage des HLR bereitgestellt und führt bei der Ziffernauswertung immer zur MSC des B-Teilnehmers.

Es gibt zwei Strategien, die vom Netzbetreiber individuell konfiguriert werden können:

- Die aktuelle MSRN-Nummer (Mobile Suscriber Roaming Number) des B-Teilnehmers ist im HLR gespeichert, mit der das kommende Gespräch zum aktuellen lokalen MSC weitergeleitet werden kann, der das geographische Gebiet versorgt, in dem sich der B-Teilnehmer gerade befindet. Dazu sind folgende Aktivitäten erforderlich:

[5] Im VLR wird von jedem Mobilteilnehmer des zu verwaltenden Gebietes die Location Area Identity (LAI) und die temporäre Rufnummer (TMSI) gespeichert

- Die IAM (Initial Adress Message) ist eine ZGV-7-Message, die entsprechend der Rufnummer (hier +436642012345) zum richtigen GMSC durchstellt. Durch die MSRN-Nummer, kann sie zum lokalen MSC weiter gesendet werden.
- Bei dieser Konfiguration muss bei jedem Location Update die MSRN-Nummer im HLR aktualisiert werden.

- Die aktuelle MSRN-Nummer des B-Teilnehmers ist im VLR gespeichert. Die MSRN wir bei jedem Passivruf vergeben. Im HLR ist dafür die VLR-Adresse für die ZGV-7-Signalisierung gespeichert. Bei einer Passivverbindung wird die VLR-Adresse aus dem HLR ins lokalen VLR übertragen und eine MSRN angefordert. Diese MSRN wird über das HLR zum (Gateway-) MSC geschickt, sodass die IAM zum MSC des B-Teilnehmers weitergeroutet werden kann.

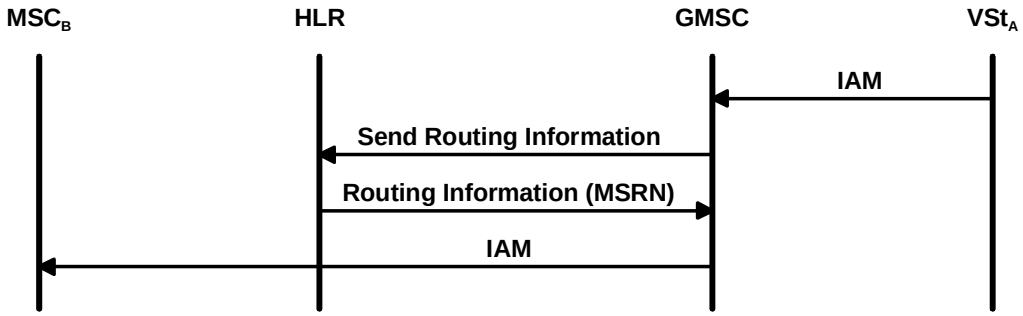


Bild 17 Interrogation - MSRN befindet sich im HLR

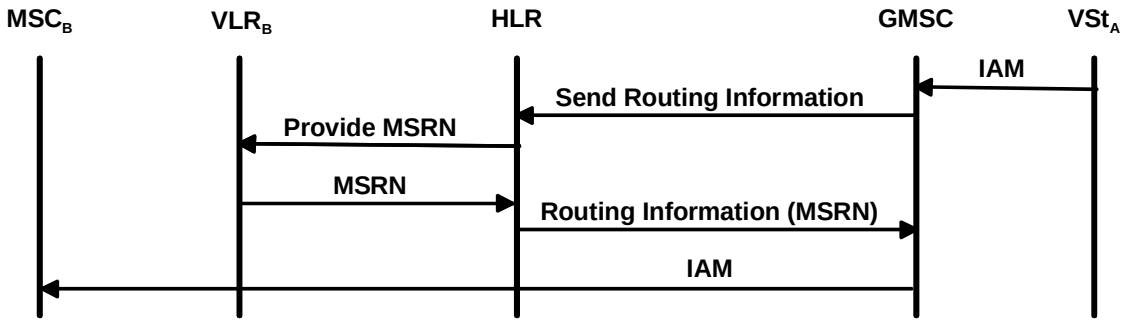


Bild 18 Interrogation - MSRN befindet sich im VLR

Ablauf einer Passivverbindung (Mobile Terminated Call)

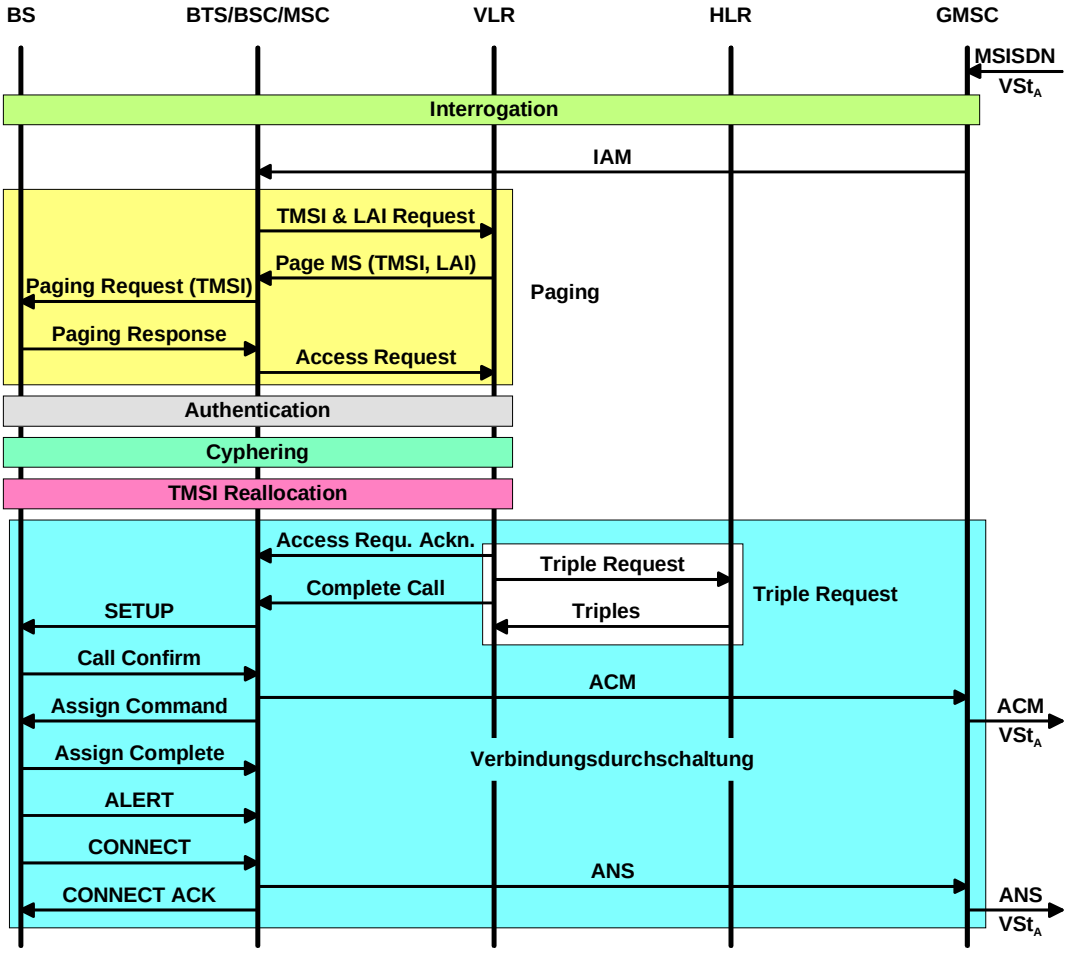


Bild 19 Ablauf einer Passivverbindung

Paging

(20) Unter Paging wird jener Ablauf verstanden mit dessen Hilfe die Zelle festgestellt wird in deren Bereich sich der B-Teilnehmer aufhält. Dafür sind folgende Aktivitäten erforderlich:

- Das MSC_B erhält in der IAM die MSISDN und die IMSI des B-Teilnehmers und fordert von seinem VLR die zugehörigen TMSI und LAI an.
- Durch einen Paging Auftrag an den dieser LAI zugehörigen BSC wird in allen Zellen Die TMSI gesucht welche der B-Teilnehmer auf seiner SIM-Karte gespeichert hat.
- Durch die Paging Response der MS werden dem BSC sowohl die Zelle als auch die verwendbaren Frequenzen bekannt.
- Nach Eintreffen der Paging Response wird vom VLR mit einem Service Request die Authentifizierung eingeleitet.

Authentifizieren des B-Teilnehmers

Bei der Authentication wird die Zugangsberechtigung einer SIM-Karte zum Netz überprüft. Sie wird vom VLR mit Hilfe sog. Triples durchgeführt, die bei Bedarf vom VLR im Authentication Center angefordert werden. Im Rahmen der Authentication werden folgende Aktivitäten durchgeführt:

- Übertragen der RAND (random number) vom VLR zur MS
- Errechnen der SRES (signed response) durch die MS und Übertragen derselben zum VLR

- Vergleichen der über die Funkstrecke an das VLR zurückgesendeten SRES mit der vom Authentication Center zur Verfügung gestellten.
- Bei Gleichheit einleiten der Funkkanal-Verschlüsselung (Cyphering).

Verschlüsseln des Funkkanals

- Senden des Verschlüsselungsbefehls nach erfolgreicher Authentifizierung vom VLR an die MS
- „Einschalten“ der Verschlüsselung in der MS und übertragen einer Quittungsnachricht an das VLR

TMSI Reallocation

Da die „alte“TMSI über die unverschlüsselte Funkschnittstelle übertragen wurde, kann aus Sicherheitsgründen für den B-Teilnehmer optional eine neue TMSI generiert und zur MS übertragen werden.

Anfordern neuer Triples

Wurde bei der vorangegangenen Authentifizierung das letzte Triple verbraucht, fordert das VLR einen neuen Satz Triples vom AC an.

Verbindungsdurchschaltung

Zur Verbindungsdurchschaltung zwischen MS_A und MS_B wird folgender Signalisierungsablauf durchgeführt:

- Sobald die MSC_B die SETUP Message vom MSC_B erhält schaltet sie das Rufsignal an und quittiert mit Call Confirm zum MSC_B.
- Anschließend wird der auf der Luftschnittstelle für diese Verbindung zu benützende Traffic Channel zugewiesen.
- Rufen und Abheben des B-Teilnehmers werden dem MSC_B und weiter dem A-Teilnehmer mit den Nachrichten Alert und Connect mitgeteilt.

4 Kontrollfragen

1. Welche Eigenschaften besitzt ein physikalischer Kanal?
2. Welche Burst-Strukturen gibt es und welche Aufgaben haben die einzelnen Bursts?
3. Welche Mehrfachrahmen gibt es und wofür werden sie eingesetzt?
4. Wie viele Gruppen von Signalisierungskanälen gibt es und für welche Aufgaben sind sie vorgesehen?
5. Wofür wird die IMSI benötigt und wie ist sie zusammengesetzt?
6. Wofür wird die LAI benötigt und wie ist sie zusammengesetzt?
7. Welche Daten sind auf der SIM-Karte enthalten und wofür werden sie benötigt?
8. Welche Aufgaben hat das Authentication Center?
9. Welche Daten sind im HLR gespeichert?
10. Wofür wird das VLR benötigt und welche Daten enthält es?
11. Beschreiben Sie den Ablauf einer Authentication.
12. Welche Aufgaben werden dem Location Management zugeordnet?
13. Was verstehen Sie unter einem Location Update?
14. Wann wird ein Handover durchgeführt und wie läuft es ab?
15. Welche Varianten von Handover gibt es?
16. Beschreiben Sie den Ablauf eines Intra-MSC Handover.
17. Beschreiben Sie den Ablauf einer Aktivverbindung.
18. Nennen Sie die Ablaufschritte für die Durchschaltung einer Passivverbindung.
19. Beschreiben Sie den Ablauf der Interrogation?
20. Warum und wie wird das „Paging“ durchgeführt?

5 Bilder und Tabellen

6 Abkürzungen

AC.....Authentication Center
ACCH.....Associated Control Channels
AMPS.....American (Advanced) Mobile Phone System
ARFCN .....Kanalnummer, absolute radio frequency channel number,
AuC.....Authentication Center
BCH .....Broadcast Channel
BSC .....Base Station Controller
BSS .....Base Station System
BTS.....Base Transeiver Station
CCCH .....Common Control Channels
CDM.....Code Division Multiplexing, Codemultiplex
CDMA .....Code Division Multiplex Access
CEPT .....Conference Européenne des Administrations des Postes et Telecommunications, Europäische Konferenz für das Post- und Fernmeldewesen
DCCH .....Dedicated Control Channels
DCS .....Digital Communication System
DECT .....Digital Enhanced Cordless Telephone
EI .....Equipment Identity
EIR.....Equipment Identity (Identification) Register
ETSI.....European Telecommunications Institute
FDM.....Frequency Division Multiplexing, Frequenzmultiplex
FDMA.....Frequency Division Multiple Access
GPRS.....General Packed Radio Services
GSM .....Global System for Mobile Communication
HLR .....Home Location Register
HON.....Handover Number
HPMLN .....Home Public Land Mobile Network
HSCSD .....High-Speed Circuit-Switched Data
IMEI .....International Mobile Equipment Identity
IMSI .....International Mobile Station (Subscriber) Identity
ISDN .....Integrated Services Digital Network
ISO .....International Standards Organization
ITU.....International Telecommunications Union
IVPN .....International VPN
Kc .....cipher key
LAC.....Location Area Code
LAI .....Location Area Identity
LEO .....Low Earth Orbit
LMSI .....Local Mobile Subscriber Identity
MCC.....Mobile Country Code
MNC.....Mobile National Code
MOC .....Mobile Originating Call
MoU .....Memorandum of Understanding
MS .....Mobile Station
MSC.....Mobile Services Switching Center
MSISDN.....Mobile Station International ISDN Number
MSRN .....Mobile Station Roaming Number
MTC.....Mobile Terminating Call

OMC .....Operation and Maintenance Center
OMS .....Operation and Maintenance Subsystem
OSI .....Open Systems Interconnection
OSS .....Operation & Maintenance Subsystem
PCN .....Personal Communications Network
PCS .....Personal Communications System
PHS .....Personal Hand-phone System
PIN.....Personal Identification Number
PLMN.....Public Land Mobile Network
PSDN.....Public Switched Data Network
PSTN .....Public Switched Telephone Network
PUK .....Personal unblocking Key
RAND.....Random Number, Zufallszahl
RFC .....Radio Frequency Channel
RSS .....Radio Subsystem
SDM.....Space Division Multiplexing, Raummultiplex
SIM .....Subscriber Identity Module
SRES.....signed response
SSS .....Switching Subsystem
TA .....Timing Advance
TACS .....Total Access Communications System
TCDMA.....Time CDMA
TDM.....Time Division Multiplexing, Zeitmultiplex
TDMA.....Time Division Multiple Access
TMN.....Telecommunication Management Network
TMSI .....Temporary Mobile Station Identity
TRAU.....Transcoding and Rate Adaption Unit
UMTS.....Universal Mobile Telecommunication System
UTRA.....UMTS Terrestrial Radio Access
VAS .....Value added Service
VLR.....Visitor Location Register
VPMLN .....Visited Public Land Mobile Network
VPN .....Virtual Private Network
WAP .....Wireless Application Protocoll
WCDMA.....Wideband CDMA

7 Literatur

[1] Ulrich Freyer, Nachrichtenübertragungstechnik, 3. Auflage, Carl Hanser Verlag, 1994, ISBN 3-446-17724-8

[2] Taschenbuch der Telekommunikation 1999, Fachbuchverlag Leipzig

[3] Bernhard Walke, Mobilfunknetze und ihre Protokolle, Band 1, Teubner Verlag, 1998, ISBN 3-519-06430-8

[4] Siegmund Redl, GSM Technik und Messpraxis; Netzeigenschaften, 2. Auflage, Franzis Verlag, 1995, ISBN 3-7723-4852-1