Über Signalisierung im UMTS

Es wird vorausgesetzt dass der Leser die Ausführungen des Autors über GSM und IP-GPRS - EDGE gelesen hat, da dort definierte Termini und Mechanismen hier nicht noch einmal erklärt werden.

1. Die Erfindung des CDMA-Prinzips

Das Prinzip, Signale über mehrere Funkfrequenzen mit zufälliger Verteilung zu verwenden wurde von . Hedy Lamer und George Antiheil im zweiten Weltkrieg in den USA patentiert. Damals wurde diese Idee von der Industrie als nicht machbar verworfen.
Die Idee, bekannt als Frequenzsprung, später als Frequenzsprung Spread Spektrum Technik ruhte bis 1957. Zu dieser Zeit, das Lamer – Antheil Patent war ausgelaufen, benutzten Ingenieure der *Sylvania Electronic System Division Buffalo* die Idee zur Entwicklung geheimer Nachrichtenübertragungstechnik, die dann während der Cuba-Krise 1962 eingesetzt wurde.
Nachdem diese Technik ein Bestandteil der Sicherheitstechnologie der Regierung geworden war, hat das US-Militär sie Mitte der 80iger Jahre deklassifiziert und es entstand die CDMA (Spread Spectrum) Technologie.
1998 rief das ITU zum IMT 2000 Wettbewerb (RTT-Radio Transmission Technologie) auf. Im Ergebnis entstanden 5 Technologien in der **I**nternational **M**obile **T**elecommunication von denen drei heute interessant sind. In Europa heißt eine davon, IMT-DS Direct Spread UTRA FDD (WCDMA = **UMTS**).

2. Die Instrumentierung

Wie aus den nachfolgenden Abbildungen hervorgeht, existieren die Netze der Generationen 2 (GSM), 2,5 (GPRS) und 3 (UMTS) parallel. Zur Sicherung der internationalen Mobilfunk-Verbindungen müssen Mobilfunkgeräte der 3. Generation zu GSM und GPRS kompatibel sein. Damit ist für den Besitzer eines UMTS-fähigen Mobiles die durchgängige Funkverbindung auf den Territorien gewährleistet.

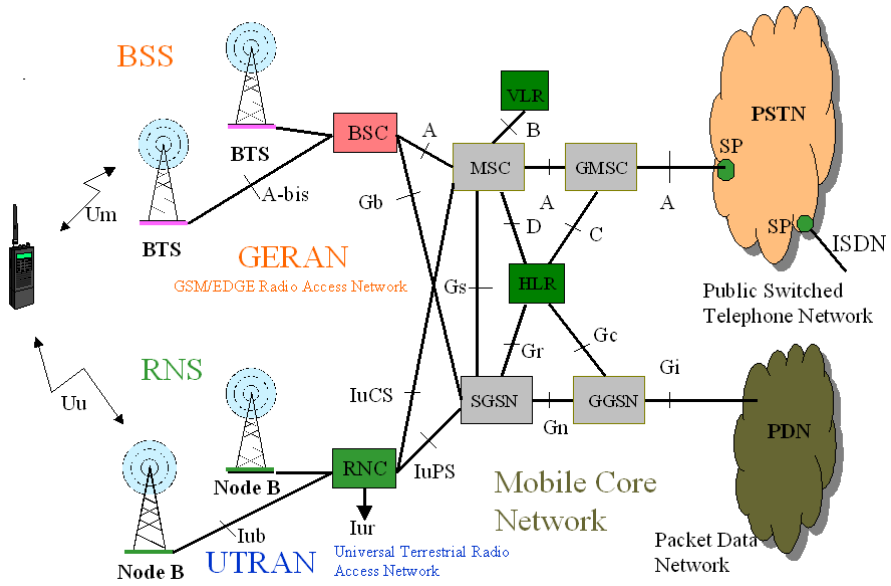


Bild 1: Verbund von UMTS und GSM-Netz

Das Universal Terrestrial Radio Access Network UTRAN oder auch das Radio Network Subsystem RNS hat prinzipiell den gleichen Aufbau wie das Base Station Subsystem BSS im GSM. Es besteht aus dem Node-B (vergleichbar mit der Base Transceiver Station BTS im GSM) und dem Radio Network Controller RNC (vergleichbar mit dem Base Station Controller BSC im GSM).
Ein wesentlicher Unterschied der beiden Technologien besteht unter anderem in der Physik der Luftschnittstelle.
Während im GSM der Funkkanal durch Frequenz- und Zeit- Multiplex gebildet wurde, ist UMTS ein Codemultiplex (CDMA) System. Da wir uns, wie im GSM, *nur* mit der Signalisation auf der Luftschnittstelle beschäftigen wollen soll letztere Gegenstand der folgenden Ausführungen sein
Während das GSM-Netz , durch zusätzliche Komponenten wie PDU und *Serving GPRS Support Node* sowie *Gateway GPRS Support Node* für die Datenübertragung tauglich gemacht werden musste, sind im UMTS Sprach und Datenübertragung integriert.

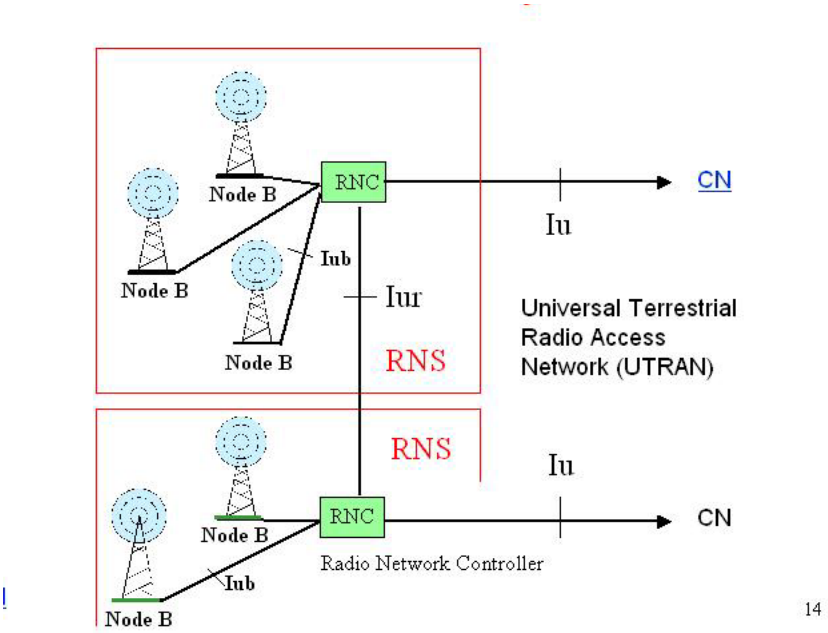


Bild 2: Das Radio Network Subsystem

Die Iu-Schnittstelle stellt, wie in Bild 3 dargestellt, den Zugang des UTRAN zum Kernnetz dar.
Der Zugang erfolgt gleichberechtigt mit dem Broadband Radio Access Network (bei Organisation eines General Access Network) .
Die Gleichberechtigung besteht auch zum Satellite Radio Access Network.

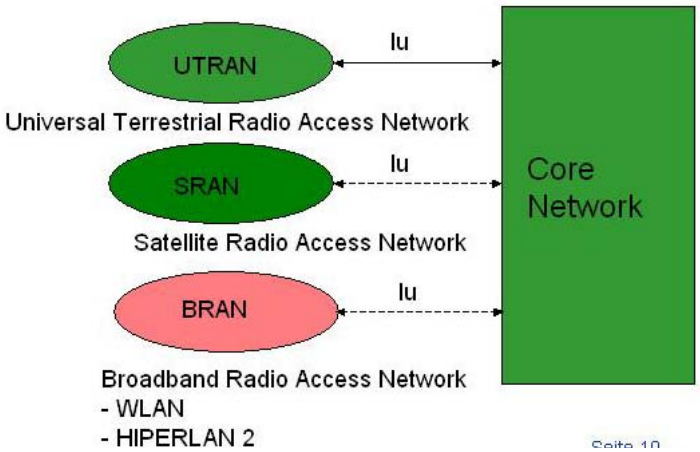


Bild 3: Die IU-Schnittstelle ist der Zugang zum Kernnetz

2.1 Die Aufgaben des Node B

Der Node B bildet den Physical Layer des Uu-Protokolls, realisiert die Verbindung zum RNC über das Iub-Protokoll und gewährleistet die Frequenz- und Zeit-Synchronisation.
Der Node B stellt die innere Schleife der Leistungskontrolle sicher, führt Feldstärke-messungen aus und überträgt Systeminformationsmeldungen
Der Node B übernimmt die Macrodiversity Signalverteilung und Kombination .

2.2 Die Aufgaben des RNC

Der Radio Network Controller vermittelt den RadioBearer breitbandig zwischen dem Core Network (Iu), dem Node B (Iub) und zwischen Nachbar RNC (Iur)
Der RNC erledigt das Radio Ressource Management:
- Handover Steuerung zur Gewährleistung der User Mobilität
- Regelung der Senderleistung minimiert Interferenzen
- Regelt die Übergabe erforderlicher neuer RadioBearer
- Codemanagement bei Einrichtung von Downlink Spreizcodes

Der RNC ist verantwortlich für das UTRAN Control, bestehend aus:
- dem Broadcasting der Systeminformationen
- der Steuerung der zufälligen Zugriffswünsche von Mobilfunkgeräten
- den UTRAN security functions
- dem Mobility management im Zustand der Verbindung
- dem Zugriff auf Datenbanken und zellspezifische Daten durch das UE
- der Unterstützung der Lokalisierung des UE-Standortes

Der RNC bildet das Network Management Interface für den Zugriff auf den RNC für Kontroll- und Reparaturzwecke

3. Gemeinsamkeiten von UMTS, GSM und GPRS Netzen.

Die Mobilfunknetze 2G und 2,5 G, sind wie in Bild 1 gezeigt. mit dem UMTS (3G) verknüpft. Die Verknüpfung erfolgt über das Kern-Netzwerk. Es muss somit eine Ebene geben in der für alle drei Netze vergleichbare Protokolle existieren.
Diese allen Netzen gemeinsame Ebene ist losgelöst von den physikalischen Prozessen des Kanalaufbaus. Diese „Nicht mit dem Zugriff auf die physikalischen Prozesse befasste Schicht“ wird daher

Non Access Stratum

genannt. In ihr wirken die aus dem GSM bekannten Protokolle CC, SS und SMS über das MM sowie die aus dem GPRS bekannten Protokolle GSMS und SMS über das GMM.
Damit heißt folgerichtig der Teil des Netzes, der die Kanalbildenten Prozesse beschreibt das

Access Stratum

des UMTS, besser der kombinierte Netze 2G, 2,5 G und 3G.

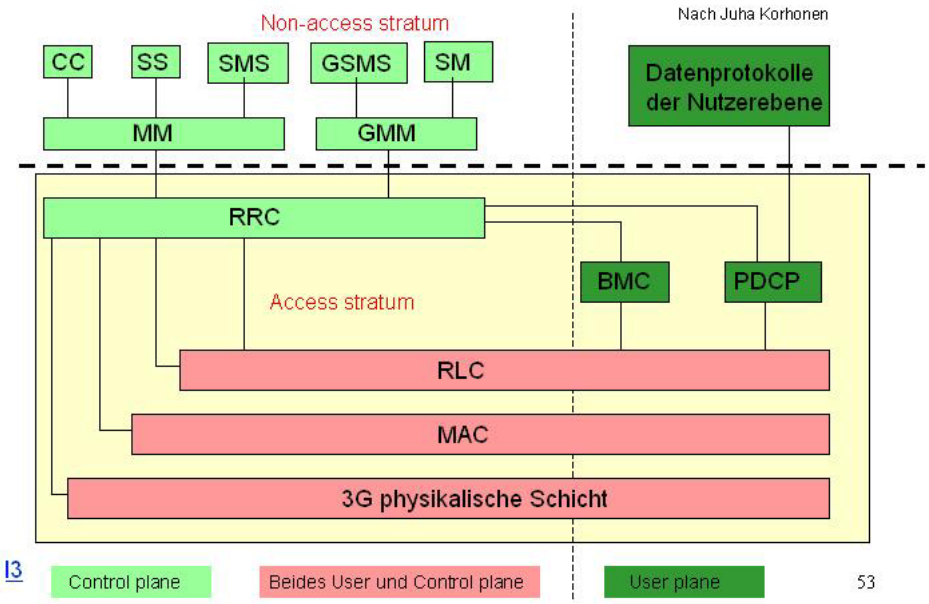


Bild 4: Zusammenhang von *Access* und *Non-Acces* Stratum

3.1 Das *Non-Access* Stratum

Zum *Non-Access* Stratum zählen gemäß Bild 4:

CC. Die Call Control Messages, die bereits im ISDN definiert wurden
SS: Die Suplemetary Services, die ebenfalls bereits im ISDN erklärt sind. Ein sehr bekannter SS ist die Rufumleitung .
SMS: Der Short Message Service
GSMS: GPRS SMS
SM: Das Session Management im GPRS
MM: Mobility Management
GMM: GPRS Mobility Management

Die Meldungen aus dem *Non-Access* Stratum werden nach den im GSM (oder auch schon im ISDN) definierten Regeln formuliert und in UMTS Trace eingebaut.
Bild 5 zeigt eine CC Meldung die in einen UMTS Trace eingebaut ist. Die Meldung des *NAS*-Stratum nimmt dabei eine Dienstleistung des *ACCES* Stratum in Anspruch.

```
00 04 00 70  f4 34 2b 17  29 40 00 b0  60 23 c0 5d  50

:WDCMA L3 RRC Peer messages

00  00000000  Channel LSB
:Channel Type MSB
04  00000100  Downlink DCCH

00  0000000001110000  length=112
          1  Integrity Check Info present
    11101000  MessageAuthenticationCode,
    01101000  MessageAuthenticationCode,
    01010110  MessageAuthenticationCode,
    00101110  MessageAuthenticationCode,
        0101  RRC-MessageSequenceNumber  = 5

: Message Type:
       00101  DOWNLINK DIRECT TRANSFER
           0  r3 SEQUENCE
           0  sw1 not present
DownlinkDirectTransfer-r3
          00  RRC-TransactionIdentifier = 0
:CN-DomainIdentity
           0  cs-domain,
:nas-Message
    000000000101  length=5
    1-------  direction to        : originating site
    -000----  TransactionID       : 0
    ----0011  Protocol Discrim.   : Call control and call related SS messages
    00------  SendSequenceNumber  : 0

    --000001  MESSAGE TYPE        : ALERTING

    00011110  INFORMATION ELEMENT : Progress indicator
    00000010  L. OF IE PROG.IND.  : 2
    1-------  Extension           : 1
    -11-----  Coding standard     : Stand. Def. for the GSM-PLMNS as descry.
    ---0----  Spare               : 0
    ----1010  Location            : Network beyond interworking point
:
```

Bild 5: Ausschnitt aus dem MOC eines UMTS-Telefons

3.2 Das Access Stratum

3.2.1 Die RRC-Schicht

Die RRC-Schicht im UMTS hat vergleichbare Funktionen wie die RR-Schicht im GSM, GPRS.
Gemäß ETSI TS 125 331 besitzt die RRC-Schicht im UMTS nachstehende Aufgaben:

- Die Aussendung von Systeminformationen
- Aufbau, Unterhaltung und Freigabe von RRC-Verbindungen zwischen UE und UTRAN
- Aufbau, Reconfiguration und Freigabe von Radio Bearern
- Zuweisung und Reconfiguration sowie Freigabe von Radio Ressourcen der RRC-Verbindung
- Steuerung der Mobility Funktionen der RRC-Verbindung

- Steuerung der angeforderten Qualität der Verbindung (QoS)
- Steuerung und Auswertung von Kanalmessungen durch das Endgerät (Measurement Control und Report)
- Leistungssteuerung der äußeren Schleife
- Steuerung der Verschlüsselung
- Paging
- Zellauswahl im idle mode
- Festlegung der Radio Ressourcen für die Uplink DCH-Verbindungen
- Steuerung des Cell Broadcast Service

Bei Telephonie- und SMS Verbindung ist gemäß Bild 4 die RRC-Schicht direkt mit der physikalischen Schicht verbunden.
Müssen Datenpakete übertragen werden, so werden die Dienste der RLC-Schicht benötigt

3.2.2 Die RLC-Schicht

Die RLC-Schicht wird der Schicht 2 zugeordnet. Das RLC-Protokoll ähnelt sehr stark den Protokollen LAPD und HDLC.
Die RLC-Schicht empfängt von übergeordneten Schichten Protokolleinheiten die *RLC-Service Data Unit*, RLC-SDU heißen.
Nach Umformung durch den zugeteilten Fehlersicherungsmode (TM, UM, AM) wird die Protokolleinheit als *RLC-Protocol Data UNIT,* RLC-PDU weitergegeben.
Es existieren die Fehlersicherungsmodi:

Transparent Mode TM
Unacknowledge Mode UM
Acknowledge Mode AM

3.2.2.1 Transparent Mode TM

Gemäß Bild 6 werden die SDU Blöcke im Transparent Mode ohne Kontrolle durch die RLC-Schicht durchgereicht.

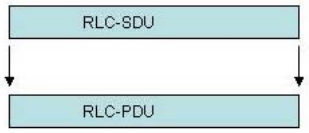


Bild 6: Übergabe von Blöcken im Transparent Mode

Die SDU Blöcke bestehen damit nur aus einem Datenfeld, das aber eine Segmentierung in eine festgelegte Größe erfährt.
In der ETS ts_125331 werden die Formate sdu1 sdu4 sdu16, sdu64 unterschieden

3.2.2.2 Unacknowledge Mode UM

Im unbestätigten Modus (UM) werden die RLC-SDU‘s gemäß Bild 7 segmentiert und den so entstehenden PDU`s wird ein Header hinzugefügt

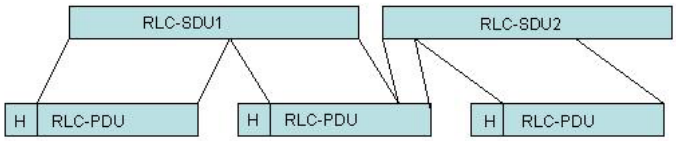


Bild 7: Segmentieren der Nachricht im Unacknowledge Mode

Im Header H ist, wie in Bild 8 gezeigt, eine Sequence Number enthalten und ein Lenght Indicator. Das Extension Bit „E“ steht in der letzten Zeile auf „0“
Mittels Sequence Number wird die Vollständigkeit der Sendung überprüft

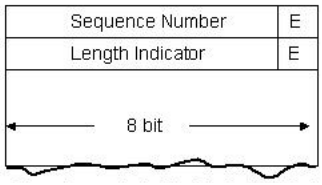


Bild 8: Aufbau einer RLC.PDU im UM

3.2.2.3 Acknowledge Mode AM

Im Acknowledge Mode wird die SDU wie in Bild 7 gezeigt segmentiert

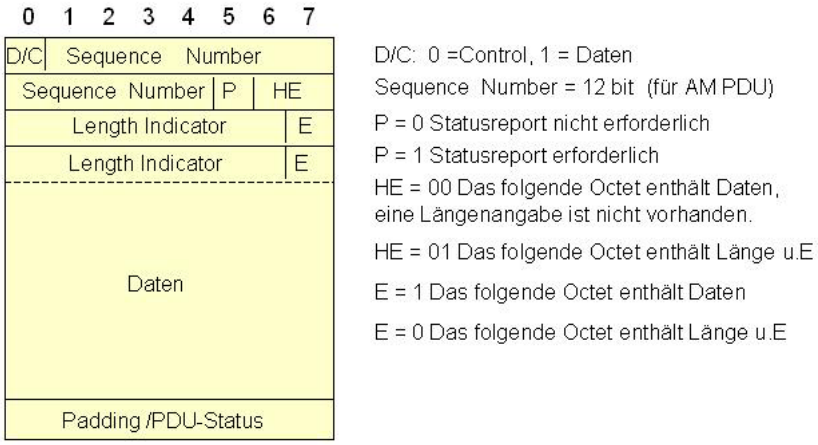


Bild 9: Aufbau der RLC PDU im AM

Die RLC-PDU transportiert in Abhängigkeit des D/C Bits entweder Daten oder Control Informationen.
Werden Daten übertragen, so wird eine Fenstergröße vereinbart, die festlegt, wie viele Datenblöcke unbestätigt übertragen werden.

Entsprechend der Fenstergröße die Werte zwischen 0 und $2^{12}-1$ annehmen kann wird die Sequenznummer, die die jeweilige PDU identifiziert, hochgezählt. Nachdem das Fenster gefüllt ist, wird das Polling-Bit (P-Bit) gesetzt und ein Statusreport angefordert. Die Länge der PDU soll 7 oder maximal 14 Oktett umfassen. Tritt in einer PDU ein Übertragungsfehler auf, so meldet der Empfänger, in einer Status PDU, die Sequenznummer der betroffenen PDU dem Sender und veranlasst so eine Wiederholung.

3.2.3 Die MAC-Schicht

Die MAC-Schicht ist ganz allgemein die unterste Schicht der Sicherungsschicht (Data Link Layer) im OSI-Referenzmodell. Die MAC-Schicht steuert die Algorithmen zur Kanalverwaltung, den Frame-Aufbau, sowie die Kollisions- und Fehlererkennung. In der Erstausbaustufe des UTRANs (Rel.99) befinden sich sämtliche MAC-Funktionen netzwerkseitig im RNC. Eine deren wichtigsten Aufgaben besteht im Ausregeln von Verkehrslasten der verschiedenen an den RNC angeschlossenen Zellen. So kann die MAC innerhalb gewisser Vorgaben, die sie vom RRC bei Dienstaufbau bekommt, die Kanalcharakteristik für jeden Dienst der Verkehrslast anpassen, wie z.B. Datenraten einzelner Benutzerdienste verringern, wenn die Gesamtlast einer Zelle zu groß wird. Erst seit der Einführung von HSDPA wurden MAC-Funktionalitäten auch in die NodeB für eine Optimierung der Netzwerkperformance ausgelagert

In der MAC-Schicht von UMTS werden die logischen Kanäle auf die Transportkanäle abgebildet. Die MAC-Schicht ist also für die Auswahl eines geeigneten Transportformats für jeden Transportkanal in Abhängigkeit der momentanen Übertragungsrate bzw. Datensensitivität des logischen Kanals zuständig. Das Transportformat wird in Bezug auf das Transport Format Combination Set (TFCS) gewählt, das vom Zugangs-Controller für jede Verbindung definiert wird.

3.2.4 Aufgaben der 3G Physikalischen Schicht

In der Physikalischen Schicht erfolgt die Synchronisation der Kanäle, die Modulation, die Codespreizung und das Scrambling.
Diese Schicht ist verantwortlich für die Sendeleistungssteuerung (inner loop) und die ständige Messung der Kanalqualität.
Hier werden die Transportkanäle gemultiplext. Es erfolgt das Interleaving, Rate Matching und die Fehlerschutzkodierung.

4. Frequenzen und Kanalerzeugung

4.1 Arbeitsfrequenzen

Für UMTS FDD stehen 2 Frequenzbänder zu Verfügung:
Uplink: 1920,3 bis 1980 MHz
Downlink: 2110 bis 2170 MHz
Duplexabstand: 190 MHz
Es ist ein Kanalraster von 200 MHz festgelegt:
Die Absolute Radio Frequency Channel Number UARFCN berechnet sich aus 5 x Frequenz damit hat die Frequenz 1920 MHz die UARFCN 9600
Da die Bandbreite eines WCDMA Signals ~5 MHz beträgt, lassen sich im Band 6 UMTS FDD Sender für je einen Operator unterbringen.

4.2 Die Modulation im UMTS

Die verwendete Modulationsart ist Code Division Multiple Access CDMA, genauer, in Abgrenzung vom Frequency-Hopping CDMA, direct-sequence CDMA (DS-CDMA) mit 3.840.000 c/s.

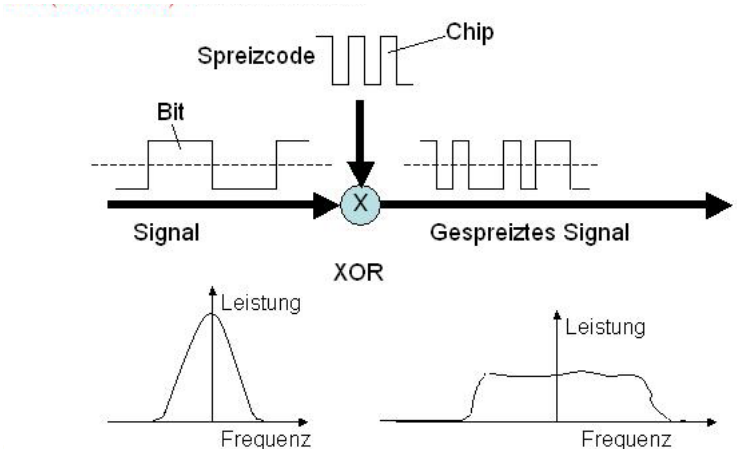


Bild 10: Das Prinzip der Modulation im UMTS

Das Prinzip der UMTS-Modulation ist in Bild 10 dargestellt. Dabei wird ein Signal (z.B. digitalisierte Sprache) mit einem hochfrequenten Träger (Spreizcode) über eine „Exklusive Oder“ Schaltung moduliert.
Für den Spreizcode wird zur Unterscheidung vom Begriff Bit, der für das Signal reserviert ist, der Begriff Chip eingeführt.
Am Ausgang der exklusiven Oderschaltung erscheint das gespreizte Signal, dessen Leistung über der Frequenz eine Kurve wie in Bild 10 unten rechts darstellt.
Für den Transport mehrerer Signale über einen Kanal muss jedes Signal mit einem Spreizcode moduliert werden der zu jedem anderen orthogonal ist .
Den Apparat dazu liefert die Mathematik.
Alle Codes, die in einer Hadamard Matrix entwickelt werden sind zueinander orthogonal .
Die Codes lassen sich auch in einen Codebaum (Walshtree) entwickeln. (Bild 11)

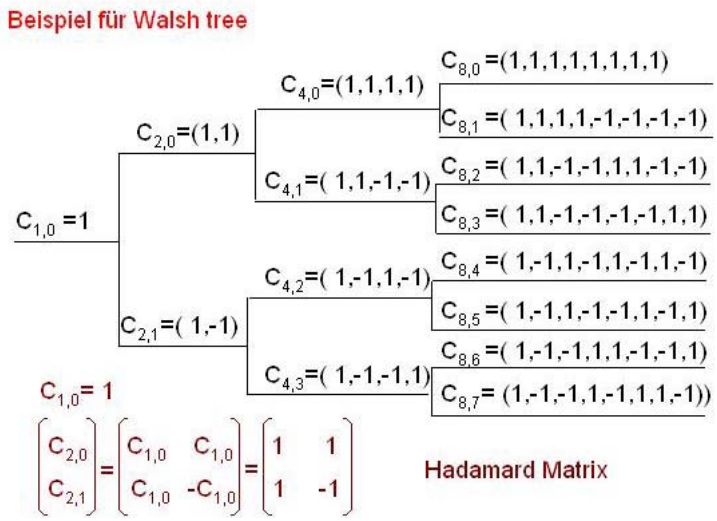


Bild 11: Der Baum der orthogonalen , variablen Spreizfunktionen (OVSF)

Die Chiprate im UMTS beträgt wie oben gesagt 3,84 Mcps (Megachips pro Sekunde)
Die Symbolrate ist die Frequenz des zu übertragenden Signals. Das Verhältnis von Chiprate zu Symbolrate heißt Spreizfaktor (Spreizfaktor = Chiprate/ Symbolrate)

Zwischen Diensten und OVSF besteht folgender Zusammenhang:

Spreizfaktor	Theoret. Übertragungsr.	Übertragungsrate/Dienst	
SF512	7,5 kbit/s	1,7 kbit/s	SMS
SF256	15 kbit/s	5,15 kbit/s	Sprache
SF128	30 kbit/s	12,2 kbit/s	Sprache
SF64	60 kbit/s	32 kbit/s	Daten
SF32	120 kbit/s	64 kbit/s	Daten
SF16	240 kbit/s	128 kbit/s	Daten
SF8	480 kbit/s	384 kbit/s (48 kByte)	Daten
SF4	960 kbit/s	2 Mbit/s	Daten (3Kan)

Bild 12: Die Erzeugung von Kanälen im Kodebaum

In Bild 12 stellen die ersten beiden Spalten den Zusammenhang zwischen Spreizfaktor und der theoretisch möglichen Übertragungsrate dar. Die dritte Spalte zeigt die mit dem entsprechenden Spreizfaktor praktisch realisierte Übertragungsrate.
So begrenzt bei 12,2 kbit/s Sprache (SF128) das Rauschen die Teilnehmerzahl pro Zelle auf etwa 100 (anstelle der theoretisch möglichen 128).
Würde die Last beim Spreizfaktor 4 auf 3 Kanäle verteilt, so könnte eine Übertragungsrate von 2 Mbit/sec erreicht werden. Demgegenüber wir jedoch im UMTS-Netz für Datenübertragung höchstens der SF8 zugeteilt, womit eine praktische Datenrate von 384 kbit/s erzielt wird.

Problematisch ist in einer UMTS-Zelle die Zuteilung der Äste des Codebaums an die Teilnehmer. Es gilt die Regel (Bild 13) : Alle Codes, die sich durch eine gerade Linie nach links oder rechts verbinden lassen , blockieren sich gegenseitig.[1].

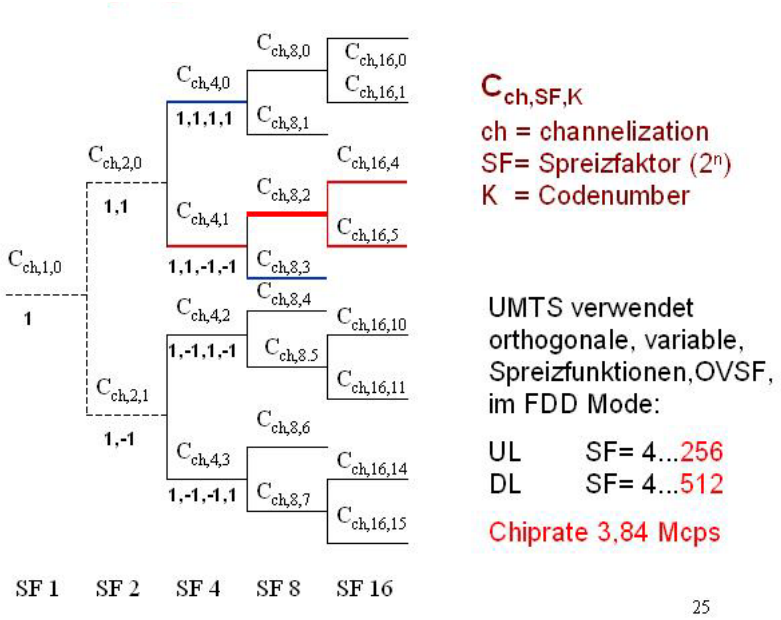


Bild 13: Mögliche Blockierungen im Kodebaum

Das gespreizte Signal hat nicht bei Verwendung aller Zweige des OVSF Baumes das in Bild 10 unten rechts dargestellte Leistungsspektrum. Daher wird in einer zweiten Stufe der Kodierung mit einer Zufallsfolge der gleichen Frequenz (3,84 MHz) die Signalenergie vollständig über die Funkbandbreite verteilt. Die PN Folge hat eine Wiederholungsrate von 10 ms.
Funkzellen wie sie aus dem GSM bekannt sind, haben im UMTS zwar die gleiche Frequenz, eine jede besitzt aber einen der 512 möglichen primäre Scrambling Codes

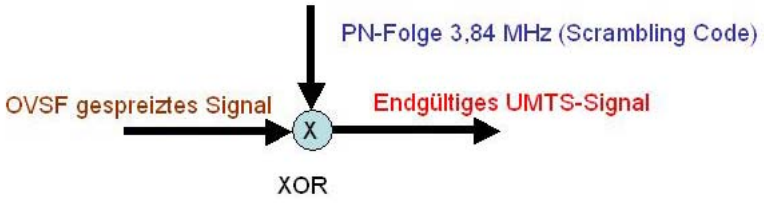


Bild 14: Modulation des gespreizten Signals mit einem Scrambling Code

4.3 Die Kanäle im UMTS

4.3.1 Kanäle im UMTS, FDD-Mode Downlink

Im GSM existiert physikalisch gesehen nur ein Kanal, der durch zeitliche Zuteilung verschiedenen Zwecken zugeordnet werden kann. Aus den Bildern 12 und 13 geht hervor,

dass im UMTS mehrere Kanäle, mit unterschiedlichen Bandbreiten, gleichzeitig gebildet werden können Dabei kann Bandbreite, je nach Belastung durch die Teilnehmer eingeschränkt oder vergrößert werden.

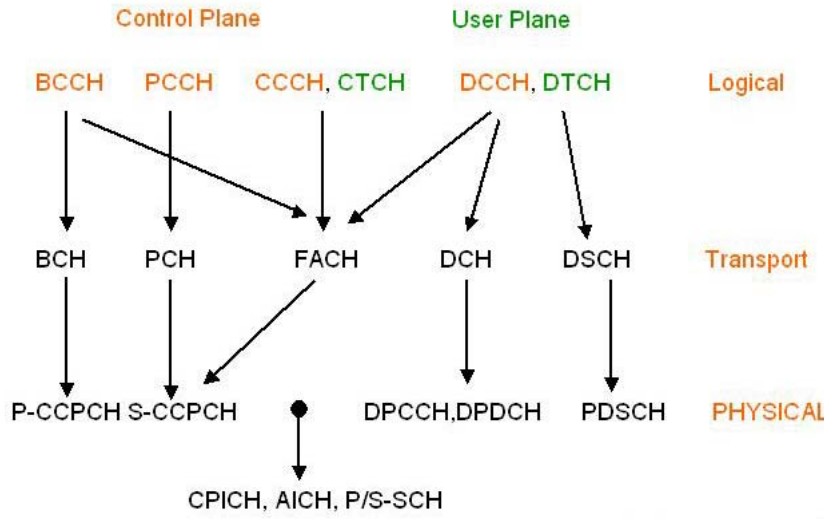


Bild 15: Kanäle im Downlink (nach Juha Korhonen)

Gemäß ETS I **TS 125 321** erfolgt der Datentransfer im MAC-Layer auf logischen Kanälen. Ebenfalls im MAC- Layer erfolgt das Mapping der logischen Kanäle auf Transport Kanäle. Das Mapping von Transport Kanälen auf Physikalische Kanäle erfolgt nach **ETSI TS 125211**. Die Aufgaben der Logischen Downlink-Kanäle sind nachstehend erklärt:

BCCH Broadcast Control Channel, strahlt Systeminformationen aus:
Dazu gehören Masterinformations- und Systeminformationsblocks

PCCH Paging Control Channel, überträgt Paging Informationen.

CCCH Common Control Channel, überträgt Steuerungsinformationen: Beispiel
z. B. RRC Kommandos zu Beginn des Verbindungsaufbaus.

DCCH Dedicated Control Channel, zugeordnete Steuerungsinformationen: Beispiel
z.B. RRC Kommandos nachdem dem UE Kanäle zugeordnet sind.
Dazu gehören auch Meldungen wie INITIAL DIRECT TRANSFER, die MM und CC Messages „einhüllen“ und übertragen.

DTCH Dedicated Traffic Channel, bidirektional, transportiert Nutzerdaten.

CTCH Common Traffic Channel, transportiert Nutzerdaten für Gruppen.

Transportkanäle Downlink haben die Aufgabe:

BCH Broadcast Channel, Broadcast-Kanal für System und Zellspezifische Nachrichten.

PCH Paging Channel, Übertragung von Paging- und Notification- Informationen.

FACH Forward Access Channel, allgemeiner Downlink-Kanal, für kleine Mengen von Nutzerdaten.

DSCH Downlink Shared Channel, für mehrere Nutzer, für zugeordnete Steuer- und Traffic-Daten.

DCH Dedicated Channel, ausschließlich für ein UE.

Aufgaben der Physikalischen Downlink-Kanäle.

P-SCH PrimarySynchronisation Channel, Länge = 256 Chips, (10% jedes Slots). Der Primäre Synchronisations- Code (PSC) ist in allen UTRAN Basis-Stationen gleich. Er entdeckt den Zeitschlitzbeginn.

S-SCH Secondary Synchronization Channel, Länge = 256 Chips, (10% jedes Slots). Der Sekundäre Synchronisations- Code (SSC) besteht aus 16 orthogonalen Codeworten. Er gestattet Rahmensynchronisation.

CPICH Common Pilot Channel, transportiert eine vordefinierte Bitfolge (30 KB/sec)
. Er gestattet die Identifizierung des Scrambling Codes. Allgemeiner Referenzkanal (Signalleistung und Qualität).

P-CCPCH Primary Common Control Physical Channel. Auf diesem Kanal sendet das Netz die Systeminformationen, er enthält P-SCH und S-SCH.

S-CCPCH Secondary Common Control Physical Channel. transportiert den PCH (Paging Channel) und den FACH (Forward Access Channel).

PDSCH Physikal Downlink Shared Channel, transportiert den DSCH und ist stets mit dem DPCH (Steuerinformationen) gemultiplext.

DPDCH Dedicated Physical Data Channel, transportiert Nutzerdaten und Steuerungsdaten.

DPCCH Dedicated Physical Control Channel, transportiert speziell Daten für die Steuerung der physikalischen Schicht.

AICH Acquisitation Indicator Channel, bestätigt den RACH-Empfang.

4.3.2 Kanäle im UMTS, FDD-Mode UP-link

Wie Bild 16 zeigt, ist die Anzahl der Kanäle im Uplink deutlich geringer als im Downlink. Die Verantwortlichkeit der Schichten für die Kanalbildung entspricht denen im Downlink.

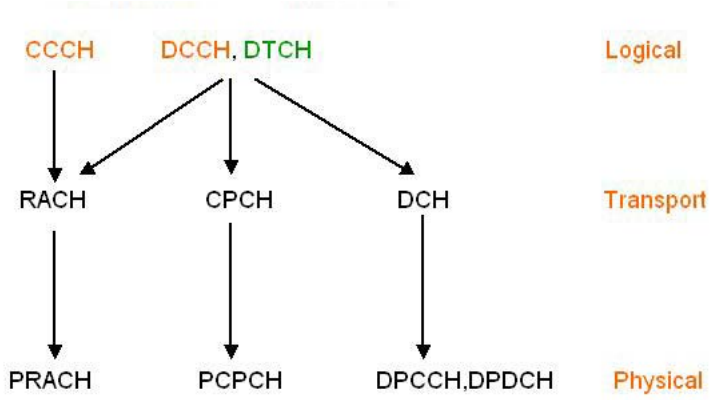


Bild 16: Kanäle im Uplink (nach Juha Korhonen)

Die Aufgaben der Logischen Uplink-Kanäle sind nachstehend erklärt:

CCCH Common Control Channel, überträgt Steuerungsinformationen: z. B. RRC Kommandos zu Beginn des Verbindungsaufbaus

DCCH Dedicated Control Channel, zugeordnete Steuerungsinformationen: z.B. RRC Kommandos nachdem dem UE Kanäle zugeordnet sind. Dazu gehören auch Meldungen wie UPLINK DIRECT TRANSFER die die (NAS-Messages) MM und CC Messages „einhüllen“ und übertragen.

DTCH Dedicated Traffic Channel, bidirektional, transportiert Nutzerdaten

Transportkanäle Uplink haben die Aufgabe

RACH Random Access Channel, Uplink Kanal für kleine Control- oder Traffic-Datenmengen im Wettbewerb mit anderen Teilnehmern.

CPCH Common Packet Channel, für Paket Daten im Burst Mode.

DCH Dedicated Channel, ausschließlich für ein UE.

Aufgaben der Physikalischen Uplink-Kanäle.

PRACH Physical Random Access Channel, transportiert die Anforderung des UE zum Verbindungsaufbau.

PCPCH Physical Common Packed Channel. Transportiert den CPCH-Common Packet Channel, für Paket Daten im Burst Mode.

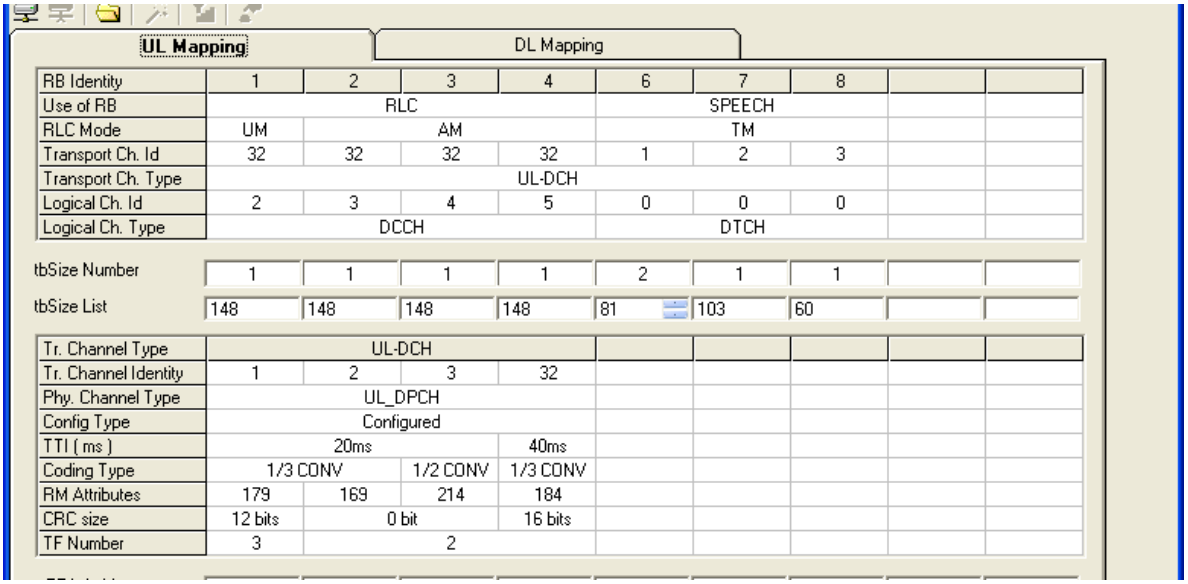
DPDCH Dedicated Physical Data Channel, transportiert Nutzerdaten und Steuerungsdaten.

.

DPCCH Dedicated Physical Control Channel, transportiert speziell Daten für die Steuerung der physikalischen Schicht.

4.3.3 Kanäle für eine Telephonieverbindung als Beispiel

Die Fa. SAGEM Wireless hatte für in eine frühere Entwicklung eines UMTS Trace Mobiles ein Auswerteprogramm mit Namen „OTDriveDual 1.6 beta“ geschaffen. Diese Software gestattet es die Kanalzuteilung einer Verbindung live zu beobachten. In den Bildern 17 und 18 kann sich der Leser, im Vorgriff auf spätere Erklärungen, ein Bild machen, wie Kanäle in den einzelnen Modi gebildet werden.



UL Mapping | DL Mapping

RB Identity	1	2	3	4	6	7	8		
Use of RB	RLC				SPEECH				
RLC Mode	UM	AM			TM				
Transport Ch. Id	32	32	32	32	1	2	3		
Transport Ch. Type	UL-DCH								
Logical Ch. Id	2	3	4	5	0	0	0		
Logical Ch. Type	DCCH				DTCH				
tbSize Number	1	1	1	1	2	1	1		
tbSize List	148	148	148	148	81	103	60		

Tr. Channel Type	UL-DCH								
Tr. Channel Identity	1	2	3	32					
Phy. Channel Type	UL_DPCH								
Config Type	Configured								
TTI (ms)	20ms			40ms					
Coding Type	1/3 CONV		1/2 CONV	1/3 CONV					
RM Attributes	179	169	214	184					
CRC size	12 bits	0 bit		16 bits					
TF Number	3	2							

Bild 17: Uplink-Kanäle einer UMTS Telephonieverbindung

Es findet im Uplink eine IQ-Modulation statt wobei drei Datenkanäle den I-Anteil und vier Steuerkanäle den Quadraturanteil bilden. .

Wie später noch dargestellt wird, findet im Downlink ein Zeitmultiplex zwischen Daten und Steuerkanälen statt.

UL Mapping | DL Mapping

RB Identity	1	2	3	4	6	7	8
Use of RB	RLC				SPEECH		
RLC Mode	UM	AM			TM		
Transport Ch. Id	32	32	32	32	1	2	3
Transport Ch. Type	DL-DCH						
Logical Ch. Id	2	3	4	5	0	0	0
Logical Ch. Type	DCCH				DTCH		

Tr. Channel Type	DL-DCH			
Tr. Channel Identity	1	2	3	32
Phy. Channel Type	DL_DPCH			
Phy. Channel Identity	0	0	0	0
Config Type	Configured			
Bler target	- 20	- 63		- 20
TTI (ms)	20ms			40ms
Coding Type	1/3 CONV		1/2 CONV	1/3 CONV
RM Attributes	179	169	214	184
CRC size	12 bits	0 bit		16 bits
TF Number	3	2		

Bild 18: Downlink-Kanäle einer UMTS Telephonieverbindung

5. Funkrahmen und Zeitschlitze

Auf der Luftschnittstelle werden Funkrahmen mit einer Dauer von 10 ms ausgesendet. Jeder Rahmen enthält 15 Slots mit insgesamt 38400 Chips enthalten. (Bild 19 a)

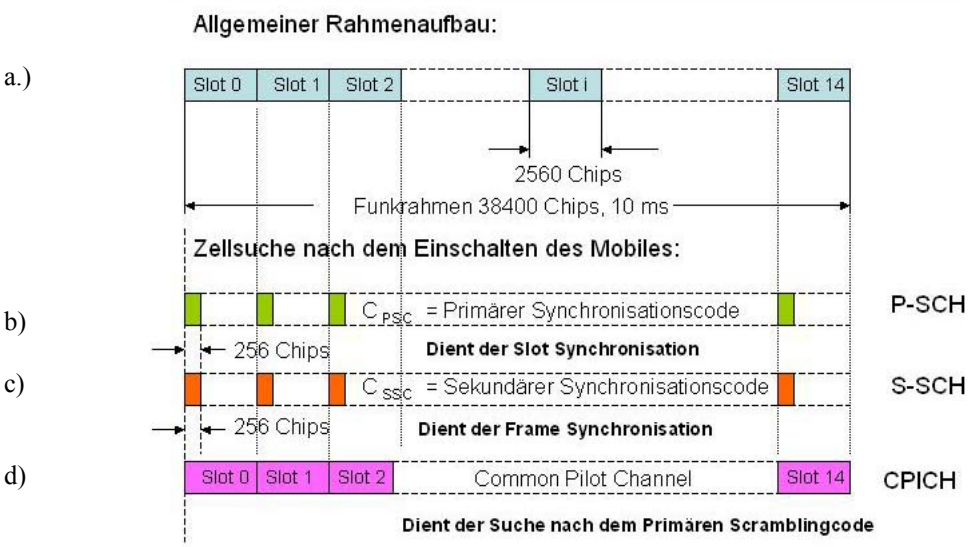


Bild 19: Allgemeiner Rahmenaufbau und Synchronisatiopnscodes

5.1 Einschalten des Mobiles

5.1.1 Zeitschlitzsynchronisation

Die Basis-Stationen aller Operatoren (Provider) strahlen auf dem Primären Synchronisationskanal P-SCH den Primären Synchronisations-Code C_{PSC} aus. (Bild 19 b)
Nach dem Einschalten sucht das Mobile das gesamte UMTS-FDD Frequenzband nach dem stärksten Sender ab, der den Primären Synchronisationscode ausstrahlt.
Mit diesem Sender stellt das Mobile Slot-Synchronisation her.

5.1.2 Rahmensynchronisation

Der Sekundäre Synchronisationscode (SS) besteht aus 256 Chips, die in 16 Code-Mustern (SSC) zur Verfügung stehen. Diese 16 Kodes sind dem Mobile bekannt. In jedem Zeitschlitz wird ein anderer SSC ausgesendet. (Bild 19 c)
Die 16 verschiedenen SCC‘s können 64 eindeutige sekundäre SCH Sequenzen bilden. Eine Sequence besteht aus 15 SCC‘s und diese Sequenzen sind so angeordnet, dass bei einer weniger als 15 fachen zyklischen Verschiebung keine Äquivalenz zu einer der anderen 63 Sequenzen entsteht.
Das bedeutet, dass das Mobile, nachdem es 15 sukzessive SCC‘s identifiziert hat, die Kodegruppe bestimmen kann und damit die Rahmengrenzen, wodurch die Rahmensynchronisation möglich ist.
Gemäß TS 25.213
sieht die Gruppe 6 so aus: (1 4 11 3 4 10 9 2 11 2 10 12 12 9 13).

5.1,3 Feststellen des Scramblingcodes

Anhand der Scramblingcodes könne Mobiles Basisstationen unterscheiden
Es existieren 512 verschiedene primäre Scramblingcodes. Es wird vorausgesetzt, dass diese Anzahl für die UMTS Netzplanung ausreicht. Diese 512 Codes sind in 64 Gruppen à 8 Codes eingeteilt.
Bei der Auswertung des sekundären Synchronisationscodes wurde bereits die Gruppe des primären Scramblingcodes gefunden. Damit muss nun nur noch der für die Zelle gültige Code, aus einer Gruppe von 8 Codes ausgewählt werden.

Im Sinne dieser Auswahl wird eine Scheindatenfolge von logischen Nullen mit dem Spreizcode $C_{ch,256,0}$ moduliert.
Das Ergebnis ist eine Folgen von Nullen. Diese Nullenfolge wird mit dem primären Scramblingkode der Zelle multipliziert (XOR), auf 38400 Chips begrenzt und als CPICH (Bild 19 d) ausgestrahlt.
Das Modulationsergebnis ist der reine primäre Scramblingcode

Durch Korrelation des CPICH mit den 8 mögliche Scramblingcodes der Zelle wird der gültige Code gefunden worauf nun die Systeminformationen auf dem P-CCPCH gelesen und ausgewertet werden können

5.2 Das Mobile im idle-Mode

5.2.1 Der BCH-Transportkanal

Im P-CCPCH (Primary Common Control Physical Channel) überträgt das Netz die Systeminformationen des BCH Transportkanals. Die ersten 256 Chips eines Slots werden durch Impulse des Primären Synchronisationscodes dargestellt. Gleichzeitig werden auf diesen Raum die mit (1+j) multiplizierten Impulse des Sekundären Synchronisationscodes gemultiplext.

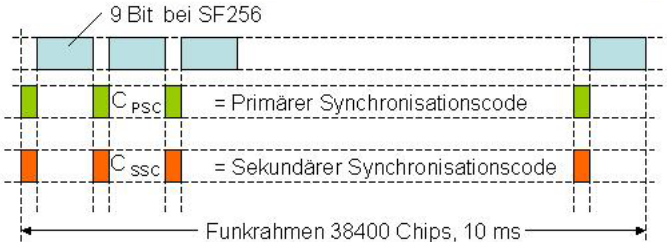


Bild 20: Rahmenaufbau des Primary Common Control Physical Channel

Die Nutzdatenrate des P-CCPCH beträgt ca. 13,5 kbit/sec.

5.2.2 Der Paging-Kanal

Der S-CCPCH (Secondary Common Control Physical Channel) fasst gemäß Bild 15 den PCH (Paging Channel) und den FACH (Forward Access Channel) zusammen.

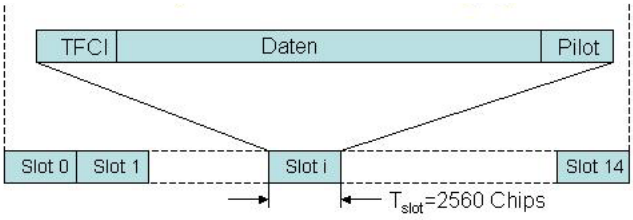


Bild 21: Rahmenaufbau des Secondary Common Control Physical Channel

Die beim Paging übertragenen Daten sind im Bild 22 dargestellt.

```
_____[ 1 ]_____[ group ID: 00 07 ]_____[ trace ID: 00 01 ]______

00 02 00 f0  40 c3 26 02  cf 88 00 00  00 00 00 00  00 00 00 00
00 00 00 00  00 00 00 00  00 00 00 00  00 00

:WDCMA L3 RRC Peer messages
00  00000000  Channel LSB
:Channel Type MSB
02  00000010  PCCH
00  0000000011110000  length=240
00          0  MESSAGE TYPE: PAGING TYPE 1
            1  sw1 present
            0  sw2 not present
            0  sw3 not present
 1..8 Paging records
          000  val1: 0
            0  cn-Identity
:Paging cause
          110  terminatingCauseUnknown
:Cn-Domain identity
            0  cs-domai
```

```
:cn-pagedUE-Identity
         001  TMSI-GSM-MAP
    10010011  hex
    00000001  hex
    01100111  hex
     11000100  hex
```

Bild 22: Trace eines Paging Signals

Über Transportformate und den Transportformat Identifier TFCI, sowie die Pilotbits die bei Datenübertragung über den FACH eine Rolle spielen, soll hier nicht eingegangen werden.

5.3 Verbindungsaufbau

Im GSM/GPRS/EDGE wurde zum Zwecke der Verbindungsaufnahme vom Mobile ein Accessburst gesendet, der vom Netz mit der Meldung IMMIDIATE ASSIGNMENT beantwortet wird.
Eine solche Methode scheidet im UMTS aus, da das Netz sehr empfindlich gegenüber Signalen zu großer Leistung ist. Es muss vielmehr beim Netz auf dem PRACH (Physical Random Access Channel) mit zunächst niedriger und danach, bei nicht Erhörung, mit höherer Leistung angeklopft werden.

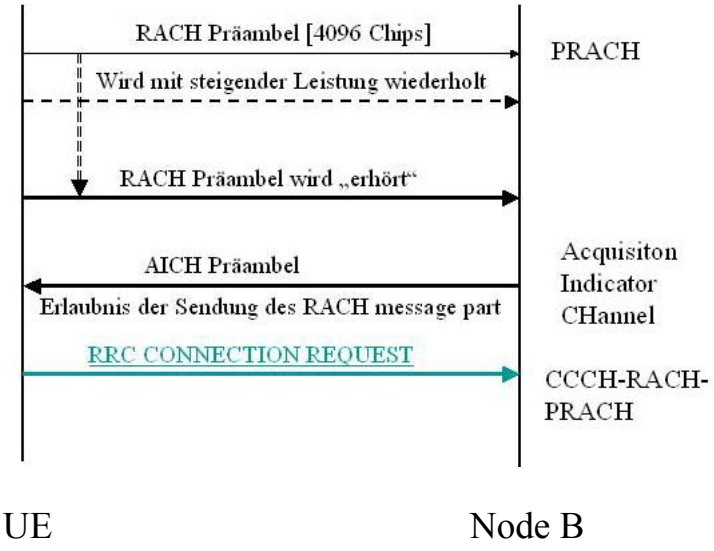


Bild 23: Anklopfen beim Netz zur Verbindungsaufnahme

Wird die RACH Präambel vom Netz richtig empfangen, erhält das Mobile auf dem AICH (Acquisition Indicator Channel)die Erlaubnis einen RRC CONNECTION REQUEST zu senden.

5.4 Das Mobile im Connect-Mode

5.4.1 Uplink-Kanäle

Die Subkanäle DPDCH und PPCCH werden durch I Q Modulation übertragen (Bild 24). Die maximale Übertragungsrate eines DPDCH im Uplink beträgt 480 kbit/s. Die FBI-Bits tragen die *Feedback Information*. Das Transportformat wird durch den *Tranport Format Combination Indicator* TFCI angegeben. Die TPC .Bits (*Transmit Power Control*) dienen der Steuerung der Sendeleistung..

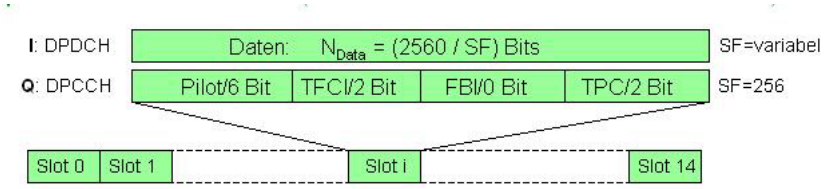


Bild 24: Rahmenaufbau des Uplink DPCH

5.4.2 Downlink-Kanäle

Der DPCH als einer der meist eingesetzten Kanäle besteht aus zwei physikalischen Subkanälen, dem DPDCH (*Dedicated Physical Data Channel*) und dem DPCCH (*Dedicated Physical Control Channel)*(Bild 25) . Wie im UPLINK wird das Transportformat durch den *Tranport Format Combination Indicator* TFCI angegeben und die TPC .Bits (*Transmit Power Control*) dienen der Steuerung der Sendeleistung..
Die Übertragungsrate kann 49 verschiedenen Formaten genügen, d.h. von 1,5 kbit/s bis zu theoretisch 936 kbit/sec.

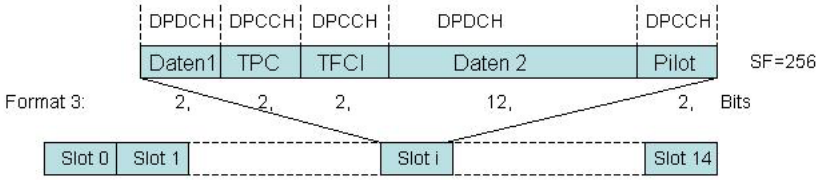


Bild 25: Rahmenaufbau des Downlink DPCH

6. Informationsaustausch auf der Luftschnittstelle

Die nachstehenden Aufzeichnungen wurden anhand von exportierten Tracefiles gemacht, die freundlicherweise von der Fa. SAGEM zur Verfügung gestellt wurden.
Die im Abschnitt 8 vorgestellten Übersetzungen von Tracefiles wurden nicht von den hier dargestellten Files abgeleitet.

6.1 Idle Mode

Ein UMTS-Trace-Mobile zeichnet im Leerlauf Meldungen auf, wie im Bild 26 dargestellt.

1	Stamp	Dir	Type Message	Message	Rb Id	Size (bits)	Data
2	58708	DOWN	BCCH_BCH_Message		0	246	D1 64 53 00 00
3	58710	DOWN	BCCH_BCH_Message		0	205	D1 8E 00 AC 1(
4	58710	DOWN	MasterInformationBlock		0	173	10 82 00 24 00 (
5	58712	DOWN	BCCH_BCH_Message		0	246	D1 A6 54 D5 00
6	58714	DOWN	BCCH_BCH_Message		0	121	D1 CE 1B 58 01
7	58716	DOWN	BCCH_BCH_Message		0	15	D1 E0
8	58718	DOWN	BCCH_BCH_Message		0	205	D2 0E 00 AC 1(
9	58720	DOWN	BCCH_BCH_Message		0	15	D2 20
10	58722	DOWN	BCCH_BCH_Message		0	15	D2 40
11	58724	DOWN	BCCH_BCH_Message		0	15	D2 60
12	58726	DOWN	BCCH_BCH_Message		0	205	D2 8E 00 AC 1(
13	58728	DOWN	BCCH_BCH_Message		0	15	D2 A0
14	58730	DOWN	BCCH_BCH_Message		0	15	D2 C0
15	58732	DOWN	BCCH_BCH_Message		0	15	D2 E0
16	58734	DOWN	BCCH_BCH_Message		0	205	D3 0E 00 AC 1(
17	58736	DOWN	BCCH_BCH_Message		0	15	D3 20
18	58738	DOWN	BCCH_BCH_Message		0	15	D3 40
19	58740	DOWN	BCCH_BCH_Message		0	15	D3 60
20	58742	DOWN	BCCH_BCH_Message		0	205	D3 8E 00 AC 1(
21	58744	DOWN	BCCH_BCH_Message		0	15	D3 A0
22	58746	DOWN	BCCH_BCH_Message		0	15	D3 C0
23	58748	DOWN	BCCH_BCH_Message		0	15	D3 E0
24	58750	DOWN	BCCH_BCH_Message		0	205	D4 0E 00 AC 1(
25	58752	DOWN	BCCH_BCH_Message		0	52	D4 2E 07 13 41
26	58754	DOWN	BCCH_BCH_Message		0	108	D4 4E 03 4B 00
27	58754	DOWN	SysInfoType3		0	76	00 64 29 04 42 (
28	58756	DOWN	BCCH_BCH_Message		0	246	D4 62 BE 80 3(
29	58758	DOWN	BCCH_BCH_Message		0	205	D4 8E 00 AC 1(
30	58760	DOWN	BCCH_BCH_Message		0	246	D4 A4 B0 BB B

Bild 26: Meldungen die ein Mobile im Idle Mode empfängt

Der Inhalt der BCCH-Messages wird im Abschnitt 7 beschrieben.

6.2 Attach im CS-Mode

In den nachfolgenden Bildern sind zur besseren Übersicht die Meldungen farbig hinterlegt.
Mit gelber Farbe sind Meldungen gekennzeichnet, die aus dem GSM/GPRS bekannt sind.
Liest man allein diese Meldungen, so erschließt sich bereits der Sinn der Kommunikation.
Grün (wie Gras) sind alle UPLINK Meldungen markiert, und
blau (wie der Himmel) sind Meldungen gefärbt die vom Netz, also von oben kommen.

Im vorliegenden Fall, eines MOC (Mobile Originated Call) muss sich das Mobile als erstes beim Netz anmelden. Dazu wird gemäß Abschnitt 5.3 beim Netz angeklopft und nach

erfolgter Erlaubnis wird die Meldung RRC CONNECTION REQUEST ausgesandt. (Zeile 117).
In Zeile 121 sendet das Netz die umfangreiche Vorschrift, welche Parameter das Mobile einstellen muss, damit eine Verständigung mit dem Netz möglich ist. Die Meldung wird in 3 Paketen im RLC Unacknowledge Mode übertragen.
Die Meldung des Mobiles über die erfolgte Einstellung ist kürzer, daher ist nur ein Paket uplink (im Acknowledge Mode) erforderlich.

Die NAS-Meldung LOCATION UPDATING REQUEST.. wird eingehüllt in der Meldung INITIAL DIRECT TRANSFER (sie ist die erste NAS-Meldung) an das Netz übertragen .

Lfd Nr.	Timestamp	Dir	Type Message	Message	Rb Id	Size (bits)	Data
115	58923	DOWN	BCCH_BCH_Message		0	246	DE C6 BD D5 00 00 00 00
116	58923	DOWN	SysInfoType11		0	509	80 3D F1 45 CC 2D BB 26
117	58940	UP	UL_CCCH_M	RRC CONNECTION REQUEST	0	166	31 00 05 9A 06 20 80 0C E
118	58974	DOWN	RLC UM	MAC_DATA_IND (3 Pdu) (C-C-C)	0	160	53 F8 30 E7 20 00 B3 40 C
119	58975	DOWN	RLC UM	MAC_DATA_IND (3 Pdu) (C-C-C)	0	160	58 D3 E6 94 F9 C6 CF 48 .
120	58976	DOWN	RLC UM	MAC_DATA_IND (1 Pdu) (C)	0	160	5F 05 FE C1 40 00 00 00 C
121	58977	DOWN	DL_CCCH_M	RRC CONNECTION SETUP	0	920	30 E7 20 00 B3 40 C4 10 C
122	58986	UP	UL_DCCH_M	RRC CONNECTION SETUP COMPLETE	2	296	4B 08 00 00 A0 00 05 11 A
123	58986	UP	RLC AM	MAC_DATA_REQ (3 Pdu) (D-D-D)	2	144	80 00 4B 08 00 00 A0 00 0
124	58986	UP	MM	LOCATION UPDATING REQUEST		160	05 08 02 02 F8 10 96 06 47
125	58986	UP	UL_DCCH_M	INITIAL DIRECT TRANSFER	3	224	15 00 16 00 98 28 40 10 17
126	58986	UP	RLC AM	MAC_DATA_REQ (2 Pdu) (D-D)	3	144	80 00 15 00 16 00 98 28 40
127	59033	DOWN	RLC AM	MAC_DATA_IND (1 Pdu) (C)	2	144	03 10 00 12 00 3F FF FF F
128	59033	UP	RLC AM	MAC_DATA_REQ (2 Pdu) (D-D)	2	144	80 00 4B 08 00 00 A0 00 0
129	59041	DOWN	RLC AM	MAC_DATA_IND (1 Pdu) (C)	3	144	02 00 2F FF FF FF FF FF
130	59069	DOWN	RLC AM	MAC_DATA_IND (1 Pdu) (C)	2	144	02 00 3F FF FF FF FF FF
131	59077	DOWN	RLC AM	MAC_DATA_IND (1 Pdu) (D)	2	144	80 00 EE F0 98 F1 8C 0E I
132	59081	DOWN	RLC AM	MAC_DATA_IND (1 Pdu) (D)	2	144	80 0D 15 FE 00 00 C0 02 C
133	59081	UP	RLC AM	MAC_DATA_REQ (1 Pdu) (C)	2	144	02 00 20 FF FF FF FF FF
134	59081	DOWN	DL_DCCH_M	SECURITY MODE COMMAND	2	208	EE F0 98 F1 8C 0E 00 01 I
135	59081	UP	UL_DCCH_M	SECURITY MODE COMPLETE	2	144	A8 BE 46 5C 8D 31 00 00 I
136	59081	UP	RLC AM	MAC_DATA_REQ (2 Pdu) (D-D)	2	144	80 18 A8 BE 46 5C 8D 31 I
137	59121	DOWN	RLC AM	MAC_DATA_IND (1 Pdu) (C)	2	144	02 00 5F FF FF FF FF FF
138	59125	DOWN	RLC AM	MAC_DATA_IND (1 Pdu) (D)	3	144	80 00 D6 8C 83 C8 09 40 C
139	59129	DOWN	RLC AM	MAC_DATA_IND (1 Pdu) (D)	3	144	80 08 FF FF FF FF FF FF
140	59133	DOWN	RLC AM	MAC_DATA_IND (1 Pdu) (D)	3	144	80 15 01 FE FF FF FF FF
141	59133	UP	RLC AM	MAC_DATA_REQ (1 Pdu) (C)	3	144	02 00 30 FF FF FF FF FF
142	59133	DOWN	DL_DCCH_M	DOWNLINK DIRECT TRANSFER	3	256	D6 8C 83 C8 09 40 02 E0 A
143	59133	DOWN	MM	LOCATION UPDATING ACCEPTED		192	05 02 02 F8 10 96 06 4A 0
144	59137	DOWN	RLC UM	MAC_DATA_IND (1 Pdu) (C)	1	144	01 F9 0F FE A1 9C C0 A8
145	59137	DOWN	DL_DCCH_M	RRC CONNECTION RELEASE	1	56	A1 9C C0 A8 8B C8 00
146	59137	UP	UL_DCCH_M	RRC CONNECTION RELEASE COMPLETI	1	48	FC 70 9D F9 8C 40
147	59137	UP	RLC UM	MAC_DATA_REQ (1 Pdu) (C)	1	144	01 0D FE FC 70 9D F9 8C
148	59153	UP	UL_DCCH_M	RRC CONNECTION RELEASE COMPLETI	1	48	91 F3 5E E5 94 40
149	59153	UP	RLC UM	MAC_DATA_REQ (1 Pdu) (C)	1	144	03 0D FE 91 F3 5E E5 94

Bild 27: Meldungen die beim Attach im CS-Mode mit dem Netz ausgetauscht werden.

Es erfolgt die Einstellung des Security Mode in den Zeilen 134 135. Eingepackt in die Meldung DOWNLINK DIRECT TRANSFER sendet das Netz ein LOCATION UPDATING ACCEPT. Anschließend wir vom Netz die Verbindung aufgelöst.

6.3. Attach im PS-Mode

Zwischen den Zeilen 149 und 217 geht das Mobile wieder in den Idle Mode über. Nach dem Attach im CS-Mode wird nun Attach im PS-Mode ausgeführt. Bitte betrachten Sie das Procedere anhand der gelben Eintragungen. Die typischen UMTS-Meldungen sind wieder RRC CONNECTION REQUEST, RRC CONNECTION SETUP, RRC CONNECTION SETUP COMPLETE, die Meldungen DOWNLINK- und UPLINK DIRECT TRANSFER für den Transport der NAS-Messages, SECURITY MODE COMMAND und SECURITY

MODE COMPLETE und wieder RRC CONNECTION RELEASE und RRC CONNECTION RELEASE COMPLETE.

Lfd Nr	Timestamp	Dir	Type Message	Message	Rb Id	Size (bits)	Data
216	59308	DOWN	SysInfoType11		0	509	80 3D F1 45 CC
217	59322	UP	UL_CCCH_Message	RRC CONNECTION REQUEST	0	166	32 C0 12 60 82
218	59355	DOWN	RLC UM	MAC_DATA_IND (3 Pdu) (C-C-C)	0	160	61 F8 30 E7 58
219	59356	DOWN	RLC UM	MAC_DATA_IND (3 Pdu) (C-C-C)	0	160	66 53 D3 E6 94
220	59357	DOWN	RLC UM	MAC_DATA_IND (1 Pdu) (C)	0	160	6D 07 FE 00 C1
221	59357	DOWN	DL_CCCH_Message	RRC CONNECTION SETUP	0	928	30 E7 58 02 4C
222	59367	UP	UL_DCCH_Message	RRC CONNECTION SETUP COMPLETE	2	296	4B 08 00 01 20
223	59367	UP	RLC AM	MAC_DATA_REQ (3 Pdu) (D-D-D)	2	144	80 00 4B 08 00
224	59368	UP	GMM	ATTACH REQUEST		288	08 01 02 C5 00
225	59368	UP	UL_DCCH_Message	INITIAL DIRECT TRANSFER	3	352	15 80 49 01 18
226	59368	UP	RLC AM	MAC_DATA_REQ (3 Pdu) (D-D-D)	3	144	80 00 15 80 49
227	59417	DOWN	RLC AM	MAC_DATA_IND (1 Pdu) (C)	2	144	02 00 3F FF FF
228	59429	DOWN	RLC AM	MAC_DATA_IND (1 Pdu) (C)	3	144	02 00 3F FF FF
229	59433	DOWN	RLC AM	MAC_DATA_IND (1 Pdu) (D)	3	144	80 00 14 20 4E
230	59437	DOWN	RLC AM	MAC_DATA_IND (1 Pdu) (D)	3	144	80 08 AD 6B A9
231	59441	DOWN	RLC AM	MAC_DATA_IND (1 Pdu) (D)	3	144	80 15 17 FE BC
232	59441	UP	RLC AM	MAC_DATA_REQ (1 Pdu) (C)	3	144	02 00 30 FF FF
233	59441	DOWN	DL_DCCH_Message	DOWNLINK DIRECT TRANSFER	3	344	14 20 4E 10 24
234	59441	DOWN	GMM	AUTHENTICATION AND CIPHERING REQUEST		320	08 12 00 50 21
235	59573	UP	GMM	AUTHENTICATION AND CIPHERING RESPONSE		112	08 13 05 22 C6
236	59573	UP	UL_DCCH_Message	UPLINK DIRECT TRANSFER	3	136	6C 80 68 40 98
237	59573	UP	RLC AM	MAC_DATA_REQ (2 Pdu) (D-D)	3	144	80 18 6C 80 68
238	59610	DOWN	RLC AM	MAC_DATA_IND (1 Pdu) (C)	3	144	02 00 5F FF FF
239	59614	DOWN	RLC AM	MAC_DATA_IND (1 Pdu) (D)	2	144	80 00 D1 FE EA
240	59618	DOWN	RLC AM	MAC_DATA_IND (1 Pdu) (D)	2	144	80 0D 15 FE 00
241	59618	UP	RLC AM	MAC_DATA_REQ (1 Pdu) (C)	2	144	02 00 20 FF FF
242	59618	DOWN	DL_DCCH_Message	SECURITY MODE COMMAND	2	208	D1 FE EA 00 80
243	59618	UP	UL_DCCH_Message	SECURITY MODE COMPLETE	2	144	EA 65 41 2A 0D
244	59618	UP	RLC AM	MAC_DATA_REQ (2 Pdu) (D-D)	2	144	80 18 EA 65 41
245	59658	DOWN	RLC AM	MAC_DATA_IND (1 Pdu) (C)	2	144	02 00 5F FF FF
246	59662	DOWN	RLC AM	MAC_DATA_IND (1 Pdu) (D)	3	144	80 18 A1 4F 2F
247	59666	DOWN	RLC AM	MAC_DATA_IND (1 Pdu) (D)	3	144	80 25 1D FE CD
248	59666	UP	RLC AM	MAC_DATA_REQ (1 Pdu) (C)	3	144	02 00 50 FF FF
249	59666	DOWN	DL_DCCH_Message	DOWNLINK DIRECT TRANSFER	3	240	A1 4F 2F 3E 89
250	59666	DOWN	GMM	ATTACH ACCEPT		176	08 02 01 3E 04
251	59666	UP	GMM	ATTACH COMPLETE		16	08 03
252	59666	UP	UL_DCCH_Message	UPLINK DIRECT TRANSFER	3	80	FB 63 EA 56 0E
253	59666	UP	RLC AM	MAC_DATA_REQ (1 Pdu) (D)	3	144	80 2D 15 FE FE
254	59702	DOWN	RLC AM	MAC_DATA_IND (1 Pdu) (C)	3	144	02 00 6F FF FF
255	59706	DOWN	RLC AM	MAC_DATA_IND (1 Pdu) (D)	3	144	80 28 FB 7F E8
256	59710	DOWN	RLC AM	MAC_DATA_IND (1 Pdu) (D)	3	144	80 35 1E A5 D0
257	59710	UP	RLC AM	MAC_DATA_REQ (1 Pdu) (C)	3	144	02 00 70 FF FF
258	59710	DOWN	DL_DCCH_Message	DOWNLINK DIRECT TRANSFER	3	248	FB 7F E8 2E 11
259	59710	DOWN	GMM	GMM INFORMATION		184	08 21 43 09 89
260	59714	DOWN	RLC UM	MAC_DATA_IND (1 Pdu) (C)	1	144	01 F9 0F FE 89
261	59714	DOWN	DL_DCCH_Message	RRC CONNECTION RELEASE	1	56	89 D9 2F 8A 8E
262	59714	UP	UL_DCCH_Message	RRC CONNECTION RELEASE COMPLETI	1	48	B9 E8 7D 68 0C

Bild 28: Meldungen die beim Attach im PS-Mode mit dem Netz ausgetauscht werden.

Danach geht das Mobile wieder bis zur Zeile 393 in den idle Mode über.

6.4 Das Telephoniesetup

Der Trace musste aus Platzgründen getrennt werden. Im ersten Teil (auf dieser Seite gibt es keine neuen UMTS-Meldungen. Es dominieren die aus dem GSM bekannten NAS-Messages.

Lfd Nr	Timestamp	Dir	Type Message	Message	Rb Id	Size (bits)	Data
393	61750	UP	UL_CCCH_M	RRC CONNECTION REQUEST	0	166	31 00 05 9A 06 20 80 0C E
394	61786	DOWN	RLC UM	MAC_DATA_IND (3 Pdu) (C-C-C)	0	160	6F F8 30 E7 20 00 B3 40 C
395	61788	DOWN	RLC UM	MAC_DATA_IND (3 Pdu) (C-C-C)	0	160	74 D3 E6 94 F9 C6 CF 48 .
396	61788	DOWN	RLC UM	MAC_DATA_IND (1 Pdu) (C)	0	160	7B 05 FE C1 40 00 00 00 0
397	61789	DOWN	DL_CCCH_M	RRC CONNECTION SETUP	0	920	30 E7 20 00 B3 40 C4 10 0
398	61798	UP	UL_DCCH_M	RRC CONNECTION SETUP COMPLETE	2	296	4B 08 00 01 20 00 05 11 A
399	61798	UP	RLC AM	MAC_DATA_REQ (3 Pdu) (D-D-D)	2	144	80 00 4B 08 00 01 20 00 0
400	61798	UP	MM	CM SERVICE REQUEST		104	05 24 01 03 47 18 80 05 F
401	61798	UP	UL_DCCH_M	INITIAL DIRECT TRANSFER	3	168	15 00 16 00 60 29 20 08 1
402	61798	UP	RLC AM	MAC_DATA_REQ (2 Pdu) (D-D)	3	144	80 00 15 00 16 00 60 29 2
403	61846	DOWN	RLC AM	MAC_DATA_IND (1 Pdu) (C)	2	144	02 00 3F FF FF FF FF FF
404	61854	DOWN	RLC AM	MAC_DATA_IND (1 Pdu) (C)	3	144	02 00 2F FF FF FF FF FF
405	61862	DOWN	RLC AM	MAC_DATA_IND (1 Pdu) (D)	3	144	80 00 14 00 48 0A 24 04 C
406	61866	DOWN	RLC AM	MAC_DATA_IND (1 Pdu) (D)	3	144	80 08 30 7E F9 5B 55 98 4
407	61870	DOWN	RLC AM	MAC_DATA_IND (1 Pdu) (D)	3	144	80 15 11 FE CC 57 88 F9 E
408	61870	UP	RLC AM	MAC_DATA_REQ (1 Pdu) (C)	3	144	02 00 30 FF FF FF FF FF
409	61870	DOWN	DL_DCCH_M	DOWNLINK DIRECT TRANSFER	3	320	14 00 48 0A 24 04 C6 A0 3
410	61870	DOWN	MM	AUTHENTICATION REQUEST		296	05 12 02 63 50 1F 86 2F F
411	61906	UP	MM	AUTHENTICATION RESPONSE		96	05 54 EA DB B3 FA 21 04
412	61906	UP	UL_DCCH_M	UPLINK DIRECT TRANSFER	3	120	6C 00 58 2A A7 56 DD 9F
413	61906	UP	RLC AM	MAC_DATA_REQ (1 Pdu) (D)	3	144	80 15 1E 6C 00 58 2A A7 5
414	61938	DOWN	RLC AM	MAC_DATA_IND (1 Pdu) (C)	3	144	02 00 3F FF FF FF FF FF
415	61946	DOWN	RLC AM	MAC_DATA_IND (1 Pdu) (D)	2	144	80 00 8F A4 6F D2 0C 0E
416	61950	DOWN	RLC AM	MAC_DATA_IND (1 Pdu) (D)	2	144	80 0D 15 FE 00 00 C0 02 0
417	61950	UP	RLC AM	MAC_DATA_REQ (1 Pdu) (C)	2	144	02 00 20 FF FF FF FF FF
418	61950	DOWN	DL_DCCH_M	SECURITY MODE COMMAND	2	208	8F A4 6F D2 0C 0E 00 01
419	61951	UP	UL_DCCH_M	SECURITY MODE COMPLETE	2	144	DF B0 FF 4C 8D 31 00 00
420	61951	UP	RLC AM	MAC_DATA_REQ (2 Pdu) (D-D)	2	144	80 18 DF B0 FF 4C 8D 31
421	61990	DOWN	RLC AM	MAC_DATA_IND (1 Pdu) (C)	2	144	02 00 5F FF FF FF FF FF
422	61990	UP	CC	SETUP		104	03 85 04 01 A0 5E 06 81 1
423	61990	UP	UL_DCCH_M	UPLINK DIRECT TRANSFER	3	168	C7 C2 63 DD 8E C0 06 01
424	61990	UP	RLC AM	MAC_DATA_REQ (2 Pdu) (D-D)	3	144	80 18 C7 C2 63 DD 8E C0
425	61994	DOWN	RLC AM	MAC_DATA_IND (1 Pdu) (D)	3	144	80 1D 17 FE EF AB 57 AE
426	61994	UP	RLC AM	MAC_DATA_REQ (1 Pdu) (C)	3	144	02 00 40 FF FF FF FF FF
427	61994	DOWN	DL_DCCH_M	DOWNLINK DIRECT TRANSFER	3	88	EF AB 57 AE 89 40 00 40
428	61994	DOWN	MM	IDENTITY REQUEST		24	05 18 03
429	61994	UP	MM	IDENTITY RESPONSE		96	05 D9 09 33 03 01 02 03 0
430	61994	UP	UL_DCCH_M	UPLINK DIRECT TRANSFER	3	160	BB DB 24 AA 96 C0 05 82
431	61995	UP	RLC AM	MAC_DATA_REQ (2 Pdu) (D-D)	3	144	80 28 BB DB 24 AA 96 C0
432	62026	DOWN	RLC AM	MAC_DATA_IND (1 Pdu) (C)	3	144	02 00 5F FF FF FF FF FF
433	62030	DOWN	RLC AM	MAC_DATA_IND (1 Pdu) (D)	3	144	80 25 15 FE 9C 1E D0 D2
434	62030	UP	RLC AM	MAC_DATA_REQ (1 Pdu) (C)	3	144	02 00 50 FF FF FF FF FF
435	62030	DOWN	DL_DCCH_M	DOWNLINK DIRECT TRANSFER	3	80	9C 1E D0 D2 91 40 00 30 6
436	62030	DOWN	CC	CALL PROCEEDING		16	83 02
437	62046	DOWN	RLC AM	MAC_DATA_IND (1 Pdu) (C)	3	144	02 00 7F FF FF FF FF FF
438	62054	DOWN	RLC AM	MAC_DATA_IND (1 Pdu) (D)	2	144	80 10 86 B2 D8 99 93 82 0
439	62058	DOWN	RLC AM	MAC_DATA_IND (1 Pdu) (D)	2	144	80 18 A8 0A 2B 88 30 32 E
440	62062	DOWN	RLC AM	MAC_DATA_IND (1 Pdu) (D)	2	144	80 20 12 62 41 49 A9 2D 2
441	62066	DOWN	RLC AM	MAC_DATA_IND (1 Pdu) (D)	2	144	80 28 0A 20 47 A2 86 10 8
442	62070	DOWN	RLC AM	MAC_DATA_IND (1 Pdu) (D)	2	144	80 30 00 1E 01 17 50 20 8
443	62074	DOWN	RLC AM	MAC_DATA_IND (1 Pdu) (D)	2	144	80 38 86 8D 5C 3C 7A C1

Bild 29: Meldungen beim Aufbau einer Telefonieverbindung. Teil1/3

Nach der Meldung SETUP in Zeile 422 und dem CALL PROCEEDING in Zeile 436 sendet das Netz in Zeile 446 (bild 25) die Einstellvorschrift für die notwendige Kommunikation mit der Meldung RADIO BEARER SETUP.

Wie aus der vorletzten Spalte rechts in Bild 25 hervorgeht ist diese Einstellvorschrift mit 800 bit nicht ganz so groß wie übertragenen Bits der Meldung RRC CONNECTION SETUP mit 920 Bit.

In Bild 30 treten 4 neue Meldungen auf. Das sind: MEASUREMENT CONTROL und MEASUREMENT REPORT, sowie ACTIVE SET UPDATE und ACTIVE SET UPDATE COMPLETE.

Lfd Nr	Timestamp	Dir	Type Message	Message	Rb Id	Size (bits)	Data
444	62078	DOWN	RLC AM	MAC_DATA_IND (1 Pdu) (D)	2	144	80 45 09 FE C0 0A 14 00 F
445	62078	UP	RLC AM	MAC_DATA_REQ (1 Pdu) (C)	2	144	02 00 90 FF FF FF FF FF
446	62078	DOWN	DL_DCCH_M	RADIO BEARER SETUP	2	800	86 B2 D8 99 93 82 04 AA 7
447	62163	UP	UL_DCCH_M	RADIO BEARER SETUP COMPLETE	2	80	93 55 59 FB 13 CC 00 00 0
448	62163	UP	RLC AM	MAC_DATA_REQ (1 Pdu) (D)	2	144	80 2D 15 FE 93 55 59 FB 1
449	62195	DOWN	RLC AM	MAC_DATA_IND (1 Pdu) (C)	2	144	02 00 6F FF FF FF FF FF
450	62199	DOWN	RLC AM	MAC_DATA_IND (1 Pdu) (D)	2	144	80 48 B2 FE 65 06 1A 08 3
451	62203	DOWN	RLC AM	MAC_DATA_IND (1 Pdu) (D)	2	144	80 55 01 FE FF FF FF FF
452	62203	UP	RLC AM	MAC_DATA_REQ (1 Pdu) (C)	2	144	02 00 B0 FF FF FF FF FF
453	62203	DOWN	DL_DCCH_M	MEASUREMENT CONTROL	2	128	B2 FE 65 06 1A 08 38 78 8
454	62323	DOWN	RLC AM	MAC_DATA_IND (1 Pdu) (D)	3	144	80 2D 1D FE 82 48 4F 1B 9
455	62323	UP	RLC AM	MAC_DATA_REQ (1 Pdu) (C)	3	144	02 00 60 FF FF FF FF FF
456	62323	DOWN	DL_DCCH_M	DOWNLINK DIRECT TRANSFER	3	112	82 48 4F 1B 99 40 00 B0 6
457	62323	DOWN	CC	ALERTING		48	83 01 1E 02 E4 A0
458	62615	DOWN	RLC AM	MAC_DATA_IND (1 Pdu) (D)	3	144	80 35 15 FE BF 21 90 47 2
459	62615	UP	RLC AM	MAC_DATA_REQ (1 Pdu) (C)	3	144	02 00 70 FF FF FF FF FF
460	62616	DOWN	DL_DCCH_M	DOWNLINK DIRECT TRANSFER	3	80	BF 21 90 47 21 40 00 30 6
461	62616	DOWN	CC	CONNECT		16	83 07
462	62616	UP	CC	CONNECT ACKNOWLEDGE		16	03 0F
463	62616	UP	UL_DCCH_M	UPLINK DIRECT TRANSFER	3	80	C0 39 24 A4 9E C0 00 81 8
464	62616	UP	RLC AM	MAC_DATA_REQ (1 Pdu) (D)	3	144	80 3D 15 FE C0 39 24 A4 9
465	62652	DOWN	RLC AM	MAC_DATA_IND (1 Pdu) (C)	3	144	02 00 8F FF FF FF FF FF
466	63099	UP	UL_DCCH_M	MEASUREMENT REPORT	2	240	F3 E9 51 DF 1A 24 00 45 0
467	63099	UP	RLC AM	MAC_DATA_REQ (2 Pdu) (D-D)	2	144	80 30 F3 E9 51 DF 1A 24 0
468	63137	DOWN	RLC AM	MAC_DATA_IND (1 Pdu) (C)	2	144	02 00 8F FF FF FF FF FF
469	63165	DOWN	RLC AM	MAC_DATA_IND (1 Pdu) (D)	2	144	80 5D 1B FE 81 75 FD 42 .
470	63165	UP	RLC AM	MAC_DATA_REQ (1 Pdu) (C)	2	144	02 00 C0 FF FF FF FF FF
471	63165	DOWN	DL_DCCH_M	ACTIVE SET UPDATE	2	104	81 75 FD 42 A0 00 10 03 1
472	63165	UP	UL_DCCH_M	ACTIVE SET UPDATE COMPLETE	2	48	CC 54 09 BC A0 00
473	63165	UP	RLC AM	MAC_DATA_REQ (1 Pdu) (D)	2	144	80 45 0D FE CC 54 09 BC
474	63201	DOWN	RLC AM	MAC_DATA_IND (1 Pdu) (C)	2	144	02 00 9F FF FF FF FF FF
475	63205	DOWN	RLC AM	MAC_DATA_IND (1 Pdu) (D)	2	144	80 65 1E B1 3A A0 61 2A I
476	63205	UP	RLC AM	MAC_DATA_REQ (1 Pdu) (C)	2	144	02 00 D0 FF FF FF FF FF
477	63205	DOWN	DL_DCCH_M	MEASUREMENT CONTROL	2	120	B1 3A A0 61 2A 08 48 3E 1
478	63209	DOWN	RLC AM	MAC_DATA_IND (1 Pdu) (D)	2	144	80 6D 1D FE A1 9B DA 69
479	63209	DOWN	DL_DCCH_M	MEASUREMENT CONTROL	2	112	A1 9B DA 69 B2 08 21 B4
480	63213	DOWN	RLC AM	MAC_DATA_IND (1 Pdu) (D)	2	144	80 70 A8 57 90 2C BA 00 0
481	63217	DOWN	RLC AM	MAC_DATA_IND (1 Pdu) (D)	2	144	80 78 A0 69 FB 2A 46 98 E
482	63221	DOWN	RLC AM	MAC_DATA_IND (1 Pdu) (D)	2	144	80 85 0B FE 41 64 FB 39 7
483	63221	DOWN	DL_DCCH_M	MEASUREMENT CONTROL	2	296	A8 57 90 2C BA 00 03 11 4
484	63225	UP	RLC AM	MAC_DATA_REQ (1 Pdu) (C)	2	144	02 01 10 FF FF FF FF FF
485	64510	UP	UL_DCCH_M	MEASUREMENT REPORT	2	192	F3 95 2B 1A 2A 24 00 25 0
486	64510	UP	RLC AM	MAC_DATA_REQ (2 Pdu) (D-D)	2	144	80 48 F3 95 2B 1A 2A 24 0
487	64547	DOWN	RLC AM	MAC_DATA_IND (1 Pdu) (C)	2	144	02 00 BF FF FF FF FF FF
488	64551	DOWN	RLC AM	MAC_DATA_IND (1 Pdu) (D)	2	144	80 8D 13 FE C9 DB 5A 2A
489	64551	UP	RLC AM	MAC_DATA_REQ (1 Pdu) (C)	2	144	02 01 20 FF FF FF FF FF
490	64551	DOWN	DL_DCCH_M	ACTIVE SET UPDATE	2	72	C9 DB 5A 2A C0 00 08 09
491	64552	UP	UL_DCCH_M	ACTIVE SET UPDATE COMPLETE	2	48	B2 BD EF A2 B0 00
492	64552	UP	RLC AM	MAC_DATA_REQ (1 Pdu) (D)	2	144	80 5D 0D FE B2 BD EF A2
493	64588	DOWN	RLC AM	MAC_DATA_IND (1 Pdu) (C)	2	144	02 00 CF FF FF FF FF FF
494	64591	DOWN	RLC AM	MAC_DATA_IND (1 Pdu) (D)	2	144	80 95 0F FE 87 1F 68 EC 4
495	64592	UP	RLC AM	MAC_DATA_REQ (1 Pdu) (C)	2	144	02 01 30 FF FF FF FF FF F
496	64592	DOWN	DL_DCCH_M	MEASUREMENT CONTROL	2	56	87 1F 68 EC 4A 00 4C
497	64596	DOWN	RLC AM	MAC_DATA_IND (1 Pdu) (D)	2	144	80 9D 0F FE E0 27 0F 93 D
498	64596	DOWN	DL_DCCH_M	MEASUREMENT CONTROL	2	56	E0 27 0F 93 D2 00 24
499	64600	DOWN	RLC AM	MAC_DATA_IND (1 Pdu) (D)	2	144	80 A0 9B 04 19 EE 5A 00 0
500	64604	DOWN	RLC AM	MAC_DATA_IND (1 Pdu) (D)	2	144	80 AD 0F FE 80 28 2C 9F 8
501	64604	DOWN	DL_DCCH_M	MEASUREMENT CONTROL	2	184	9B 04 19 EE 5A 00 03 11 0
502	64612	DOWN	RLC AM	MAC_DATA_IND (1 Pdu) (D)	2	144	80 B5 0F FE FE F5 5B 1A I
503	64612	UP	RLC AM	MAC_DATA_REQ (1 Pdu) (C)	2	144	02 01 70 FF FF FF FF FF F
504	64612	DOWN	DL_DCCH_M	MEASUREMENT CONTROL	2	56	FE F5 5B 1A 62 00 3C
505	66674	UP	UL_DCCH_M	MEASUREMENT REPORT	2	240	86 43 D7 DC 3A 24 00 45 0
506	66674	UP	RLC AM	MAC_DATA_REQ (2 Pdu) (D-D)	2	144	80 60 86 43 D7 DC 3A 24 0

Bild 30: Meldungen beim Aufbau einer Telephonieverbindung. Teil 2/3

Eine Meldung MEASUREMENT REPORT gibt es bereits im GSM/GPRS/EDGE . Sie meldet dem Netz die Feldstärkeverhältnisse aus der Sicht des Mobiles. Das Netz kann aufgrund dieser Meldung entscheiden wann und zu welcher Zelle ein Handover erforderlich ist.

507	66712	DOWN	RLC AM	MAC_DATA_IND (1 Pdu) (C)	2	144	02 00 EF FF FF FF FF FF
508	66732	DOWN	RLC AM	MAC_DATA_IND (1 Pdu) (D)	2	144	80 BD 1B FE C6 2D 8D 76
509	66732	UP	RLC AM	MAC_DATA_REQ (1 Pdu) (C)	2	144	02 01 80 FF FF FF FF FF
510	66732	DOWN	DL_DCCH_M	ACTIVE SET UPDATE	2	104	C6 2D 8D 76 68 00 10 04
511	66732	UP	UL_DCCH_M	ACTIVE SET UPDATE COMPLETE	2	48	B5 4D 88 47 40 00
512	66732	UP	RLC AM	MAC_DATA_REQ (1 Pdu) (D)	2	144	80 75 0D FE B5 4D 88 47
513	66758	UP	UL_DCCH_M	MEASUREMENT REPORT	2	192	CF 31 84 AA CA 24 00 25
514	66758	UP	RLC AM	MAC_DATA_REQ (2 Pdu) (D-D)	2	144	80 78 CF 31 84 AA CA 24
515	66768	DOWN	RLC AM	MAC_DATA_IND (1 Pdu) (C)	2	144	02 00 FF FF FF FF FF FF
516	66772	DOWN	RLC AM	MAC_DATA_IND (1 Pdu) (D)	2	144	80 C5 1E 8E 91 4C 76 72
517	66772	UP	RLC AM	MAC_DATA_REQ (1 Pdu) (C)	2	144	02 01 90 FF FF FF FF FF
518	66772	DOWN	DL_DCCH_M	MEASUREMENT CONTROL	2	120	8E 91 4C 76 72 08 48 3E
519	66776	DOWN	RLC AM	MAC_DATA_IND (1 Pdu) (D)	2	144	80 CD 1D FE B7 0D 69 7B
520	66776	DOWN	DL_DCCH_M	MEASUREMENT CONTROL	2	112	B7 0D 69 7B FA 08 21 B4
521	66780	DOWN	RLC AM	MAC_DATA_IND (1 Pdu) (D)	2	144	80 D0 85 5E BA 46 82 00
522	66784	DOWN	RLC AM	MAC_DATA_IND (1 Pdu) (D)	2	144	80 DD 0F FE 80 28 2C 9F
523	66784	DOWN	DL_DCCH_M	MEASUREMENT CONTROL	2	184	85 5E BA 46 82 00 03 11
524	66792	UP	RLC AM	MAC_DATA_REQ (1 Pdu) (C)	2	144	02 01 C0 FF FF FF FF FF
525	66796	DOWN	RLC AM	MAC_DATA_IND (1 Pdu) (C)	2	144	02 01 1F FF FF FF FF FF
526	66800	DOWN	RLC AM	MAC_DATA_IND (1 Pdu) (D)	2	144	80 E5 13 FE D3 92 15 80
527	66800	DOWN	DL_DCCH_M	ACTIVE SET UPDATE	2	72	D3 92 15 80 08 00 08 06
528	66800	UP	UL_DCCH_M	ACTIVE SET UPDATE COMPLETE	2	48	FF BA 3F E2 D0 00
529	66800	UP	RLC AM	MAC_DATA_REQ (1 Pdu) (D)	2	144	80 8D 0D FE FF BA 3F E2
530	66812	UP	RLC AM	MAC_DATA_REQ (1 Pdu) (C)	2	144	02 01 D0 FF FF FF FF FF
531	66832	DOWN	RLC AM	MAC_DATA_IND (1 Pdu) (C)	2	144	02 01 2F FF FF FF FF FF
532	66836	DOWN	RLC AM	MAC_DATA_IND (1 Pdu) (D)	2	144	80 ED 0F FE CB B3 07 0C
533	66836	UP	RLC AM	MAC_DATA_REQ (1 Pdu) (C)	2	144	02 01 E0 FF FF FF FF FF
534	66836	DOWN	DL_DCCH_M	MEASUREMENT CONTROL	2	56	CB B3 07 0C 12 00 4C
535	66840	DOWN	RLC AM	MAC_DATA_IND (1 Pdu) (D)	2	144	80 F5 0F FE 83 D7 D9 BB
536	66840	DOWN	DL_DCCH_M	MEASUREMENT CONTROL	2	56	83 D7 D9 BB 1A 00 24
537	66844	DOWN	RLC AM	MAC_DATA_IND (1 Pdu) (D)	2	144	80 F8 C7 79 71 51 A2 00
538	66848	DOWN	RLC AM	MAC_DATA_IND (1 Pdu) (D)	2	144	81 05 15 FE 09 77 10 90
539	66848	DOWN	DL_DCCH_M	MEASUREMENT CONTROL	2	208	C7 79 71 51 A2 00 03 11
540	66856	UP	RLC AM	MAC_DATA_REQ (1 Pdu) (C)	2	144	02 02 10 FF FF FF FF FF
541	68804	DOWN	RLC AM	MAC_DATA_IND (1 Pdu) (D)	3	144	80 3D 1B FE 99 FD 17 C7
542	68804	UP	RLC AM	MAC_DATA_REQ (1 Pdu) (C)	3	144	02 00 80 FF FF FF FF FF
543	68804	DOWN	DL_DCCH_M	DOWNLINK DIRECT TRANSFER	3	104	99 FD 17 C7 29 40 00 90
544	68804	DOWN	CC	DISCONNECT		40	83 25 02 E2 90
545	68804	UP	CC	RELEASE		16	03 6D
546	68804	UP	UL_DCCH_M	UPLINK DIRECT TRANSFER	3	80	8F 93 4C 79 A6 C0 00 81
547	68805	UP	RLC AM	MAC_DATA_REQ (1 Pdu) (D)	3	144	80 45 15 FE 8F 93 4C 79
548	68840	DOWN	RLC AM	MAC_DATA_IND (1 Pdu) (C)	3	144	02 00 9F FF FF FF FF FF
549	68844	DOWN	RLC AM	MAC_DATA_IND (1 Pdu) (D)	3	144	80 45 15 FE C1 1D 8F 83
550	68844	UP	RLC AM	MAC_DATA_REQ (1 Pdu) (C)	3	144	02 00 90 FF FF FF FF FF
551	68844	DOWN	DL_DCCH_M	DOWNLINK DIRECT TRANSFER	3	80	C1 1D 8F 83 B1 40 00 30
552	68844	DOWN	CC	RELEASE COMPLETE		16	83 2A
553	68848	DOWN	RLC UM	MAC_DATA_IND (1 Pdu) (C)	1	144	01 F9 0F FE C8 41 07 CD
554	68848	DOWN	DL_DCCH_M	RRC CONNECTION RELEASE	1	56	C8 41 07 CD 8B C8 00
555	68848	UP	UL_DCCH_M	RRC CONNECTION RELEASE COMPLETI	1	48	CE D1 4A B8 0C 40
556	68848	UP	RLC UM	MAC_DATA_REQ (1 Pdu) (C)	1	144	01 0D FF CE D1 4A B8 0C

Bild 31: Meldungen beim Aufbau einer Telefonieverbindung. Teil3/3

Der Empfänger eines UMTS-Mobiles ist ein sog. Rake-Empfänger. (siehe Abschnitt 7).
Er empfängt gleichzeitig sowohl Signale aus einem Mehrwegeempfang als auch die Sendung mehrerer Node B die sich in Reichweite befinden. Die messtechnisch erfassten Zellen werden in drei Kategorien (sets) eingeteilt: active, monitored, detected. Der active set enthält alle diejenigen Basisstationen die in eine Softhandoverkonstellation einbezogen sind
Die Meldung ACTIVE SET UPDATE bedeutet, dass aufgrund der MEASUREMENT REPORTs die Liste der active sets neu geschrieben wird. Damit ist auch nachvollziehbar dass

die Meldungen MEASUREMENT CONTROL und MEASUREMENT REPORT umfangreicher sind als im GSM/GPRS/EDGE.

7. WCDMA Empfangstechnik

7.1 DER RAKE Empfänger

Das von einem Node-B ausgesendete Signal wird von unterschiedlichen Hindernissen reflektiert und erreicht dadurch den Empfänger auf mehreren Wegen zeitverschoben und in unterschiedlicher Stärke.
Die Signale dieser Mehrwegeausbreitung können von einem sogenannten RAKE-Empfänger getrennt empfangen und zusammengefügt werden, wobei ein Gewinn erzielt wird.
Mit Hilfe der Zinken des Rechens (RAKE), auch Finger genannt, wird das Empfangssignal aus den verschiedenen zeitverschobenen Komponenten zusammengesetzt.

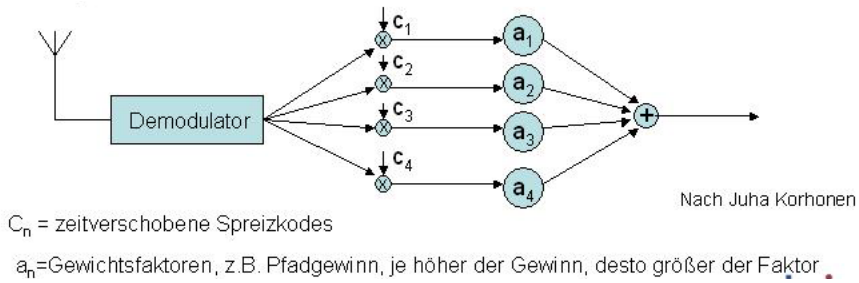
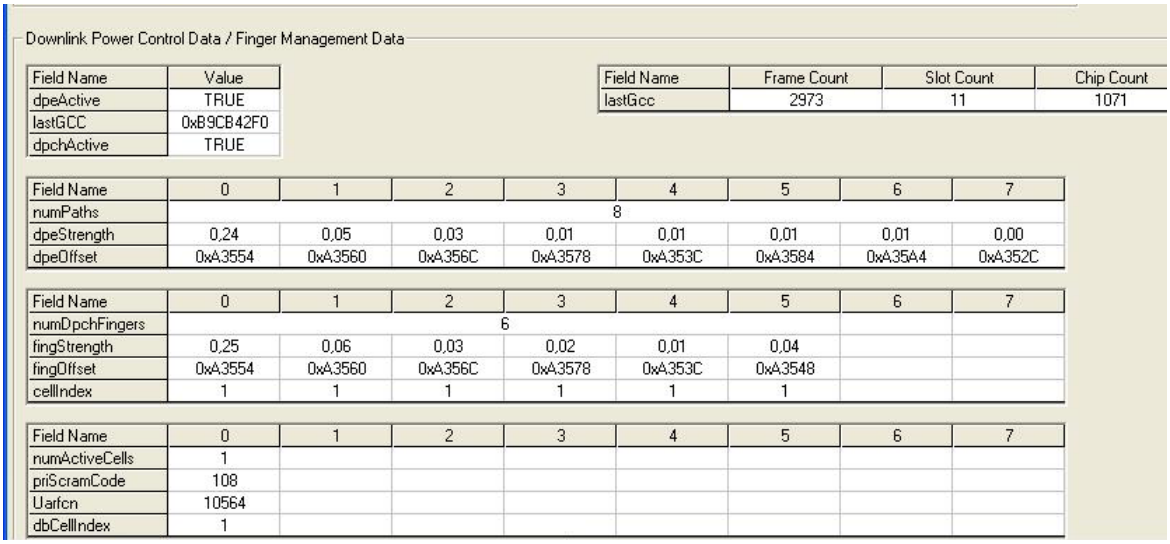


Bild 32: Prinzip eines RAKE-Empfängers

Eine Liste der Sets zeigt Bild 33. Der active set enthält nur ein Element. Die graphische Darstellung der Fingerstärke ist in Bild 28 dargestellt.



Downlink Power Control Data / Finger Management Data

Field Name	Value
dpeActive	TRUE
lastGCC	0xB9CB42F0
dpchActive	TRUE

Field Name	Frame Count	Slot Count	Chip Count
lastGcc	2973	11	1071

Field Name	0	1	2	3	4	5	6	7
numPaths	8							
dpeStrength	0,24	0,05	0,03	0,01	0,01	0,01	0,01	0,00
dpeOffset	0xA3554	0xA3560	0xA356C	0xA3578	0xA353C	0xA3584	0xA35A4	0xA352C

Field Name	0	1	2	3	4	5	6	7
numDpchFingers	6							
fingStrength	0,25	0,06	0,03	0,02	0,01	0,04		
fingOffset	0xA3554	0xA3560	0xA356C	0xA3578	0xA353C	0xA3548		
cellIndex	1	1	1	1	1	1		

Field Name	0	1	2	3	4	5	6	7
numActiveCells	1							
priScramCode	108							
Uarfcn	10564							
dbCellIndex	1							

Bild 33: Liste der registrierten Finger

Die Differenz der Fingerstärken in den Bildern 34 und 35 ist Ergebnis der Bewegung des Mobiles.

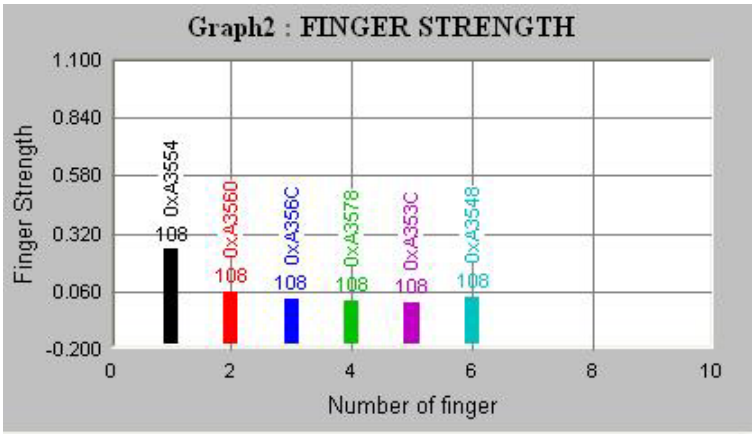


Bild 34: Graphische Darstellung der In Bild 27 erfassten Finger

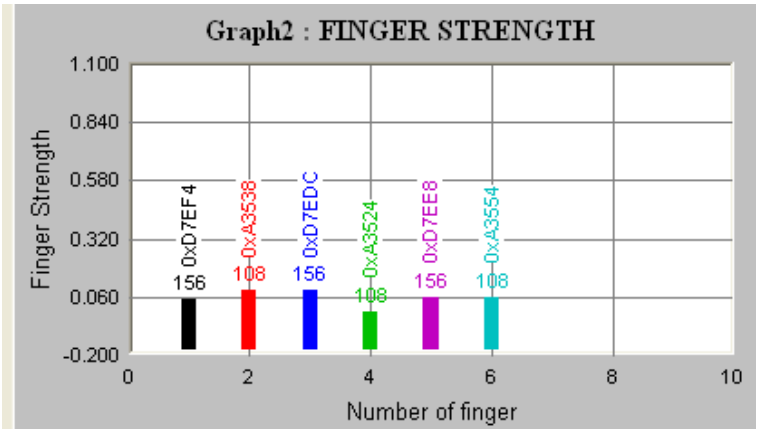


Bild 35: Bei Bewegung des Mobiles ändern sich die Feldstärken der einzelnen Finger.

7.2 Soft Handover

Wenn ein UE das Signal von mehreren Node-B mit einem RAKE-Empfänger detektiert, besteht eine ähnliche Situation wie beim Mehrwegeempfang, nur besitzen die verschiedenen Wege jetzt verschiedene Spreizkodes.
Wie im GSM werden alle Handover durch das Netz bestimmt. Entscheidungsgrundlage sind Messungen der Uplink-Verbindungen durch das Netz und der Downlink-Verbindungen durch das UE. Die messtechnisch erfassten Zellen werden, wie oben erklärt, in drei Kategorien (sets) eingeteilt: active, monitored, detected.
Der active set enthält alle diejenigen Basisstationen die in eine Softhandoverkonstellation einbezogen sind. Das bedeutet, jeder Node-B im active set könnte auch alleine die Verbindung sicherstellen. Ob diese Mehrfachbelastung des Netzes notwendig ist muss das Netz entscheiden.

Für den Übergang vom monitored set zum active set ist die *addition threshold* entscheidend. Diese Feldstärkeschwelle wird vom Netz festgelegt. Genauso wie die *drop threshold*, die festlegt bei welcher Feldstärke Unterschreitung die Verbindung aus dem active set und damit aus der Softhandoverkonstellation herausfällt
Der detected set enthält alle anderen Zellen, die vom UE erkannt wurden

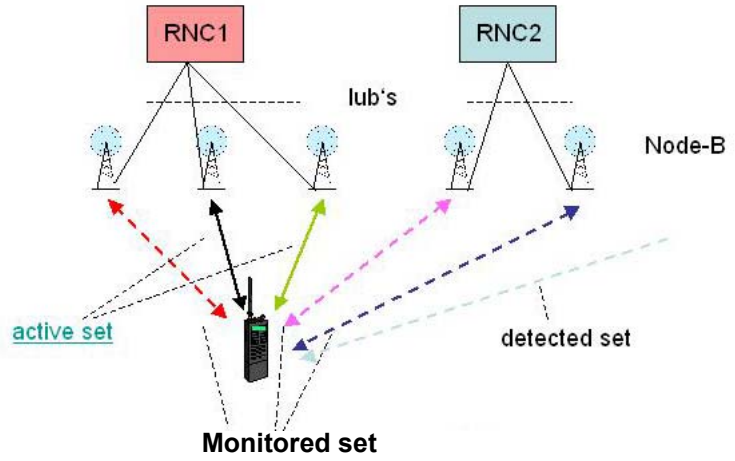


Bild 36: Ausgangspunkt für Softhandover

Der rot eingezeichnete RNC soll Serving RNC heißen, der Blaue in der in Bild 37 dargestellten Situation Drift RNC.

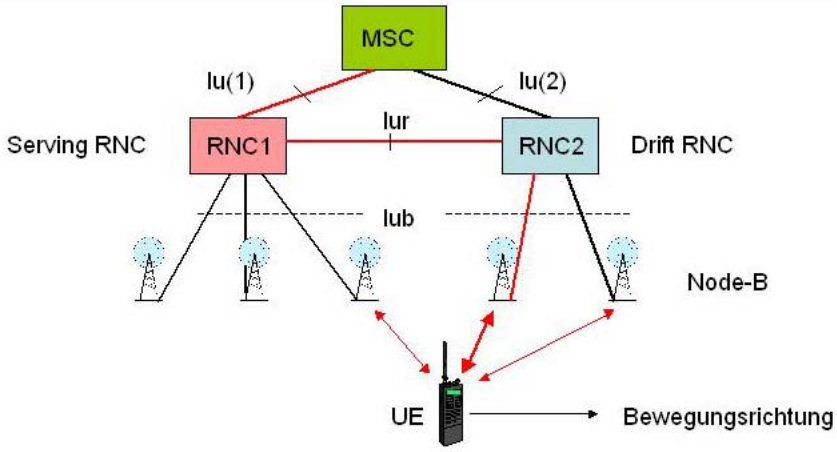


Bild 37: Das Mobile wird in Richtung Drift RNC bewegt

Das Mobile wird vom RNC1 weg hin zum Drift RNC2 bewegt. Obgleich der Hauptteil der Signalverarbeitung im RNC2 liegt verläuft der Signaltransport weiter über den Serving RNC1. Der Vorgang verläuft ausschließlich im UTRAN.

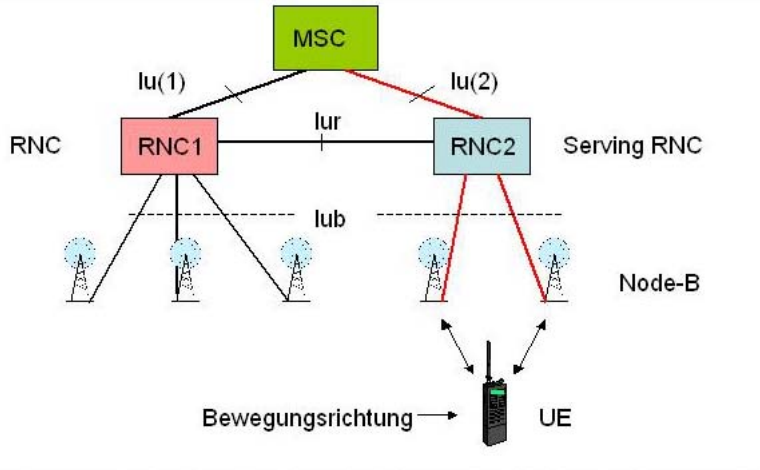


Bild 38: Relocation

Relocation ist ein Prozess, bei dem der RNC-Status vom RNC1 zum RNC2 weitergegeben und dadurch die Iur-Schnittstelle entlastet wird. Der Vorgang verläuft ausschließlich im UTRAN.

7.3 Hard Handover

Hard Handover bedeutet dass die Verbindung wegen eines Frequenzwechsels (kurzzeitig) unterbrochen wird (brake-before-make).
Das ist der Fall wenn zwischen UMTS und GSM umgeschaltet werden muss.
Wie aus dem Vortrag „DieGSMDmKanäle.pdf“ bekannt ist, wird ein Handover durch Feldstärkemessungen der Nachbarzellen vorbereitet.
Der Befehl zum Umschalten kommt vom RNC im Falle des Handover UMTS->GSM, oder vom BSC im Falle GSM -> UMTS. Dieses Umschalten kann in Regionen in denen UMTS existent aber nur mit schwacher Feldstärke vorhanden ist relativ häufig vorkommen.

Wenn das Mobile nicht über einen zweiten Empfänger verfügt, müssen das Mobile und der Node-B im *compressed mode* arbeiten können. Wenn der Node-B im *compressed mode* sendet, lässt er in bestimmten *radio frames* eine Lücke von 3, 4,7,10 oder 14 *time slots* (J.Korhonen) In diesen Lücken kann das Mobile die Feldstärke der Zielfrequenzen messen.

Im *radio frame* dem durch die Kompression Zeitschlitze fehlen, muss die Datenrate kurzzeitig erhöht werden, was durch Verringerung des Spreizfaktors und Erhöhung der Sendeleistung erfolgt.

8. Meldungen in einem MOC

8.1. Meldungen im Idle Mode

Entsprechend der Recommendation ts_125331 wird im Idle Mode neben Systems-Informationen ein Master Information Block ausgestrahlt.
Der Master Information Block, zeigt an , welche Systeminformationen auf dem Kanal ausgestrahlt werden. Das können sein.

SysinfoType 1	Enthält NAS Systeminformationen sowie UE Timer und Zähler die im idle und im connected Mode verwendet werden.
SysinfoType 2	Enthält UTRAN Registration Area Namen.
SysinfoType 3	Enthält die Parameter für Cell selection und reselektion.
SysinfoType 4	Enthält die Parameter wie Type 3 aber nur für connected mode.
SysinfoType 5	Enthält Parameter für die Konfiguration der Common Physical Channels.der Zelle.
SysinfoType 6	Enthält Parameter für die Konfiguration der Common und shared Physical Channels der Zelle im connected mode.
SysinfoType 7	Enthält die sich schnell ändernden Parameter im Uplink.
SysinfoType 8	Enthält die statischen CPCH Informationen die in der Zelle zu verwenden sind.
SysinfoType 9	Enthält alle CPCH Informationen die in der Zelle zu verwenden sind.
SysinfoType 10	Enthält Informationen für UE's die ihren DCH mit einer DRAC (Dynamic Relay Authorization Control) Procedure steuern.
SysinfoType 11	Enthält die in der Zelle zu verwendenden Measurement Control Informationen.
SysinfoType 12	Wie SIB 11, jedoch nur im connected Mode zu verwenden.
SysinfoType 13	Enthält ANSI-41 System Informationen. Auch SIB 13.1-13.4
SysinfoType 14	nur im TDD mode verwendet.
SysinfoType 15	Enthält unterstützende Informationen für die Lokalisierung von Mobiles auch SIB 15.1 –15.5.
SysinfoType 16	Enthält vordefinierte Kanal Konfigurationen für Handover zum UTRAN.
SysinfoType 17	Nur für TDD Mode.
SysinfoType 18	Enthält die PLM Namen der Nachbarzellen.

8.1.1 Master Information Block

Bei Verwendung eines vorgegeben Transportkanals (BCH) ist die Anzahl der Informationselemente und damit die Länge eines jeden System Informations-Blocks (SIB) unterschiedlich..
Damit muss die Segmentierung längerer SIBs in zwei oder mehr Segmente erfolgen. Genauso kann die Verkettung von zwei oder mehr SIBs erfolgen um eine Syteminformations Meldung exakt in einem Transportblock unterzubringen . Das Transportformat für den BCH ist mit 246 bits, einer CRC-Länge von 16 bits, einem ½ Convolutionalcode und einem TTI (Transmit Time Interval) von 20 ms festgelegt.

Was die Segmentierung betrifft, so kann ein SIB komplett übertragen werden oder in den Segmenten als erstes, folgendes (subsequentes) oder letztes Segment eines SIB. Ein SIB kann

in bis zu 16 Segmente zerlegt werden. Daraus folgt, dass eine Systeminformationsmeldung verschiedenste Kombinationen enthalten kann: First Segment, subsequent Segment, last Segment, last + first, last + one or several complete, last + one or several complete+first, one or several complete. Usw.

In Bild 39 ist eine BCCH-BCH Message dargestellt, die einen komplette Master Information Block enthält.

```
_____[ 2 ]_____[ group ID: 00 07 ]_____[ trace ID: 00 01 ]______

00 00 01 00  af 92 06 09  88 04 50 08  06 41 84 30  a1 0e 4b 25
28 40 8c 19  aa dd 56 60  20 20 a0 00  00 00 00 59


:WDCMA L3 RRC Peer messages

00  00000000  Channel LSB
:Channel Type MSB
00  00000000  BCCH-BCH

    0000000100000000  length=256
BCCH_BCH Message
: Sfn-Prime
    10101111100  System Frame Number-Prime = 1404

: payload
       1001  CompleteSIB
: sib- Type
      00000  masterInformationBlock,
:sib-Data-fixed (226 bit)
60  01100000  data8
98  10011000  data16
80  10000000  data24
45  01000101  data32
00  00000000  data40
80  10000000  data48
64  01100100  data56
18  00011000  data64
43  01000011  data72
0a  00001010  data80
10  00010000  data88
e4  11100100  data96
b2  10110010  data104
52  01010010  data112
84  10000100  data120
08  00001000  data128
c1  11000001  data136
9a  10011010  data144
ad  10101101  data152
d5  11010101  data160
66  01100110  data168
02  00000010  data176
02  00000010  data184
0a  00001010  data192
00  00000000  data200
00  00000000  data208
00  00000000  data216
00  00000000  data224
00        00  data226
```

Bild 39: BCCH-BCH Message mit payload eines MIB

Die Entschlüsselung der in Bild 39 fettgedruckten Oktette ist in Bild 40 dargestellt.

```
_____[ 3 ]_____[ group ID: 00 07 ]_____[ trace ID: 00 01 ]______

00 09 00 e2  60 98 80 45  00 80 64 18  43 0a 10 e4  b2 52 84 08
c1 9a ad d5  66 02 02 0a  00 00 00 00  00


:WDCMA L3 RRC Peer messages

00  00000000  Channel LSB
:Channel Type MSB
09  00001001  mib

    0000000011100010  length = 226
:sw1, nonCriticalExtensions
           0  sw1 not present
: MIB Value tag
         110  MIB-ValueTag = 6 + 1

: Supported PLM types
          00  PLMN-Identity
: MCC
        0010  2
        0110  6
        0010  2
: MNC
           0  val0: 0
        0000  0
        0010  2

:SIBsb-ReferenceList
       00101  val2: 5

:SchedulingInformationSIBSb
:sibSb-Type
       00000  sysInfoType1:
    00010000  16 + 1
:scheduling
           0  sw2 not present
        0001  segCount = 1
:sib-Pos
        1001  rep2048
    0000011000  24

:SchedulingInformationSIBSb
:sibSb-Type
       01000  sysInfoType9
:scheduling
           0  sw2 not present
        1100  segCount = 12
:sib-Pos
        0010  rep16
         100  4

:SchedulingInformationSIBSb
:sibSb-Type
       00100  sysInfoType5
          00  0 + 1
:scheduling
           1  sw2 present
        1100  segCount = 12
:sib-Pos
        1001  rep2048
    0110010010  402
:SibOFF-List
        1001  val3: 9
:SibOFF
        0100  so10
:SibOFF
        0010  so6
:SibOFF
        0000  so2
:SibOFF
        0100  so10
:SibOFF
```

```
        0110  so14
:SibOFF
        0000  so2
:SibOFF
        1100  so26
:SibOFF
        1101  so28
:SibOFF
        0101  so12
:SibOFF
        0110  so14
:SchedulingInformationSIBSb
:sibSb-Type
       11101  spare
:scheduling
           0  sw2 not present
        1010  segCount = 10
:sib-Pos
:SchedulingInformationSIBSb
:sibSb-Type
       11000  sysInfoType15-2
        0000  SIBOccurIdentity = 0
        1000  SIBOccurValueTag = 8
:scheduling
           0  sw2 not present
        0001  segCount = 1
:sib-Pos
        0000  rep4
           0  0
:SchedulingInformationSIBSb
:sibSb-Type
       10100  sysInfoType17
:scheduling
           0  sw2 not present
         0000  segCount = 0
:sib-Pos
         0000  rep4
            0  0
```

Bild 40: Masterinformationsblock zeigt die auf dem BCCH enthaltenes System Informationen an

8.1.2 Leerer Block

Vergleichbar mit den Verhältnissen im GSM ist das Aussenden von Meldungen auf dem BCCH an ein Zeitraster gebunden. Wenn zu einem bestimmten Zeitpunkt keine Systeminformation oder ein Masterinformation Block vorliegt muss ein leerer Block (ein Dummy) gesendet werden. Ein solcher Block ist in Bild 41 dargestellt..

```
_____[ 9 ]_____[ group ID: 00 07 ]_____[ trace ID: 00 01 ]______

00 00 01 00  b0 20 00 00  00 00 00 00  00 00 00 00  00 00 00 00
00 00 00 00  00 00 00 00  00 00 00 00  00 00 01 1d


:WDCMA L3 RRC Peer messages

00  00000000  Channel LSB
:Channel Type MSB
00  00000000  BCCH-BCH

    0000000100000000  length=256
BCCH_BCH Message
: Sfn-Prime
    10110000001  System Frame Number-Prime = 1409

: payload
        0000  no Segment
```

Bild 41: BCCH-BCH Block ohne Inhalt

8.1.3 Systeminformationen

Die Systeminformation Type 1 wird wieder in einem BCCH-BCH Block (Bild 42) und explizit (Bild 43) übertragen.

```
_____[ 10 ]_____[ group ID: 00 07 ]_____[ trace ID: 00 01 ]______

00 00 01 00  b0 52 1c 40  63 50 85 00  b1 01 01 7f  f5 ff a4 bd
97 08 04 2c  b0 39 10 40  00 00 00 00  00 00 03 87


:WDCMA L3 RRC Peer messages

00  00000000  Channel LSB
:Channel Type MSB
00  00000000  BCCH-BCH

    0000000100000000  length=256
BCCH_BCH Message
: Sfn-Prime
    10110000010  System Frame Number-Prime = 1410

: payload
        1001  CompleteSIB
: sib- Type
       00001  systemInformationBlockType1,
:sib-Data-fixed (226 bit)
c4  11000100  data8
06  00000110  data16
35  00110101  data24
08  00001000  data32
50  01010000  data40
0b  00001011  data48
10  00010000  data56
10  00010000  data64
17  00010111  data72
ff  11111111  data80
5f  01011111  data88
fa  11111010  data96
4b  01001011  data104
d9  11011001  data112
70  01110000  data120
80  10000000  data128
42  01000010  data136
cb  11001011  data144
03  00000011  data152
91  10010001  data160
04  00000100  data168
00  00000000  data176
00  00000000  data184
00  00000000  data192
00  00000000  data200
00  00000000  data208
00  00000000  data216
00  00000000  data224
00        00  data226
```

Bild 42: BCCH-BCH Message mit payload eines SIB 1

Bitte beachten Sie die Übereinstimmung der fettgedruckten Hexadezimalzahlen in den Bildern 42 und 43.

```
_____[ 11 ]_____[ group ID: 00 07 ]_____[ trace ID: 00 01 ]______

00 0a 00 e2  c4 06 35 08  50 0b 10 10  17 ff 5f fa  4b d9 70 80
42 cb 03 91  04 00 00 00  00 00 00 00  00


:WDCMA L3 RRC Peer messages

00  00000000  Channel LSB
:Channel Type MSB
0a  00001010  sib1
    0000000011100010  length=226
:               MESSAGE TYPE: SysInfoType1

          1  sw1 present
          1  sw2 present
          0  sw3 not present
:NAS-SystemInformationGSM-MAP
        001  val1: 1
01  00000001  nas
8d  10001101  nas
:CN-DomainSysInfoList
         01  val2: 1
:CN-DomainIdentity
          0  cs-domain
:cn-Type
          0  NAS-SystemInformationGSM-MAP
        001  val5: 1
0a  00001010  nas
01  00000001  nas
:cn-DRX-CycleLengthCoeff
          01  1 +  6
:CN-DomainIdentity
          1  ps-domain
:cn-Type
          0  NAS-SystemInformationGSM-MAP
        001  val5: 1
01  00000001  nas
01  00000001  nas
:cn-DRX-CycleLengthCoeff
          01  1 +  6
:ue-ConnTimersAndConstants
:T-301
       1111  spare
        111  N301=7,
:T-302
       1110  ms8000
        101  N302=5
:T-304
        111  spare1
        111  N304=7
:T-305
        111  m720
:T-307
        010  s15
T-308
         01  ms80
        001  T309=1+1
:T-310
        011  ms160
        110  N310=6
:T-311
        110  ms1750
       0101  T312=5
:N-312
        110  s800
       0001  T313=1
:N-313
        000  s1
:T-314
        000  s1
:T-315
        001  s10
:N-315
        000  s1
:T-316
        010  s20
```

```
:T-317
         110  s1200
:ue-IdleTimersAndConstants
:T-300
        0101  ms1000
         100  N300=4, INTEGER
        0000  T312=0, INTEGER
:N-312
          111  s1000
```

Bild 43: Explizite Darstellung eines System Information Block 1

8.2. Registrierung im Netz

In Bild 28: sind die Meldungen dargestellt, die beim Attach im CS-Mode mit dem Netz ausgetauscht werden. Mit dem dem Autor zur Verfügung stehenden Trace Mobile lässt sich dieser Vorgang nicht tracen. Es müssen daher Ausschnitte aus den von der Fa. SAGEM zur Verfügung gestellten Raw –Trace übersetzt und dargestellt werden.

Jeder Informationsaustausch auf der Luftschnittstelle beginnt mit der Meldung RRC CONNECTION REQUEST, die nach erfolgter Genehmigung (über den AICH) gesendet wird.
Im Bild 44 wird als Grund für den Verbindungsaufbau *Registration* angegeben.
Zum Verständnis der Schreibweise in den nachfolgenden Bildern sei folgendes erklärt. Die Entschlüsselungsvorschriften wurden anhand der ASN.1 Beschreibung in der ETSI TS 125 331 Abschnitt 11 formuliert. In den ETS Beschreibungen sind optionale Elemente enthalten. Das Vorhandensein der optionalen Elemente wird mit Schaltern (switches) abgeprüft. So sind z.B. in Bild 44 die *measured Results on Rach* nicht vorhanden.

```
_____[ 1 ]_____[ group ID: 00 07 ]_____[ trace ID: 00 01 ]______

00 06 00 96  21 92 81 53  d6 20 80 82  32 b3 00 00 00 00 00 00 00
00 00 00 00  00

:WDCMA L3 RRC Peer messages

00  00000000  Channel LSB
:Channel Type MSB
06  00000110  Uplink CCCH
00  0000000010010110  length=150
          0  IntegrityCheckinfo absent
: Message Type:
         01  RRC CONNECTION REQUEST
-- User equipment IEs
: switches
             measuredResultsOnRach sw1
          0  sw1 not present
             v3d0NonCriticalExtensions sw2
          0  sw2 not present
InitialUE-Identity::= Choice{
        001  Choice: TMSI-and-LAI-GSM-MAP
: TMSI
92  10010010  take hex value
81  10000001  take hex value
53  01010011  take hex value
d6  11010110  take hex value
: LAI
: PLMN-identity
: MCC
        0010  Mobile CC digit 1   : 2
        0000  Mobile CC digit 2   : 0
        1000  Mobile CC digit 3   : 8
```

```
: MNC
           0  val2: 0
        0001  Mobile NC digit     : 1
        0000  Mobile NC digit     : 0
:LAC
46  01000110  Loc. area code (LAI) = ID of MSC (hex)
56  01010110  Loc. area code (LAI) = ID of BSC (hex)
}
Establishment cause ::= ENUMERATED {
       01100  registration,
}
ProtocolErrorIndicator ::= Enumerated {
           0  No Error
```

Bild 44: RRC CONNECTION REQUEST zum Zwecke der Registrierung im Netz

Grundsätzlich antwortet das Netz darauf mit der Meldung RRC CONNECTION SETUP, die nicht an dieser Stelle, sondern zusammen mit dem Telefoniesetup behandelt werden soll. Es folgt die Meldung LOCATION UPDATING REQUEST.

```
_____[ n ]_____[ group ID: 00 07 ]_____[ trace ID: 00 01 ]______

00 07 00 96  15 02 05 00  98 28 43 10  17 c0 0a 32  b2 38 2f a4
94 0a 9e b1  98 1a 38 c4  02 00 01 00
:WDCMA L3 RRC Peer messages
00  00000000  Channel LSB
:Channel Type MSB
07  00000111  Uplink DCCH
00  0000000010010110  length=150
           0  IntegrityCheckinfo absent
: Message Type:
       00101  INITIAL DIRECT TRANSFER
: switches
              measuredResultsOnRach sw1
           0  sw1 not present
              v3a0NonCriticalExtensions sw2
           1  sw2 present
              -- Core network IEs
:CN-DomainIdentity
           0  cs-domain,
IntraDomainNasNodeSelector
              Version:
           0  release99
              cn-Type:
           0  Gsm-map-IntraDomainNASNodeSelection
              routingbasis
         000  localPTMSI
              RoutingParameter
    1000000101  bit
            0  enteredparameter = false
:nas-Message
    000000010011  length=19
    0-------  direction from      : originating site
    -000----  TransactionID       : 0
    ----0101  Protocol Discrim.   : mobility management messages non GPRS
    00------  SendSequenceNumber  : 0
    --001000  MESSAGE TYPE        : LOCATION UPDATING REQUEST
: Location updating type
    ----0---  No follow-on request pending
    -----0--  Spare
    ------10  IMSI attach
: Ciphering key sequence number
    0-------  spare
    -110----  Ciph. Key Sequ.Numb.: 6
: Local area identification
    ----0010  Mobile CC digit 1   : 2
    0000----  Mobile CC digit 2   : 0
    ----1000  Mobile CC digit 3   : 8
    1111----  Mobile NC digit 3   : 15
    ----0001  Mobile NC digit 1   : 1
    0000----  Mobile NC digit 2   : 0
    01000110  Loc. area code (LAI) = ID of MSC (hex)
    01010110  Loc. area code (LAI) = ID of BSC (hex)
: Mobile station classmark 1
```

```
    0-------  Spare
    ---0----  "Controlled Early Classmark Sending" option is not implemented in the MS
    ----0---  encryption algorithm A5/1 available
: Mobile identity
    00000101  length of Mob.ident.: 5
    1111----  Identity Digit 1    : 15
    ----0---  No. of ID digits    : even
    -----100  Type of identity    : TMSI/P-TMSI
    10010010  Identity Digit 2,3  : take hex value
    10000001  Identity Digit 4,5  : take hex value
    01010011  Identity Digit 6,7  : take hex value
    11010110  Identity Digit 8,9  : take hex value
v3a0NonCriticalExtensions SEQUENCE {
              InitialDirectTransfer-v3a0ext ::= SEQUENCE {
    00110011000000110100  START-Value = 208948
```

Bild 45: DieNAS Meldung LOCATION UPDATING REQUEST in INITIAL DIRECT TRANSFER eingepackt

Die NAS-Message LOCATION UPDATING REQUEST wird über den UMTS-Kanal mittels der Meldung INITIAL DIRECT TRANSFER transportiert. Die Struktur ist aus dem GSM bekannt. Das Wort INITIAL bedeutet hier, dass dieser Direkttranfer der erste im Trace ist, dem nun Uplink und Downlink Direkttransfer folgen.
Eine “echte” UMTS-Meldung ist die nun folgende Meldung SECURITY MODE COMMAND. Auf die Bedeutung der *Integrity Check Info* und der *Ciphering Algorithm Capability* wird in Abschnitt 11 eingegangen.

```
_____[ m ]_____[ group ID: 00 07 ]_____[ trace ID: 00 01 ]______

00 04 00 96  89 ac 88 d3  8c 0c 00 01  80 01 28 c0  00 01 00 71
00 18 c0 02  42 38 4c 0f

:WDCMA L3 RRC Peer messages

00  00000000  Channel LSB
:Channel Type MSB
04  00000100  Downlink DCCH
00  0000000010010110  length=150
          1  Integrity Check Info present
    00010011  MessageAuthenticationCode,
    01011001  MessageAuthenticationCode,
    00010001  MessageAuthenticationCode,
    10100111  MessageAuthenticationCode,
        0001  RRC-MessageSequenceNumber  = 1

       10000  Message Type: SECURITY MODE COMMAND
              Choice ::= {
           0  r3
             laterNonCriticalExtensions sw1
           0  sw1 not present
SecurityModeCommand-r3-IEs
              cipheringModeInfo sw2
           1  sw2 present
              integrityProtectionModeInfo
           1  sw3 present
              ue-SystemSpecificSecurityCap
           0  sw4 not present
       -- User equipment IEs
              Radio Resource Control transaction identifier
          00  RRC transaction identifier  : 0
    SecurityCapability
              cipheringAlgorithmCap
       -- For each bit value “0” means false/ not supported
           0  spare15(0),
           0  spare14(1),
           0  spare13(2),
           0  spare12(3),
           0  spare11(4),
           0  spare10(5),
           0  spare9(6),
           0  spare8(7),
```

```
           0  spare7(8),
           0  spare6(9),
           0  spare5(10),
           0  spare4(11),
           0  spare3(12),
           0  spare2(13),
           1  uea1(1)(14),
           1  uea0(0)(15)

              integrityProtectionAlgorithmCap
        -- For each bit value "0" means false/ not supported
           0  spare15(0),
           0  spare14(1),
           0  spare13(2),
           0  spare12(3),
           0  spare11(4),
           0  spare10(5),
           0  spare9(6),
           0  spare8(7),
           0  spare7(8),
           0  spare6(9),
           0  spare5(10),
           0  spare4(11),
           0  spare3(12),
           0  spare2(13),
           1  uia1(14),
           0  spare0(15)

CipheringModeInfo
             activationTimeForDPCH sw1
           0  sw1 not present
             rb-DL-CiphActivationTimeInfo sw2
           1  sw2 present

        CipheringModeCommand
           0  CipheringAlgorithm
           1  uea1

              RB-ActivationTimeInfoList
         activationTimeInfo
           0  flag
        0011  val1: 3
              Number-Of-RB-ActivationTimeInfo = val1
              (val1 + 1) x RB-ActivationTimeInfo
       00000  RB-identity = 0+1
    000000000000  RLC-Sequence Number = 0
       00001  RB-identity = 1+1
    000000000111  RLC-Sequence Number = 7
       00010  RB-identity = 2+1
    000000000011  RLC-Sequence Number = 3
       00011  RB-identity = 3+1
    000000000000  RLC-Sequence Number = 0

IntegrityProtectionModeInfo
            integrityProtectionAlgorithm sw1
           1  sw1 present
        IntegrityProtectionModeCommand
           0  startIntegrityProtection
    01000010  integrityProtInitNumber
    00111000  integrityProtInitNumber
    01001100  integrityProtInitNumber
    00001111  integrityProtInitNumber
```

Bild 46: Trace der Meldung SECURITY MODE COMMAND

Die aus dem GPRS bekannte Meldung LOCATION UPDATING ACCEPT wird wie gehabt in die UMTS-Meldung DOWNLINK DIRECT TRANSFER eingepackt.

```
_____[ n ]_____[ group ID: 00 07 ]_____[ trace ID: 00 01 ]______

00 04 00 96  9f 3f 6c 36  91 48 01 a0  a0 40 5f 00  28 ca c2 e0
be 92 50 2e  89

:WDCMA L3 RRC Peer messages

00  00000000  Channel LSB
:Channel Type MSB
04  00000100  Downlink DCCH

00  0000000010010110  length=150
          1  Integrity Check Info present
    00111110  MessageAuthenticationCode,
    01111110  MessageAuthenticationCode,
    11011000  MessageAuthenticationCode,
    01101101  MessageAuthenticationCode,
        0010  RRC-MessageSequenceNumber  = 2

: Message Type:
       00101  DOWNLINK DIRECT TRANSFER
           0  r3 SEQUENCE
           0  sw1 not present
DownlinkDirectTransfer-r3
          10  RRC-TransactionIdentifier = 2
:CN-DomainIdentity
           0  cs-domain,
:nas-Message
    000000001101  length=13
    0-------  direction from      : originating site
    -000----  TransactionID       : 0
    ----0101  Protocol Discrim.   : mobility management messages non GPRS
    00------  SendSequenceNumber  : 0

    --000010  MESSAGE TYPE        : LOCATION UPDATING ACCEPT

: Location area identification
    ----0010  Mobile CC digit 1   : 2
    0000----  Mobile CC digit 2   : 0
    ----1000  Mobile CC digit 3   : 8
    1111----  Mobile NC digit 3   : 15
    ----0001  Mobile NC digit 1   : 1
    0000----  Mobile NC digit 2   : 0
    01000110  Loc. area code (LAI) = ID of MSC (hex)
    01010110  Loc. area code (LAI) = ID of BSC (hex)

    00010111  INFORMATIONSELEMET   : Mobile Identity 3
    00000101  length of Mob.ident.3: 5
    1111----  Identity Digit 1     : 15
    ----0---  No. of ID digits     : even
    -----100  Type of identity     : TMSI/P-TMSI
    1001----  Identity Digit 3     : 9
    ----0010  Identity Digit 2     : 2
    1000----  Identity Digit 5     : 8
    ----0001  Identity Digit 4     : 1
    0111----  Identity Digit 7     : 7
    ----0100  Identity Digit 6     : 4
```

Bild 47: LOCATION UPDATING ACCEPT in DOWNLINK DIRECT TRANSFER eingepackt

Die Meldungen RRC- CONNECTION RELEASE und RRC-CONNECTION RELEASE COMPLETE sind wieder “reine” UMTS Meldungen

```
_____[ n ]_____[ group ID: 00 07 ]_____[ trace ID: 00 01 ]______

00 04 00 96  f9 49 44 34  8b c8

:WDCMA L3 RRC Peer messages

00  00000000  Channel LSB
:Channel Type MSB
04  00000100  Downlink DCCH
00  0000000010010110  length=150
          1  Integrity Check Info present
    11110010  MessageAuthenticationCode,
    10010010  MessageAuthenticationCode,
    10001000  MessageAuthenticationCode,
    01101001  MessageAuthenticationCode,
        0001  RRC-MessageSequenceNumber  = 1

       01111  Message Type : RRC-CONNECTION RELEASE
           0  r3-SEQUENCE {
              laterNonCriticalExtensions sw1
           0  sw1 not present
RRCConnectionRelease-r3-IEs
              n-308 sw1
           1  sw1 present
              rplmn-information sw2
           0  sw2 not present
-- User equipment IEs
              Radio Resource Control transaction identifier
          00  RRC transaction identifier  : 0
```

Bild 48: Die Meldung RRC- CONNECTION RELEASE

Die in den Kopfleisten der Trace stehende lfd. Nr. [n] zeigt an, dass die Trace aus einen Zusammenhang herausgerissen sind. Ab Abschnitt 8.3. zeigen diese Nummern die Stellung im gesamten Taceverlauf.

```
_____[ n ]_____[ group ID: 00 07 ]_____[ trace ID: 00 01 ]______

00 07 00 96  95 99 6f 83  14 40

:WDCMA L3 RRC Peer messages

00  00000000  Channel LSB
:Channel Type MSB
07  00000111  Uplink DCCH

00  0000000010010110  length=150
          1  Integrity Check Info present
    00101011  MessageAuthenticationCode,
    00110010  MessageAuthenticationCode,
    11011111  MessageAuthenticationCode,
    00000110  MessageAuthenticationCode,
        0010  RRC-MessageSequenceNumber  = 2


       10001  Message Type : RRC-CONNECTION RELEASE COMPLETE

              errorIndication sw1
           0  sw1 not present
              laterNonCriticalExtensions sw2
           0  sw2 not present

              Radio Resource Control transaction identifier
          00  RRC transaction identifier  : 0
```

Bild 49: Die Meldung RRC-CONNECTION RELEASE COMPLETE

8.3 Aufbau einer Telephonieverbindung

8.3.1 Verbindungsanforderung

Der Trace der Meldung in Bild 50 unterscheidet sich von dem in Bild 44 dadurch, dass er die PLMN-identity von Deutschland Vodafone enthält, als Establishment cause den Rufaufbau (originatingConversationalCall) und die Measurement IEs enthält .

```
_____[ 14 ]_____[ group ID: 00 07 ]_____[ trace ID: 00 01 ]______

00 06 00 a6  31 90 86 8e  2b 26 20 10  0c 68 00 f0  00 00 00 00
00 00 00 00  00

:WDCMA L3 RRC Peer messages

00  00000000  Channel LSB
:Channel Type MSB
06  00000110  Uplink CCCH

00  0000000010100110  length=166
          0  IntegrityCheckinfo absent
: Message Type:
         01  RRC CONNECTION REQUEST
-- User equipment IEs
: switches
             measuredResultsOnRach sw1
          1  sw1 present
             v3d0NonCriticalExtensions sw2
          0  sw2 not present
InitialUE-Identity::= Choice{
        001  Choice: TMSI-and-LAI-GSM-MAP
: TMSI
90  10010000  take hex value
86  10000110  take hex value
8e  10001110  take hex value
2b  00101011  take hex value
: LAI
: PLMN-identity
: MCC
       0010  Mobile CC digit 1   : 2
       0110  Mobile CC digit 2   : 6
       0010  Mobile CC digit 3   : 2
: MNC
          0  val2: 0
       0000  Mobile NC digit     : 0
       0010  Mobile NC digit     : 2
:LAC
01  00000001  Loc. area code (LAI) = ID of MSC (hex)
8d  10001101  Loc. area code (LAI) = ID of BSC (hex)

Establishment cause
      00000  originatingConversationalCall,
ProtocolErrorIndicator
           0  No Error
-- Measurement IEs
MeasuredResultsOnRach
             monitoredCells (sw3)
           0  sw3 not present
              currentCell
              modeSpecification
           0  fdd
              measurementQuantity
          00  CPICH-EC-NO: Common Pilot Channel,The received energy per chip
              divided by the power density in the band
: Measurement Value
      011110  30 dB
```

Bild 50: RRC CONNECTION REQUEST zum Zwecke der Rufaufbaus

8.3.2 Die Zuweisung von Kanälen durch RRC CONNECTION SETUP

Als Antwort auf die Meldung RRC CONNECTION REQUEST sendet das Netz die Meldung RRC CONNECTION SETUP, in der dem Mobile die Einstellvorschrift für die zu verwendenden Logischen- Transport- und Physikalischen Kanäle zugewiesen werden.
Die Länge der Meldung beträgt 864 Bit, siehe auch die 6 Zeilen Hexzahlen . Die Übersetzung hat eine Länge von 15 Seiten. Für den Leser dürfte das Studium dieser Seiten keine Erhellung der Zusammenhänge ergeben. Daher wird in Bild 51 nur der Beginn der Übersetzung dargestellt.
Die Bilder 52 und 53 zeigen als „Ersatz“ welche Kanäle konfiguriert werden.

```
_____[ 15 ]_____[ group ID: 00 07 ]_____[ trace ID: 00 01 ]______

00 03 03 60  30 f7 32 10  d1 c5 64 c4  02 01 8d 00  21 3a 46 c7
83 03 49 d3  e2 84 f8 ea  30 00 14 61  67 b3 20 b2  a6 89 c2 e7
4f 92 53 e5  a9 40 01 52  8a 13 a7 cd  49 f3 d4 e0  01 29 c7 09
d3 e8 b4 fa  6a 90 00 d5  08 00 06 17  81 4a fc 03  e0 19 00 04
80 11 dc 32  00 01 04 13  f7 e4 65 8e  a5 11 27 90  0a 15 09 82
14 60 06 02  90 00

:WDCMA L3 RRC Peer messages

00  00000000  Channel LSB
:Channel Type MSB
03  00000011  Downlink CCCH

03  0000001101100000  length=864
           0  IntegrityCheckinfo absent
: Messagetype
         011  RRC CONNECTION SETUP
           0  r3 SEQUENCE {
           0  laterNonCriticalExtensions not present
RRC CONNECTION SETUP r3
              activation Time sw1
           0  sw1 not present
              new-c-RNTI sw2
           0  sw2 not present
              capabilityUpdateRequirement sw3
           1  sw3 present
              ul-CommonTranChInfo sw4
           1  sw4 present
              dl-CommonTranChInfo sw5
           1  sw5 present
              frequencyInfo present sw6
           1  sw6 present
              maxAllowedUL-TX-Power sw7
           0  sw7 not present
                ul-ChannelRequirement sw8
            1  sw8 present
                dl-CommonInformation sw9
            1  sw9 present
              dl-InformationPerRL-List sw10
           1  sw10 present

---->User equipment IEs

InitialUE-Identity
         001  Choice: TMSI-and-LAI-GSM-MAP
: TMSI
90  10010000  take hex value
86  10000110  take hex value
8e  10001110  take hex value
2b  00101011  take hex value
: LAI
: PLMN-identity
: MCC
        0010  Mobile CC digit 1   : 2
        0110  Mobile CC digit 2   : 6
        0010  Mobile CC digit 3   : 2
: MNC
           0  val2: 0
        0000  Mobile NC digit     : 0
```

```
        0010  Mobile NC digit     : 2
:LAC
01  00000001  Loc. area code (LAI) = ID of MSC (hex)
8d  10001101  Loc. area code (LAI) = ID of BSC (hex)

              Radio Resource Control transaction identifier
          00  RRC transaction identifier  : 0

New UTRAN Radio Network Temporary Identity, U-RNTI ::= SEQUENCE {
    000000001000  SRNC identity 8
    01001110100100011011  S-RNTI 321819

RRC-StateIndicator ::= ENUMERATED {
          00  CELL_DCH,
UTRAN-DRX-CycleLengthCoefficient
         011  DRX cycle length coeff.  : 3+3
           1  systemSpecificCapUpdateReqList present
CapabilityUpdateRequirement ::= SEQUENCE {
           1  UE radio access FDD capability update requirement : True
           0  UE radio access 3.84 Mcps TDD capability update requirement : False
              SEQUENCE (Sice Of 1..16) SystemSpecificCapUpdateReq
         000  Number-of-SystemSpecificCapUpdateReqs = 0
              SystemSpecificCapUpdateReq ENUMERATED {
           0  gsm
              }
```

usw. ……

Bild 51: Beginn der Meldung RRC CONNECTION SETUP

Wie aus den Bilder 52 und 53 zu ersehen ist, werden in jeder Richtung 4 logische Kanäle aufgebaut einer im Unacknowledge Mode und drei im Acknowledge Mode .
Die logischen Kanäle werde in jedem der Fälle auf einen Physikalischen Kanal gemappt.
Es wird später gezeigt, dass nach der CC-Meldung SETUP das Netz einen RADIO BEARER SETUP sendet, der die Konfiguration des Transportkanals für die Sprachübertragung veranlasst.
Zum Vergleich, im GSM wurden vom Netz nach Empfang des ACCESS BURSTS mit der Meldung IMMEDIATE ASSIGNMENT ein Signalkanal und nach Empfang von SETUP mit ASSIGNMENT COMMAND ein Transportkanal zugewiesen.

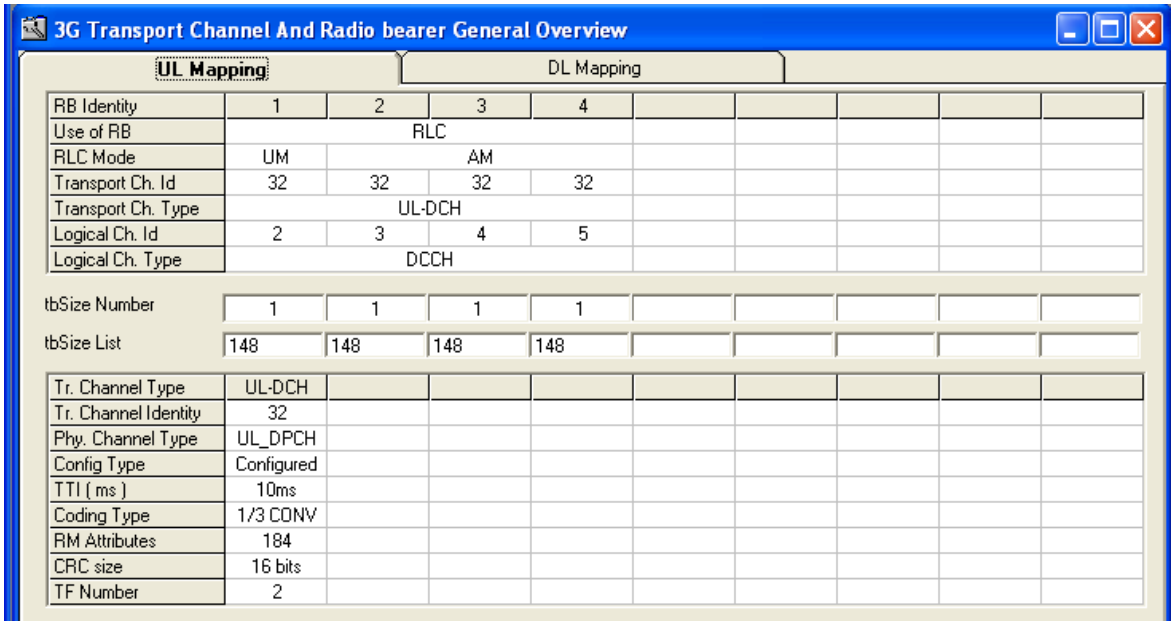


Bild 52: UPLINK Kanäle die durch RRC CONNECTION SETUP zugeteilt werden

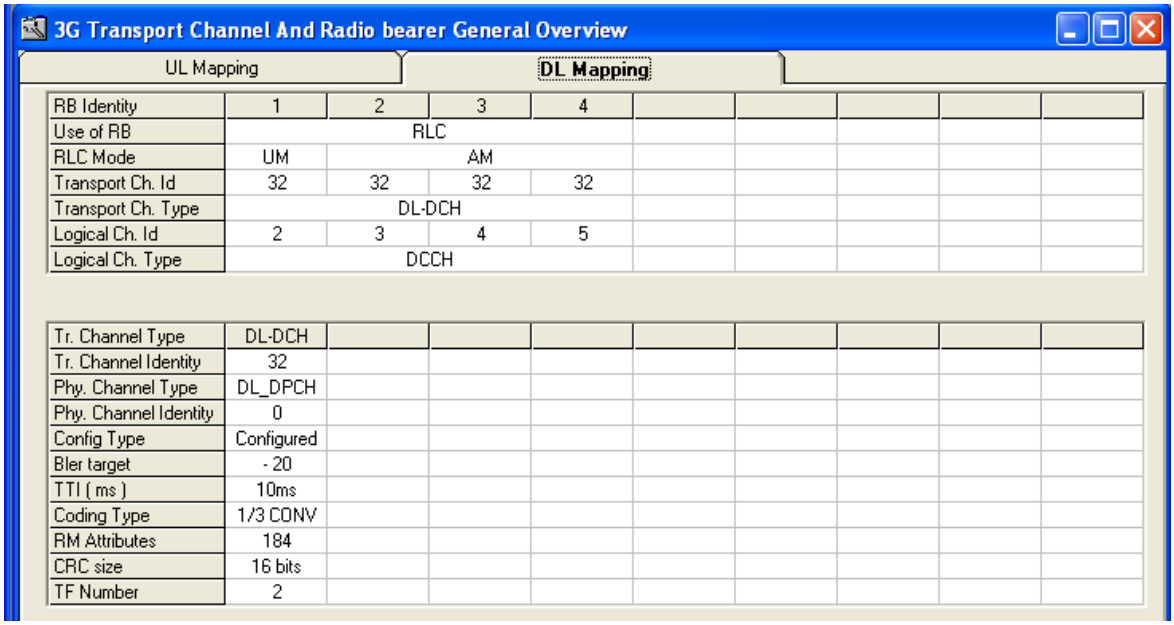


Bild 53: DOWNLINK Kanäle die durch die Meldung RRC CONNECTION SETUP zugeteilt werden

8.3.3 Quittung mit RRC CONNECTION SETUP COMPLETE

Mit der Meldung RRC CONNECTION SETUP COMPLETE gibt das Mobile dem Netz bekannt welche Parameter es eingestellt hat und in Gestalt der IE Classmark2 und 3 seine technischen Eigenschaften. In der Meldung SECURITY MODE COMMAND in Bild 46 wurden bereits die CipheringAlgorithmCapability und die IntegrityProtectionAlgorithm-Capability festgelegt. Das Mobile meldet, dass es die Algorithmen uea1 sowie uia1 und für GSM den Algorithmus A5/1 unterstützt..

```
_____[ 16 ]_____[ group ID: 00 07 ]_____[ trace ID: 00 01 ]______

00 07 01 28  4b 08 00 00  a0 00 05 11  b8 dd 06 a4  c6 68 8a 2c
83 03 48 00  18 00 11 8f  cf c0 cc 0d  5c 62 84 8c  02 89 90 10
00

:WDCMA L3 RRC Peer messages
00  00000000  Channel LSB
:Channel Type MSB
07  00000111  Uplink DCCH
01  0000000100101000  length=296
          0  IntegrityCheckinfo absent

: MESSAGE Type :
       10010  RRC CONNECTION SETUP COMPLETE

              sw1 = UE-RadioAccessCapability
           1  sw1 present
              sw2 = ue-RATSpecificCapability
           1  sw2 present
              sw3 = v370NonCriticalExtensions
           0  sw3 not present
              Radio Resource Control transaction identifier
          00  RRC transaction identifier  : 0
STARTList ::= SEQUENCE (SIZE (1..4)) OF STARTSingle
          01  val1 1
              (Number-of-STARTSingles+1) x STARTSingle
              CN-DomainIdentity
```

```
           0  cs-domain, (Circuit Switched)
              START-Value
    00000000000000000010  START-Value = 2

              CN-DomainIdentity
           1  ps-domain, (Packet Switched)

              START-Value
    00000000000000000010  START-Value = 2

UE-RadioAccessCapability

           1  measurementCapability expected
              AccessStratumReleaseIndicator
              r99
    PDCP-Capability
           0  losslessSRNS-RelocationSupport = False
              supportForRfc2507 CHOICE {
           0  notSupported NULL,

    RLC-Capability ::= SEQUENCE {
              TotalRLC-AM-BufferSize
         010  kb50,

              MaximumRLC-WindowSize
           0  mws2047,

              MaximumAM-EntityNumberRLC-Cap
         011  am6,

    TransportChannelCapability
           DL-TransChCapability
              maxNoBitsReceived
        0111  b8960,

              maxConvCodeBitsReceived
        0001  b1280,
              turboDecodingSupport TurboSupport
           1  MaxNoBits
        0111  b8960,
              MaxSimultaneousTransChsDL
          01  e8,

         000  MaxSimultaneousCCTrCH-Count = 0+1
              maxReceivedTransportBlocks MaxTransportBlocksDL
        0011  tb32,

              MaxNumberOfTFC-DL
        0101  tfc128,

              MaxNumberOfTF
         001  tf64,

           UL-TransChCapability
              maxNoBitsTransmitted
        0011  b3840,

              maxConvCodeBitsTransmitted
        0001  b1280,

              turboEncodingSupport TurboSupport
           1  supported
              MaxNoBits
        0011  b3840,

              MaxSimultaneousTransChsUL
         010  e8,

              modeSpecificInfo
           0  fdd NULL,

              MaxTransportBlocksUL
        0100  tb32,

              MaxNumberOfTFC-UL
        0101  tfc64,

              MaxNumberOfTF
```

```
     000  tf32,


RF-Capability

          sw10 = fddRF-Capability
       1  sw10 present
          sw11 = tddRF-Capability
       0  sw11 not present

          fddRF-Capability
      11  UE-PowerClass = 3+1
          TxRxFrequencySeparation
      00  mhz190,

 PhysicalChannelCapability

          sw10 = fddPhysChCapability
       1  sw10 present
          sw11 = tddPhysChCapability
       0  sw11 not present

    fddPhysChCapability
        DL-PhysChCapabilityFDD
     000  maxNoDPCH-PDSCH-Codes = 0+1
          MaxNoPhysChBitsReceived
    0110  b9600,

       0  supportForSF-512 False
       0  supportOfPDSCH False
          SimultaneousSCCPCH-DPCH-Reception ::= CHOICE {
       0  notSupported NULL,

    UL-PhysChCapabilityFDD
          MaxNoDPDCH-BitsTransmitted
    0011  b4800,
       0  supportOfPCPCH = False

UE-MultiModeRAT-Capability
    MultiRAT-Capability
       1  supportOfGSM Yes
       0  supportOfMulticarrier No

    MultiModeCapability
      01  fdd,

SecurityCapability
          cipheringAlgorithmCap
          -- For each bit value "0" means false/ not supported
       0  spare15(0),
       0  spare14(1),
       0  spare13(2),
       0  spare12(3),
       0  spare11(4),
       0  spare10(5),
       0  spare9(6),
       0  spare8(7),
       0  spare7(8),
       0  spare6(9),
       0  spare5(10),
       0  spare4(11),
       0  spare3(12),
       0  spare2(13),
       1  uea1(1)(14),
       1  uea0(0)(15)

          integrityProtectionAlgorithmCap
          -- For each bit value "0" means false/ not supported
       0  spare15(0),
       0  spare14(1),
       0  spare13(2),
       0  spare12(3),
       0  spare11(4),
       0  spare10(5),
       0  spare9(6),
       0  spare8(7),
       0  spare7(8),
       0  spare6(9),
```

```
           0  spare5(10),
           0  spare4(11),
           0  spare3(12),
           0  spare2(13),
           1  uia1(14),
           0  spare0(15)

     UE-Positioning-Capability
           0  standaloneLocMethodsSupported = False
           0  ue-BasedOTDOA-Supported = False
              NetworkAssistedGPS-Supported
          11  noNetworkAssistedGPS

           0  supportForUE-GPS-TimingOfCellFrames = False
           0  supportForIPDL = False

    MeasurementCapability
      downlinkCompressedMode

              sw13 = ttd-Measurement
           0  sw13 not present
              sw14 = gsm-Measurements
           1  sw14 present
              sw15 = multiCarrierMeasurements
           1  sw15 present

           1  fdd-Measurements = True
        GSM-Measurements
           1  gsm900 = True
           1  dcs1800 = True
           1  gsm1900 = True

           0  multiCarrierMeasurements = False
      uplinkCompressedMode
              sw16 = ttd-Measurement
           0  sw16 not present
              sw17 = gsm-Measurements
           1  sw17 present
              sw18 = multiCarrierMeasurements
           1  sw18 present

           1  fdd-Measurements = True
        GSM-Measurements
           1  gsm900 = True
           1  dcs1800 = True
           1  gsm1900 = True

           0  multiCarrierMeasurements = False
    ue-RATSpecificCapability  InterRAT-UE-RadioAccessCapabilityList
          00  Number-of-InterRat-UE-RadioAccessCapabilitys
           0  gsm
        GSM-Classmark2
33  00110011  Mobile station classmark for UMTS
03  00000011  length = 3
57  0-------  spare
    -10-----  Used by mobile stations supporting this version of the protocol
    ----0---  encryption algorithm A5/1 available
    -----111  not defined
18  0-------  spare
    -0------  PS capability not present
    --01----  defined in TS 24.080
    ----1---  Mobile station supports mobile terminated point to point SMS
    -----0--  no VBS capability or no notifications wanted
    ------0-  no VGCS capability or no notifications wanted
    -------0  The MS does not support the E-GSM or R-GSM band
a1  1-------  The MS supports options that are indicated in classmark 3 IE
    -0------  spare
    --1-----  LCS value added location request notification capability supported
    ---0----  the ME has a preference for the default alphabet over UCS2.
    ----0---  The ME does not support SoLSA.
    ------0-  encryption algorithm A5/3 not available
    -------1  encryption algorithm A5/2 available

GSM-Classmark3
0 0
8C  02 89 90 10 00
```

Bild 54: Trace der Meldung RRC CONNECTION SETUP COMPLETE

8.3.4 Diensteanforderungen mit CM SERVICE REQUEST

Die Meldung CM SERVICE REQUEST unterscheidet sich nicht von der aus dem GSM bekannten, außer dass sie durch die Meldung INITIAL DIRECT TRANSFER transportiert wird.

```
_____[ 17 ]_____[ group ID: 00 07 ]_____[ trace ID: 00 01 ]______

00 07 00 a8  15 02 1a 00  60 29 20 88  1a b8 c5 08  2f a4 84 34
71 5a 00 00  40

:WDCMA L3 RRC Peer messages

00  00000000  Channel LSB
:Channel Type MSB
07  00000111  Uplink DCCH
00  0000000010101000  length=168
           0  IntegrityCheckinfo absent
: Message Type:
       00101  INITIAL DIRECT TRANSFER

: switches
              measuredResultsOnRach sw1
           0  sw1 not present
              v3a0NonCriticalExtensions sw2
           1  sw2 present

              -- Core network IEs
:CN-DomainIdentity
           0  cs-domain,
IntraDomainNasNodeSelector
              version
           0  release99
              cn-Type
           0  Gsm-map-IntraDomainNASNodeSelector
              routingbasis
         000  localPTMSI
              RoutingParameter
    1000011010  bit
           0  enteredparameter = false

:nas-Message
    000000001100  length=12
    0-------  direction from      : originating site
    -000----  TransactionID       : 0
    ----0101  Protocol Discrim.   : mobility management messages non GPRS
    00------  SendSequenceNumber  : 0

    --100100  MESSAGE TYPE        : CM SERVICE REQUEST

    0-------  spare               : 0
    -001----  value for the ciphering key sequence number = 1
    ----0001  Requ.service type   : Mobile originating call establishment, or packet mode
                                    connection establishment
: Mobile Station Classmark 2
    00000011  length              : 3
    0-------  1 spare             : 0
    ---1----  "Controlled Early Classmark Sending" option is implemented in the MS
    ----0---  Encryp.Algor. A5_1  : available

    0-------  1 spare bit         : 0
    -0------  pseudo-synch.capab. : not present
    --01----  SS Screening Indic. : phase 2 error handling
    ----1---  Mobile station supports mobile terminated point to point SMS
    -----0--  no VoiceBroadcastService (VBS) capability or no notifications wanted
    ------0-  no VoiceGroupCallService (VGCS) capability or no notifications wanted
    -------0  The MS does not support the E-GSM or R-GSM band

    1-------  The MS does support any options that are indicated in CM3
    -0------  1 spare bit         : 0
    --1-----  LocationServiceValueAdded Capability supported
    ---0----  1 spare bit         : 0
    ----0---  SoLSA Capability    : not supported
```

```
    -----0--  Network initiated MO CM connection request not supported.
    ------0-  encryp.algorith.A5/3: not available
    -------1  encryp.algorith.A5/2: available

: Mobile identity
    00000101  length              : 5
    ----0---  No. of ID digits     : even
    -----100  Type of identity     : TMSI/P-TMSI
    1111----  Identity Digit 1     : 95
    10010000  Identity Digit 2,3  : take hex value
    10000110  Identity Digit 4,5  : take hex value
    10001110  Identity Digit 6,7  : take hex value
    00101011  Identity Digit 8,9  : take hex value

v3a0NonCriticalExtensions
              InitialDirectTransfer-v3a0ext ::= SEQUENCE {
    0100000000000000000  START-Value = 262144
```

Bild 55: Der CM Service Request

8.3.5 MEASUREMENT CONTROL

Die nachstehende Meldung MEASURENT CONTROL hat ein Länge von 632 bit. Das ist recht lang. Da die Meldung ASN.1 kodiert ist, empfiehlt sich eine Übersetzung mit Hilfe eines Tools, wie es z.B. der SNACC darstellt. Im Bild 99 wird eine 528 bit lange Meldung MEASURENT CONTROL vollständig entschlüsselt dargstellt.
Im Bild 56 soll die Darstellung des Inhalts der Meldung nur angedeutet werden. Man erkennt dass 12 Infrafrequenz Cells überprüft werden. Diese besitzen die Scrampling Codes 326, 374, 184, 368, 72, 160, 154, 448, 198, 495, 119, 336 und sind in die Messung einzubeziehen.

```
_____[ 18 ]_____[ group ID: 00 07 ]_____[ trace ID: 00 01 ]______

00 04 02 78  20 84 03 b8  64 12 8e 8d  5d 0c a3 bb  57 45 28 eb
d5 d1 ca 35  c5 74 92 8e  e1 5d 2c a3  24 57 4d 28  d4 15 d3 ca
34 d5 75 12  8f 81 5d 4c  a3 63 57 55  28 fd f5 d5  ca 33 bd 75
92 8e a1 5d  31 14 14 14  2a 02 80 2e  d2 d6 44 20  09 8b 24 fb
4c 78 80

:WDCMA L3 RRC Peer messages

00  00000000  Channel LSB
:Channel Type MSB
04  00000100  Downlink DCCH

02  0000001001111000  length=632
           0  IntegrityCheckinfo absent
:Messagetype
       01000  MeasurementControl
           0  r3 SEQUENCE {
               v390Criticalextensions  (sw0)
           0  sw0 not present

measurementControl-r3

              Begin switches
              measurementReportingMode sw1
           1  sw1 present
              additionalMeasurementList sw2
           0  sw2 not present
              dpch-CompressedModeStatusInfo sw3
           0  sw3 not present
              End switches

              -- Measurement IEs
          00  RRC-TransactionIdentifier = 0
        1000  measurementIdentity = 8+1


MeasurementCommand
setup MeasurementType
```

```
          00  setup measurement type
         000  IntraFrequencyMeasurement

              intraFreqCellInfoList sw4
           1  sw4 present
              intraFreqMeasQuantity sw5
           1  sw5 present
              intraFreqReportingQuantity sw6
           1  sw6 present
              measurementValidity sw7
           0  sw7 not present
              reportCriteria sw8
           1  sw8 present

               IntraFreqCellInfoList

              removedIntraFreqCellList sw9
           1  sw9 present
              newIntraFreqCellList sw10
           1  sw10 present
              cellsForIntraFreqMeasList sw11
           0  sw11 not present

RemovedIntraFreqCellList
          00  removeAllIntraFreqCells NULL,

               New Intra frequency cell list
       01100  val1: 12

               NewIntraFreqCells
:           IntraFreqCellID switch(sw12)
           1  sw12 present
IntraFreqCellID
       00000  IntraFreqCellID = 0
               cellinfo
               referenceTimeDifferenceToCell switch(sw13)
           1  sw13 present

      001010  cellIndividualOffset: -21
               referenceTimeDifferenceToCell
          00  accuray40
               modeSpecificInfo

               primaryCPICH-Info switch(sw14)
           1  sw14 present

               primaryCPICH-TX-Power switch(sw15)
           1  sw15 present

              PrimaryCPICH-Info
    101000110  PrimaryScramplingCode 326

               primaryCPICH-TX-Power
      101011  primaryCPICH-TX-Power

               readSFN-Indicator ::= BOOLEAN
           1  true
               tx-diversityIndicator false ::= BOOLEAN
           0  false

              NewIntraFreqCells ::= SEQUENCE {
:           IntraFreqCellID switch(sw12)
           1  sw12 present
IntraFreqCellID
       00001  IntraFreqCellID = 1
               cellinfo
               referenceTimeDifferenceToCell switch(sw13)
           1  sw13 present

      001010  cellIndividualOffset: -21
               referenceTimeDifferenceToCell
          00  accuray40

               modeSpecificInfo


               primaryCPICH-Info switch(sw14)
           1  sw14 present
```

```
                primaryCPICH-TX-Power switch(sw15)
            1   sw15 present
                PrimaryCPICH-Info ::= SEQUENCE {
    101110110    PrimaryScramplingCode 374
                }
                primaryCPICH-TX-Power
      101011    primaryCPICH-TX-Power

                readSFN-Indicator ::= BOOLEAN
            1   true

                tx-diversityIndicator false ::= BOOLEAN
            0   false

                NewIntraFreqCells ::= SEQUENCE {
:            IntraFreqCellID switch(sw12)
            1   sw12 present

.....usw
```

Bild 56: Ausschnitt aus der Meldung MeasurementControl

8.3.6. AUTHENTICATION REQUEST UND AUT. RESPONSE

In Bild 24 sind die Meldungen AUTHENTICATION REQUEST und AUTHENTIKATION RESPONSE enthalten. Wie erwähnt ist das Bild 24 von einem Trace der Fa. SAGEM abgeleitet. Die in diesem Artikel entschlüsselten Trace stammen aber von Messungen beim mit einem Nokia-Trace-Mobile. Hier fehlen diese Meldungen. Da es sich um NAS Messages handelt, kann der Interessierte Leser diese in meinen Ausführungen über GSM nachlesen.

8.3.7 SECURITY MODE COMMAND UND SEC.MODE COMPLETE

Der aufmerksame Leser hat sicherlich schon bemerkt, dass eine Reihe von Meldungen über eine *IntegrityCheckinfo* verfügen und andere nicht. Der Zusammenhang wird im Abschnitt 11 erklärt. In jedem Fall muss in sensible Meldungen der Nachweis erbracht werden, dass die Meldung von der richtigen Gegenstelle stammt. Betrachten Sie die Änderungen gegenüber Bild 46.

```
_____[ 20 ]_____[ group ID: 00 07 ]_____[ trace ID: 00 01 ]______

00 04 00 d0  ed 25 c2 9c  8c 0e 00 01  80 01 28 c0  00 01 00 91
00 00 c0 02  4a 7d 97 fc  00 c0

:WDCMA L3 RRC Peer messages
00  00000000  Channel LSB
:Channel Type MSB
04  00000100  Downlink DCCH
00  0000000011010000  length=208
            1  Integrity Check Info present
    11011010  MessageAuthenticationCode,
    01001011  MessageAuthenticationCode,
    10000101  MessageAuthenticationCode,
    00111001  MessageAuthenticationCode,
        0001  RRC-MessageSequenceNumber  = 1
       10000  Message Type: SECURITY MODE COMMAND

            0  r3
              laterNonCriticalExtensions sw1
            0  sw1 not present
SecurityModeCommand-r3-IEs ::= SEQUENCE {
               cipheringModeInfo sw2
            1  sw2 present
               integrityProtectionModeInfo
```

```
           1  sw3 present
              ue-SystemSpecificSecurityCap
           1  sw4 present
              -- User equipment IEs
              Radio Resource Control transaction identifier
          00  RRC transaction identifier  : 0
    SecurityCapability
              cipheringAlgorithmCap
              -- For each bit value "0" means false/ not supported
           0  spare15(0),
           0  spare14(1),
           0  spare13(2),
           0  spare12(3),
           0  spare11(4),
           0  spare10(5),
           0  spare9(6),
           0  spare8(7),
           0  spare7(8),
           0  spare6(9),
           0  spare5(10),
           0  spare4(11),
           0  spare3(12),
           0  spare2(13),
           1  uea1(1)(14),
           1  uea0(0)(15)
     integrityProtectionAlgorithmCap
              -- For each bit value "0" means false/ not supported
           0  spare15(0),
           0  spare14(1),
           0  spare13(2),
           0  spare12(3),
           0  spare11(4),
           0  spare10(5),
           0  spare9(6),
           0  spare8(7),
           0  spare7(8),
           0  spare6(9),
           0  spare5(10),
           0  spare4(11),
           0  spare3(12),
           0  spare2(13),
           1  uia1(14),
           0  spare0(15)
CipheringModeInfo
             activationTimeForDPCH sw1
           0  sw1 not present
             rb-DL-CiphActivationTimeInfo sw2
           1  sw2 present
        CipheringModeCommand
           0  CipheringAlgorithm
           1  uea1
          RB-ActivationTimeInfoList
ActivationTimeInfo
           0  flag
        0011  val1: 3
              Number-Of-RB-ActivationTimeInfo = val1
              (val1 + 1) x RB-ActivationTimeInfo
       00000  RB-identity = 0+1
    000000000000  RLC-SequenceNumber = 0
       00001  RB-identity = 1+1
    000000001001  RLC-SequenceNumber = 9
       00010  RB-identity = 2+1
    000000000000  RLC-SequenceNumber = 0
       00011  RB-identity = 3+1
    000000000000  RLC-SequenceNumber = 0
IntegrityProtectionModeInfo
             integrityProtectionAlgorithm sw1
           1  sw1 present
        IntegrityProtectionModeCommand
           0  startIntegrityProtection
    01001010  integrityProtInitNumber
    01111101  integrityProtInitNumber
    10010111  integrityProtInitNumber
    11111100  integrityProtInitNumber
    IntegrityProtectionAlgorithm
           0  uia1
        -- Core network IEs
:CN-DomainIdentity
```

```
          0  cs-domain,
        -- Other IEs
             InterRAT-UE-SecurityCapList ::= SEQUENCE (SIZE(1..val2)) OF
        InterRAT-UE-SecurityCapability ::= CHOICE {
          0  gsm
        GsmSecurityCapability
        -- For each IntegrityCheckinfo bit value "0" means false/ not supported
          0  a5-7(0),
          0  a5-6(1),
          0  a5-5(2),
          0  a5-4(3),
          0  a5-3(4),
          1  a5-2(5),
          1  a5-1(6)
```

Bild 57: Meldung SECURITY MODE COMMAND

```
_____[ 21 ]_____[ group ID: 00 07 ]_____[ trace ID: 00 01 ]______

00 07 00 90  9a d2 22 3b  0d 31 00 00  01 80 00 02  00 a2 00 21
80 00

:WDCMA L3 RRC Peer messages

00  00000000  Channel LSB
:Channel Type MSB
07  00000111  Uplink DCCH

00  0000000010010000  length=144
          1  Integrity Check Info present
    00110101  MessageAuthenticationCode,
    10100100  MessageAuthenticationCode,
    01000100  MessageAuthenticationCode,
    01110110  MessageAuthenticationCode,
        0001  RRC-MessageSequenceNumber  = 1
       10100  Message Type : SECURITY MODE COMPLETE
             IntegrityProtActivationInfo sw1
          1  sw1 present
            RB-ActivationTimeInfoList sw2
          1  sw2 present
            laterNonCriticalExtensions sw3
          0  sw3 not present
-- User equipment IEs
              Radio Resource Control transaction identifier
          00  RRC transaction identifier  : 0
IntegrityProtActivationInfo
RRC-MessageSequenceNumberList
          1  val1: 1
        0000  RRC-MessageSequenceNumber = 0
        0000  RRC-MessageSequenceNumber = 0
        0000  RRC-MessageSequenceNumber = 0
        0000  RRC-MessageSequenceNumber = 0
        0000  RRC-MessageSequenceNumber = 0
--Radio bearer IE's
RB-ActivationTimeInfoList
        0001  val1: 1
       10000  rb-Identity = 16 + 1
    000000000000  Rlc-SequenceNumber = 0
       00000  rb-Identity = 0 + 1
    100000000010  Rlc-SequenceNumber = 2050
```

Bild 58: Meldung SECURITY MODE COMPLETE

8.3.8 SETUP in einem MOC

Dies SETUP Meldung leitet den Rufaufbau ein. Das IE Bearer capability beschreibt die Forderungen an den Sprachkanal .

```
_____[ 22 ]_____[ group ID: 00 07 ]_____[ trace ID: 00 01 ]______

00 07 00 f0  a8 e3 54 6e  8e c0 0a 81  a2 82 02 90  02 01 00 42
af 03 c0 88  0a b9 10 01  81 8a 81 00  80 80

:WDCMA L3 RRC Peer messages

00  00000000  Channel LSB
:Channel Type MSB
07  00000111  Uplink DCCH
00  0000000011110000  length=240
          1  Integrity Check Info present
    01010001  MessageAuthenticationCode,
    11000110  MessageAuthenticationCode,
     10101000  MessageAuthenticationCode,
     11011101  MessageAuthenticationCode,
        0001  RRC-MessageSequenceNumber  = 1

       11011  Message Type :UPLINK DIRECT TRANSFER

: switches
              measuredResultsOnRach sw1
           0  sw1 not present
              laterNonCriticalExtensions sw2
           0  sw2 not present

:CN-DomainIdentity
           0  cs-domain,
:nas-Message
    000000010101  length=21
    0-------  direction from      : originating site
    -000----  TransactionID       : 0
    ----0011  Protocol Discrim.   : Call control and call related SS messages
    01------  SendSequenceNumber  : 1

    --000101  MESSAGE TYPE        : SETUP

    00000100  INFORMATION ELEMENT : Bearer capability
    00000101  length              : 5
    0-------  Extension           : 0

    -01-----  Radio Channel Req.  : full rate support only MS
    ---0----  Coding Standard     : GSM standard coding
    ----0---  Transfer Mode       : Circuit Mode
    -----000  Info Transfer Cap.  : speech
    0-------  Extension           : 0
    -0------  Coding              : octet used for extension of inf. transf. capab.
    --00----  Spare               : 00
    ----0100  speech Vers. indic. : GSM full rate speech version 3
    0-------  Extension           : 0
    -0------  Coding              : octet used for extension of inf. transf. capab.
    --00----  Spare               : 00
    ----0010  speech Vers. indic. : GSM full rate speech version 2
    0-------  Extension           : 0
    -0------  Coding              : octet used for extension of inf. transf. capab.
    --00----  Spare               : 00
    ----0000  speech Vers. indic. : GSM full rate speech version 1
    1-------  Extension           : 1
    -0------  Compression         : data compression not possible
    --00----  Structure           : service data unit integrity
    ----0---  Duplex Mode         : half duplex
    ------0-  Negot. of Int.      : No meaning is associated with this value.

    01011110  INFORMATION ELEMENT : CalledPartyBCDNumber
    00000111  length              : 7
    1-------  Extension           : 1
    -000----  Type of number      : unknown
    ----0001  Numb. plan id.      : ISDN/teleph. numb. plan (Rec. E.164/E.163) _
```

```
    10..03    number              : 015127023030
```

Bild 59: Meldung SETUP wie im GSM und ISDN

8.3.9 IDENTITY REQUEST

Die Forderung nach einem SETUP wird vom Netz mit einer Frage nach der Identität des Mobiles beantwortet (Bild 60) . Das Mobile soll sich mit seiner IMEI ausweisen.

```
_____[ 23 ]_____[ group ID: 00 07 ]_____[ trace ID: 00 01 ]______

00 04 00 58  aa 3c 19 1f  09 40 00 40  a3 00 40


:WDCMA L3 RRC Peer messages
00  00000000  Channel LSB
:Channel Type MSB
04  00000100  Downlink DCCH

00  0000000001011000  length=88
           1  Integrity Check Info present
    01010100  MessageAuthenticationCode,
    01111000  MessageAuthenticationCode,
    00110010  MessageAuthenticationCode,
    00111110  MessageAuthenticationCode,
        0001  RRC-MessageSequenceNumber  = 1

: Message Type:
       00101  DOWNLINK DIRECT TRANSFER
           0  r3 SEQUENCE
           0  sw1 not present
DownlinkDirectTransfer-r3
          00  RRC-TransactionIdentifier = 0
:CN-DomainIdentity
           0  cs-domain,
:nas-Message
    000000000010  length=2
    0-------  direction from      : originating site
    -000----  TransactionID       : 0
    ----0101  Protocol Discrim.   : mobility management messages non GPRS
    00------  SendSequenceNumber  : 0
    --011000  MESSAGE TYPE        : IDENTITY REQUEST

: Type of Identity
    -----010  IMEI
```

Bild 60: Frage nach der Identität des Forderers des SETUP

Interessanterweise schickt das Mobile an dieser Stelle nicht seine IMEI sondern Den Hinweis auf einen *asn1-ViolationOrEncodingError*- (Bild 61)

```
_____[ 24 ]_____[ group ID: 00 07 ]_____[ trace ID: 00 01 ]______

00 07 00 98  95 9b e6 7d  10 84 80 00

:WDCMA L3 RRC Peer messages

00  00000000  Channel LSB
:Channel Type MSB
07  00000111  Uplink DCCH

00  0000000010011000  length=152
           1  Integrity Check Info present
    00101011  MessageAuthenticationCode,
    00110111  MessageAuthenticationCode,
    11001100  MessageAuthenticationCode,
    11111010  MessageAuthenticationCode,
```

```
        0010  RRC-MessageSequenceNumber  = 2

       00010  Message Type: Cell Change Order from UTRAN Failure
           0  CellChangeOrderFromUTRANFailure-r3-IEs :: SEWQUENCE{
           0  sw1 not present
           0  sw2 not present
          10  RRC-TransactionIdentifier = 2
:InterRAT-ChangeFailureCause
         010  ProtocolErrorInformation
:diagnosticsType
           0  ProtocolErrorCause
         000  asn1-ViolationOrEncodingError
```

Bild 61: Antwort auf IDENTITY REQUEST beim MOC mit Tracemobile

Wie in Abschnitt 9.3.5 beschrieben ist diese Irritation im MTC nicht aufgetreten, d.h. das Mobile schickt anstandslos im IDENTITY RESPONSE seine IMEI.

8.3.10 CALL PROCEEDING

Wie im ISDN und GSM antwortet das Netz, dass die Anforderung bearbeitet wird..

```
_____[ 25 ]_____[ group ID: 00 07 ]_____[ trace ID: 00 01 ]______

00 04 00 50  e9 1b fd 20  91 44 00 30  60 40


:WDCMA L3 RRC Peer messages

00  00000000  Channel LSB
:Channel Type MSB
04  00000100  Downlink DCCH

00  0000000001010000  length=80
           1  Integrity Check Info present
    11010010  MessageAuthenticationCode,
    00110111  MessageAuthenticationCode,
    11111010  MessageAuthenticationCode,
    01000001  MessageAuthenticationCode,
        0010  RRC-MessageSequenceNumber  = 2

: Message Type:
       00101  DOWNLINK DIRECT TRANSFER
           0  r3 SEQUENCE
           0  sw1 not present
DownlinkDirectTransfer-r3
          01  RRC-TransactionIdentifier = 1
:CN-DomainIdentity
           0  cs-domain,
:nas-Message
    000000000001  length=1
    1-------  direction to        : originating site
    -000----  TransactionID       : 0
    ----0011  Protocol Discrim.   : Call control and call related SS messages
    00------  SendSequenceNumber  : 0

    --000010  MESSAGE TYPE        : CALL PROCEEDING
```

Bild 62: Die SETUP-Forderung wird bearbeitet, CALL PROCEEDING.

8.3.11 FACILITY

Die Meldung FACILITY ist aus dem ISDN und dem GSM bekannt. Das Netz informiert im vorliegenden Falle das Mobile, dass das Leistungsmerkmal Call Forwarding zur Verfügung steht.
In den Bildern 29 und 30 (die von einem anderen Trace zur Verfügung stehen) ist die Meldung FACILITY nicht enthalten.

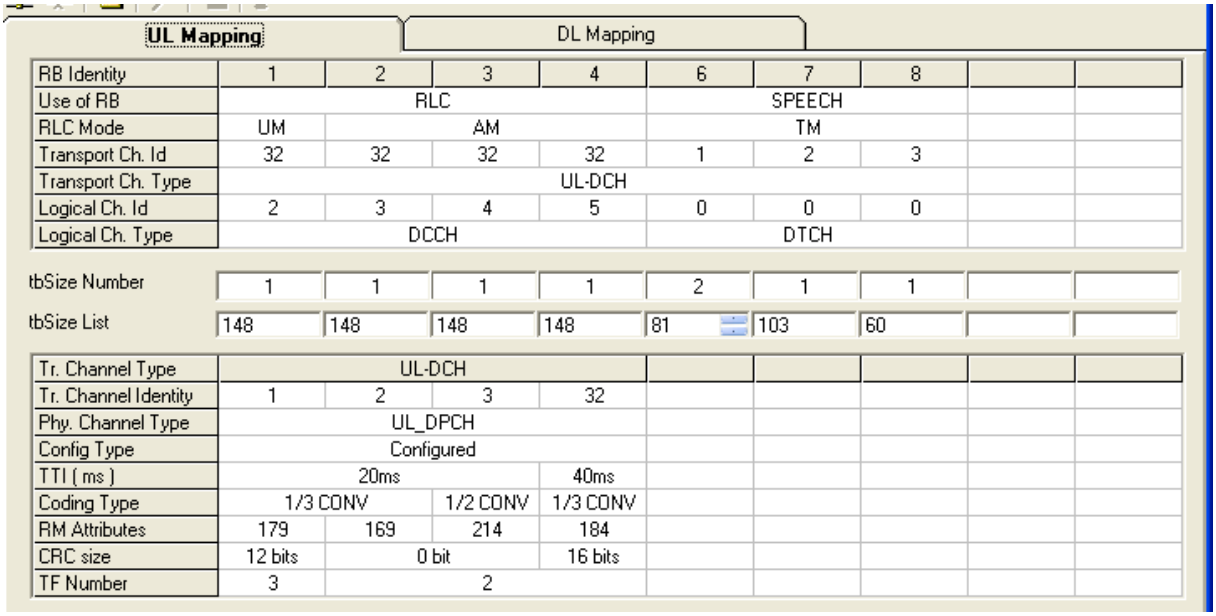
```
_____[ 26 ]_____[ group ID: 00 07 ]_____[ trace ID: 00 01 ]______

00 04 00 d8  e5 cd bb e1  19 48 02 50  67 42 14 21  c0 40 20 20
40 22 06 00  d0 20 25 10  80 20 e0


:WDCMA L3 RRC Peer messages
00  00000000  Channel LSB
:Channel Type MSB
04  00000100  Downlink DCCH
00  0000000011011000  length=216
          1  Integrity Check Info present
    11001011  MessageAuthenticationCode,
    10011011  MessageAuthenticationCode,
    01110111  MessageAuthenticationCode,
    11000010  MessageAuthenticationCode,
        0011  RRC-MessageSequenceNumber  = 3

: Message Type:
       00101  DOWNLINK DIRECT TRANSFER
           0  r3 SEQUENCE
           0  sw1 not present
DownlinkDirectTransfer-r3
          10  RRC-TransactionIdentifier = 2
:CN-DomainIdentity
           0  cs-domain,
:nas-Message
    000000010010  length=18
    1-------  direction to        : originating site
    -000----  TransactionID       : 0
    ----0011  Protocol Discrim.   : Call control and call related SS messages
    00------  SendSequenceNumber  : 0

    --111010  MESSAGE TYPE        : FACILITY
    00010000  Lgth OF IE FACILITY : 16
    10100001  Component           : Invoke
    00001110  length              : 14

    00000010  Type=INTEGER        : Invoke Identifier
    00000001  length              : 1
    00000001  Inv.ID. Value       : 1

    00000010  Type=INTEGER        : Operation Value
    00000001  length              : 1
    00010000  OperationValue      : notifySS

    00110000  Type=SEQUENCE       : Operation
    00000110  length              : 6

    10000001  IMPL.OCTETSTRING    : ss-code
    00000001  length              : 1
    00101000  ss-code Value       : allCondForwardingSS

    10000100  OCTETSTRING         : ss-status
    00000001  length              : 1
    00000111  P,R und A-bit       : Active and Operative, Registered, Provisioned
```

Bild 63: Das Vorhandensein von *Supplementary Services* .im Netz wir bekannt gegeben.

8.3.12 RADIO BEARER SETUP

Der Leser sei daran erinnert, dass im GSM dem Mobile nach dem SETUP mit der Meldung ASSIGNMENT COMMAND ein Transportkanal zugewiesen wurde.
Das Gleiche geschieht im UMTS mit der Meldung RADIO BEARER SETUP.
Da letzterer beinahe die gleiche Länge wie die Meldung RRC CONNECTION REQUEST aufweist, wird von der expliziten Darstellung des Traces abgesehen und ähnlich der Bilder

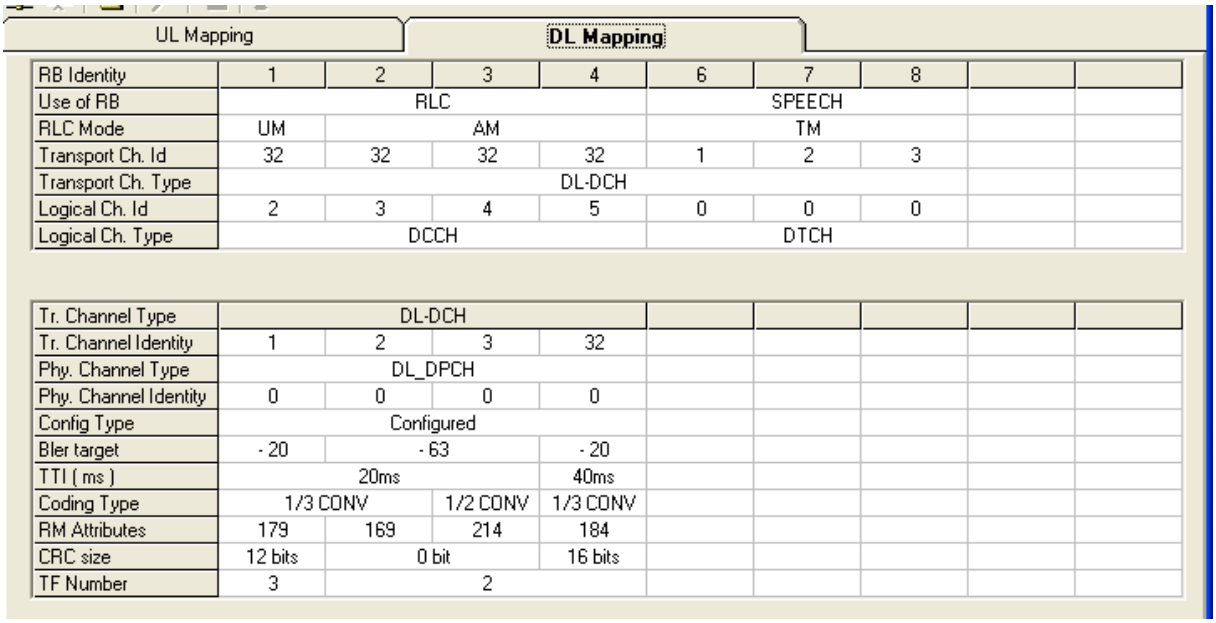
52 und 53 eine Wiedergabe der UL-DL Mappings der Kanäle gewählt.
Aus beiden Bildern ist zu ersehen, dass nunmehr ein Data Traffic Channel gebildet wird, über den im Transparent Mode die Sprache . übertragen wird..



UL Mapping | DL Mapping

RB Identity	1	2	3	4	6	7	8		
Use of RB	RLC				SPEECH				
RLC Mode	UM	AM			TM				
Transport Ch. Id	32	32	32	32	1	2	3		
Transport Ch. Type	UL-DCH								
Logical Ch. Id	2	3	4	5	0	0	0		
Logical Ch. Type	DCCH				DTCH				
tbSize Number	1	1	1	1	2	1	1		
tbSize List	148	148	148	148	81	103	60		
Tr. Channel Type	UL-DCH								
Tr. Channel Identity	1	2	3	32					
Phy. Channel Type	UL_DPCH								
Config Type	Configured								
TTI (ms)	20ms			40ms					
Coding Type	1/3 CONV		1/2 CONV	1/3 CONV					
RM Attributes	179	169	214	184					
CRC size	12 bits	0 bit		16 bits					
TF Number	3	2							

Bild 64: Uplink Kanäle die beim RADIO BEARER SETUP gebildet werden



UL Mapping | DL Mapping

RB Identity	1	2	3	4	6	7	8		
Use of RB	RLC				SPEECH				
RLC Mode	UM	AM			TM				
Transport Ch. Id	32	32	32	32	1	2	3		
Transport Ch. Type	DL-DCH								
Logical Ch. Id	2	3	4	5	0	0	0		
Logical Ch. Type	DCCH				DTCH				
Tr. Channel Type	DL-DCH								
Tr. Channel Identity	1	2	3	32					
Phy. Channel Type	DL_DPCH								
Phy. Channel Identity	0	0	0	0					
Config Type	Configured								
Bler target	- 20	- 63		- 20					
TTI (ms)	20ms			40ms					
Coding Type	1/3 CONV		1/2 CONV	1/3 CONV					
RM Attributes	179	169	214	184					
CRC size	12 bits	0 bit		16 bits					
TF Number	3	2							

Bild 65: Downlink Kanäle die beim RADIO BEARER SETUP gebildet werden

8.3.14 PROGRESS

Die Meldung PROGRESS stammt noch aus dem ISDN . Sie zeigt die Weiterverarbeitung eines Rufs im Falle des Erreichens von Netzübergängen an.

```
_____[ 31 ]_____[ group ID: 00 07 ]_____[ trace ID: 00 01 ]______

00 04 00 68  d8 3d 71 4f  a1 4c 00 90  60 60 5d 51

:WDCMA L3 RRC Peer messages

00  00000000  Channel LSB
:Channel Type MSB
04  00000100  Downlink DCCH

00  0000000001101000  length=104
          1  Integrity Check Info present
    10110000  MessageAuthenticationCode,
    01111010  MessageAuthenticationCode,
    11100010  MessageAuthenticationCode,
    10011111  MessageAuthenticationCode,
        0100  RRC-MessageSequenceNumber  = 4

: Message Type:
       00101  DOWNLINK DIRECT TRANSFER
           0  r3 SEQUENCE
           0  sw1 not present
   DownlinkDirectTransfer-r3
          11  RRC-TransactionIdentifier = 3
:CN-DomainIdentity
           0  cs-domain,
:nas-Message
    000000000100  length=4
    1-------  direction to        : originating site
    -000----  TransactionID       : 0
    ----0011  Protocol Discrim.   : Call control and call related SS messages
    00------  SendSequenceNumber  : 0

    --000011  MESSAGE TYPE        : PROGRESS
    00000010  L. OF IE PROG.IND.  : 2
    1-------  Extension           : 1
    -11-----  Coding standard     : Stand. Def. for the GSM-PLMNS as descryped.
    ---0----  Spare               : 0
    ----1010  Location            : Network beyond interworking point
```

Bild 66: Die aus dem ISDN und GSM bekannte Meldung Progress

8.3.15 ALERTING

Die Meldung ALERTING vom Netz gesendet bedeutet, dass die Wahlinformationen vollständig sind . Die Verbindung ist netzseitig bis zur Zielvermittlung aufgebaut.
Die Endeinrichtung ist zur Annahme des Rufs in der Lage. Der Teilnehmer wird gerufen.

```
_____[ 32 ]_____[ group ID: 00 07 ]_____[ trace ID: 00 01 ]______

00 04 00 70  f4 34 2b 17  29 40 00 b0  60 23 c0 5d  50

:WDCMA L3 RRC Peer messages

00  00000000  Channel LSB
:Channel Type MSB
04  00000100  Downlink DCCH

00  0000000001110000  length=112
          1  Integrity Check Info present
    11101000  MessageAuthenticationCode,
```

```
    01101000  MessageAuthenticationCode,
    01010110  MessageAuthenticationCode,
    00101110  MessageAuthenticationCode,
        0101  RRC-MessageSequenceNumber  = 5

: Message Type:
       00101  DOWNLINK DIRECT TRANSFER
           0  r3 SEQUENCE
           0  sw1 not present
DownlinkDirectTransfer-r3
          00  RRC-TransactionIdentifier = 0
:CN-DomainIdentity
           0  cs-domain,
:nas-Message
    000000000101  length=5
    1-------  direction to        : originating site
    -000----  TransactionID       : 0
    ----0011  Protocol Discrim.   : Call control and call related SS messages
    00------  SendSequenceNumber  : 0

    --000001  MESSAGE TYPE        : ALERTING

    00011110  INFORMATION ELEMENT : Progress indicator
    00000010  L. OF IE PROG.IND.  : 2
    1-------  Extension           : 1
    -11-----  Coding standard     : Stand. Def. for the GSM-PLMNS as descry.
    ---0----  Spare               : 0
    ----1010  Location            : Network beyond interworking point
```

Bild 67: Die aus dem ISDN und GSM bekannte Meldung ALERTING

8.3.16 CONNECT

Dem Mobile wird mitgeteilt, dass ein Sprachkanal zugeteilt und im Netz durchgeschaltet wurde.

```
_____[ 34 ]_____[ group ID: 00 07 ]_____[ trace ID: 00 01 ]______

00 04 00 50  db 15 ad 23  b1 44 00 30  60 e0

:WDCMA L3 RRC Peer messages
00  00000000  Channel LSB
:Channel Type MSB
04  00000100  Downlink DCCH
00  0000000001010000  length=80
           1  Integrity Check Info present
    10110110  MessageAuthenticationCode,
    00101011  MessageAuthenticationCode,
    01011010  MessageAuthenticationCode,
    01000111  MessageAuthenticationCode,
        0110  RRC-MessageSequenceNumber  = 6
: Message Type:
       00101  DOWNLINK DIRECT TRANSFER
           0  r3 SEQUENCE
           0  sw1 not present
DownlinkDirectTransfer-r3
          01  RRC-TransactionIdentifier = 1
:CN-DomainIdentity
           0  cs-domain,
:nas-Message
    000000000001  length=1
    1-------  direction to        : originating site
    -000----  TransactionID       : 0
    ----0011  Protocol Discrim.   : Call control and call related SS messages
    00------  SendSequenceNumber  : 0

    --000111  MESSAGE TYPE        : CONNECT
```

Bild 68: Die aus dem ISDN und GSM bekannte Meldung CONNECT

8.3.17 CONNECT ACKNOWLEDGE

Das Mobile schaltet den Sprachkanal an und quittiert dies dem Netz.

```
_____[ 35 ]_____[ group ID: 00 07 ]_____[ trace ID: 00 01 ]______

00 07 00 50  f5 c4 c3 36  9e c0 00 81  e7 80

:WDCMA L3 RRC Peer messages

00  00000000  Channel LSB
:Channel Type MSB
07  00000111  Uplink DCCH
00  0000000001010000  length=80
          1  Integrity Check Info present
    11101011  MessageAuthenticationCode,
    10001001  MessageAuthenticationCode,
    10000110  MessageAuthenticationCode,
    01101101  MessageAuthenticationCode,
        0011  RRC-MessageSequenceNumber  = 3
       11011  Message Type :UPLINK DIRECT TRANSFER
: switches
              measuredResultsOnRach sw1
          0  sw1 not present
              laterNonCriticalExtensions sw2
          0  sw2 not present

:CN-DomainIdentity
          0  cs-domain,
:nas-Message
    000000000001  length=1
    0-------  direction from      : originating site
    -000----  TransactionID       : 0
    ----0011  Protocol Discrim.   : Call control and call related SS messages
    11------  SendSequenceNumber  : 1

    --001111  MESSAGE TYPE        :CONNECT ACKNOWLEDGE
```

Bild 69 : Die aus dem ISDN und GSM bekannte Meldung CONNECT ACKNOWLEDGE

Nunmehr wird auf dem Sprachkanal Information ausgetauscht. Aus dem Bild 30 und Bild 31 geht hervor, dass zwischen den Zeitmarken 62616 und 68804 der Sprachkanal aktiv ist . In dieser Zeit finden regelmäßig Kanalmessungen statt. Im Ergebnis dessen sendet das Netz erforderlichenfalls Anweisungen für ein Update des Active Sets. Das Mobile antwortet mit ACTIVE SET UPDATE COMPLETE.

8.3.18 DISCONNECT

In unserem Beispiel wird die Verbindung von der Gegenstelle ausgelöst.. Das Netz zeigt an dass die Ende zu Ende Verbindung ausgelöst ist..

```
_____[ 36 ]_____[ group ID: 00 07 ]_____[ trace ID: 00 01 ]______

00 04 00 68  dc e9 11 a6  b9 48 00 90  64 a0 5c 12

:WDCMA L3 RRC Peer messages

00  00000000  Channel LSB
:Channel Type MSB
04  00000100  Downlink DCCH
00  0000000001101000  length=104
          1  Integrity Check Info present
    10111001  MessageAuthenticationCode,
    11010010  MessageAuthenticationCode,
```

```
    00100011  MessageAuthenticationCode,
    01001101  MessageAuthenticationCode,
        0111  RRC-MessageSequenceNumber  = 7

: Message Type:
       00101  DOWNLINK DIRECT TRANSFER
           0  r3 SEQUENCE
           0  sw1 not present
DownlinkDirectTransfer-r3
          10  RRC-TransactionIdentifier = 2
:CN-DomainIdentity
           0  cs-domain,
:nas-Message
    000000000100  length=4
    1-------  direction to        : originating site
    -000----  TransactionID       : 0
    ----0011  Protocol Discrim.   : Call control and call related SS messages
    00------  SendSequenceNumber  : 0

    --100101  MESSAGE TYPE        : DISCONNECT

    00000010  LENGTH OF IE CAUSE  : 2
    1-------  Extension Bit       : 1
    -11-----  Coding stand.       : Standard defined for the GSM-PLMNS
    ---0----  spare               : 0
    ----0000  location            : user
```

Bild 70 : Die aus dem ISDN und GSM bekannte Meldung DISCONNECT

8.3.19 RELEASE

Das Mobile reagiert auf DISCONNECT und gibt den Sprachkanal frei.

```
_____[ 37 ]_____[ group ID: 00 07 ]_____[ trace ID: 00 01 ]______

00 07 00 50  a6 89 05 24  26 c0 00 81  96 80

:WDCMA L3 RRC Peer messages
00  00000000  Channel LSB
:Channel Type MSB
07  00000111  Uplink DCCH
00  0000000001010000  length=80
           1  Integrity Check Info present
    01001101  MessageAuthenticationCode,
    00010010  MessageAuthenticationCode,
    00001010  MessageAuthenticationCode,
    01001000  MessageAuthenticationCode,
        0100  RRC-MessageSequenceNumber  = 4
       11011  Message Type :UPLINK DIRECT TRANSFER
: switches
              measuredResultsOnRach sw1
           0  sw1 not present
              laterNonCriticalExtensions sw2
           0  sw2 not present
:CN-DomainIdentity
           0  cs-domain,
:nas-Message
    000000000001  length=1
    0-------  direction from      : originating site
    -000----  TransactionID       : 0
    ----0011  Protocol Discrim.   : Call control and call related SS messages
    00------  SendSequenceNumber  : 0

    --101101  MESSAGE TYPE          : RELEASE
```

Bild 71: Die aus dem ISDN und GSM bekannte Meldung RELEASE

8.3.20 RELEASE COMPLETE

Das Netz quittiert das vom Mobile gesendete RELEASE und gibt seinerseits die Ressource frei.

```
_____[ 38 ]_____[ group ID: 00 07 ]_____[ trace ID: 00 01 ]______

00 04 00 70  f0 bf c1 2a  41 4c 00 b0  65 41 00 5c  12

:WDCMA L3 RRC Peer messages

00  00000000  Channel LSB
:Channel Type MSB
04  00000100  Downlink DCCH

00  0000000001110000  length=112
          1  Integrity Check Info present
    11100001  MessageAuthenticationCode,
    01111111  MessageAuthenticationCode,
    10000010  MessageAuthenticationCode,
    01010100  MessageAuthenticationCode,
        1000  RRC-MessageSequenceNumber  = 8

: Message Type:
       00101  DOWNLINK DIRECT TRANSFER
           0  r3 SEQUENCE
           0  sw1 not present
DownlinkDirectTransfer-r3
          11  RRC-TransactionIdentifier = 3
:CN-DomainIdentity
           0  cs-domain,
:nas-Message
    000000000101  length=5
    1-------  direction to        : originating site
    -000----  TransactionID       : 0
    ----0011  Protocol Discrim.   : Call control and call related SS messages
    00------  SendSequenceNumber  : 0

    --101010  MESSAGE TYPE        : RELEASE COMPLETE

    00001000  INFORMATION ELEMENT : Cause
    00000010  LENGTH OF IE CAUSE  : 2
    1-------  Extension Bit       : 1
    -11-----  Coding stand.       : Standard defined for the GSM-PLMNS
    ---0----  spare               : 0
    ----0000  location            : user
```

Bild 72: Die aus dem ISDN und GSM bekannte Meldung RELEASE COMPLETE

8.3.21 RRC CONNECTION RELEASE

Es folgt nun die Auflösung der UMTS-Verbindung durch das Netz.

```
_____[ 39 ]_____[ group ID: 00 07 ]_____[ trace ID: 00 01 ]______

00 04 00 38  d8 41 6e 8b  8b c8

:WDCMA L3 RRC Peer messages

00  00000000  Channel LSB
:Channel Type MSB
04  00000100  Downlink DCCH
00  0000000000111000  length=56
          1  Integrity Check Info present
    10110000  MessageAuthenticationCode,
    10000010  MessageAuthenticationCode,
    11011101  MessageAuthenticationCode,
    00010111  MessageAuthenticationCode,
        0001  RRC-MessageSequenceNumber  = 1
```

```
       01111  Message Type : RRC-CONNECTION RELEASE
           0  r3
              laterNonCriticalExtensions sw1
           0  sw1 not present

RRCConnectionRelease-r3-IEs
              n-308 sw1
           1  sw1 present
              rplmn-information sw2
           0  sw2 not present
-- User equipment IEs
              Radio Resource Control transaction identifier
          00  RRC transaction identifier  : 0
```

Bild 73: Der UMTS-Kanal wird durch das Netz frei gegeben

8.3.22 RRC CONNECTION RELEASE COMPLETE

Das Mobile quittiert die Freigabe des Kanals.

```
_____[ 40 ]_____[ group ID: 00 07 ]_____[ trace ID: 00 01 ]______

00 07 00 30  e6 e0 3c 5c  0c 40

:WDCMA L3 RRC Peer messages

00  00000000  Channel LSB
:Channel Type MSB
07  00000111  Uplink DCCH

00  0000000000110000  length=48
           1  Integrity Check Info present
    11001101  MessageAuthenticationCode,
    11000000  MessageAuthenticationCode,
    01111000  MessageAuthenticationCode,
    10111000  MessageAuthenticationCode,
        0001  RRC-MessageSequenceNumber  = 1


       10001  Message Type : RRC-CONNECTION RELEASE COMPLETE

              errorIndication sw1
           0  sw1 not present
              laterNonCriticalExtensions sw2
           0  sw2 not present

              Radio Resource Control transaction identifier
          00  RRC transaction identifier  : 0
```

Bild 74: RRC-CONNECTION RELEASE COMPLETE durch das Mobile

9. MELDUNGEN IM MTC

9.1. Idle Mode im MTC

Das Procedere im Mobile Terminated Call (MTC) im UMTS unterscheidet sich vom MOC in der gleichen Weise wie MOC UND MTC im GSM.
Im Idle Mode tritt außer den im Abschnitt 8.1 beschriebenen Systeminformationen noch die Meldung PAGING REQUEST auf.

9.1.1 Die Meldung PAGING REQUEST

In der Meldung PAGING REQUEST wird das Mobile anhand seiner TMSI gerufen

```
_____[ 1 ]_____[ group ID: 00 07 ]_____[ trace ID: 00 01 ]______

00 02 00 f0  40 c3 26 02  cf 88 00 00  00 00 00 00  00 00 00 00
00 00 00 00  00 00 00 00  00 00 00 00  00 00


:WDCMA L3 RRC Peer messages

00  00000000  Channel LSB
:Channel Type MSB
02  00000010  PCCH

00  0000000011110000  length=240
00         0  MESSAGE TYPE: PAGING TYPE 1

           1  sw1 present
           0  sw2 not present
           0  sw3 not present
 1..8 Paging records
         000  val1: 0
           0  cn-Identity
:Paging cause
         110  terminatingCauseUnknown
:Cn-Domainidentity
           0  cs-domain
:cn-pagedUE-Identity
         001  TMSI-GSM-MAP
    10010011  hex
    00000001  hex
    01100111  hex
    11000100  hex
```

Bild 75: Die Meldung PAGING REQUEST Type 1

9.2 Das gerufene Mobile muss sich im Netz anmelden

Wie mit Bild 23 erklärt klopft das Mobile beim Netz an und sendet nach Empfang der AICH Präambel die in Abschnitt 8.3.1 beschriebene Meldung RRC CONNECTION REQUEST. Das Netz sendet die Einstellvorschrift für das Mobile mit der Meldung RRC CONNECTION SETUP, die das Mobile mit RRC CONNECTION SETUP COMPLETE bestätigt.

9.3 Meldungen die sich vom Aufbau des MOC unterscheiden

Der mit dem Rufaufbau im GSM vertraute, findet nun alle bekannten NAS-Messages des MTC im UMTS-Trace wieder.

9.3.1 Die Meldung PAGING RESPONSE

In der Meldung PAGING RESPONSE sendet das Mobile seine technischen Eigenschaften im IE. CLASSMARK 2 und seine Identität in Gestalt der TMSI

```
_____[ 11 ]_____[ group ID: 00 07 ]_____[ trace ID: 00 01 ]______

00 07 00 a8  15 00 0b 00  60 31 38 08  1a b8 c5 08  2f a4 98 17
41 d2 00 00  40

:WDCMA L3 RRC Peer messages

00  00000000  Channel LSB
:Channel Type MSB
07  00000111  Uplink DCCH

00  0000000010101000  length=168
           0  IntegrityCheckinfo absent

: Message Type:
       00101  INITIAL DIRECT TRANSFER

: switches
              measuredResultsOnRach sw1
           0  sw1 not present
              v3a0NonCriticalExtensions sw2
           1  sw2 present
              -- Core network IEs
:CN-DomainIdentity
           0  cs-domain,
IntraDomainNasNodeSelector
              version
           0  release99
              cn-Type Choice {
           0  Gsm-map-IntraDomainNASNodeSelector
              routingbasis
         000  localPTMSI
              RoutingParameter ::= BIT STRING (SIZE (10))
    0000001011  bit

           0  entered parameter
:nas-Message
    000000001100  length=12
    0-------  direction from      : originating site
    -000----  TransactionID       : 0
    ----0110  Protocol Discrim.   : radio resource management messages

    0-------  1 spare bit         : 0
    -0------  Send sequence number: value

    --100111  MESSAGE TYPE        : PAGING RESPONSE

: Ciphering Key Sequence  Number
    ----0---  1 spare bit         : 0
    -----001  Ciph. key sequ. num.: 1 (7=no key available)
    0000----  4 spare bits        : 0

: Mobile Station Classmark 2
    00000011  lgth of MS Cl.Mark2 : 3

    0-------  1 spare             : 0
    ---1----  "Controlled Early Classmark Sending" option is implemented in the MS
    ----0---  Encryp.Algor. A5_1  : available

    0-------  1 spare bit         : 0
    -0------  pseudo-synch.capab. : not present
    --01----  SS Screening Indic. : phase 2 error handling
    ----1---  Mobile station supports mobile terminated point to point SMS
     -----0--  no VoiceBroadcastService (VBS) capability or no notifications wanted
    ------0-  no VoiceGroupCallService (VGCS) capability or no notifications wanted
    -------0  The MS does not support the E-GSM or R-GSM band

     -0------  1 spare bit         : 0
    --1-----  LocationServiceValueAdded Capability supported
    ---0----  1 spare bit         : 0
    ----0---  SoLSA Capability    : not supported
    -----0--  Network initiated MO CM connection request not supported.
    ------0-  encryp.algorith.A5/3: not available
    -------1  encryp.algorith.A5/2: available

: Mobile Identity

    00000101  length of Mob. ident: 5
```

```
    1111----  Identity Digit 1    : 15
    ----0---  No. of ID digits    : even
    -----100  Type of identity    : TMSI/P-TMSI
    10010011  Identity Digit 2,3  : take hex value
    00000010  Identity Digit 4,5  : take hex value
    11101000  Identity Digit 6,7  : take hex value
    00111010  Identity Digit 8,9  : take hex value

v3a0NonCriticalExtensions SEQUENCE {
              InitialDirectTransfer-v3a0ext
    0100000000000000000  START-Value = 262144
```

Bild 76: Die Meldung PAGING RESPONSE

9.3.2 Die Meldungen zwischen PAGING RESPONSE UND SETUP

Nach PAGING RESPONSE fordert das Netz auf zum MEASUREMENT CONTROL und danach zum Einstellen der Sicherheitsparameter mit der Meldung SECURITY MODE COMMAND.
Das Mobile quittiert mit SECURITY MODE COMPLETE. Beim folgenden IDENTITY REQUEST verlangt das Netz die IMEI des Mobiles, die letzteres im IDENTITY RESPONSE schickt.

9.3.3 Das SETUP im Mobile Terminated Call

Der BEARER im SETUP hat im Unterschied zum MOC nur ein Element, dort 5.
Außerdem wird die Nummer des Rufenden Partners gezeigt.

```
_____[ 18 ]_____[ group ID: 00 07 ]_____[ trace ID: 00 01 ]______

00 04 00 e8  92 6e 6c 45  91 44 02 82  60 a0 80 34  0b 81 22 30
72 8a 24 20  e6 46 1e 0f
:WDCMA L3 RRC Peer messages
00  00000000  Channel LSB
:Channel Type MSB
04  00000100  Downlink DCCH
00  0000000011101000  length=232
          1  Integrity Check Info present
    00100100  MessageAuthenticationCode,
    11011100  MessageAuthenticationCode,
    11011000  MessageAuthenticationCode,
    10001011  MessageAuthenticationCode,
        0010  RRC-MessageSequenceNumber  = 2
: Message Type:
       00101  DOWNLINK DIRECT TRANSFER
           0  r3 SEQUENCE
           0  sw1 not present
DownlinkDirectTransfer-r3
          01  RRC-TransactionIdentifier = 1
:CN-DomainIdentity
           0  cs-domain,
:nas-Message
    000000010100  length=20
    0-------  direction from      : originating site
    -001----  TransactionID       : 1
    ----0011  Protocol Discrim.   : Call control and call related SS messages
    00------  SendSequenceNumber  : 0

    --000101  MESSAGE TYPE        : SETUP

    00000100  INFORMATION ELEMENT : Bearer capability
    00000001  length              : 1
    1-------  Extension           : 1
    -01-----  Radio Channel Req.  : full rate support only MS
    ---0----  Coding Standard     : GSM standard coding
    ----0---  Transfer Mode       : Circuit Mode
    -----000  Info Transfer Cap.  : speech
```

```
    01011100  INFORMATION ELEMENT : Calling party BCD number
    00001001  length              : 9
    0-------  Extension           : 0
    -001----  Type of number      : international number
    ----0001  Numb. plan id.      : ISDN/telephony numb. pl. (Rec. E.164/E.163)
    1-------  Extension           : 1
    -00-----  Present.indic.      : Presentation allowed
    ---000--  spare               : 0
    ------11  Present.indic.      : Network provided
94..f0        number              : 4915127023030
```

Bild 77: SETUP im MTC

9.3.4 Die Meldung CALL CONFIRMED

Das Mobile bestätigt mit CALL CONFIRMED dass es den Ruf annehmen kann. Hier wird ausführlich die Eigenschaft des einzustellenden Beares mitgeteilt.

```
_____[ 19 ]_____[ group ID: 00 07 ]_____[ trace ID: 00 01 ]______

00 07 00 a8  eb d6 b2 e6  16 c0 06 49  a4 02 02 90  02 01 00 42
8a 81 00 80  80
:WDCMA L3 RRC Peer messages
00  00000000  Channel LSB
:Channel Type MSB
07  00000111  Uplink DCCH
00  0000000010101000  length=168
          1  Integrity Check Info present
    11010111  MessageAuthenticationCode,
    10101101  MessageAuthenticationCode,
    01100101  MessageAuthenticationCode,
    11001100  MessageAuthenticationCode,
        0010  RRC-MessageSequenceNumber  = 2
       11011  Message Type :UPLINK DIRECT TRANSFER
: switches
              measuredResultsOnRach sw1
          0  sw1 not present
              laterNonCriticalExtensions sw2
          0  sw2 not present
:CN-DomainIdentity
          0  cs-domain,
:nas-Message
    000000001100  length=12
    1-------  direction to        : originating site
    -001----  TransactionID       : 1
    ----0011  Protocol Discrim.   : Call control and call related SS messages
    01------  SendSequenceNumber  : 1

    --001000  MESSAGE TYPE        : CALL CONFIRMED

    00000100  INFORMATION ELEMENT : Bearer capability
    00000101  length              : 5
    0-------  Extension           : 0
    -01-----  Radio Channel Req.  : full rate support only MS
    ---0----  Coding Standard     : GSM standard coding
    ----0---  Transfer Mode       : Circuit Mode
    -----000  Info Transfer Cap.  : speech
    0-------  Extension           : 0
    -0------  Coding              : octet used for extension of inf. transf. capab.
    --00----  Spare               : 00
    ----0100  speech Vers. indic. : GSM full rate speech version 3
    0-------  Extension           : 0
    -0------  Coding              : octet used for extension of inf. transf. capab.
    --00----  Spare               : 00
    ----0010  speech Vers. indic. : GSM full rate speech version 2
    0-------  Extension           : 0
    -0------  Coding              : octet used for extension of inf. transf. capab.
    --00----  Spare               : 00
    ----0000  speech Vers. indic. : GSM full rate speech version 1
    1-------  Extension           : 1
    -0------  Compression         : data compression not possible
```

```
   --00----  Structure           : service data unit integrity
   ----0---  Duplex Mode         : half duplex
   ------
```

Bild 78: Die Meldung CALL CONFIRMED

9.3.5 Die Meldungen nach CALL CONFIRMED

Wie im MOC muss nun ein Sprachkanal aufgebaut werden. Dazu wird vom Netz die Meldung RADIO BEARER SETUP gesendet und vom Mobile mit RADIO BEARER SETUP COMPLETE quittiert. Die Bereitschaft das Gespräch nun anzunehmen wird vom MOBILE mit ALERTING angezeigt. Interessanter Weise kann das Gespräch nun ohne Austausch der Meldung CONNECT stattfinden.
Der Meldungsaustausch während des Gesprächs entspricht dem im MOC.

10. MELDUNGEN in einer WAP-Verbindung

Die beschriebene ps –Verbindung hat denselben Aufbau wie eine Verbindung im GPRS/EDGE.

10.1 IDLE MODE

Im Idle-Mode des Traces findet man die Meldungen Sysinfo Type 1, 3, 18, 2 und 7 den MasterInformationsBlock sowie SystemInformationen-BCCH wie in Abschnitt 8.1 beschrieben.

10.2 Verbindungsprozedur für das GMM ATTACH

10.2.1 RRC CONNECTION REQUEST

Aktivierung des Icons *WEB* im Menü des Mobiles und Herstellen der Verbindung zum Server von Vodafone.live! löst das in Bild 23 dargestellte Anklopfen beim Netz aus. Nach Empfang .der Genehmigung über den AICH, sendet das Mobile die Meldung RRC CONNECTION REQUEST zum Netz (Bild 79).

```
_____[ 41 ]_____[ group ID: 00 07 ]_____[ trace ID: 00 01 ]______

00 06 00 a6  31 92 46 eb  3c 26 20 10  09 b3 01 10  00 00 00 00
00 00 00 00  00

:WDCMA L3 RRC Peer messages
00  00000000  Channel LSB
:Channel Type MSB
06  00000110  Uplink CCCH
00  0000000010100110  length=166
          0  IntegrityCheckinfo absent
: Message Type:
         01  RRC CONNECTION REQUEST
-- User equipment IEs
: switches
             measuredResultsOnRach sw1
          1  sw1 present
             v3d0NonCriticalExtensions sw2
          0  sw2 not present
InitialUE-Identity::= Choice{
```

```
         001  Choice: TMSI-and-LAI-GSM-MAP
: TMSI
92  10010010  take hex value
46  01000110  take hex value
eb  11101011  take hex value
3c  00111100  take hex value
: LAI
: PLMN-identity
: MCC
        0010  Mobile CC digit 1   : 2
        0110  Mobile CC digit 2   : 6
        0010  Mobile CC digit 3   : 2

: MNC
           0  val2: 0
        0000  Mobile NC digit     : 0
        0010  Mobile NC digit     : 2

:LAC
01  00000001  Loc. area code (LAI) = ID of MSC (hex)
36  00110110  Loc. area code (LAI) = ID of BSC (hex)

Establishment cause
       01100  registration,
}

ProtocolErrorIndicator ::= Enumerated {
           0  No Error
}

-- Measurement IEs
MeasuredResultsOnRach ::= SEQUENCE {

               monitoredCells (sw3)
           0  sw3 not present

              currentCell
              modeSpecification
           0  fdd
              measurementQuantity
          00  CPICH-EC-NO: Common Pilot Channel,The received energy per chip divided by the
power density in the band
: Measurement Value
      100010  2 dB
```

Bild 79: Meldung RRC CONNECTION REQUEST eine WAP-Anrufes

Man beachte den Establishment cause der mit "*registration*" angegeben wird. In Bild 50 wurde die Telephonieverbindung mit der Begründung „*originatingConversationaCall"* angefordert.
.Im Trace folgt nun nicht sofort das RRC CONNECTION SETUP wie im Zusammenhang mit dem MOC beschrieben, sondern das Mobile verbleibt noch für die Dauer von 4 Meldungen im Idle Mode.
Sodann werden die Meldungen RRC CONNECTION SETUP und RRC CONNECTION COMPLETE ausgetauscht (vergl. Pkt. 8.2.2 und 8.3.3)

10.2.2 RRC CONNECTION SETUP

Die Meldung RRC CONNECTION SETUP ist wieder sehr umfangreich, da mehrere Kanäle eingerichtet werden müssen. (Im Gegensatz zum GPRS bei dem die Meldung IMMEDIATE ASSIGNMENT nur einen SDDCH als Signalkanal zuweist)
Die für die Signalisation aufzubauenden Kanäle sind in Bild 80 Uplink und in Bild 81 Downlink dargestellt

UL Mapping | DL Mapping

RB Identity	1	2	3	4					
Use of RB	RLC								
RLC Mode	UM	AM							
Transport Ch. Id	32	32	32	32					
Transport Ch. Type	UL-DCH								
Logical Ch. Id	2	3	4	5					
Logical Ch. Type	DCCH								
tbSize Number	1	1	1	1					
tbSize List	148	148	148	148					
Tr. Channel Type	RACH								
Tr. Channel Identity	1								
Phy. Channel Type	PRACH								
Config Type	Configured								
TTI (ms)	20ms								
Coding Type	1/2 CONV								
RM Attributes	149								
CRC size	16 bits								
TF Number	2								

Bild 80: Die für die Signalisation im UPLINK gebildeten Kanäle

UL Mapping | DL Mapping

RB Identity	1	2	3	4					
Use of RB	RLC								
RLC Mode	UM	AM							
Transport Ch. Id	32	32	32	32					
Transport Ch. Type	DL-DCH								
Logical Ch. Id	2	3	4	5					
Logical Ch. Type	DCCH								
Tr. Channel Type	FACH								
Tr. Channel Identity	6	7							
Phy. Channel Type	S_CCPCH								
Phy. Channel Identity	0	0							
Config Type	Configured								
Bler target	0								
TTI (ms)	10ms								
Coding Type	1/2 CONV	1/3 TURBO							
RM Attributes	219	129							
CRC size	16 bits								
TF Number	3	2							

Bild 81: Die für die Signalisation im DOWNLINK gebildeten Kanäle

Der Inhalt der Meldung RRC SETUP COMPLETE entspricht dem in Bild 54 gezeigten.

10.2.3 ATTACH REQUEST

Genau wie im GPRS muss nun ein GMM Context aufgebaut werden. Das Mobile sendet dem Netz seine technischen Eigenschaften, die Identität und die alte Routing Area identity.

```
_____[ 48 ]_____[ group ID: 00 07 ]_____[ trace ID: 00 01 ]______

00 07 01 50  15 80 0d 01  08 40 08 17  2a 00 08 38  20 2f a6 00
1a 42 2b 17  91 00 09 b0  08 58 af 9c  11 9a a1 51  99 32 25 0c
c0 b8 b2 00  00 80

:WDCMA L3 RRC Peer messages
00  00000000  Channel LSB
:Channel Type MSB
07  00000111  Uplink DCCH
01  0000000101010000  length=336
          0  IntegrityCheckinfo absent
: Message Type:
       00101  INITIAL DIRECT TRANSFER
: switches
              measuredResultsOnRach sw1
          0  sw1 not present
              v3a0NonCriticalExtensions sw2
          1  sw2 present
              -- Core network IEs
:CN-DomainIdentity
          1  ps-domain
IntraDomainNasNodeSelector
              version
          0  release99 SEQUENCE {
              cn-Type
          0  Gsm-map-IntraDomainNASNodeSelector
              routingbasis
        000  localPTMSI
              RoutingParameter
    0000001101  bit
              }
          0  enteredparameter = false

:nas-Message
    000000100001  length=33
    0-------  direction from      : originating site
    -000----  TransactionID       : 0
    ----1000  Protocol Discrim.   : GPRS mobility management messages

    00000001  MESSAGE TYPE        : ATTACH REQUEST

: Network Capability

    00000010  Lgth Netw. Capabil. : 2

    1-------  GPRS encryption algor GEA/1  available
    -1------  pp SMS via dedicated sign. channels MS supports mobile terminated
    --1-----  pp SMS via GPRS packet data channels. MS supports mobile terminated
    ---0----  the ME has a preference for the default alphabet over UCS2
    ----01--  Suppl.Serv. Screening Indicator capability of handling of ellipsis notation and
phase 2 error handling
    ------0-  The ME does not support SoLSA
    -------1  Revision level indicator
    0-------  Mobile station does not support BSS packet flow procedures
    -1------  Encryption algorithm GEA/2 available
    --0-----  Encryption algorithm GEA/3 not available
    ---0----  Encryption algorithm GEA/4 not available
    ----0---  Encryption algorithm GEA/5 not available
    -----0--  Encryption algorithm GEA/6 not available
    ------0-  Encryption algorithm GEA/7 not available
    -------0  location request notification via PS domain not supported

: Attach Type & Ciphering key sequence number

    ----0---  spare bit           : 0
    -----001  Attach Type         : GPRS attach
    0-------  spare               : 0
    -000----  Cipher.key seq.numb.: 0
```

```
: DRX Parameter

    00000111  Split PG Cycle Code : 7, see Table 10.5.139/GSM 04.08: DRX parameter information
element

    0000----  spare bits          : 0
    ----0---  Split On CCCH       : not supported by MS
    -----100  max. 8 sec non-DRX mode after transfer state

: Mobile Identity

    00000101  length of Mob.ident.: 5
    1111----  Identity Digit 1    : 95
    ----0---  No. of ID digits    : even
    -----100  Type of identity    : TMSI/P-TMSI
    1100----  Identity Digit 2    : 12
    ----0000  Identity Digit 3    : 0
    0000----  Identity Digit 4    : 0
    ----0011  Identity Digit 5    : 3
    0100----  Identity Digit 6    : 4
    ----1000  Identity Digit 7    : 8
    0100----  Identity Digit 8    : 4
    ----0101  Identity Digit 9    : 5

: Old Routing Area Identification

    ----0010  MCC digit 1        : 2
    0110----  MCC digit 2        : 6
    ----0010  MCC digit 3        : 2

    1111----  MNC digit 3        : 15
    ----0000  MNC digit 1        : 0
    0010----  MNC digit 2        : 2

    00000001  Location area code : take hex-value
    00110110  cont'd LAC         : take hex-value
    00000001  Routing Area Code  : take hex-value

: MS Radio Access capability IE
    00001011  length             : 11

: MS RA capability value part struct
: Access Technology Type
       0001  GSME -- note that GSM E covers GSM P
: Access capabilities struct
     0101111  length in bits of Content and spare bits = 47
: Access capabilities: Content
         100  RF power capability  : 4
           1  A5 bits Present
     1------  encryption algorithm A5/1  available
     -1-----  encryption algorithm A5/2  available
     --0----  encryption algorithm A5/3 not available
     ---0---  encryption algorithm A5/4 not available
     ----0--  encryption algorithm A5/5 not available
     -----0-  encryption algorithm A5/6 not available
     ------0  encryption algorithm A5/7 not available

        1---  "controlled early Classmark Sending" option is implemented
        -0--  Pseudo Synchronisation capability not present
        --0-  no Voice Group Call Service capability or no notifications wanted
        ---0  no Voice Broadcast Service capability or no notifications wanted
:Multislot capability
           1  Multislot capability  present
           1  HSCSD Multi Slot Capability
       00110  HSCSD Multi Slot Class = 6
           1  GPRS multislot class present
: GPRS multislot class
:       Slots Rx Tx Sum (max number)
       01010  4  2  5
           0  Extended Dynamic Allocation Capability for GPRS is not implemented
           0  SMS_VALUE , SM_VALUE not present
:Additions in release 99
           0  ECSD multislot class not present
           1  EGPRSmultiSlotClass
       01010  Class = 10 see TS 45.002
: EGPRS Extended Dynamic Allocation Capability
           0  Extended Dynamic Allocation Capability for GPRS is not implemented
           0  DTM GPRS multislot class not present
```

```
: Additions in Release 99
           1  8 PSK Power Capability present
          10  Power class E2
           0  COMPACT Interference Measurement Capability is not implemented
           1  The ME is Release "99 onwards
           1  UMTS FDD supported
           0  UMTS 3.84 Mcps TDD not supported
           0  CDMA 2000 not supported
           1  New MS Radio Access capability IE
: Access Technology Type
        0011  GSM 1800
: Access capabilities struct
     0010001  length in bits of Content and spare bits = 17
: Access capabilities: Content
         001  RF power capability  : 1
           0  A5 bits  not  present
        1---  "controlled early Classmark Sending" option is implemented
        -0--  Pseudo Synchronisation capability not present
        --0-  no Voice Group Call Service capability or no notifications wanted
        ---0  no Voice Broadcast Service capability or no notifications wanted
           0  Multislot capability not present
: Additions in Release 99
           1  8 PSK Power Capability present
          10  Power class E2
           0  COMPACT Interference Measurement Capability is not implemented
           1  The ME is Release "99 onwards
           1  UMTS FDD supported
           0  UMTS 3.84 Mcps TDD not supported
           0  CDMA 2000 not supported
:Timer IE
0b  000-----  Value is incremented in multiples of 2 seconds
    ---01011  Value = 11

v3a0NonCriticalExtensions SEQUENCE {
              InitialDirectTransfer-v3a0ext ::= SEQUENCE {
8b  10001011001000000000  START-Value = 569856
```

Bild 82: Die Meldung ATTACH REQUEST

Es folgt eine Meldung MEASUREMENT CONTROL ohne Kommentar.

10.2.4 IDENTITY REQUEST

Wie üblich fordert das Netz das Mobile sich auszuweisen (Wer sind Sie?). Das Mobile soll seine IMSI mitteilen.

```
_____[ 50 ]_____[ group ID: 00 07 ]_____[ trace ID: 00 01 ]______

00 04 00 30  14 20 04 10  2a 02

:WDCMA L3 RRC Peer messages

00  00000000  Channel LSB
:Channel Type MSB
04  00000100  Downlink DCCH

00  0000000000110000  length=48
           0  IntegrityCheckinfo absent

: Message Type:
       00101  DOWNLINK DIRECT TRANSFER
           0  r3 SEQUENCE
           0  sw1 not present
DownlinkDirectTransfer-r3
          00  RRC-TransactionIdentifier = 0
:CN-DomainIdentity
           1  ps-domain
:nas-Message
    000000000010  length=2
    0-------  direction from      : originating site
    -000----  TransactionID       : 0
```

```
    ----1000  Protocol Discrim.   : GPRS mobility management messages

    00010101  MESSAGE TYPE        : IDENTITY REQUEST

    0-------  spare
    -000----  Force to standby not indicated
    ----0---  spare
    -----001  IMSI
```

Bild 83: Die Meldung IDENTITY REQUEST

10.2.5 IDENTITY RESPONSE

Die Übertragung derIMSI zum Netz erfolgt im Rahmen 51.

```
_____[ 51 ]_____[ group ID: 00 07 ]_____[ trace ID: 00 01 ]______

00 07 00 70  6c 80 50 40  b0 41 49 31  01 b1 89 a8  b4 c0

:WDCMA L3 RRC Peer messages
00  00000000  Channel LSB
:Channel Type MSB
07  00000111  Uplink DCCH

00  0000000001110000  length=112
          0  IntegrityCheckinfo absent
      11011  Message Type :UPLINK DIRECT TRANSFER
: switches
             measuredResultsOnRach sw1
          0  sw1 not present
             laterNonCriticalExtensions sw2
          0  sw2 not present
:CN-DomainIdentity
          1  ps-domain
:nas-Message
    000000001010  length=10
    0-------  direction from      : originating site
    -000----  TransactionID       : 0
    ----1000  Protocol Discrim.   : GPRS mobility management messages

    00010110  MESSAGE TYPE        : IDENTITY RESPONSE

    00001000  length of Mob. ident.: 8
    ----1---  No. of ID digits     : Odd
    -----001  Type of identity     : IMSI
    0010----  Identity Digit 1     : 2
    ----0110  Identity Digit 2     : 6
    0010----  Identity Digit 3     : 2
    ----0000  Identity Digit 4     : 0
    0010----  Identity Digit 5     : 2
    ----0110  Identity Digit 6     : 6
    0011----  Identity Digit 7     : 3
    ----0001  Identity Digit 8     : 1
    0011----  Identity Digit 9     : 3
    ----0101  Identity Digit 10    : 5
    0011----  Identity Digit 11    : 3
    ----0110  Identity Digit 12    : 6
    0001----  Identity Digit 13    : 1
    ----1000  Identity Digit 14    : 8
     1001----  Identity Digit 15    : 9
```

Bild 84: Die Meldung IDENTITY RESPONSE

10.2.6 AUTHENTICATION AND CIPHERING REQUEST

Nachdem sich das Mobile ausgewiesen hat, wird es, wie in Abschnitt 11 erklärt, nach der „Parole“ gefragt. Das Netz sendet den *Authentication parameter RAND.*

```
_____[ 52 ]_____[ group ID: 00 07 ]_____[ trace ID: 00 01 ]______

00 04 01 58  14 60 4e 10  24 20 00 43  04 ab d3 61  0e 27 e0 30
ae 38 87 75  5d 64 37 a1  00 50 21 de  b5 8e 64 8d  ab ff fe aa
80 b8 f7 40  6f 50 1a

:WDCMA L3 RRC Peer messages
00  00000000  Channel LSB
:Channel Type MSB
04  00000100  Downlink DCCH
01  0000000101011000  length=344
          0  IntegrityCheckinfo absent
: Message Type:
       00101  DOWNLINK DIRECT TRANSFER
           0  r3 SEQUENCE
           0  sw1 not present
DownlinkDirectTransfer-r3
          01  RRC-TransactionIdentifier = 1
:CN-DomainIdentity
           1  ps-domain
:nas-Message
    000000100111  length=39
    0-------  direction from      : originating site
    -000----  TransactionID       : 0
    ----1000  Protocol Discrim.   : GPRS mobility management messages

    00010010  MESSAGE TYPE        : AUTHENTICATION AND CIPHERING REQUEST

    0-------  spare
    -001----  IMEISV requested
    ----0---  spare
    -----000  ciphering not used
    0000----  A&C reference number value = 0
    ----0---  spare
    -----000  Force to standby not indicated
: Authentication parameter RAND
    00100001  INFORMATION ELEMENT : Authentication parameter RAND
    10000010  RAND Value octet 2
    01010101  RAND Value octet 3
    11101001  RAND Value octet 4
    10110000  RAND Value octet 5
    10000111  RAND Value octet 6
    00010011  RAND Value octet 7
    11110000  RAND Value octet 8
    00011000  RAND Value octet 9
    01010111  RAND Value octet 10
    00011100  RAND Value octet 11
    01000011  RAND Value octet 12
    10111010  RAND Value octet 13
    10101110  RAND Value octet 14
    10110010  RAND Value octet 15
     00011011  RAND Value octet 16
    11010000  RAND Value octet 17


: Ciphering Key Sequence Number
    1000----  INFORMATION ELEMENT : Ciphering Key Sequence Number
    ----0---  spare
    -----000  Key sequence (111  no key available)

    00101000  Authentication Token AUTN
    00010000  length = 16
    11101111  AUTN
    01011010  AUTN
    11000111  AUTN
    00110010  AUTN
    01000110  AUTN
    11010101  AUTN
    11111111  AUTN
    11111111  AUTN
    01010101  AUTN
    01000000  AUTN
    01011100  AUTN
    01111011  AUTN
    10100000  AUTN
    00110111  AUTN
```

```
    10101000  AUTN
    00001101  AUTN
```

Bild 85: Das Netz sendet den Authentication parameter RAND und Authentication Token AUTN

10.2.7 AUTHENTICATION AND CIPHERING RESPONSE

Das Mobile antwortet mit dem *Authentication parameter SRES* und bestätigt mit seiner IMEISV.

```
_____[ 53 ]_____[ group ID: 00 07 ]_____[ trace ID: 00 01 ]______

00 07 00 b0  6c 80 90 40  98 01 10 6d  9e e3 b9 18  49 9c 2a 98
43 82 33 48  cf c0

:WDCMA L3 RRC Peer messages
00  00000000  Channel LSB
:Channel Type MSB
07  00000111  Uplink DCCH
00  0000000010110000  length=176
           0  IntegrityCheckinfo absent
       11011  Message Type :UPLINK DIRECT TRANSFER
: switches
              measuredResultsOnRach sw1
           0  sw1 not present
              laterNonCriticalExtensions sw2
           0  sw2 not present
:CN-DomainIdentity
           1  ps-domain
:nas-Message
    000000010010  length=18
    0-------  direction from      : originating site
    -000----  TransactionID       : 0
    ----1000  Protocol Discrim.   : GPRS mobility management messages

    00010011  MESSAGE TYPE        : AUTHENTICATION AND CIPHERING RESPONSE

    0000----  spare half octet
    ----0000  A&C reference number value = 0
: Authentication parameter SRES
    00100010  INFORMATION ELEMENT : Authentication parameter SRES
    00001101  SRES value octet 2
    10110011  SRES value octet 3
    11011100  SRES value octet 4
    01110111  SRES value octet 5
    00100011  INFORMATION ELEMENT : Mobile Identity
    00001001  length of Mob. ident.: 9
    0011----  Identity Digit 1     : 147
    ----0---  No. of ID digits     : even
    -----011  Type of identity     : IMEISV
    1000----  Identity Digit 2     : 8
    ----0101  Identity Digit 3     : 5
    0101----  Identity Digit 4     : 5
    ----0011  Identity Digit 5     : 3
    0000----  Identity Digit 6     : 0
    ----1000  Identity Digit 7     : 8
    0111----  Identity Digit 8     : 7
    ----0000  Identity Digit 9     : 0
    0100----  Identity Digit 10    : 4
    ----0110  Identity Digit 11    : 6
    0110----  Identity Digit 12    : 6
    ----1001  Identity Digit 13    : 9
    0001----  Identity Digit 14    : 1
    ----1001  Identity Digit 15    : 9
```

Bild 86: Authentication and Ciphering Response mit SRES und IMEISV

10.2.8 SECURITY MODE COMMAND

Ehe das Netz Anweisungen zum Security Mode gibt weist es sich mit der *Integrity Check Info* aus. Man beachte, der Ciphering Algorithm uea1 bedeutet dass verschlüsselt wird, uea0 bedeutet, dass nicht verschlüsselt wird. Uia1 repräsentiert den Integrity protection Algorithmus. Für GSM ist der Algorithmus A5/1zuständig.

```
_____[ 54 ]_____[ group ID: 00 07 ]_____[ trace ID: 00 01 ]______

00 04 00 d0  b1 90 a3 05  0c 0e 00 01  80 01 28 c2  00 60 00 11
00 28 c0 06  e7 45 ea 15  80 c0

:WDCMA L3 RRC Peer messages
00  00000000  Channel LSB
:Channel Type MSB
04  00000100  Downlink DCCH
00  0000000011010000  length=208
          1  Integrity Check Info present
    01100011  MessageAuthenticationCode,
    00100001  MessageAuthenticationCode,
    01000110  MessageAuthenticationCode,
    00001010  MessageAuthenticationCode,
        0001  RRC-MessageSequenceNumber  = 1

       10000  Message Type: SECURITY MODE COMMAND

           0  r3
              laterNonCriticalExtensions sw1
           0  sw1 not present
SecurityModeCommand-r3-IEs ::= SEQUENCE {
              cipheringModeInfo sw2
           1  sw2 present
              integrityProtectionModeInfo
           1  sw3 present
              ue-SystemSpecificSecurityCap
           1  sw4 present
              -- User equipment IEs
              Radio Resource Control transaction identifier
          00  RRC transaction identifier  : 0
    SecurityCapability
              cipheringAlgorithmCap
              -- For each bit value "0" means false/ not supported
           0  spare15(0),
           0  spare14(1),
           0  spare13(2),
           0  spare12(3),
           0  spare11(4),
           0  spare10(5),
           0  spare9(6),
           0  spare8(7),
           0  spare7(8),
           0  spare6(9),
           0  spare5(10),
           0  spare4(11),
           0  spare3(12),
           0  spare2(13),
           1  uea1(1)(14),
           1  uea0(0)(15)

              integrityProtectionAlgorithmCap BIT STRING {
              -- For each bit value "0" means false/ not supported
           0  spare15(0),
           0  spare14(1),
           0  spare13(2),
           0  spare12(3),
           0  spare11(4),
           0  spare10(5),
           0  spare9(6),
           0  spare8(7),
           0  spare7(8),
           0  spare6(9),
           0  spare5(10),
           0  spare4(11),
           0  spare3(12),
```

```
           0  spare2(13),
           1  uia1(14),
           0  spare0(15)
CipheringModeInfo ::= SEQUENCE {
             activationTimeForDPCH sw1
           0  sw1 not present
             rb-DL-CiphActivationTimeInfo sw2
           1  sw2 present

        CipheringModeCommand
           0  CipheringAlgorithm
           1  uea1

              RB-ActivationTimeInfoList
           0  flag
        0011  val1: 3
              Number-Of-RB-ActivationTimeInfo = val1
              (val1 + 1) x RB-ActivationTimeInfo ::= SEQUENCE {
       00001  RB-identity = 1+1
    000000000011  RLC-SequenceNumber = 3
       00000  RB-identity = 0+1
    000000000001  RLC-SequenceNumber = 1
       00010  RB-identity = 2+1
    000000000101  RLC-SequenceNumber = 5
       00011  RB-identity = 3+1
    000000000001  RLC-SequenceNumber = 1
}
IntegrityProtectionModeInfo
             integrityProtectionAlgorithm sw1
           1  sw1 present

        IntegrityProtectionModeCommand
           0  startIntegrityProtection
    11100111  integrityProtInitNumber
    01000101  integrityProtInitNumber
    11101010  integrityProtInitNumber
    00010101  integrityProtInitNumber

    IntegrityProtectionAlgorithm

              -- Core network IEs
:CN-DomainIdentity
           1  ps-domain
              -- Other IEs
        InterRAT-UE-SecurityCapList
        InterRAT-UE-SecurityCapability
           0  gsm
        GsmSecurityCapability
        -- For each bit value "0" means false/ not supported
           0  a5-7(0),
           0  a5-6(1),
           0  a5-5(2),
           0  a5-4(3),
           0  a5-3(4),
           0  a5-2(5),
           1  a5-1(6)
```

Bild 87: SECURITY MODE KOMMAND bestimmt die Algorithmen uea1, uia1 und a5/1

10.2.9 SECURITY MODE COMPLETE

In der Meldung SECURITY MODE COMPLETE wird der bisherige Integrity Check zurückgesetzt und neu gestartet..

```
_____[ 55 ]_____[ group ID: 00 07 ]_____[ trace ID: 00 01 ]______

00 07 00 90  f1 0a 99 50  0d 31 00 00  01 80 00 02  00 a2 00 61
80 00

:WDCMA L3 RRC Peer messages

00  00000000  Channel LSB
```

```
:Channel Type MSB
07  00000111  Uplink DCCH

00  0000000010010000  length=144
          1  Integrity Check Info present
    11100010  MessageAuthenticationCode,
    00010101  MessageAuthenticationCode,
    00110010  MessageAuthenticationCode,
    10100000  MessageAuthenticationCode,
        0001  RRC-MessageSequenceNumber  = 1

       10100  Message Type : SECURITY MODE COMPLETE

             IntegrityProtActivationInfo sw1
           1  sw1 present
             RB-ActivationTimeInfoList sw2
           1  sw2 present
             laterNonCriticalExtensions sw3
           0  sw3 not present

-- User equipment IEs
              Radio Resource Control transaction identifier
          00  RRC transaction identifier  : 0
IntegrityProtActivationInfo
RRC-MessageSequenceNumberList
           1  val1: 1
        0000  RRC-MessageSequenceNumber = 0
        0000  RRC-MessageSequenceNumber = 0
        0000  RRC-MessageSequenceNumber = 0
        0000  RRC-MessageSequenceNumber = 0
        0000  RRC-MessageSequenceNumber = 0
}
--Radio bearer IE's
RB-ActivationTimeInfoList
        0001  val1: 1
       10000  rb-Identity = 16 + 1
    000000000000  Rlc-SequenceNumber = 0
       00000  rb-Identity = 0 + 1
    100000000010  Rlc-SequenceNumber = 2050
```

Bild 88: SECURITY MODE COMPLETE startet den Mode uia1 neu

10.2.10 ATTACH ACCEPT

Der Aufbau des GMM Contextes wird vom Netz bestätigt, eine neue Routing Area Identification wird zugewiesen, die TMSI wird erneuert und zum Nachweis ihrer Echtheit eine TMSI-Signatur festgelegt.

```
_____[ 56 ]_____[ group ID: 00 07 ]_____[ trace ID: 00 01 ]______

00 04 01 08  82 b3 44 e6  89 4a 03 01  00 41 2b e0  2c 5e 44 00
26 c0 23 21  cb 8b 83 00  be 98 40 14  88 a5 40 25  80

:WDCMA L3 RRC Peer messages
00  00000000  Channel LSB
:Channel Type MSB
04  00000100  Downlink DCCH
01  0000000100001000  length=264
          1  Integrity Check Info present
    00000101  MessageAuthenticationCode,
    01100110  MessageAuthenticationCode,
    10001001  MessageAuthenticationCode,
    11001101  MessageAuthenticationCode,
        0001  RRC-MessageSequenceNumber  = 1
: Message Type:
       00101  DOWNLINK DIRECT TRANSFER
           0  r3 SEQUENCE
           0  sw1 not present
DownlinkDirectTransfer-r3
          10  RRC-TransactionIdentifier = 2
```

```
:CN-DomainIdentity
          1  ps-domain
:nas-Message
    000000011000  length=24
    0-------  direction from      : originating site
    -000----  TransactionID       : 0
    ----1000  Protocol Discrim.   : GPRS mobility management messages

    00000010  MESSAGE TYPE        : ATTACH ACCEPT

    0-------  spare
    -000----  Force to standby not indicated
    -----001  Attach Result       : GPRS only attached

: Timer
    010-----  value is incremented in multiples of decihours
    ---11111  GPRS Timer value    : 31
: Radio Priority Level & Spare
    0000----  spare half octet
    ----0---  spare bit
    -----001  Radio priority level: 1 (highest)
: Routing Area Identification

    ----0010  MCC digit 1         : 2
    0110----  MCC digit 2         : 6
    ----0010  MCC digit 3         : 2
    1111----  MNC digit 3         : 15
    ----0000  MNC digit 1         : 0
    0010----  MNC digit 2         : 2
    00000001  Location area code  : take hex-value
    00110110  cont'd LAC          : take hex-value
    00000001  Routing Area Code   : take hex-value

    00011001  INFORMATION ELEMENT : P-TMSI signature
    00001110  P-TMSI signature    : 14
    01011100  P-TMSI signature    : 92
    01011100  P-TMSI signature    : 92

    00011000  INFORMATION ELEMENT : Allocated P-TMSI
05  00000101  length=5
    1111----  Identity digit 1    : 15
    ----0---  even number of identity digits and also when the TMSI/P-TMSI is used
    -----100  TMSI/P-TMSI
    ----0010  Identity digit 2    : 2
    1100----  Identity digit 3    : 12
    ----0000  Identity digit 4    : 0
    0000----  Identity digit 5    : 0
    ----0100  Identity digit 6    : 4
    1010----  Identity digit 7    : 10
    ----0101  Identity digit 8    : 5
    0100----  Identity digit 9    : 4
```

Bild 89: ATTACH ACCEPT

10.2.11 ATTACH COMPLETE

Das Mobile meldet , dass es die zum GMM Context empfangenen Informationen eingestellt hat.

```
_____[ 57 ]_____[ group ID: 00 07 ]_____[ trace ID: 00 01 ]______

00 07 00 50  cc b6 d4 c6  8e c8 00 84  01 80

:WDCMA L3 RRC Peer messages

00  00000000  Channel LSB
:Channel Type MSB
07  00000111  Uplink DCCH

00  0000000001010000  length=80
          1  Integrity Check Info present
    10011001  MessageAuthenticationCode,
    01101101  MessageAuthenticationCode,
```

```
    10101001  MessageAuthenticationCode,
    10001101  MessageAuthenticationCode,
        0001  RRC-MessageSequenceNumber  = 1

       11011  Message Type :UPLINK DIRECT TRANSFER
: switches
              measuredResultsOnRach sw1
           0  sw1 not present
              laterNonCriticalExtensions sw2
           0  sw2 not present
:CN-DomainIdentity
           1  ps-domain
:nas-Message
    000000000001  length=1
    0-------  direction from      : originating site
    -000----  TransactionID       : 0
    ----1000  Protocol Discrim.   : GPRS mobility management messages

    00000011  MESSAGE TYPE        : ATTACH COMPLETE
```

Bild 90: ATTACH COMPLETE

10.2.12 RRC CONNECTION RELEASE

Das Netz legt fest, die zum Zwecke des Aufbaus eines GMM Contextes eingerichtete Verbindung abzubauen.

```
_____[ 58 ]_____[ group ID: 00 07 ]_____[ trace ID: 00 01 ]______

00 04 00 38  f0 42 df 46  0b c8 20

:WDCMA L3 RRC Peer messages
00  00000000  Channel LSB
:Channel Type MSB
04  00000100  Downlink DCCH
00  0000000000111000  length=56

1Integrity Check Info present
    11100000  MessageAuthenticationCode,
    10000101  MessageAuthenticationCode,
    10111110  MessageAuthenticationCode,
    10001100  MessageAuthenticationCode,
        0001  RRC-MessageSequenceNumber  = 1

       01111  Message Type : RRC-CONNECTION RELEASE
           0  r3
              laterNonCriticalExtensions sw1
           0  sw1 not present
RRCConnectionRelease-r3-IEs

              n-308 sw1
           1  sw1 present
              rplmn-information sw2
           0  sw2 not present
-- User equipment IEs
              Radio Resource Control transaction identifier
          00  RRC transaction identifier  : 0
-- n-308 is conditional on the UE state
         001  N-308= 1+1
              ReleaseCause ::= ENUMERATED {
         000  normalEvent,
```

Bild 91: Befehl zur Freigabe der Verbindung durch das Netz

10.2.13 RRC CONNCTION RELEASE COMPLETE

Das Mobile gibt seinerseits die Verbindung frei.

```
_____[ 59 ]_____[ group ID: 00 07 ]_____[ trace ID: 00 01 ]______

00 07 00 30  ca e6 f1 0b  8c 40

:WDCMA L3 RRC Peer messages

00  00000000  Channel LSB
:Channel Type MSB
07  00000111  Uplink DCCH

00  0000000000110000  length=48
           1  Integrity Check Info present
    10010101  MessageAuthenticationCode,
    11001101  MessageAuthenticationCode,
    11100010  MessageAuthenticationCode,
    00010111  MessageAuthenticationCode,
        0001  RRC-MessageSequenceNumber  = 1

       10001  Message Type : RRC-CONNECTION RELEASE COMPLETE

              errorIndication sw1
           0  sw1 not present
              laterNonCriticalExtensions sw2
           0  sw2 not present

              Radio Resource Control transaction identifier
          00  RRC transaction identifier  : 0
```

Bild 92: RRC-CONNECTION RELEASE COMPLETE

Das Mobile geht nach dem RELEASE wieder in den IDLE MODE über. Es werden mehrere BCCH Messages empfangen, bis das MOBILE erneut einen RRC CONNECTION REQUEST aussendet.

10.3 Verbindungsprozedur für das PDP ATTACH

Nach dem GPRS Mobility Management Context muss nun der PDP (Packet Data Protokoll) Context aufgebaut werden. Der PDP Context spezifiziert den Zugriff zu einer externen Paketvermittlung. Die Daten die dem PDP Context zuzurechnen sind, enthalten Informationen wie den Typ des Paket-Netzwerkes, die IP-Adresse der Paketvermittlung, den Bezug zum GGSN (Gateway GPRS Support Node) und den erforderlichen QoS (Quality of Service).

10.3.1 RRC CONNECTION REQUEST

Von der im Punkt 10.2.1 dargestellten Meldung unterscheidet sich die Nachfolgende in erster Linie durch den Establishment cause, der hier *originatingHighPrioritySignalling* genannt wird.

```
_____[ 72 ]_____[ group ID: 00 07 ]_____[ trace ID: 00 01 ]______

00 06 00 a6  31 92 46 eb  3c 26 20 10  09 b3 81 18  00 00 00 00
00 00 00 00  00

:WDCMA L3 RRC Peer messages
00  00000000  Channel LSB
:Channel Type MSB
06  00000110  Uplink CCCH
00  0000000010100110  length=166
           0  IntegrityCheckinfo absent
: Message Type:
          01  RRC CONNECTION REQUEST
```

```
-- User equipment IEs
: switches
              measuredResultsOnRach sw1
           1  sw1 present
              v3d0NonCriticalExtensions sw2
           0  sw2 not present
InitialUE-Identity
         001  Choice: TMSI-and-LAI-GSM-MAP
: TMSI
92  10010010  take hex value
46  01000110  take hex value
eb  11101011  take hex value
3c  00111100  take hex value
: LAI
: PLMN-identity
: MCC
        0010  Mobile CC digit 1   : 2
        0110  Mobile CC digit 2   : 6
        0010  Mobile CC digit 3   : 2

: MNC
           0  val2: 0
        0000  Mobile NC digit     : 0
        0010  Mobile NC digit     : 2
:LAC
01  00000001  Loc. area code (LAI) = ID of MSC (hex)
36  00110110  Loc. area code (LAI) = ID of BSC (hex)

Establishment cause
       01110  originatingHighPrioritySignalling,


ProtocolErrorIndicator
           0  No Error
-- Measurement IEs
MeasuredResultsOnRach
               monitoredCells (sw3)
           0  sw3 not present
              currentCell
              modeSpecification
           0  fdd
              measurementQuantity
          00  CPICH-EC-NO: Common Pilot Channel,The received energy per chip divided by the
                            power density in the band
: Measurement Value
      100011  3 dB
```

Bild 92: RRC-CONNECTION REQUEST für originatingHighPrioritySignalling

10.3.2 RRC CONNECTION SETUP

Mit der Meldung RRC CONNECTION SETUP werden an dieser Stelle Kanäle für die Signalisation aufgebaut. Folglich unterscheiden sich die Kanäle nicht von den in den Bildern 80 und 81 dargestellten.

10.3.3 RRC CONNECTION SETUP COMPLETE

Der Inhalt der Meldung RRC CONNECT ION COMPLETE entspricht dem im Bild 54 dargestellten.

10.3.4 SERVICE REQUEST

Der Service Request ist aus dem GPRS bekannt. Die Anforderung ist *Signalling.* Als Identität wird die TMSI/P-TMSI angegeben.

```
_____[ 79 ]_____[ group ID: 00 07 ]_____[ trace ID: 00 01 ]______

00 07 00 a8  15 80 02 00  60 40 60 00  2f a6 10 05  22 29 90 10
00 02 00 00  40

:WDCMA L3 RRC Peer messages
00  00000000  Channel LSB
:Channel Type MSB
07  00000111  Uplink DCCH
00  0000000010101000  length=168
           0  IntegrityCheckinfo absent
: Message Type:
       00101  INITIAL DIRECT TRANSFER
: switches
              measuredResultsOnRach sw1
           0  sw1 not present
              v3a0NonCriticalExtensions sw2
           1  sw2 present
              -- Core network IEs
:CN-DomainIdentity
           1  ps-domain
IntraDomainNasNodeSelector
              version
           0  release99
              cn-Type
           0  Gsm-map-IntraDomainNASNodeSelector
              routingbasis
         000  local PTMSI
              RoutingParameter
    0000000010  bit

           0  enteredparameter = false
:nas-Message
    000000001100  length=12
    0-------  direction from      : originating site
    -000----  TransactionID       : 0
    ----1000  Protocol Discrim.   : GPRS mobility management messages

    00001100  Service Request
:Ciphering Key Sequence Number
    0-------  spare
    -000----  0
:Service type
    ----0---  spare
    -----000  Signalling
:Mobile Identity IE
05  00000101  length=5
f4  1111----  Identity digit 1
    ----0---  even number of identity digits
    -----100  TMSI/P-TMSI
c2  ----0010  Identity digit 2
    1100----  Identity digit 3
00  ----0000  Identity digit 4
    0000----  Identity digit 5
a4  ----0100  Identity digit 6
    1010----  Identity digit 7
45  ----0101  Identity digit 8
    0100----  Identity digit 9

v3a0NonCriticalExtensions SEQUENCE {
              InitialDirectTransfer-v3a0ext ::= SEQUENCE {
32  00110010000000100000  START-Value = 204832
```

Bild 93: Die NAS-Meldung SERVICE REQUEST

10.3.5 MEASUREMENT CONTROL

Das Mobile empfängt nachstehende Weisungen für das *TrafficVolumeMeasurement* insbesondere die *TrafficVolumeReportingCriteria* wie die nachstehenden TrafficVolumeEventParameter:

- TrafficVolumeEventType e4a,
- TrafficVolumeThreshold th128,
- TimeToTrigger ttt0,
- pendingTimeAfterTrigger ptat2,
- tx-InterruptionAfterTrigger txiat2

10.3.6 SECURITY MODE COMMAND

Der nachstehende Befehl SECURITY MODE COMMAND entspricht weitestgehend dem im Bild 87 dargestellten. Er ist noch einmal aufgeführt um zu zeigen was sich im Verlaufe der Kommandofolge ändert, bzw. nicht ändert.

```
_____[ 81 ]_____[ group ID: 00 07 ]_____[ trace ID: 00 01 ]______

00 04 00 d0  dd dc fc ae  0c 0e 00 01  80 01 28 c2  00 60 00 11
00 08 c0 06  89 a5 21 17  80 c0

:WDCMA L3 RRC Peer messages
00  00000000  Channel LSB
:Channel Type MSB
04  00000100  Downlink DCCH
00  0000000011010000  length=208
          1  Integrity Check Info present
    10111011  MessageAuthenticationCode,
    10111001  MessageAuthenticationCode,
    11111001  MessageAuthenticationCode,
    01011100  MessageAuthenticationCode,
        0001  RRC-MessageSequenceNumber  = 1

       10000  Message Type: SECURITY MODE COMMAND
              Choice ::= {
           0  r3
             laterNonCriticalExtensions sw1
           0  sw1 not present
SecurityModeCommand-r3-IEs ::= SEQUENCE {
              cipheringModeInfo sw2
           1  sw2 present
              integrityProtectionModeInfo
            1  sw3 present
               ue-SystemSpecificSecurityCap
            1  sw4 present
              -- User equipment IEs
              Radio Resource Control transaction identifier
          00  RRC transaction identifier  : 0
    SecurityCapability ::= SEQUENCE {
              cipheringAlgorithmCap BIT STRING {
              -- For each bit value "0" means false/ not supported
           0  spare15(0),
           0  spare14(1),
           0  spare13(2),
           0  spare12(3),
           0  spare11(4),
           0  spare10(5),
           0  spare9(6),
           0  spare8(7),
           0  spare7(8),
           0  spare6(9),
           0  spare5(10),
           0  spare4(11),
           0  spare3(12),
           0  spare2(13),
           1  uea1(1)(14),
           1  uea0(0)(15)
```

```
               } (SIZE (16)),
               integrityProtectionAlgorithmCap BIT STRING {
               -- For each bit value "0" means false/ not supported
            0  spare15(0),
            0  spare14(1),
            0  spare13(2),
            0  spare12(3),
            0  spare11(4),
            0  spare10(5),
            0  spare9(6),
            0  spare8(7),
            0  spare7(8),
            0  spare6(9),
            0  spare5(10),
            0  spare4(11),
            0  spare3(12),
            0  spare2(13),
            1  uia1(14),
            0  spare0(15)

CipheringModeInfo ::= SEQUENCE {
              activationTimeForDPCH sw1
            0  sw1 not present
              rb-DL-CiphActivationTimeInfo sw2
            1  sw2 present
         CipheringModeCommand
            0  CipheringAlgorithm
            1  uea1

               RB-ActivationTimeInfoList ::= SEQUENCE (SIZE (1..maxRB)) OF RB-
ActivationTimeInfo
            0  flag
         0011  val1: 3
               Number-Of-RB-ActivationTimeInfo = val1
               (val1 + 1) x RB-ActivationTimeInfo
        00001  RB-identity = 1+1
    000000000011  RLC-SequenceNumber = 3
        00000  RB-identity = 0+1
    000000000001  RLC-SequenceNumber = 1
        00010  RB-identity = 2+1
    000000000001  RLC-SequenceNumber = 1
        00011  RB-identity = 3+1
    000000000001  RLC-SequenceNumber = 1

IntegrityProtectionModeInfo
              integrityProtectionAlgorithm sw1
            1  sw1 present
         IntegrityProtectionModeCommand
            0  startIntegrityProtection{
    10001001  integrityProtInitNumber
    10100101  integrityProtInitNumber
    00100001  integrityProtInitNumber
    00010111  integrityProtInitNumber

IntegrityProtectionAlgorithm
                  -- Core network IEs
:CN-DomainIdentity
            1  ps-domain
               -- Other IEs
              InterRAT-UE-SecurityCapList
         InterRAT-UE-SecurityCapability
            0  gsm
         GsmSecurityCapability
         -- For each bit value "0" means false/ not supported
            0  a5-7(0),
            0  a5-6(1),
            0  a5-5(2),
            0  a5-4(3),
            0  a5-3(4),
            0  a5-2(5),
            1  a5-1(6)
```

Bild 94: SECURITY MODE COMMAND

10.3.7 SECURITY MODE COMPLETE

Die Meldung entspricht der Darstellung in Bild 88.

10.3.8 ACTIVATE PDP CONTEXT REQUEST

Anforderung eines Kontextes bedeutet Anforderung einer IP Nummer bei gleichzeitiger Festlegung des Quality of Service. Es muss der *Access Point Name* angegeben werden.

```
_____[ 83 ]_____[ group ID: 00 07 ]_____[ trace ID: 00 01 ]______

00 07 02 c0  c6 66 82 f2  0e c8 27 85  20 82 81 85  80 00 0f 80
00 00 00 00  00 00 00 01  00 90 94 08  01 bb b0 b8  04 3b 37 b2
30 b3 37 b7  32 81 32 32  93 94 c0 60  11 89 00 80  00 09 04 3b
37 b2 30 b3  37 b7 32 82  36 34 bb 32  c0 10 88 00  80 00 08 40
83 00 00 00  00 41 83 00  00 00 00 00

:WDCMA L3 RRC Peer messages

00  00000000  Channel LSB
:Channel Type MSB
07  00000111  Uplink DCCH

02  0000001011000000  length=704
          1  Integrity Check Info present
    10001100  MessageAuthenticationCode,
    11001101  MessageAuthenticationCode,
    00000101  MessageAuthenticationCode,
    11100100  MessageAuthenticationCode,
        0001  RRC-MessageSequenceNumber  = 1

       11011  Message Type :UPLINK DIRECT TRANSFER

: switches
              measuredResultsOnRach sw1
          0  sw1 not present
              laterNonCriticalExtensions sw2
          0  sw2 not present

:CN-DomainIdentity
          1  ps-domain
:nas-Message
    000001001111  length=79
    0-------  direction from      : originating site
    -000----  TransactionID       : 0
     ----1010  Protocol Discrim.   : Session Management Messages

    01000001  MESSAGE TYPE        : ACTIVATE PDP CONTEXT REQUEST

: Network Service Accesspoint
    ----0101  NSAPI value         : 5
    0000----  spare
: LLC SAPI
    ----0011  SAPI value          : 3
    0000----  spare
: Quality of Service
    00001011  length              : 11
    00------  spare
    --000---  Delay class         : 32 (4 = best effort)
    -----000  Reliability class   : Subscribed
    0000----  peak throughput     : subscribed
    ----0---  spare
    -----000  precedence class    : Subscribed
    000-----  spare
    ---11111  Mean throughput     : Best effort
    000-----  traffic class       : Subscribed
    ---00---  delivery order      : Subscribed
    -----000  Subscribed delivery : of erroneous SDUs
    00000000  Maximum SDU size    : 0, 0 = Subscribed
    00000000  Maximum bit rate up : 0, 0 = Subscribed
    00000000  Max. bit rate down  : 0, 0 = Subscribed
    0000----  Residual BER        : Subscribed
    ----0000  SDU error ratio     : Subscribed
    ------00  traffic handl prior : Subscribed
```

```
    000000--  Transfer delay      : Subscribed
    000000--  Transfer delay      : 0 x 10 ms (up to 200 ms) ,etc
    00000000  Guaranteed bit rate for downlink
    00000000  Guaranteed bit rate for uplink

: Packet Data Protocol Address
    00000010  length              : 2
    ----0001  PDP type organisat. : IETF allocated address

    00100001  PDP type number     : IPv4 address

: Access Point Name value
    00101000  INFORMATION ELEMENT : Access point name
10  00010000  length=16

00000011..01100101  _wap_vodafone_de

: Protocol Configuration Options
    00100111  INFORMATION ELEMENT : Protocol Configuration Options

    00101001  length              : 41
: Configuration Protocol
    -----000  PPP for use with IP PDP type
    -0000---  spare
    1-------  Extension bit       : 1

: PROTOCOL ID 1
    11000000  C021(LCP),C023(PAP)
    00100011  C023(PAP),C223(CHAP);

    00010010  Lgth of P ID 1 cont.: 18
    00000001  protocol ID 1 contents
    00000000  protocol ID 1 contents
    00000000  protocol ID 1 contents
    00010010  protocol ID 1 contents
    00001000  protocol ID 1 contents
    01110110  protocol ID 1 contents
    01101111  protocol ID 1 contents
    01100100  protocol ID 1 contents
    01100001  protocol ID 1 contents
    01100110  protocol ID 1 contents
    01101111  protocol ID 1 contents
    01101110  protocol ID 1 contents
    01100101  protocol ID 1 contents
    00000100  protocol ID 1 contents
    01101100  protocol ID 1 contents
    01101001  protocol ID 1 contents
    01110110  protocol ID 1 contents
    01100101  protocol ID 1 contents

: PROTOCOL ID 1
    10000000  8021(IPCP).
    00100001  C021(LCP),8021(IPCP)

    00010000  Lgth of P ID 2 cont.: 16
    00000001  protocol ID 2 contents
    00000000  protocol ID 2 contents
    00000000  protocol ID 2 contents
    00010000  protocol ID 2 contents
    10000001  protocol ID 2 contents
    00000110  protocol ID 2 contents
    00000000  protocol ID 2 contents
    00000000  protocol ID 2 contents
    00000000  protocol ID 2 contents
    00000000  protocol ID 2 contents
    10000011  protocol ID 2 contents
    00000110  protocol ID 2 contents
    00000000  protocol ID 2 contents
    00000000  protocol ID 2 contents
    00000000  protocol ID 2 contents
    00000000  protocol ID 2 contents
```

Bild 95: ACTIVATE PDP CONTEXT REQUEST

10.3.9 RADIO BEARER SETUP

Anstelle des Traces der sehr langen Meldung RADIO BEARER SETUP wird wieder das Fenster *„3G Transport Channel And Radio bearer General Overview“* des Tools OTDriveDual 1.6 abgebildet . Gegenüber der in den Bildern 80 und 81 dargestellten Kanäle Wird hier zusätzlich mit der RB-Identity 6 ein Data Traffic Channel gebildet, der als Physikalischer Kanal turbokodiert ist.

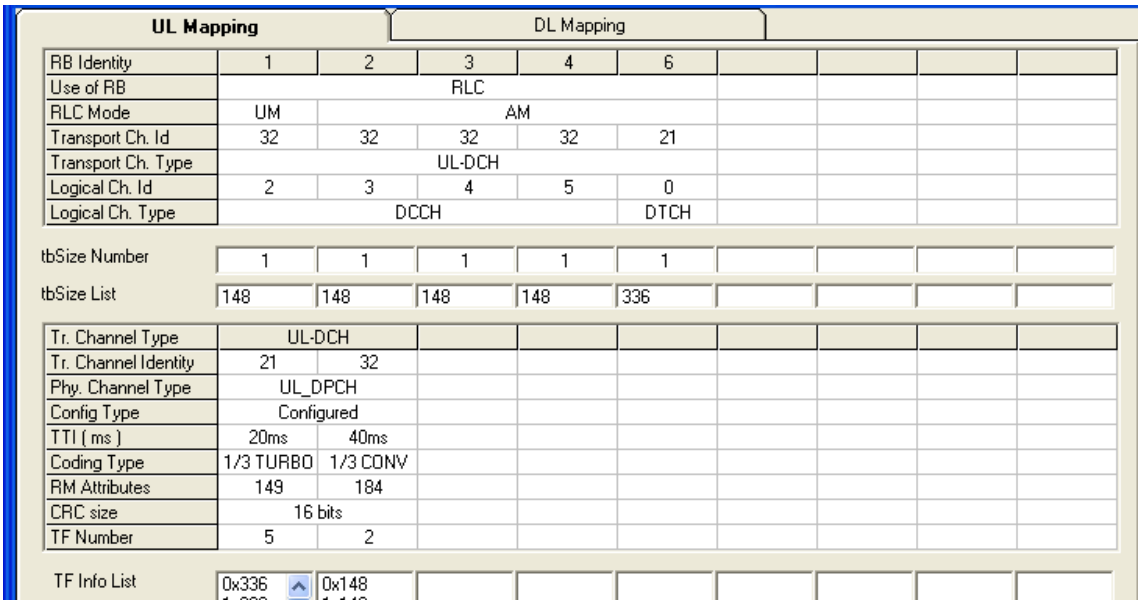


Bild 96: Uplink Kanäle des Radio Beares einer WAP Verbindung

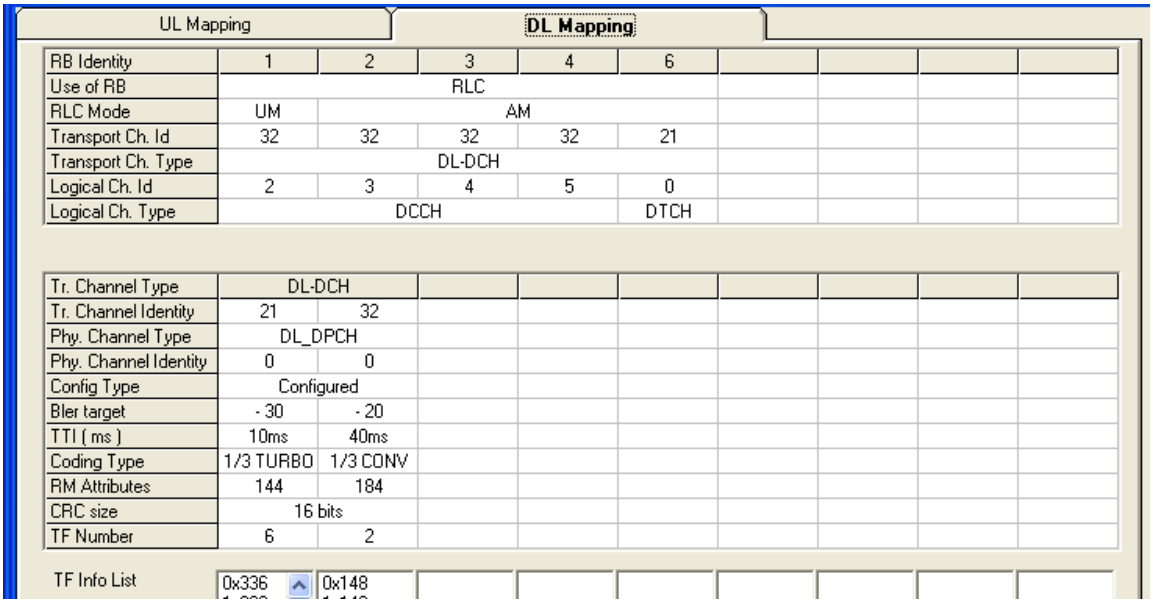


Bild 97: Downlink Kanäle des Radio Beares einer WAP Verbindung

10.3.10 RADIO BEARER SETUP COMPLETE

In dieser Meldung wird lediglich der START-Value zurückgegeben.

```
_____[ 85 ]_____[ group ID: 00 07 ]_____[ trace ID: 00 01 ]______

00 07 00 48  8e 1e 9b 47  13 c8 00 00  08

:WDCMA L3 RRC Peer messages
00  00000000  Channel LSB
:Channel Type MSB
07  00000111  Uplink DCCH
00  0000000001001000  length=72
           1  Integrity Check Info present
    00011100  MessageAuthenticationCode,
    00111101  MessageAuthenticationCode,
    00110110  MessageAuthenticationCode,
    10001110  MessageAuthenticationCode,
        0010  RRC-MessageSequenceNumber  = 2
: MESSAGE TYPE:
       01111  RadioBearerSetupComplete
              ul-IntegProtActivationInfo sw1
           0  sw1 not present
              ul-TimingAdvance sw2
           0  sw2 not present
              start-Value sw3
           1  sw3 present
              count-C-ActivationTime sw4
           0  sw4 not present
              rb-UL-CiphActivationTimeInfo sw5
           0  sw5 not present
              ul-CounterSynchronisationInfo sw6
           0  sw6 not present
              laterNonCriticalExtensions sw7
           0  sw7 not present
              -- User equipment IEs
Radio Resource Control transaction identifier
          00  RRC transaction identifier  : 0
Start-Value
    0000000000000000100  START-Value=4
```

Bild 98: Radio Bearer Setup Complete mit START-Value

10.3.11 MEASUREMENT CONTROL

Das Mobile empfängt nachstehende Weisungen für das *TrafficVolumeMeasurement* insbesondere die *TrafficVolumeReportingCriteria* wie die nachstehenden TrafficVolumeEventParameter:

- TrafficVolumeEventID e4a,
- ReportingThreshold th8,
- TimeToTrigger ttt0,
- pendingTimeAfterTrigger ptat2,

10.3.12 MEASUREMENT CONTROL vollst.

Im Bild 99 wurde zur Demonstration der vom Mobile durchzuführenden Messungen eine Meldung MEASUREMENT CONTROL vollständig entschlüsselt.
Aufgrund der Komplexität des nachfolgenden Traces, ist die Wahrscheinlichkeit von Fehlern, die durch die Entschlüsselung von Hand entstanden sind, groß.

```
_____[ 87 ]_____[ group ID: 00 07 ]_____[ trace ID: 00 01 ]______

00 04 02 10  95 e4 54 cd  a2 19 00 3b  86 40 2a 35  08 ae d5 42
f7 d5 88 ef  58 2a 85 10  ab d4 62 5c  52 0a e1 4a  22 45 30 94
14 e2 4d 54  0b 81 52 26  35 31 16 16  16 2a 08 60  2e c2 5e c4
28 01 8f 64  fb 4c 7a d3  2e 80

:WDCMA L3 RRC Peer messages

00  00000000  Channel LSB
:Channel Type MSB
04  00000100  Downlink DCCH

02  0000001000010000  length=528
          1  Integrity Check Info present
    00101011  MessageAuthenticationCode,
    11001000  MessageAuthenticationCode,
    10101001  MessageAuthenticationCode,
    10011011  MessageAuthenticationCode,
        0100  RRC-MessageSequenceNumber  = 4
:Messagetype
       01000  MeasurementControl
           0   r3
               v390Criticalextensions  (sw0)
           1   sw0 present
measurementControl-r3
              Begin switches
              measurementReportingMode sw1
           1  sw1 present
              additionalMeasurementList sw2
           0  sw2 not present
              dpch-CompressedModeStatusInfo sw3
           0  sw3 not present
              End switches
              -- Measurement IEs
          10  RRC-TransactionIdentifier = 2
        0000  measurementIdentity = 0+1
MeasurementCommand
setup MeasurementType
          00  setup measurement type
          000  IntraFrequencyMeasurement
              intraFreqCellInfoList sw4
           1  sw4 present
              intraFreqMeasQuantity sw5
           1  sw5 present
              intraFreqReportingQuantity sw6
           1  sw6 present
              measurementValidity sw7
           0  sw7 not present
              reportCriteria sw8
           1  sw8 present

               IntraFreqCellInfoList
              removedIntraFreqCellList sw9
           1  sw9 present
              newIntraFreqCellList sw10
           1  sw10 present
              cellsForIntraFreqMeasList sw11
           0  sw11 not present

RemovedIntraFreqCellList
          00  removeAllIntraFreqCells NULL,

               New Intra frequency cell list
       01100  val1: 12

               NewIntraFreqCells
             IntraFreqCellID switch(sw12)
           1  sw12 present
IntraFreqCellID
       00000  IntraFreqCellID = 0
               cellinfo
               referenceTimeDifferenceToCell switch(sw13)
           0  sw13 not present
      001010  cellIndividualOffset: -21
               modeSpecificInfo
               primaryCPICH-Info switch(sw14)
```

```
           1  sw14 present
               primaryCPICH-TX-Power switch(sw15)
           0  sw15 not present

              PrimaryCPICH-Info ::= SEQUENCE {
    001101010  PrimaryScramplingCode 106

               readSFN-Indicator ::= BOOLEAN
           0  false

               tx-diversityIndicator false ::= BOOLEAN
           0  false

               NewIntraFreqCells ::= SEQUENCE {
:           IntraFreqCellID switch(sw12)
           0  sw12 not present
               cellinfo
               referenceTimeDifferenceToCell switch(sw13)
           1  sw13 present

      000101  cellIndividualOffset: -26
               referenceTimeDifferenceToCell
          01  accuray256
               modeSpecificInfo

               primaryCPICH-Info switch(sw14)
            1  sw14 present

               primaryCPICH-TX-Power switch(sw15)
           1  sw15 present

              PrimaryCPICH-Info ::= SEQUENCE {
    011010101  PrimaryScramplingCode 213
              }
               primaryCPICH-TX-Power
      010000  primaryCPICH-TX-Power

               readSFN-Indicator ::= BOOLEAN
           1  true

               tx-diversityIndicator false ::= BOOLEAN
           0  false

               NewIntraFreqCells ::= SEQUENCE {
:           IntraFreqCellID switch(sw12)
           1  sw12 present
IntraFreqCellID
       11101  IntraFreqCellID = 29
               cellinfo ::= SEQUENCE {
               referenceTimeDifferenceToCell switch(sw13)
           1  sw13 present

      111010  cellIndividualOffset: -5
               referenceTimeDifferenceToCell
          10  accuray2560
               modeSpecificInfo
               primaryCPICH-Info switch(sw14)
           1  sw14 present

               primaryCPICH-TX-Power switch(sw15)
           1  sw15 present

              PrimaryCPICH-Info
    000100011  PrimaryScramplingCode 35

               primaryCPICH-TX-Power
      101111  primaryCPICH-TX-Power

               readSFN-Indicator ::= BOOLEAN
           0  false

               tx-diversityIndicator false ::= BOOLEAN
           1  true

               NewIntraFreqCells ::= SEQUENCE {
:           IntraFreqCellID switch(sw12)
           0  sw12 not present
```

```
                cellinfo

                referenceTimeDifferenceToCell switch(sw13)
             1  sw13 present

        100000  cellIndividualOffset: -31
                referenceTimeDifferenceToCell
            10  accuray2560
                modeSpecificInfo
                primaryCPICH-Info switch(sw14)
             1  sw14 present

                primaryCPICH-TX-Power switch(sw15)
             0  sw15 not present

               PrimaryCPICH-Info ::= SEQUENCE {
     101000010  PrimaryScramplingCode 322

                readSFN-Indicator
             1  true

                tx-diversityIndicator false
             0  false

                NewIntraFreqCells
:             IntraFreqCellID switch(sw12)
             0  sw12 not present

                cellinfo

                referenceTimeDifferenceToCell switch(sw13)
             0  sw13 not present

        100001  cellIndividualOffset: -30

                modeSpecificInfo

             0  fdd

                primaryCPICH-Info switch(sw14)
             1  sw14 present

                primaryCPICH-TX-Power switch(sw15)
             0  sw15 not present

               PrimaryCPICH-Info
     101111010  PrimaryScramplingCode 378

                readSFN-Indicator
             1  true

                tx-diversityIndicator false ::= BOOLEAN
             0  false


                NewIntraFreqCells ::= SEQUENCE {
:             IntraFreqCellID switch(sw12)
             0  sw12 not present

                cellinfo ::= SEQUENCE {

                referenceTimeDifferenceToCell switch(sw13)
             0  sw13 not present

        110001  cellIndividualOffset: -14

                modeSpecificInfo

             0  fdd ::= SEQUENCE {

                primaryCPICH-Info switch(sw14)
             0  sw14 not present

                primaryCPICH-TX-Power switch(sw15)
             1  sw15 present

                primaryCPICH-TX-Power
        011100  primaryCPICH-TX-Power
```

```
                readSFN-Indicator ::= BOOLEAN
            0   false

                tx-diversityIndicator false ::= BOOLEAN
            1   true


                NewIntraFreqCells ::= SEQUENCE {
:            IntraFreqCellID switch(sw12)
            0   sw12 not present

                cellinfo ::= SEQUENCE {

                referenceTimeDifferenceToCell switch(sw13)
            1   sw13 present

       001000   cellIndividualOffset: -23
                referenceTimeDifferenceToCell
           00   accuray40

                modeSpecificInfo

                primaryCPICH-Info switch(sw14)
            1   sw14 present

                primaryCPICH-TX-Power switch(sw15)
            0   sw15 not present

               PrimaryCPICH-Info
    101110000   PrimaryScramplingCode 368
               }

                readSFN-Indicator
            1   true

                tx-diversityIndicator false
            0   false


                NewIntraFreqCells
:            IntraFreqCellID switch(sw12)
            1   sw12 present
IntraFreqCellID
        00101   IntraFreqCellID = 5

                cellinfo

                referenceTimeDifferenceToCell switch(sw13)
            0   sw13 not present

       001000   cellIndividualOffset: -23

                modeSpecificInfo

                primaryCPICH-Info switch(sw14)
            1   sw14 present

                primaryCPICH-TX-Power switch(sw15)
            0   sw15 not present

               PrimaryCPICH-Info ::= SEQUENCE {
    010001010   PrimaryScramplingCode 138

                readSFN-Indicator
            0   false

                tx-diversityIndicator false
            1   true

                NewIntraFreqCells
:            IntraFreqCellID switch(sw12)
            1   sw12 present
IntraFreqCellID
        00001   IntraFreqCellID = 1

                cellinfo
```

```
                referenceTimeDifferenceToCell switch(sw13)
           0  sw13 not present

      010100  cellIndividualOffset: -11

                modeSpecificInfo

           0  fdd

                primaryCPICH-Info switch(sw14)
           0  sw14 not present

                primaryCPICH-TX-Power switch(sw15)
           0  sw15 not present


                readSFN-Indicator
           1  true

                tx-diversityIndicator false
           0  false

                NewIntraFreqCells
:           IntraFreqCellID switch(sw12)
           1  sw12 present
IntraFreqCellID
       00111  IntraFreqCellID = 7

                cellinfo ::= SEQUENCE {

                referenceTimeDifferenceToCell switch(sw13)
           0  sw13 not present

      001001  cellIndividualOffset: -22

                modeSpecificInfo

           0  fdd ::= SEQUENCE {

                primaryCPICH-Info switch(sw14)
           0  sw14 not present

                primaryCPICH-TX-Power switch(sw15)
           1  sw15 present

                primaryCPICH-TX-Power
      101010  primaryCPICH-TX-Power

                readSFN-Indicator ::= BOOLEAN
           1  true

                tx-diversityIndicator false ::= BOOLEAN
           0  false


                NewIntraFreqCells ::= SEQUENCE {
:           IntraFreqCellID switch(sw12)
           1  sw12 present
IntraFreqCellID
       00000  IntraFreqCellID = 0

                cellinfo ::= SEQUENCE {

                referenceTimeDifferenceToCell switch(sw13)
           0  sw13 not present

      101110  cellIndividualOffset: -17

                modeSpecificInfo

           0  fdd ::= SEQUENCE {

                primaryCPICH-Info switch(sw14)
           0  sw14 not present

                primaryCPICH-TX-Power switch(sw15)
           0  sw15 not present
```

```
                readSFN-Indicator
            0   false

                tx-diversityIndicator false
            0   false

                NewIntraFreqCells
:            IntraFreqCellID switch(sw12)
            1   sw12 present
IntraFreqCellID
         01010  IntraFreqCellID = 10

                cellinfo ::= SEQUENCE {

                referenceTimeDifferenceToCell switch(sw13)
            0   sw13 not present

        100010  cellIndividualOffset: -29

                modeSpecificInfo

            0   fdd

                primaryCPICH-Info switch(sw14)
            1   sw14 present

                primaryCPICH-TX-Power switch(sw15)
            1   sw15 present

               PrimaryCPICH-Info
     000110101  PrimaryScramplingCode 53

                primaryCPICH-TX-Power
        001100  primaryCPICH-TX-Power

                readSFN-Indicator
            0   false

                tx-diversityIndicator false
            1   true


                NewIntraFreqCells
:            IntraFreqCellID switch(sw12)
            0   sw12 not present

                cellinfo

                referenceTimeDifferenceToCell switch(sw13)
            0   sw13 not present

        010110  cellIndividualOffset: -9

                modeSpecificInfo

            0   fdd

                primaryCPICH-Info switch(sw14)
            0   sw14 not present

                primaryCPICH-TX-Power switch(sw15)
            0   sw15 not present

                readSFN-Indicator
            1   true

                tx-diversityIndicator false
            0   false

                IntraFreqMeasQuantity
:               FilterCoefficient
          1100  fc15
:                           }
                mode SpecificInfo
            0   fdd
                intraFreqMeasQuantity-FDD
           01   cpich-RSCP
                           }
```

```
}
:IntraFreqReportingQuantity

               detectedSetReportingQuantities sw30
            0  sw30 not present

               activeSetReportingQuantities
               dummy
               cellIdentity-reportingIndicator
            0  false
               cellSynchronisationReportingIndicator
            0  false
               modeSpecificInfo
            0  fdd
               cpich-Ec-NO-reportingIndicator
            1  true
               cpich-RSCP-reportingIndicator
            0  false
               Pathloss-reportingIndicator
            1  true

               monitoredSetReportingQuantities
               dummy
           01  type1
               cellIdentity-reportingIndicator
            0  false
               cellSynchronisationReportingIndicator
            0  false
               modeSpecificInfo
            0  fdd
               cpich-Ec-NO-reportingIndicator
            0  false
               cpich-RSCP-reportingIndicator
            0  false
               Pathloss-reportingIndicator
            1  true

: Report Criteria
            0  IntraFreqReportingCriteria

               eventCriteriaList (sw31)
            0  sw31 not present

          001  val20: 1

intraFreqEventCriteria
               reportingCellStatus (sw32)
            1  sw32 present

               event
         0000  e1a

               forbiddenAffectCellList (sw33)
            0  sw33 not present

               triggerCondition
          001  monitoredSetCellsOnly

        01110  reportingRange = 14

        11000  value of w = 24

               reportDeactivationThreshold
          010  T2

               reportingAmount
          010  ra4

               reportingInterval
          111  ri16


         1011  hysteresis = 11

               timeToTrigger
         0001  ttt10

               reportingCellStatus
```

```
        0000  withinActiveSet
         101  e6

intraFreqEventCriteria
               reportingCellStatus sw32
           0  sw32 not present

               event
        0000  e1a

               forbiddenAffectCellList (sw33)
           0  sw33 not present

               triggerCondition
         000  activeSetCellsOnly

       01100  reportingRange = 12

       01111  value of w = 15
               reportDeactivationThreshold
         011  T3
               reportingAmount
         001  ra2
               reportingInterval
         001  ri0-25

        1111  hysteresis = 15
               timeToTrigger
        0110  ttt100
               reportingCellStatus
        1001  withinMonitoredSetNonUsedFreq
         100  e5

MeasurementReportingMode

               measurementReportTransferMode
           0  acknowledgedModeRLC

               periodicalOrEventTrigger
           1  eventTrigger
```

Bild 99: Entschlüsselung eines Measurement Report Kommandos

10.3.13 ACTIVATE PDP CONTEXT ACCEPT

Die NAS-Message ACTIVATE PDP CONTEXT ACCEPT liefert, wie aus dem GPRS bekannt, die *Packet data protocol address*, sowie den gewährten Quality of Service.

```
_____[ 88 ]_____[ group ID: 00 07 ]_____[ trace ID: 00 01 ]______

00 04 01 b0  85 1a 22 0f  09 42 05 b1  48 40 61 61  72 23 ee 72
d1 dd 0e 80  a0 20 20 85  60 c0 24 21  5d 81 78 64  e2 90 10 04
22 00 60 00  02 10 20 d1  60 e3 cf b0  60 d1 60 e3  cf c0

:WDCMA L3 RRC Peer messages

00  00000000  Channel LSB
:Channel Type MSB
04  00000100  Downlink DCCH

01  0000000110110000  length=432
          1  Integrity Check Info present
    00001010  MessageAuthenticationCode,
    00110100  MessageAuthenticationCode,
    01000100  MessageAuthenticationCode,
    00011110  MessageAuthenticationCode,
        0001  RRC-MessageSequenceNumber  = 1

: Message Type:
```

```
       00101  DOWNLINK DIRECT TRANSFER
           0  r3 SEQUENCE
           0  sw1 not present
DownlinkDirectTransfer-r3
          00  RRC-TransactionIdentifier = 0
:CN-DomainIdentity
           1  ps-domain
:nas-Message
    000000101101  length=45
    1-------  direction to        : originating site
    -000----  TransactionID       : 0
    ----1010  Protocol Discrim.   : Session Management Messages

    01000010  MESSAGE TYPE        : ACTIVATE PDP CONTEXT ACCEPT

    0000----  spare
    ----0011  Requested LLC service access point identifier SAPI = 3

    00001011  Length of quality of service IE = 11

    00------  spare
    --001---  Delay class         : 1 (4 = best effort)
    -----011  Reliability class   : Unacknowledged GTP and LLC; Acknowledged RLC,
                                    Protected data
    1001----  peak throughput     : Up to 256000 octet/s
    ----0---  spare
    -----001  precedence class    : High priority
    000-----  spare
    ---11111  Mean throughput Best effort

    011-----  Interactive class
    ---10---  Without delivery order ('no')
    -----011  Erroneous SDUs are not delivered ('no')
    10010110  Maximum SDU size
    10001110  Maximum bit rate for uplink
    11101000  Maximum bit rate for downlink
    0111----  Residual Bit Error Rate 1*10-5
    ----0100  SDU error ratio 1*10-4
    000001--  Transfer delay
    ------01  Traffic handling Priority level 1
    00000001  Guaranteed bit rate for uplink
    00000001  Guaranteed bit rate for downlink
    0000----  spare half octet
    ----0---  spare bit
    -----100  Radio priority level: 4 (lowest)

    00101011  INFORMATION ELEMENT : Packet data protocol address

    00000110  Length of PDP address contents = 6
    ----0001  PDP type organisation: IETF allocated address
    00100001  PDP type number      : IPv4 address
    00001010  Number 1             : 10
    11101100  Number 2             : 236
    00001011  Number 3             : 11
    11000011  Number 4             : 195

: Protocol Configuration Options
    00100111  INFORMATION ELEMENT : Protocol Configuration Options

    00010100  length              : 20
: Configuration Protocol
    -----000  PPP for use with IP PDP type
    -0000---  spare
    1-------  Extension bit       : 1
: PROTOCOL ID 1
    10000000  8021(IPCP).
    00100001  C021(LCP),8021(IPCP)

    00010000  Lgth of P ID 1 cont.: 16
    00000011  protocol ID 1 contents
    00000000  protocol ID 1 contents
    00000000  protocol ID 1 contents
    00010000  protocol ID 1 contents
    10000001  protocol ID 1 contents
    00000110  protocol ID 1 contents
    10001011  protocol ID 1 contents
    00000111  protocol ID 1 contents
    00011110  protocol ID 1 contents
```

```
01111101  protocol ID 1 contents
10000011  protocol ID 1 contents
00000110  protocol ID 1 contents
10001011  protocol ID 1 contents
00000111  protocol ID 1 contents
00011110  protocol ID 1 contents
01111110  protocol ID 1 contents
```

Bild 100: Aktivierter Kontext

10.3.14 Die folgenden Meldungen

Im Folgenden treten nun noch periodisch die Meldungen
MEASUREMENT REPORT und MEASUREMENT CONTROL auf.

Damit keine Ressourcen verschenkt werden entscheidet sich das Netz auch zur RADIO BEARER RECONFIGURATION und zur PHYSICAL CHANNEL RECONFIGURATION

11 Authentisierung

Die Sicherheitsarchitektur von 3G wurde auf Grundlage der bewährten GSM Sicherheits-Architektur aufgebaut. Einige Schwachstellen wurden beseitigt.
Im UMTS wird nicht nur die Teilnehmeridentität geprüft, sondern auch die Identität des Netzbetreibers. D.h. das Sicherheitskonzept besteht aus den Komponenten Verschlüsselung und Integrität. Die Teilnehmeridentität wird ähnlich dem Verfahren im GSM mit einer Parole (RAND) geprüft. Die der Teilnehmer mit Rückgabe von RES beantwortet. Die Verschlüsselung besteht aus den beiden Algorithmen UEA0 und UEA1, dabei bedeutet der Algorithmus UEA0 das Gleiche wie „Keine Verschlüsselung“

Bevor sich der Teilnehmer gegenüber dem Netz identifiziert prüft er jedoch ob der Operator „echt“ ist. Das Authentication Center im Netz generiert mittels des Algorithmus UIA1 dazu ein *Authentication Token* AUTN. Dieses besteht aus einem *Authentication and Key Management Field* AMF, *dem Message Authendication Code* MAC und der *Sequenznummer* SQN‘. RAND und AUTN werden dem Mobile vom Netz mit der Meldung AUTHENTICATION AND CIPHERING REQUEST übergeben. Im Mobile werden diese Werte wie folgt bearbeitet.
Zur Sicherung der Integrität der Daten auf dem Signalkanal wird ein *Integrity Key* erzeugt. Start oder Modifikation erfolgt mit dem SECURITY MODE COMMAND. Der IK wird mit der Funktion F4 erzeugt.
Die Verschlüsselung erfolgt ähnlich dem GSM mit einer Quasizufallsfolge

11.1 Das Prinzip einerVerschlüsselung

Wird ein offener Text in einem Modulo 2 Addierer mit einer (echten) Zufallsfolge gemischt, so ist das Ergebnis wieder eine (echte) Zufallsfolge.

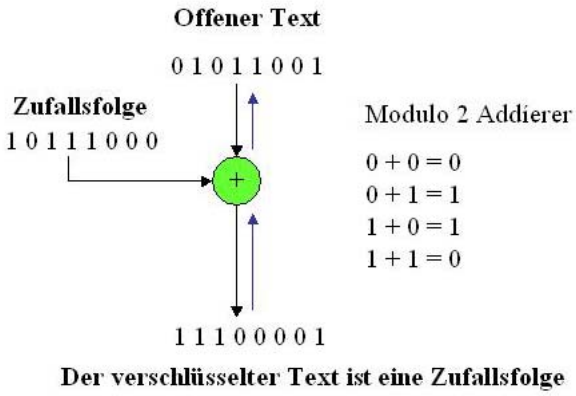


Bild 100: Das Prinzip einer Verschlüsselung

11.2 Verschlüsseln im UMTS

Die Zufallsfolge wir im UMTS aus COUNT, CK und F8 gebildet.

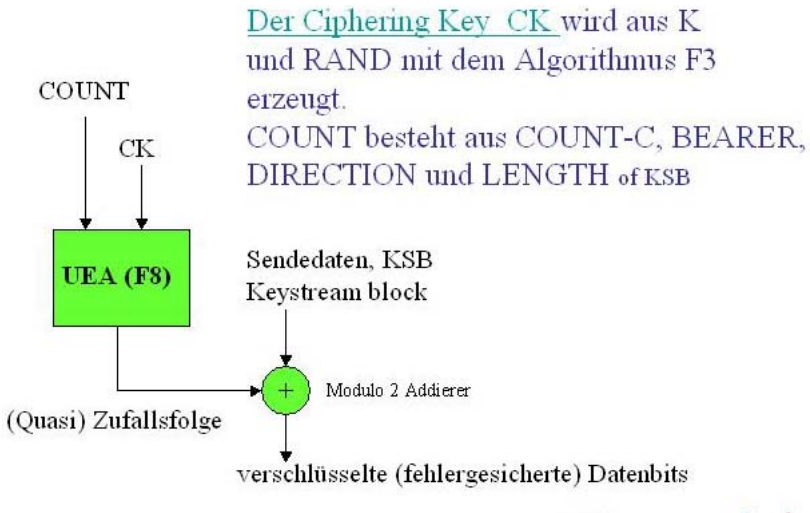


Bild 101: Das Prinzip der Bildung einer Zufallsfolge im UMTS

11.3 **Die Erzeugung einer „Parole“ (RES)**

Indem das Netz die Zufallszahl RAND dem Mobile zusendet ruft es wie ein Wachtposten „Parole!!“ Die richtige Antwort auf Parole ist „RES“

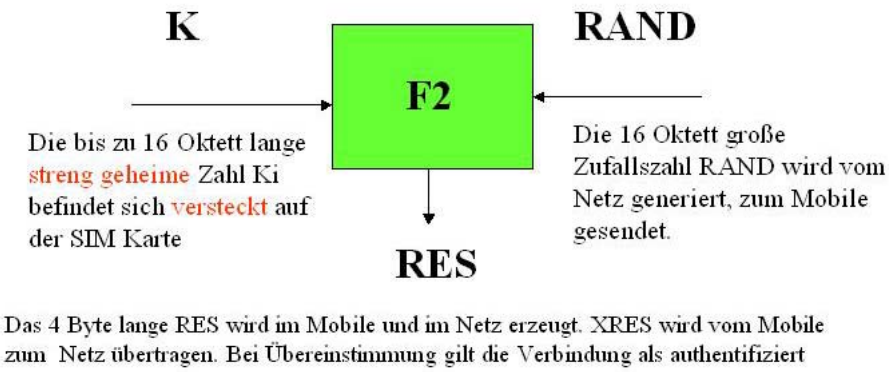


Bild 102: Das Prinzip der Bildung einer Antwort auf RAND (Parole)

11.4 Die Erzeugung des Schlüssels CK

Der Schlüssel CK und eine dazugehörende 3 bit lange *Ciphering Key Sequence Number* (CKSN) werden im Mobile und im Netz erzeugt. Die CKSN wird vom Mobile zum Netz übertragen.

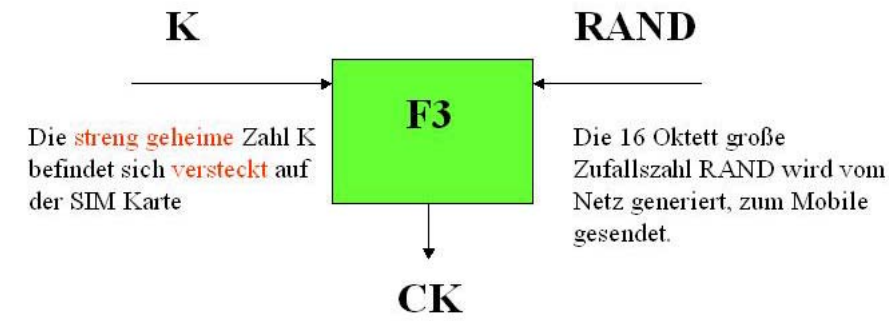


Bild 103: Das Prinzip der Bildung eines Schlüssels CK

11.4 Der Integrity Key IK

Die Erzeugung des Integrity Key mittels des Algorithmus UIA1 ist in Bild 103 dargestellt.

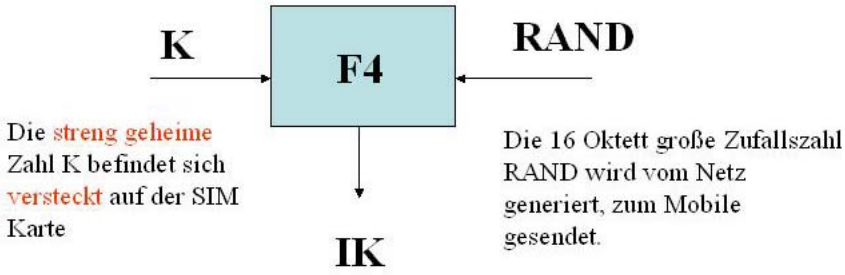


Bild 103: Das Prinzip der Integrity Protection

Die 32 bit *Integrity Checkinfo* wird an der Spitze aller RRC Messages übertragen außer:

HANDOVER TO UTRAN COMPLETE,
PAGING TYPE1,
PUSH CAPACITY REQUEST;
PHYSICAL SHARED CHANNEL ALLOCATION;
RRC CONNECTION REQUEST;
RRC CONNECTION SETUP;
RRC CONNECTION SETUP COMPLETE,
RRC CONNECTION REJECT,
RRC CONNECTION RELEASE,
SYSTEMINFORMATION,
SYSTEMINFORMATION CHANGE INDICATION;
TRANSPORT FORMAT COMBINATION CONTROL.

12 Literatur

12,1 Bücher und Lehrmaterial

12.1.1 Themen GPRS und EDGE

[1] GPRS-Gateway zu Mobilfunknetzen der 3. Generation, von Gunnar Heine und Holger Sagkob, Franzis' Verlag GmbH, 2001. ISBN 3-7723-4553-

[2] Eine CD, die einen Experimentalvortrag mit 90 PowerPoint Folien enthält, dazu Übungen auf 20 Power-Point Folien, die Traceübersetzungwerkzeuge EDGEView, sowie einen Lehrtext.
CBT-CD von Joachim Göller und Tracemobile SAGEM OT 490, EPV-Verlag Duderstadt,EPV-Best.-Nr.:GPRS/EDGE

[3] http://www2.informatik.hu-berlin.de/~goeller/isdn/IP-GPRS-EDGE.pdf.

12.1.2 Thema UMTS

[1] UMTS Einführung und Messtechnik, von Reinhold Krüger und Heinz Mellein. Franzis' Verlag GmbH, 2003. ISBN 3-7723-4999-4

[2] UMTS Grundlagen, Architektur und Standart, von Pierre Lescuyer. Übersetzt aus dem Franz. Von Peter Simon. Heidelberg: dpunkt-Verlag, 2002. ISBN 3-89864-141-4

[3] Introduction to 3G Mobile Communications Second Edition, by Juha Korhonen. 2003 Artech House, Inc. ISBN 1-58053-507-0

12.2 Technische Spezifikationen

[1] 3GPP TS 22.060 Version 6.0.0 Release 6
Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); General Packet Radio Service (GPRS); Service description; Stage 1

[2] ETSI TS 125 331 Version 5.6.0
Universal Mobile Telecommunications System (UMTS);
Radio Resource Control (RRC) protocol specification

[3] ETSI TS 124 008 Version 7.6.0
Digital cellular telecommunications system (Phase 2+);
Universal Mobile Telecommunications System (UMTS);
Mobile radio interface Layer 3 specification;
Core network protocols;
Stage 3

[4] ETSI TS 125 321 Version 8.6.0
Universal Mobile Telecommunications System (UMTS);
Medium Access Control (MAC) protocol specification

[5] ETSI TS 125 211 Version 8.4.0
Universal Mobile Telecommunications System (UMTS);
Physical channels and mapping of transport channels onto physical channels (FDD)