

# Системы сигнализаций в сетях связи

## Подсистема мобильной связи MAP

Mobile Application Part (MAP) протокол уровня приложения архитектуры SS7 систем, который предоставляет доступ к среде различным приложениям в системах UMTS и GSM.

Этот протокол используется между сетевыми компонентами сетей подвижной связи (СПС), такими как:

- MSC (Mobile services Switching Center – центр коммутации подвижной связи);
- BTS (Base Transceiver Station – базовая приемопередающая станция);
- BSC (Base Station Controller – контроллер базовых станций);
- HLR (Home Location Register – регистр домашних абонентов);
- VLR (Visitor Location Register – гостевой регистр местонахождения);
- EIR (Equipment Identity Register - регистр идентификации оборудования);

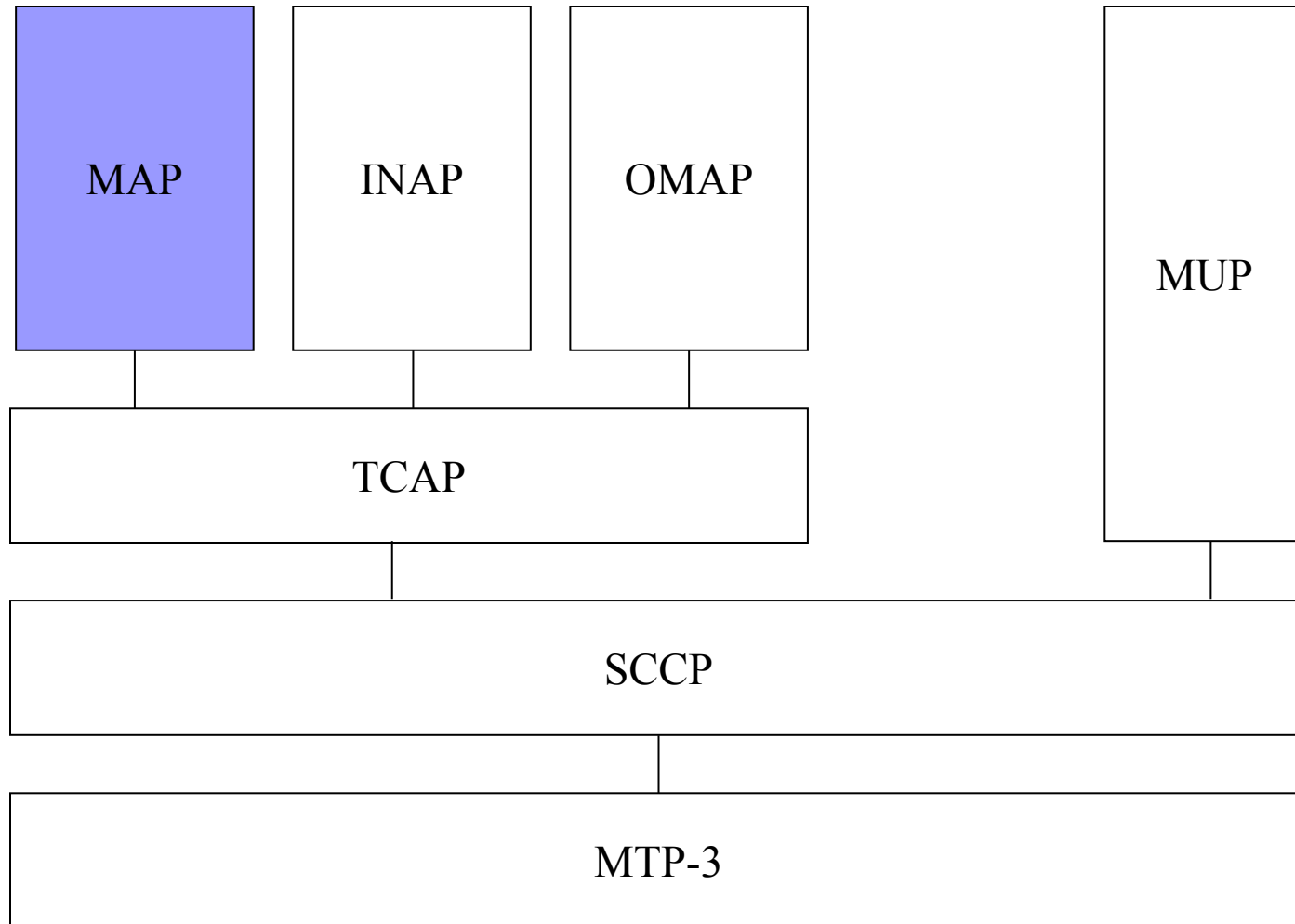
## Подсистема мобильной связи MAP

- AC (Authentication Centre – центр аутентификации);
- SGSN (Serving GPRS Support Node – пакетный коммутатор)/GGSN (Gateway General Support Node – GPRS шлюз) в GPRS.

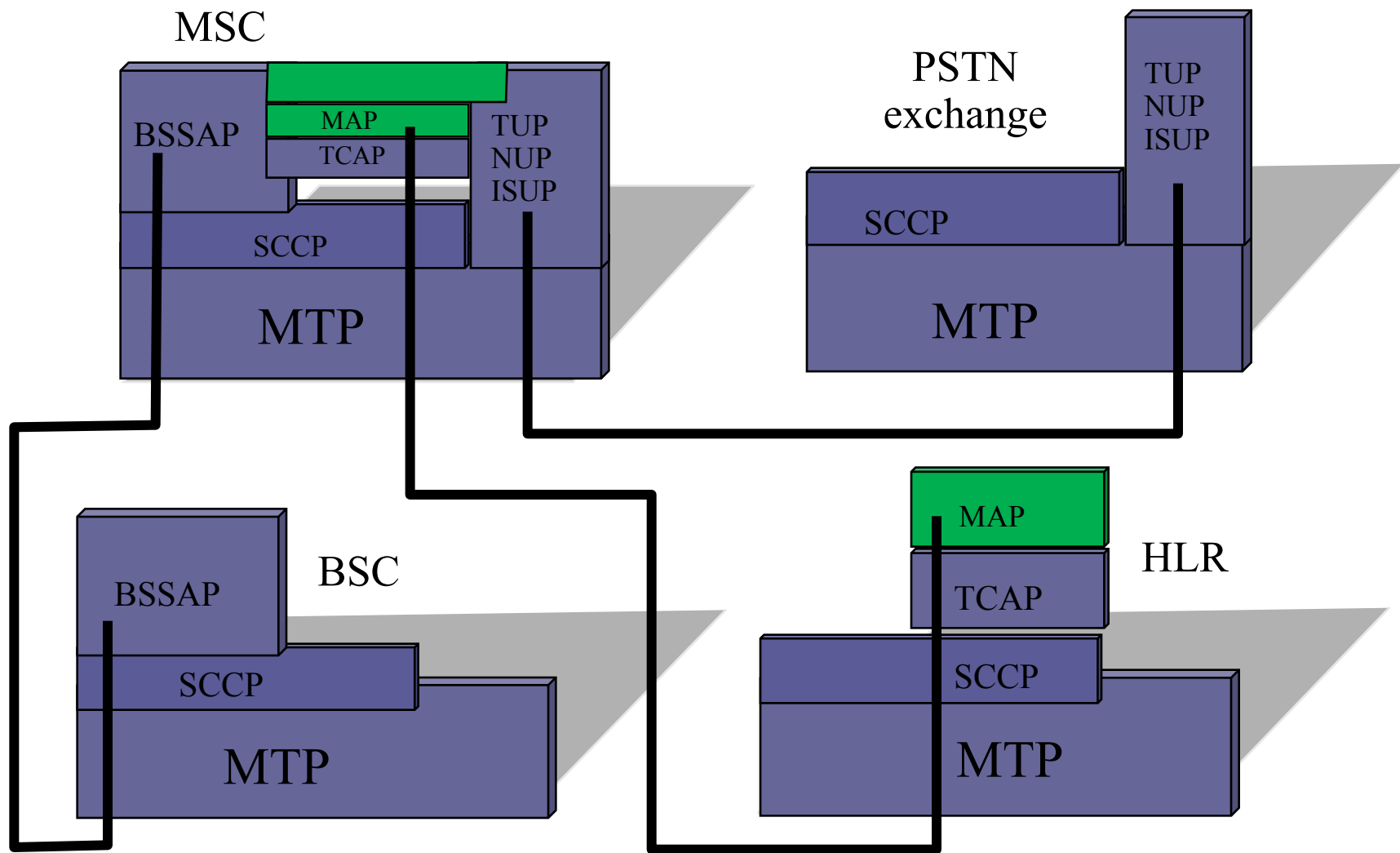
Всего определено пять приложений MAP для подсистемы коммутации (MAP-MSC, MAP-VLR, MAP-HLR, MAP-EIR, MAP-AUC) и приложение *BSSAP (BSS Application Part)* для контроллера базовых станций BSC.

Подсистема MAP представляет собой протокол, который позволяет узлам сети GSM обмениваться информацией друг с другом с целью предоставления таких услуг, как роуминг, хэндовер, маршрутизация входящих вызовов и SMS, обмен текстовыми сообщениями SMS и аутентификация абонента.

# Место подсистемы MAP в стеке протоколов ОКС7



# Подсистема MAP в различных сетевых элементах



## Глобальный заголовок подвижной связи

Помимо ТСАР и МТР протокол МАР также использует подсистему SССР, причем только классы 0 и 1. Основная задача SССР при передаче сообщений роуминга заключается в пересчете глобального заголовка (*GT – Global Title*) в маршрутную информацию, т.е. в коды пунктов сигнализации на сети ОКС №7 в соответствии с несколькими планами нумерации. Для СПС стандарта GSM используются планы нумерации, определенные в рекомендациях ITU-T (E.163/164, E.214, E.212). Параметры сообщений SССР, которые используются подсистемой МАР для обеспечения роуминга, включают данные с учетом специфики подвижной связи. Например, параметр «Адрес вызываемой/вызывающей стороны» включает глобальный заголовок GT, равный 0100, номер подсистемы SSN определяет устройства СПС, которые обмениваются сообщениями (MSC, HLR, VLR, EIR).

## Глобальный заголовок подвижной связи

Маршрутизация обращения HLR осуществляется с помощью глобального заголовка подвижной связи (MGT).

Глобальный заголовок подвижной связи дает возможность опознать страну и сеть, к которой приписана подвижная станция, а также позволяет опознавать HLR рассматриваемой подвижной станции.

CC	NC	MSIN
----	----	------

Структура глобального заголовка подвижной связи MGT, длина которого не должна превышать 15 цифр: где:

CC – код страны

NC – код сети

MSIN – опознавательный номер подвижной станции

# Основные процедуры MAP

Существуют несколько основных процедур протокола MAP:

- Location Update
- передача SMS
- запрос баланса USS
- вызов в СПС из ТфОП
- Handover



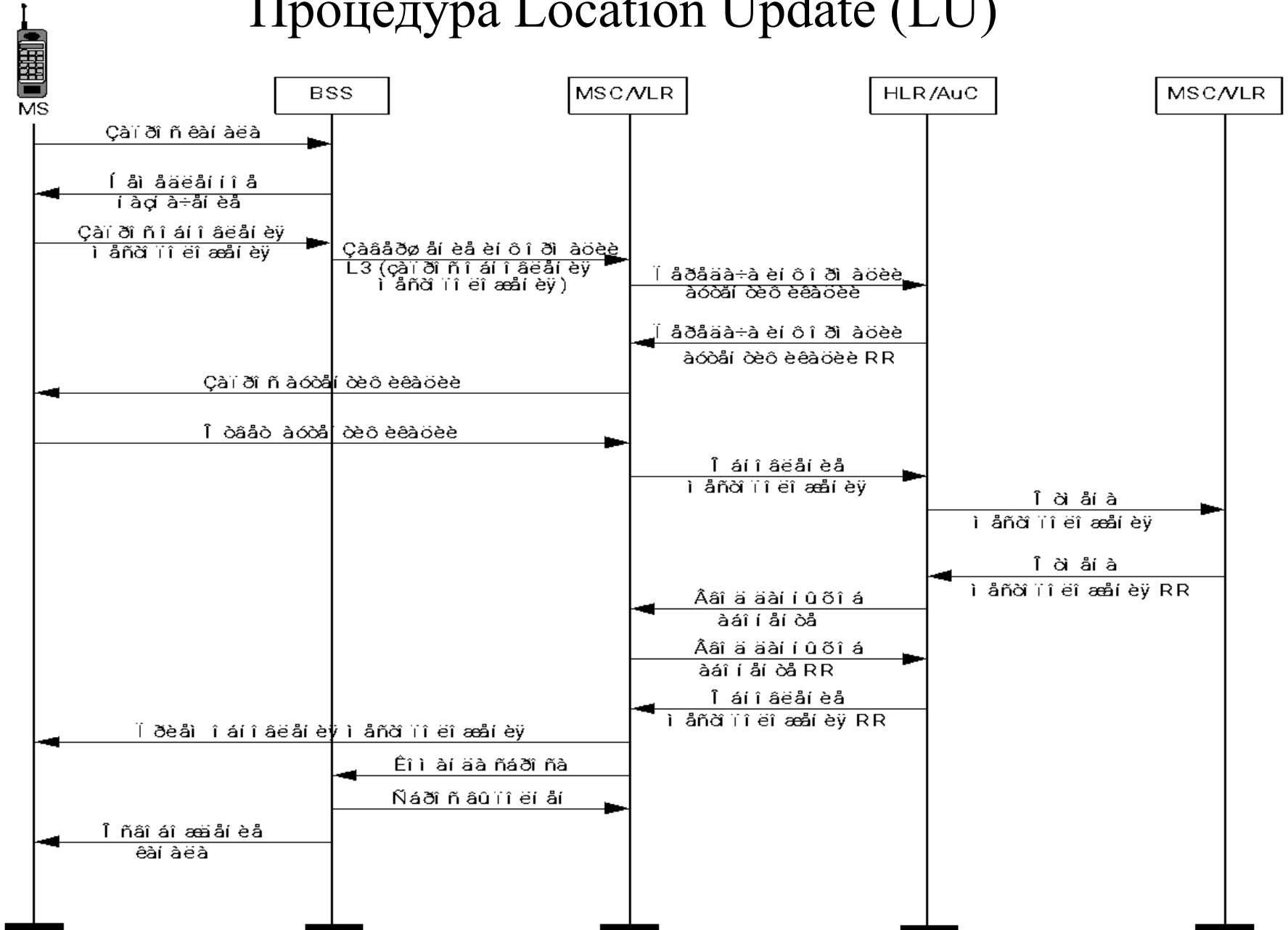
## Процедура Location Update (LU)

*Обновление данных о местонахождении (Location Update)*

может происходить, когда:

- MS (мобильная станция) только что включилась;
- MS переместилась в пределах зоны одного и того же VLR, но в новую зону местонахождения LA;
- MS переместилась в новую зону VLR;
- сработал таймер обновления местонахождения.

# Процедура Location Update (LU)



## Процедура Location Update (LU)

1. Из мобильного терминала MS в подсистему базовых станций BSS передается запрос канала.
2. BSS назначает канал *SDCCH (Stand-alone Dedicated Control Channel – автономный выделенный канал управления; двунаправленный канал, с передачей «точка-точка», используемый для запроса услуг, аутентификации абонента, создания шифра, проверки оборудования и закрепления канала трафика)* для этого мобильного терминала и дает ему команду перейти на этот канал, передав сообщение *Немедленное назначение*.
3. По получении этого сообщения мобильный терминал переходит на назначенный SDCCH и передает запрос обновления данных о местонахождении. Запрос содержит данные, включающие в себя идентификатор зоны местонахождения, полученный мобильным терминалом, и идентификатор мобильного терминала (IMSI, TMSI).

## Процедура Location Update (LU)

4. IMSI (TMSI) передается через BSS в MSC с помощью типового сообщения *Complete Layer 3 Info* (завершение информации уровня 3), входящего в состав SCCP Connection Request протокола SCCP. Если TMSI не известен в MSC/VLR, то MSC/VLR может запросить у мобильного терминала передачу IMSI. Кроме того, MSC/VLR может запросить у MS идентификатор TA IMEI для проверки.
5. После приема запроса *Location Update* MSC/VLR может попытаться произвести аутентификацию терминала. Если MSC/VLR уже не имеет аутентификационной информации, он запрашивает эту информацию у HLR, используя операцию *Send Authentication Info* протокола MAP.

## Процедура Location Update (LU)

6. HLR/AuC передает *Return Result (RR)* подсистемы MAP с несколькими (до пяти) триплетами. Каждый триплет содержит случайное число (*RAND*) и параметр *Signed Response (SRES)*.
7. Узел MSC передает в мобильный терминал запрос аутентификации *Authentication Request*, который содержит только *RAND*.
8. В MS выполняется такой же расчет, какой был сделан в HLR/AuC, затем он передает *Authentication Response*, содержащий параметр *SRES*. В свою очередь, MSC/VLR проверяет соответствие *SRES*. Если соответствие подтверждено, MS считается аутентифицированной.
9. MSC/VLR использует операцию *Update Location* протокола MAP, чтобы информировать HLR о местонахождении абонента. Сообщение содержит *IMSI* абонента и сигнал *Global Title Address (GTA)* от MSC/VLR.

## Процедура Location Update (LU)

10. HLR передает в VLR, где ранее был зарегистрирован абонент (если таковой имеется), сообщение *Cancel Location (отмена местонахождения)* протокола MAP.
11. VLR удаляет все записанные данные, относящиеся к абоненту, и посылает в HLR сигнал *Return Result*.
12. Регистр HLR использует команду *Insert Subscriber Data* протокола MAP для VLR, чтобы информировать VLR о совокупности относящихся к рассматриваемому абоненту данных, включающих в себя информацию о дополнительных услугах.
13. VLR подтверждает получение информации.
14. После получения RR MSC/VLR передает в мобильный терминал сообщение *DTAP Location Updating Accept*.
15. Затем он ликвидирует соединение SCCP с BSS. Это заставляет BSS освободиться от SDCCH путем передачи в мобильный терминал сообщения *Channel Release*.

# Сообщения процедуры Location Update (LU)

S	D	Linkset	PL	LL	CI	Message Contents	Time
W	1	E1/T1-V2 Card (P-O>	1B-03	14080 ->	15076	> CR COMP L3 INFO CM SE>	+ 00:00:54.540.156
	2	E1/T1-V2 Card (P-O>	1B-01	15076 ->	14080	1B7F03h > CC	+ 00:00:54.544.812
	2	E1/T1-V2 Card (P-O>	1B-01	15076 ->	14080	1B7F03h DT1 AUTHENTICATION REQ	+ 00:00:54.548.437
W	1	E1/T1-V2 Card (P-O>	1B-03	14080 ->	15076	978A4Ch DT1 CLASSMARK UPDATE	+ 00:00:54.773.902
	1	E1/T1-V2 Card (P-O>	1B-03	14080 ->	15076	978A4Ch DT1 AUTHENTICATION RE>	+ 00:00:55.713.015
	2	E1/T1-V2 Card (P-O>	1B-01	15076 ->	14080	1B7F03h DT1 CIPHER MODE CMD	+ 00:00:55.717.921
	1	E1/T1-V2 Card (P-O>	1B-03	14080 ->	15076	978A4Ch DT1 CIPHER MODE COMP	+ 00:00:55.947.261
	1	E1/T1-V2 Card (P-O>	1B-03	14080 ->	15076	978A4Ch DT1 REGISTER PROCESS_>	+ 00:00:56.425.757
	2	E1/T1-V2 Card (P-O>	1B-01	15076 ->	14080	1B7F03h DT1 REL_COMP PROCESS_>	+ 00:00:56.677.660
	2	E1/T1-V2 Card (P-O>	1B-01	15076 ->	14080	1B7F03h DT1 CLEAR CMD	+ 00:00:56.679.410
	1	E1/T1-V2 Card (P-O>	1B-03	14080 ->	15076	978A4Ch DT1 CLEAR COMP	+ 00:00:56.682.753
	2	E1/T1-V2 Card (P-O>	1B-01	15076 ->	14080	1B7F03h > RLSD	+ 00:00:56.688.160
	1	E1/T1-V2 Card (P-O>	1B-03	14080 ->	15076	978A4Ch > RLC	+ 00:00:56.693.878

Сообщения CR, CC, CIPHER MODE CMD, CLASSMARK UPDATE, CIPHER MODE COMP, CLEAR CMD, CLEAR COMP, RLSD, RLC являются типовыми для всех процедур и отвечают за выбор сигнального канала, передачи информации 3 уровня, шифрование данных, обновление класса службы, освобождение радиоресурса и завершение диалога.

Главными сообщениями процедуры являются Authentication Request и Authentication Response (запрос и ответ аутентификации).

# Сообщения процедуры LU (Authentication Request)

Значения строк:

- Protocol Discriminator – дискриминатор протокола (5h=Mobility Management – управление мобильностью);
- Ciphering Key Sequence Number – порядковый номер ключа шифрования;
- Authentication Parameter RAND – параметр аутентификации «случайное число»;
- Authentication Parameter SRES – параметр аутентификации, входящий в триплет.



# Сообщения процедуры LU (Authentication Request)

```
--100010      Length Indicator                34 = LI -> Message Signal Unit
*****
Service Information Octet
----0011      Service Indicator             3 = Signaling Connection Control Part
--00----      Priority Indicator            0
11-----      Network Indicator           3 = Reserved for national use
*****
SCCP (03/2001)
*****
<General Fields>
*****
Routing Label
*****
Destination Point Code                14080
*****
Originating Point Code                 15076
*****
1001----      Signalling Link Selection     9
*****
DATA FORM 1
*****
Destination Local Reference            1B7F03h
*****
Segmenting/reassembling
-----0      More data indication         0b = no more data
*****
Data
01 00 13 05 12 04 F3 48 6E F9 DD 00 00
9F E5 BE 97 FF 17h

*****
GSM 08.06 / UMTS 48.006 - BSSAP
00000001      Header                       1 = Direct Transfer Application Part
-----000      DLCI Parameter              0h
00-----      Control Channel Indication  00b = not further specified
*****
GSM 04.08 - DTAP (V 6.4.2)
*****
<General Fields>
-----0101      Protocol Discriminator     5h = Mobility Management
*****
GSM 04.08 - MM (V 6.4.2)
*****
AUTHENTICATION REQUEST
-----100      Ciphering Key Sequence Number 4h = 4
*****
Authentication Parameter RAND          F3 48 6E F9 DD 00 00 DF 1A 66 9F E5 BE
```

# Сообщения процедуры LU (Authentication Response)

	Description	Value
*****	MTP (07/96)	
*****	MSU	
*****	<General Fields>	
-1110100	Backward Sequence Number	116
1-----	Backward Indicator Bit	1
-1110110	Forward Sequence Number	118
1-----	Forward Indicator Bit	1
--010101	Length Indicator	21 = LI -> Message Signal Unit
*****	Service Information Octet	
----0011	Service Indicator	3 = Signaling Connection Control Part
--00----	Priority Indicator	0
11-----	Network Indicator	3 = Reserved for national use
*****	SCCP (03/2001)	
*****	<General Fields>	
*****	Routing Label	
*****	Destination Point Code	15076
*****	Originating Point Code	14080
1111----	Signalling Link Selection	15
*****	DATA FORM 1	
*****	Destination Local Reference	978A4Ch
*****	Segmenting/reassembling	
-----0	More data indication	0b = no more data
*****	Data	01 00 06 05 54 D8 A4 08 44h
*****	GSM 08.06 / UMTS 48.006 - BSSAP	
00000001	Header	1 = Direct Transfer Application Part
----000	DLCI Parameter	0h
00-----	Control Channel Indication	00b = not further specified
*****	GSM 04.08 - DTAP (V 6.4.2)	
*****	<General Fields>	
----0101	Protocol Discriminator	5h = Mobility Management
*****	GSM 04.08 - MM (V 6.4.2)	
*****	AUTHENTICATION RESPONSE	
*****	Authentication Parameter SRES	D8A40844h

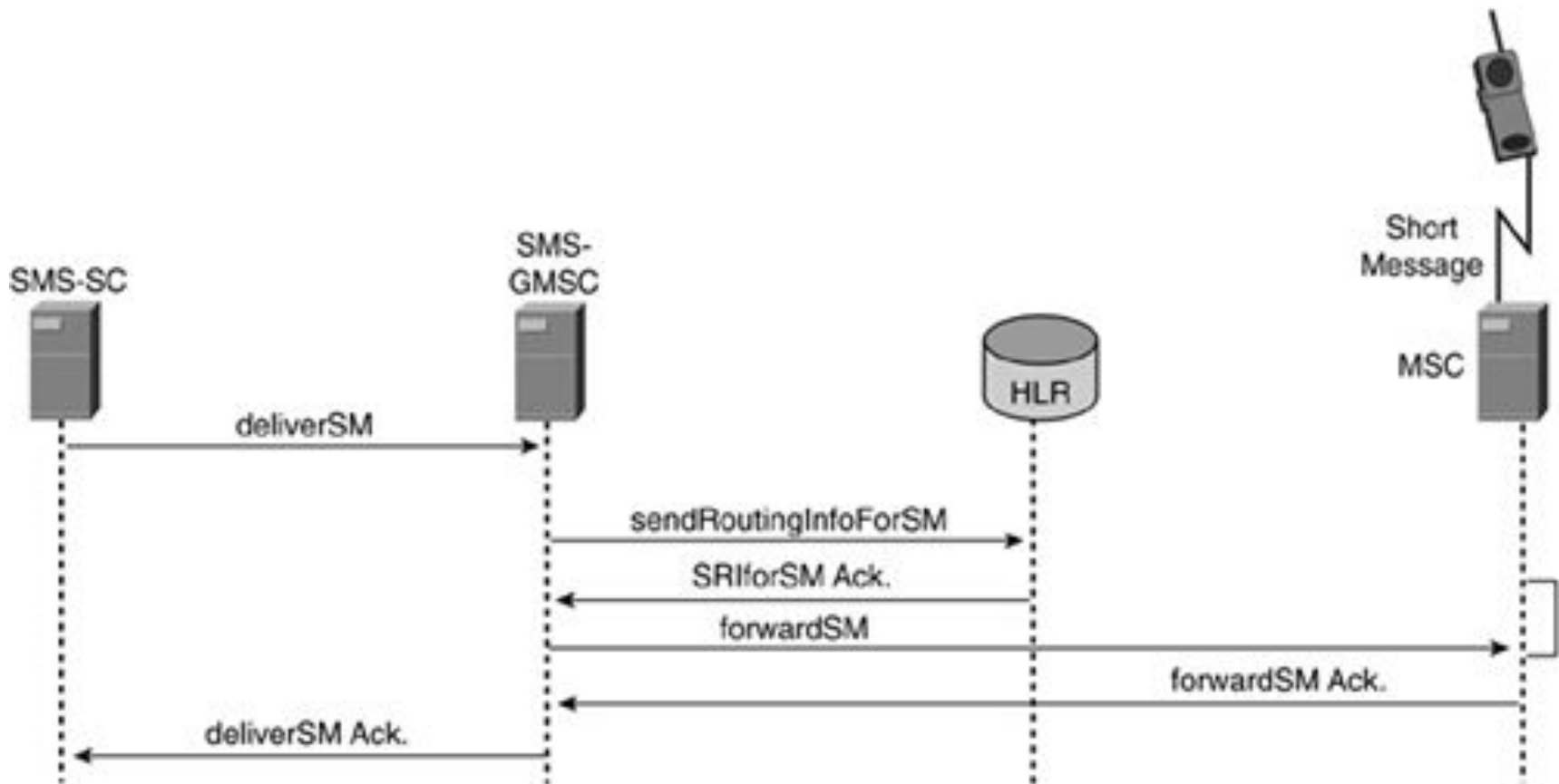
## Служба коротких сообщений (SMS)

Служба коротких сообщений предоставляет пользователям сети GSM обмениваться буквенно-цифровыми сообщениями длиной до 160 символов.

Основными операциями при обмене сообщениями являются:

- forwardSM – передать короткое сообщение;
- sendRoutingInfoForSM – посылка информации роуминга;
- reportSMDeliveryStatus – отчет о доставке;
- readyForSM – сигнал готовности для приема коротких сообщений;
- alertServiceCentre – предупреждение сервис-центра;
- informServiceCentre – информирование сервис-центра.

# Служба коротких сообщений (SMS)



## Служба коротких сообщений (SMS)

Если SMS-SC не может доставить входящее сообщение абоненту, он отправляет отрицательный результат на шлюз GMSC. При получении такого результата шлюз SMS-GMSC отправляет в HLR сообщение reportSMDeliveryStatus, а тот в свою очередь устанавливает флаг ожидания на соответствующих абонентских данных. HLR также отправляет сообщение alertServiceCentre сервисному центру SMS-IWMSC, уведомляя его об отрицательном результате доставки SMS, и ждет, когда абонент станет доступным. Когда VLR определяет, что абонент снова находится в зоне досягаемости, он отправляет сообщение readyForSM регистру HLR. HLR в свою очередь отправляет центру SMS-IWMSC сообщение alertServiceCentre, в котором содержится информация для центра SMS-SC. Затем процесс доставки начинается заново с команды ForwardSM.

# Сообщения процедуры передачи SMS

S	D	Linkset	PL	LL	CI	Message Contents	Time
W	1	E1/T1-V2 Card (P-0>	1B-05	14080 -> 15076		CR COMP L3 INFO PAGE >	+ 00:00:55.010.425
	2	E1/T1-V2 Card (P-0>	1B-07	15076 -> 14080	B6C200h >	CC	+ 00:00:55.019.957
	2	E1/T1-V2 Card (P-0>	1B-07	15076 -> 14080	B6C200h	DT1 CIPHER MODE CMD	+ 00:00:55.022.207
W	1	E1/T1-V2 Card (P-0>	1B-05	14080 -> 15076	4A4D4Dh	DT1 CLASSMARK UPDATE	+ 00:00:55.245.421
	1	E1/T1-V2 Card (P-0>	1B-05	14080 -> 15076	4A4D4Dh	DT1 CIPHER MODE COMP	+ 00:00:55.711.667
	2	E1/T1-V2 Card (P-0>	1B-07	15076 -> 14080	B6C200h	DT1 CP-DATA SMS-DELIV>	+ 00:00:55.722.074
	1	E1/T1-V2 Card (P-0>	1B-05	14080 -> 15076	4A4D4Dh	DT1 CP-ACK	+ 00:00:56.888.527
	1	E1/T1-V2 Card (P-0>	1B-05	14080 -> 15076	4A4D4Dh	DT1 CP-DATA SMS-DELIV>	+ 00:00:57.361.644
	2	E1/T1-V2 Card (P-0>	1B-07	15076 -> 14080	B6C200h	DT1 CP-ACK	+ 00:00:57.371.925
	2	E1/T1-V2 Card (P-0>	1B-07	15076 -> 14080	B6C200h	DT1 CLEAR CMD	+ 00:00:57.373.675
	1	E1/T1-V2 Card (P-0>	1B-05	14080 -> 15076	4A4D4Dh	DT1 CLEAR COMP	+ 00:00:57.377.144
	2	E1/T1-V2 Card (P-0>	1B-07	15076 -> 14080	B6C200h >	RLSD	+ 00:00:57.385.550
	1	E1/T1-V2 Card (P-0>	1B-05	14080 -> 15076	4A4D4Dh >	RLC	+ 00:00:57.390.144

Главными сообщениями процедуры передачи SMS являются SMS-Deliver, SMS-Deliver Report, CP-ACK

## Сообщения процедуры передачи SMS(SMS-Deliver)

Главное информационного сообщения подсистемы MAP

SMS-DELIVER процедуры SMS включает следующие поля:

- Plan – план нумерации;
- Type – тип абонентского номера;
- Number – номер абонента, отправляющего (получающего) смс-сообщение;
- TP Message Type Indicator – индикатор типа сообщения (исходящее или входящее);
- TP Origination Address – включает план нумерации, тип номер и номер получателя сообщения;
- TP Data Coding Scheme – указывает тип используемого алфавита и сжатие текста;
- TP Service Centre Time Stamp – содержит часовой пояс, время и дату передачи сообщения;
- поля TP User Data Length и TP User Data указывают длину и содержание переданного сообщения соответственно.

# Сообщения процедуры передачи SMS(SMS-Deliver)

Description		Value
*****	DATA FORM 1	
*****	Destination Local Reference	B6C200h
*****	Segmenting/reassembling	
-----0	More data indication	0b = no more data
*****	Data	01 83 2C 09 01 29 01 01 07 91 97 02 92 90 90 F0 00 1D 00 0B 91 97 02 36 99 70 F6 00 08 11 40 70 71 02 82 61 0A 04 1C 04 40 04 30 04 34 04 3Ch
*****	GSM 08.06 / UMTS 48.006 - BSSAP	
00000001	Header	1 = Direct Transfer Application Part
-----011	DLCI Parameter	3h
10-----	Control Channel Indication	10b = FACCH or the SDCCH
*****	GSM 04.08 - DTAP (V 6.4.2)	
*****	<General Fields>	
----1001	Protocol Discriminator	9h = Short Message Service
-000----	Transaction Identifier	0h
0-----	Transaction Identifier Flag	0b = This message is sent FROM the side that the TI originates
*****	GSM 04.11 - SMS (V 5.1.0)	
*****	CP-DATA	
*****	CP-User Data Element	
00101001	CP-User Data Len	29h
*****	Rp-Data	
----001	RP-Message Type Indicator	001b = ms->n Reserved, n->ms RP-DATA
-0-----	RP-Priority Request	0h = FALSE
00000001	Message Reference	1
*****	Rp Originator	
----0001	Plan	1h = ISDN / telephony numbering plan
-001----	Type	1h = international number
*****	Number	79202909090f
*****	Rp Destination	
*****	Rp User Data	
*****	GSM 03.40	
*****	SMS DELIVER	
-----00	TP Message Type Indicator	00b = ms->sc SMS-DELIVER-REPORT, sc->ms SMS-DELIVER



# Сообщения процедуры передачи SMS(SMS-Deliver)

```
-----0--      TP More Messages to Send      0b = more messages
--0-----      TP Status Report Indication  0b = SMS-STATUS-REPORT will not be returned
-0-----      TP User Data Header Indicator  0b = only short message available
0-----      TP Reply Path                0b = TP Reply Path parameter is not set
*****
----0001      TP Origination Address
      Numbering plan                    0001b = ISDN/telephone numbering plan (E.164, E.163)
-001-----      Type of number              001b = International number
*****      Address Value                    79206399076
*****
--0-----      TP Protocol Identifier
      Telematic interworking indicator  0b = no interworking, but SME to SME protocol
*****
TP Data Coding Scheme
----10--      Alphabet                      10b = UCS2 (16 bit)
--0-----      Compressed indicator        0b = text is uncompressed
*****
TP Service Centre Time Stamp
*****      Year                          11
*****      Month                        04
*****      Day                          07
*****      Hour                          17
*****      Minute                        20
*****      Second                        28
*****      Timezone
*****      GMT +                          1
00001010      TP User Data Length          10
*****      TP User Data                  04 1C 04 40 04 30 04 34 04 3Ch
```

## Сообщения процедуры передачи SMS(SMS-Deliver Report)

Отчет о доставке происходит с помощью сообщения подсистемы MAP SMS-Deliver Report.

Главная информация этого сообщения содержится в строке TP Message Type Indicator, показывающая, в каком порядке смс-сообщение «проходит» сетевые элементы. MS обозначает мобильную станцию, а SC – сервис-центр.

Другим сообщением подсистемы MAP является сообщение CP-ACK, содержащее информацию о канале управления (FACCH or SDCCH) и дискриминаторе протокола (9h=Short Message Service). Необходимо также отметить, что все примеры включают и строки подсистемы SCCP, в которых указывается этикетка маршрутизации (DPC, OPC, SLS).

# Сообщения процедуры передачи SMS(SMS-Deliver Report)

	Description	Value
0001----	Signalling Link Selection	1
*****	DATA FORM 1	
*****	Destination Local Reference	4A4D4Dh
*****	Segmenting/reassembling	
-----0	More data indication	0b = no more data
*****	Data	01 03 0A 89 01 07 02 01 41 03 00 01 00h
*****	GSM 08.06 / UMTS 48.006 - BSSAP	
00000001	Header	1 = Direct Transfer Application Part
-----011	DLCI Parameter	3h
00-----	Control Channel Indication	00b = not further specified
*****	GSM 04.08 - DTAP (V 6.4.2)	
*****	<General Fields>	
----1001	Protocol Discriminator	9h = Short Message Service
-000----	Transaction Identifier	0h
1-----	Transaction Identifier Flag	1b = This message is sent TO the side that the TI originates
*****	GSM 04.11 - SMS (V 5.1.0)	
*****	CP-DATA	
*****	CP-User Data Element	
00000111	CP-User Data Len	7h
*****	RP-Acknowledge	
-----010	RP-Message Type Indicator	010b = ms->n RP-ACK, n->ms Reserved
-0-----	RP-Priority Request	0h = FALSE
00000001	Message Reference	1
*****	Rp User Data	
*****	GSM 03.40	
*****	SMS DELIVER REPORT	
-----00	TP Message Type Indicator	00b = ms->sc SMS-DELIVER-REPORT, sc->ms SMS-DELIVER
-0-----	TP User Data Header Indicator	0b = only short message available
*****	TP Parameter Indicator	
-----1	TP-Protocol-Identifier	1b = present
-----0-	TP-Data-Coding-Scheme	0b = not present
-----0--	TP-User-Data-Length	0b = not present
-0000---	Reserved	0000b
0-----	Extension Bit	0b
*****	TP Protocol Identifier	
--0-----	Telematic interworking indicator	0b = no interworking, but SME to SME protocol

# Сообщения процедуры передачи SMS(CP-ACK)

```
***** SCCP (03/2001)
***** <General Fields>
***** Routing Label
***** Destination Point Code 14080
***** Originating Point Code 15076
1111---- Signalling Link Selection 15
***** DATA FORM 1
***** Destination Local Reference B6C200h
***** Segmenting/reassembling
-----0 More data indication 0b = no more data
***** Data 01 83 02 09 04h
***** GSM 08.06 / UMTS 48.006 - BSSAP
00000001 Header 1 = Direct Transfer Application Part
-----011 DLCI Parameter 3h
10----- Control Channel Indication 10b = FACCH or the SDCCH
***** GSM 04.08 - DTAP (V 6.4.2)
***** <General Fields>
----1001 Protocol Discriminator 9h = Short Message Service
-000---- Transaction Identifier 0h
0----- Transaction Identifier Flag 0b = This message is sent FROM the side that the TI originates
***** GSM 04.11 - SMS (V 5.1.0)
***** CP-ACK
```

## Запрос баланса USS

USS (неструктурированные дополнительные службы) – позволяют мобильной станции и приложению, определенному оператором PLMN, взаимодействовать между собой прозрачным для мобильной станции и промежуточных сетевых объектов способом. Такая связь осуществляется посредством передачи пакетов данных неструктурированных дополнительных служб (USSD – Unstructured Supplementary Service Data). Эти пакеты имеют длину 80 байтов и передаются с помощью команд протокола MAP. Данные USSD используют диалоговые возможности подсистемы TCAP. Они характеризуются более быстрым циклом обработки и временем ответа, чем сообщения SMS, что особенно полезно в интерактивных приложениях. Двусторонняя транзакция с помощью данных USSD осуществляется в 7 раз быстрее, чем при использовании службы SMS.

## Запрос баланса USS

При запросе баланса абонентом обслуживающий MSC связывается с HLR, который посылает запрос шлюзу USSD. Он в свою очередь пересылает запрос серверу приложений предоплаты. Этот сервер проверяет баланс и затем отсылает сообщение обратно в MSC.

# Сообщения процедуры передачи USS

S	D	Linkset	PL	LL	CI	Message Contents	Time
W	1	E1/T1-V2 Card (P-O>	1A-01	14080 ->	15076	> CR COMP L3 INFO CM_SE>	+ 00:00:13.234.886
	2	E1/T1-V2 Card (P-O>	1B-07	15076 ->	14080	ADD702h > CC	+ 00:00:13.245.789
	2	E1/T1-V2 Card (P-O>	1B-07	15076 ->	14080	ADD702h DT1 CIPHER MODE CMD	+ 00:00:13.249.164
W	1	E1/T1-V2 Card (P-O>	1A-01	14080 ->	15076	C0494Ch DT1 CLASSMARK UPDATE	+ 00:00:13.468.140
	1	E1/T1-V2 Card (P-O>	1A-01	14080 ->	15076	C0494Ch DT1 CIPHER MODE COMP	+ 00:00:13.934.632
	1	E1/T1-V2 Card (P-O>	1A-01	14080 ->	15076	C0494Ch DT1 REGISTER PROCESS_>	+ 00:00:14.413.750
	2	E1/T1-V2 Card (P-O>	1B-07	15076 ->	14080	ADD702h DT1 CP-DATA SMS-DELIV>	+ 00:00:14.436.273
	2	E1/T1-V2 Card (P-O>	1B-07	15076 ->	14080	ADD702h DT1 REL_COMP PROCESS_>	+ 00:00:14.532.273
	1	E1/T1-V2 Card (P-O>	1A-01	14080 ->	15076	C0494Ch DT1 CP-ACK	+ 00:00:19.115.687
	1	E1/T1-V2 Card (P-O>	1A-01	14080 ->	15076	C0494Ch DT1 CP-DATA SMS-DELIV>	+ 00:00:19.586.433
	2	E1/T1-V2 Card (P-O>	1B-07	15076 ->	14080	ADD702h DT1 CP-ACK	+ 00:00:19.595.078
	2	E1/T1-V2 Card (P-O>	1B-07	15076 ->	14080	ADD702h DT1 CLEAR CMD	+ 00:00:19.596.828
	1	E1/T1-V2 Card (P-O>	1A-01	14080 ->	15076	C0494Ch DT1 CLEAR COMP	+ 00:00:19.600.429
	2	E1/T1-V2 Card (P-O>	1B-07	15076 ->	14080	ADD702h > RLSD	+ 00:00:19.608.203
	1	E1/T1-V2 Card (P-O>	1A-01	14080 ->	15076	C0494Ch > RLC	+ 00:00:19.611.808

Следующей процедурой абонентов подвижной связи является запрос баланса (USS). Здесь появляются такие сообщения как REGISTER PROCESS\_UNSTRUCTURED\_SS\_REQUEST и REL\_COMP PROCESS\_UNSTRUCTURED\_SS\_REQUEST. Остальные сообщения идентичны рассмотренным выше в процедуре передачи SMS.

# Сообщения процедуры передачи USS (REGISTER PROCESS\_UNSTRUCTURED\_SS\_REQUEST)

```
***** GSM 08.06 / UMTS 48.006 - BSSAP
00000001 Header 1 = Direct Transfer Application Part
-----000 DLCI Parameter 0h
00----- Control Channel Indication 00b = not further specified
***** GSM 04.08 - DTAP (V 6.4.2)
***** <General Fields>
-----1011 Protocol Discriminator Bh = Non Call Related SS
-001---- Transaction Identifier 1h
0----- Transaction Identifier Flag 0b = This message is sent FROM the side that the TI originates
***** GSM 04.80 / UMTS 24.080 - SS
***** REGISTER
***** Facility
***** Invoke
***** Invoke Id 1
***** Operation Code
***** Local Value 59 = processUnstructuredSS-Request
***** Parameter
***** PROCESS UNSTRUCTURED SS REQUEST
***** USSD Data Coding Scheme 0Fh
***** USSD String AA 18 0C 36 02h
***** SS Version Indicator
00000000 Content 00000000b = Phase 2 service, ellipsis notation, and phase 2 err
```

Основные строки и их значения:

- Transaction Identifier и Transaction Identifier Flag – показывают использование подсистемы транзакций TCAP (1h, 1b – транзакция присутствует, 0h, 0b – транзакция отсутствует);

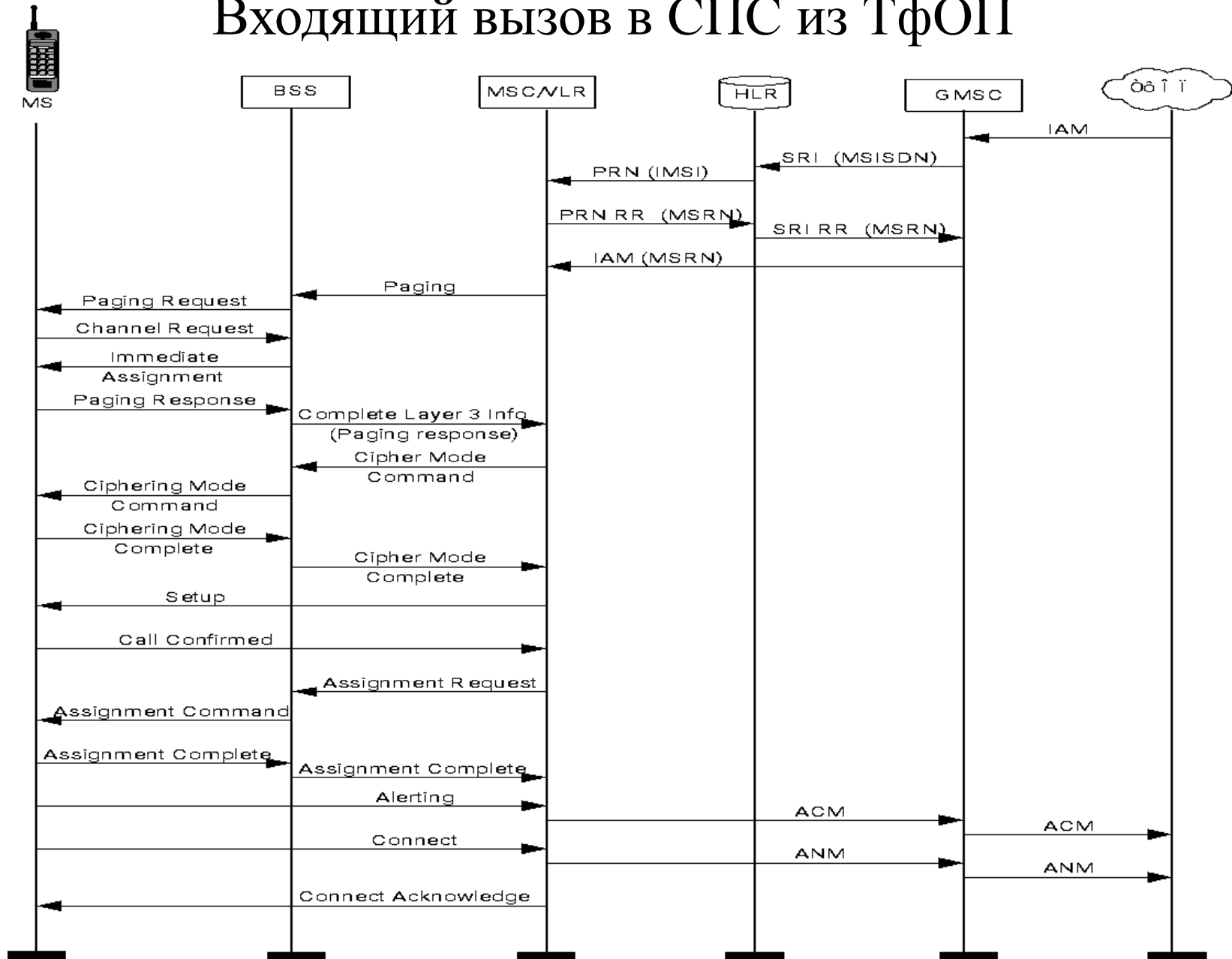


# Сообщения процедуры передачи USS (REL\_COMP PROCESS\_UNSTRUCTURED\_SS\_REQUEST)

```
***** GSM 08.06 / UMTS 48.006 - BSSAP
00000001 Header 1 = Direct Transfer Application Part
-----000 DLCI Parameter 0h
00----- Control Channel Indication 00b = not further specified
***** GSM 04.08 - DTAP (V 6.4.2)
***** <General Fields>
----1011 Protocol Discriminator Bh = Non Call Related SS
-001---- Transaction Identifier 1h
1----- Transaction Identifier Flag 1b = This message is sent TO the side that the TI originates
***** GSM 04.80 / UMTS 24.080 - SS
***** RELEASE COMPLETE
***** Facility
***** Return-Result
***** Invoke Id 1
***** Result
***** Operation Code
***** Local Value 59 = processUnstructuredSS-Request
***** Parameter
***** PROCESSUNSTRUCTURED SS REQUEST
***** USSD Data Coding Scheme 48h
***** USSD String 00 2D 00 32 00 37 00 32 00 35 00 37 00 2E 00 38
00 30 04 40 04 43 04 31 00 2E 04 1F 04 3E 04 3C
.....
00 20 00 53 00 4D 00 53 00 20 04 3D 04 30 00 20
00 35 00 30 00 33 00 35 00 3D 00 33 00 30 04 40h
```

- Parameter – указывает на то, используется ли структурированный диалог или неструктурированный, схему кодирования и строку с данными при запросе баланса и при ответе сети.

# Входящий вызов в СПС из ТфОП



## Входящий вызов в СПС из ТфОП

В случае входящего вызова к мобильному терминалу абонент сети ТфОП набирает номер мобильного абонента MSISDN (Mobile Station ISDN Number)

1. Вызов начинается с поступления на GMSC (Gateway Mobile Switching Center – шлюзовой центр коммутации мобильной связи) сообщения IAM протокола ISUP. Это сообщение содержит списочный номер вызываемого абонента MSISDN, на основании которого в GMSC определяется соответствующий этому абоненту HLR и вызывается операция *SRI (Send Routing Information)* протокола MAP в направлении к этому HLR, чтобы позиционировать мобильный терминал. Информация SRI содержит MSISDN абонента для определения IMSI.

## Входящий вызов в СПС из ТфОП

2. HLR в MSC/VLR операцию *PRN (Provide Roaming Number)* протокола MAP, которая содержит IMSI абонента. Этот MSC/VLR назначает из пула временный номер *MSRN (Mobile Station Roaming Number)* для данного вызова и возвращает этот номер в HLR. В свою очередь, HLR возвращает номер MSRN в GMSC.
3. Полученный MSRN для ТфОП является реальным (пересчитанным) номером вызываемого абонента. Его можно использовать для маршрутизации вызова через любую промежуточную сеть между GMSC и гостевым MSC/VLR. GMSC маршрутизирует вызов к MSC/VLR путем передачи IAM с MSRN в качестве номера вызываемой стороны. После того как этот IAM принят, MSC/VLR получает оттуда MSRN, узнает IMSI, для которого был назначен MSRN, после чего этот номер MSRN можно вернуть в пул.

## Входящий вызов в СПС из ТфОП

4. Далее MSC запрашивает в BSS передачу вызова абоненту с помощью сообщения *Paging Request*, которое указывает зону местонахождения, где следует искать абонента. После приема вызова мобильный терминал пытается получить доступ к сети с помощью передачи сообщения *Channel Request*, на которое подсистема BSS отвечает сообщением *Immediate Assignment* с указанием мобильному терминалу переключиться на SDCCH. Мобильный терминал переключается на этот SDCCH и указывает сети, что он отвечает на вызов. Тогда BSS пересылает ответ в MSC. На этой стадии MSC инициирует шифрование, так как передаваемые через радиointерфейс речь и данные должны быть зашифрованы.

## Входящий вызов в СПС из ТфОП

5. После получения сообщения *Setup* MS передает в MSC сообщение *Call Confirmed*, указывающее, что оно располагает необходимой для установления соединения информацией. MSC начинает процедуру назначения, которая создает канал между MSC и BSS, и канал между BSS и MS (вместо SDCCH). После создания канала в MS посылается вызов, а в MSC – сообщение *Alerting*. Запускается генерация акустического сигнала контроля посылки вызова и передачу сообщения ACM обратно к исходящей АТС ТфОП через GMSC. Как только вызываемый пользователь ответит, мобильный терминал передает в MSC сообщение *Connect*. Оно запускает передачу из MSC сообщения ANM обратно к исходящей АТС и открытие двухстороннего тракта. И, наконец, в вызываемый мобильный терминал передается сообщение *Connect Acknowledgement*, и начинается разговор.

## Сообщения процедуры «Вызов»

S	D	Linkset	PL	LL	CI	Message Contents	Time
W	1	E1/T1-V2 Card (P-0>	1A-07	14080 ->	15076	> CR COMP L3 INFO PAGE >	+ 00:00:30.254.746
	2	E1/T1-V2 Card (P-0>	1B-05	15076 ->	14080	A4E502h > CC	+ 00:00:30.262.390
	2	E1/T1-V2 Card (P-0>	1B-05	15076 ->	14080	A4E502h DT1 CIPHER MODE CMD	+ 00:00:30.264.640
W	1	E1/T1-V2 Card (P-0>	1A-07	14080 ->	15076	A24D4Ch DT1 CLASSMARK UPDATE	+ 00:00:30.488.242
	1	E1/T1-V2 Card (P-0>	1A-07	14080 ->	15076	A24D4Ch DT1 CIPHER MODE COMP	+ 00:00:30.954.488
	2	E1/T1-V2 Card (P-0>	1B-05	15076 ->	14080	A4E502h DT1 SETUP	+ 00:00:30.960.507
D	1	E1/T1-V2 Card (P-0>	1A-07	14080 ->	15076	A24D4Ch DT1 CALL CONFIRMED	+ 00:00:31.667.730
	2	E1/T1-V2 Card (P-0>	1B-05	15076 ->	14080	A4E502h DT1 ASSIGN REQ	+ 00:00:31.673.496
	1	E1/T1-V2 Card (P-0>	1A-07	14080 ->	15076	A24D4Ch DT1 ASSIGN COMP	+ 00:00:32.362.843
	1	E1/T1-V2 Card (P-0>	1A-07	14080 ->	15076	A24D4Ch DT1 ALERT	+ 00:00:32.537.593
	1	E1/T1-V2 Card (P-0>	1A-07	14080 ->	15076	A24D4Ch DT1 CONNECT	+ 00:00:34.097.570
	2	E1/T1-V2 Card (P-0>	1B-05	15076 ->	14080	A4E502h DT1 CONNECT_ACK	+ 00:00:34.102.335
	1	E1/T1-V2 Card (P-0>	1A-07	14080 ->	15076	A24D4Ch DT1 HO PERFORMED	+ 00:00:36.768.410
	2	E1/T1-V2 Card (P-0>	1B-05	15076 ->	14080	A4E502h DT1 DISCONNECT	+ 00:01:19.148.109
	1	E1/T1-V2 Card (P-0>	1A-07	14080 ->	15076	A24D4Ch DT1 RELEASE	+ 00:01:19.308.589
	2	E1/T1-V2 Card (P-0>	1B-05	15076 ->	14080	A4E502h DT1 RELEASE_COMP	+ 00:01:19.312.734
	2	E1/T1-V2 Card (P-0>	1B-05	15076 ->	14080	A4E502h DT1 CLEAR CMD	+ 00:01:19.326.109
	1	E1/T1-V2 Card (P-0>	1A-07	14080 ->	15076	A24D4Ch DT1 CLEAR COMP	+ 00:01:19.337.339
	2	E1/T1-V2 Card (P-0>	1B-05	15076 ->	14080	A4E502h > RLSD	+ 00:01:19.341.234
	1	E1/T1-V2 Card (P-0>	1A-07	14080 ->	15076	A24D4Ch > RLC	+ 00:01:19.351.964

Три описанные выше процедуры используют классы услуг подсистемы SCCP, не ориентированных на соединение. Рассмотрим процедуру вызова в мобильной сети, которая использует классы услуг подсистемы SCCP, ориентированных на соединение.

## Сообщения процедуры «Вызов» (Setup)

В сообщении Setup описываются основные параметры номера вызывающего абонента, а также возможности предоставляемых служб переноса данных.

- Information Transfer Capability – возможность переноса информации. В данном примере по каналу связи передается речь (0h = speech);
- Radio Channel Requirement – требование к радиоканалу (1h = full rate support only mobile station – полноскоростную передачу поддерживает только мобильная станция);
- Number Plan Identification – идентификатор плана нумерации;
- Number Type – тип номера;
- Screening Indicator – индикатор отображения номера (3h = network provided – предоставляется сетью).



# Сообщения процедуры «ВЫЗОВ» (Setup)

	Description	Value
--00----	Priority Indicator	0
11-----	Network Indicator	3 = Reserved for national use
*****	SCCP (03/2001)	
*****	<General Fields>	
*****	Routing Label	
*****	Destination Point Code	14080
*****	Originating Point Code	15076
0101----	Signalling Link Selection	5
*****	DATA FORM 1	
*****	Destination Local Reference	A4E502h
*****	Segmenting/reassembling	
-----0	More data indication	0b = no more data
*****	Data	01 00 0F 03 05 04 01 A0 5C 08 11 83 97 02 36 99 25 F5h
*****	GSM 08.06 / UMTS 48.006 - BSSAP	
00000001	Header	1 = Direct Transfer Application Part
-----000	DLCI Parameter	0h
00-----	Control Channel Indication	00b = not further specified
*****	GSM 04.08 - DTAP (V 6.4.2)	
*****	<General Fields>	
----0011	Protocol Discriminator	3h = Call Control
-000----	Transaction Identifier	0h
0-----	Transaction Identifier Flag	0b = This message is sent FROM the side that the
*****	GSM 04.08 - CC (V 6.4.2)	
*****	SETUP	
*****	Bearer Capability	
-----000	Information Transfer Capability	0h = speech
----0----	Transfer Mode	0h = circuit mode
---0----	Coding Standard	0h = GSM standardized coding as described below
-01-----	Radio Channel Requirement	1h = full rate support only mobile station
*****	Calling Party BCD number	
----0001	Number Plan Identification	1h = ISDN / telephony numbering plan
-001----	Number Type	1h = international number
-----11	Screening Indicator	3h = network provided
-00-----	Presentation Indication	0h = presentation allowed
*****	Number	79206399525f

## Сообщения процедуры «Вызов» (Call Confirmed )

Сообщение Call Confirmed является подтверждением вызова и содержит следующие строки:

- Speech Version Indication – индикатор речевой версии (speech version tbd – ограниченные во времени данные; GSM full rate speech version 2 – стандарт кодирования речи в сети GSM, когда данные занимают всю пропускную способность канала);
- Dual Tone Multi Frequency – поддержка DTMF набора мобильной станцией.

Сообщения Assignment Request и Assignment Complete отвечают за запрос и назначение тайм-слота в системе ИКМ для передачи сигнальной информации. Сообщение Alerting оповещает абонента о входящем вызове. Затем происходит проключение разговорного тракта и разговор абонентов. За это отвечают сообщения Connect и Connect\_Ack.

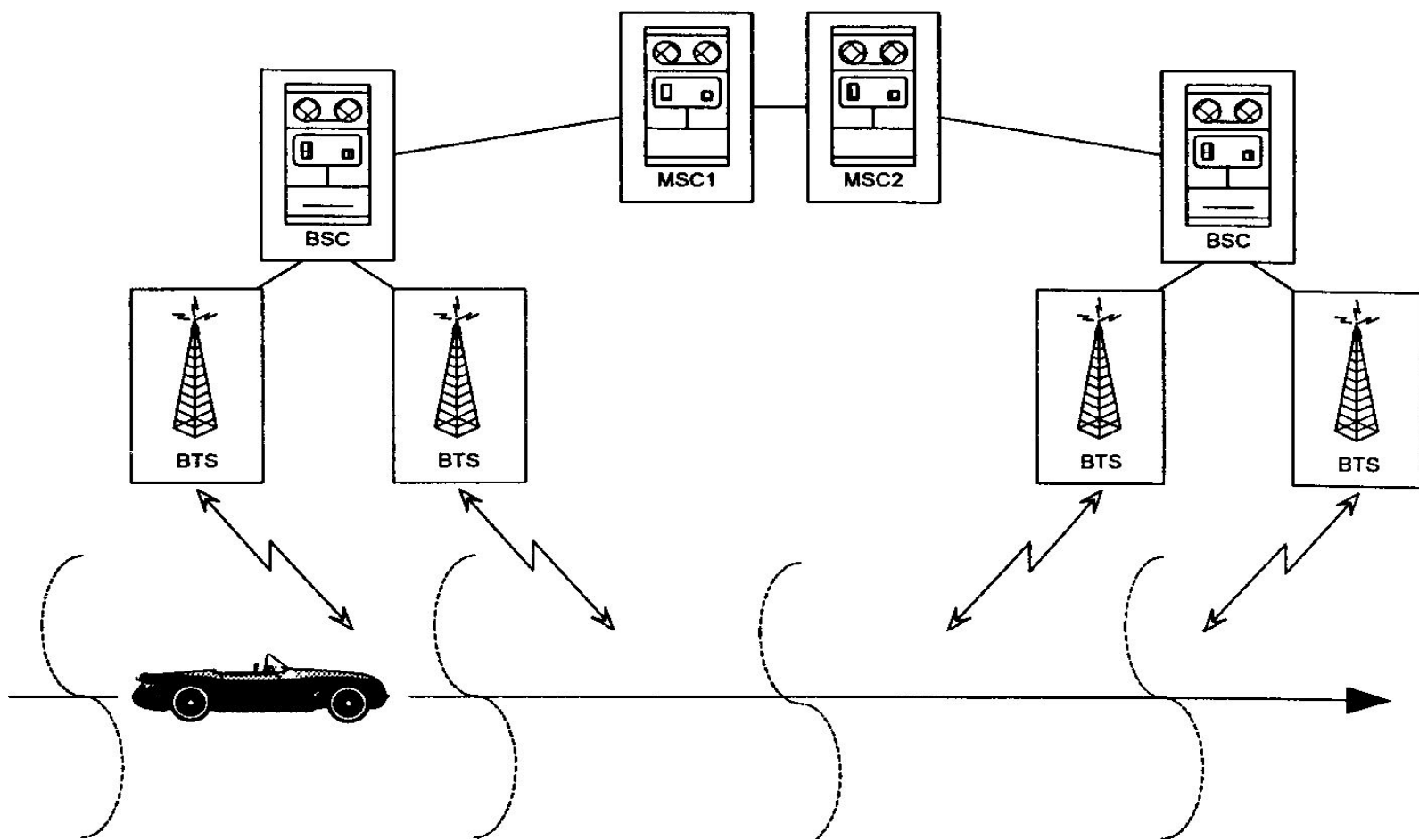
# Сообщения процедуры «Вызов» (Call Confirmed)

01 40 06 00 01 1F 04 01 60h

```
***** GSM 08.06 / UMTS 48.006 - BSSAP
00000001 Header 1 = Direct Transfer Application Part
-----000 DLCI Parameter 0h
00----- Control Channel Indication 00b = not further specified
***** GSM 04.08 - DTAP (V 6.4.2)
***** <General Fields>
----0011 Protocol Discriminator 3h = Call Control
-000---- Transaction Identifier 0h
1----- Transaction Identifier Flag 1b = This message is sent TO the side that the TI originates
***** GSM 04.08 - CC (V 6.4.2)
***** CALL CONFIRMED
***** Bearer Capability
-----000 Information Transfer Capability 0h = speech
----0--- Transfer Mode 0h = circuit mode
---0---- Coding Standard 0h = GSM standardized coding as described below
-11---- Radio Channel Requirement 3h = dual rate support mobile station/full rate preferred
----0100 Speech Version Indication 4h = speech version tbd
-0----- Coding 0h = octet used for extension of information transfer capability
----0010 Speech Version Indication 2h = GSM full rate speech version 2
-0----- Coding 0h = octet used for extension of information transfer capability
----0000 Speech Version Indication 0h = GSM full rate speech version 1
-0----- Coding 0h = octet used for extension of information transfer capability
----0101 Speech Version Indication 5h = speech version tbd
-0----- Coding 0h = octet used for extension of information transfer capability
----0001 Speech Version Indication 1h = GSM half rate speech version 1
-0----- Coding 0h = octet used for extension of information transfer capability
***** Call Control Capabilities
-----1 Dual Tone Multi Frequency 1h = mobile station supports DTMF
-----0- Prolonged Clearing Procedure 0h = is not supported
***** Unknown Information Element
00000001 Identifier 1h
01000000 Length Indicator 40h
***** Content 06 00 01 1F 04 01 60h
```

# Процедура Handover

Важной функцией MAP и TMAP также является процедура *хэндовера*, обеспечивающая переключение вызова на более качественный радиоканал.



## Сообщения процедуры Handover

При разговоре постоянно происходит мониторинг каналов радиосвязи и выбирается канал с наибольшей мощностью сигнала. Этот выбор осуществляется с помощью сообщения подсистемы MAP HO Performed (handover performed). Это сообщение содержит следующие строки:

- Cause Value – значение причины (Ch = Normal Event - better cell – нормальное явление – сота с лучшими параметрами канала связи);
- Cell Identifier – идентификатор соты;
- Chosen Channel - выбранный канал.

Сообщение Disconnect отвечает за разъединение сеанса связи и отображает причины разъединения.

Далее идут типичные сообщения по освобождению и очистке радиоресурса.

# Сообщения процедуры Handover (HO Performed )

	Description	Value
-1000000	Backward Sequence Number	64
1-----	Backward Indicator Bit	1
-0100101	Forward Sequence Number	37
1-----	Forward Indicator Bit	1
--011101	Length Indicator	29 = LI -> Message Signal Unit
*****	Service Information Octet	
----0011	Service Indicator	3 = Signaling Connection Control Part
--00----	Priority Indicator	0
11-----	Network Indicator	3 = Reserved for national use
*****	SCCP (03/2001)	
*****	<General Fields>	
*****	Routing Label	
*****	Destination Point Code	15076
*****	Originating Point Code	14080
1010----	Signalling Link Selection	10
*****	DATA FORM 1	
*****	Destination Local Reference	A24D4Ch
*****	Segmenting/reassembling	
-----0	More data indication	0b = no more data
*****	Data	00 0F 17 04 01 0C 05 05 01 18 39 8C 1A 21 98 40 21h
*****	GSM 08.06 / UMTS 48.006 - BSSAP	
00000000	Header	0 = BSS Management Application Part
*****	GSM 08.08 - BSSMAP (V 7.2.0)	
*****	HANDOVER PERFORMED	
*****	Cause	
-0001100	Cause Value	Ch = Normal Event - better cell
*****	Cell Identifier	
----0001	Cell Discriminator	1h = LAC/CI used to identify cell
*****	Location Area Code	6201
*****	Cell Identity	35866
*****	Chosen Channel	
----1000	Channel	8h = 1 full rate TCH
1001----	Channel Mode	9h = speech (full rate or half rate)
*****	Speech Version	
-0100001	Version	21h = GSM speech full rate version 3