3GPP TSG SA WG3 Security — S3#30 **S3-030559**
6. – 10. October 2003
Povoa de Varzim, Portugal

Source:	Vodafone, Siemens
Title:	Voice Group Call Services
Agenda item:	**7.21**
Document for:	Discussion and decision
Attachments:	CR for 43.020
	Ciphering VGCS Concept

Description

According to the WID description (S3-030464) the key management of group keys for VGCS has to be specified. Since the stage 3 descriptions of VCGS are already fairly complete a key management is preferable which requires minimal changes and only few additions to the existing specifications.

The following principles are proposed to be adopted by SA3:

1. For each voice group up to 15 group keys can be defined (identified by a group key number).

2. The group keys are stored in
   - the group call register (GCR) on the network side (which is co-located to an MSC),
   - USIM on the UE side.

3. On call set-up the GCR selects one group key and sends it to the BSS and the group key number to the UE which fetches the corresponding key from the USIM.

4. A key management center (KMC) takes care that the group keys are up to date at all locations and are exchanged from time to time (which is up to the operator's policy).

5. The interface between KMC and the GCRs and between the KMC and the USIM are out of scope of the 3GPP specifications. However for the latter transmission via OTA is recommended.

6. The KMC is out of scope of 3GPP specification. In an informative annex the most important tasks of the KMC can be described.

7. For encryption the same algorithms are used as for normal GSM-speech calls (i.e. A5/0-A5/7).

8. It is ffs how the UE gets the information which cipher algorithm is used for a group call. There are two options: signal the cipher algorithm via the air-interface or store it on the USIM.

For completion of the stage 3 work additions to the specification of the USIM have to reflect the storage of the group keys.

As an attachment to this contribution a pseudo-CR for 43.020 is provided. Furthermore a concept paper is added which provides a compilation of specifications which are relevant to ciphering of VGCS.

SA3 is requested

- to endorse the above principles. If so, the attached CR for 43.020 could be considered and approved, if appropriate.
- to send an LS to T3 requesting to provide the necessary changes in their specifications for storing the group keys on the USIM.

Specification Ciphering for Group Calls

Contents:

1 Scope

This document describes the requirements to establish Ciphering for the Voice Group Call Service; it comprises the standardisation means defined already and a proposal for the missing recommendations.

Additionally the procedures which are meant to be network and operator specific (e.g. key generation and distribution managment) are included as an example.

The following network entities are considered:

- Group Call Register
- Anchor MSC
- Relay MSC
- BSC
- BTS
- Mobile Equipment
- Subsciber Identity Module
- Key management center (new)

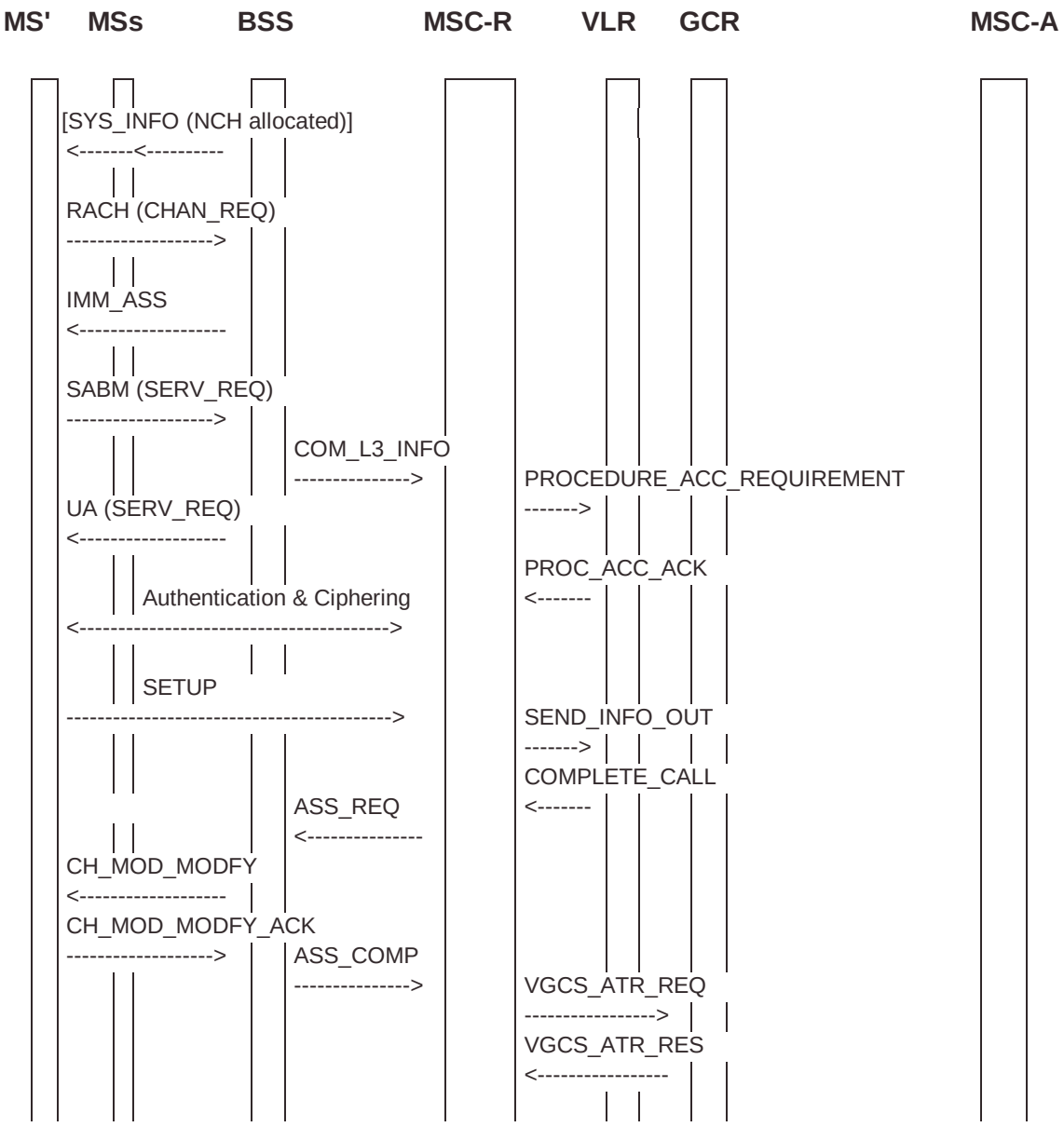
Parts of the specifications which are relevant to ciphering are marked red. Parts of the document which are not contained in specifications are marked green.

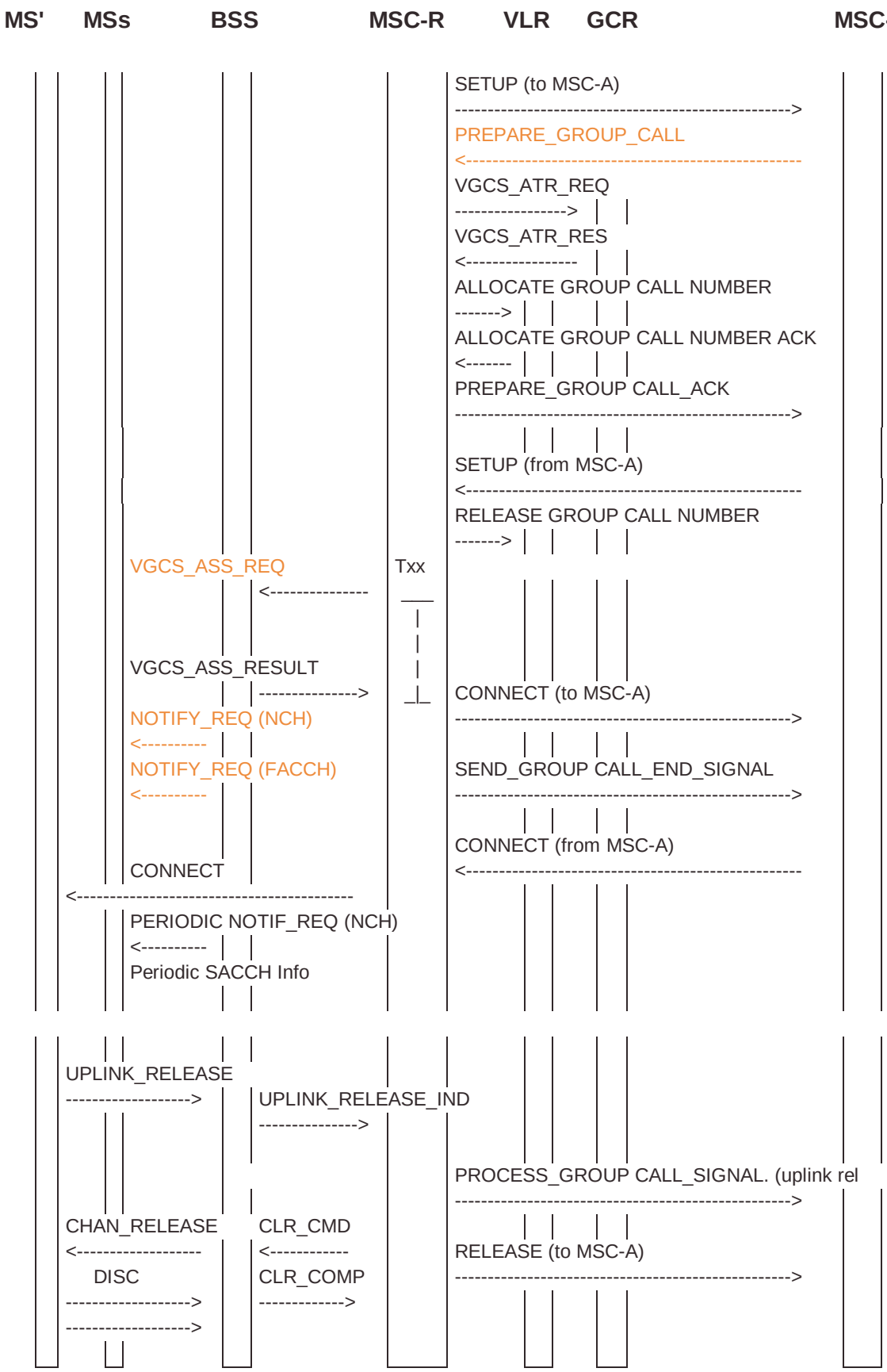
2 Overview

2.1 Signalling Flow for VGCS Setup

In the following the already defined "Signalling information required for establishing voice group calls by a service subscriber roaming in the relay MSC area" is noted down (taken from 43068-520).

NOTE: MS' = calling subscriber mobile station;
MSs = destination subscriber mobile stations;
MSC-A = anchor MSC;
MSC-R = relay MSC




MS'
MSs
BSS
MSC-R
VLR
GCR
MSC-A
SETUP (to MSC-A)
PREPARE_GROUP_CALL
VGCS_ATR_REQ
VGCS_ATR_RES
ALLOCATE GROUP CALL NUMBER
ALLOCATE GROUP CALL NUMBER ACK
PREPARE_GROUP CALL_ACK
SETUP (from MSC-A)
RELEASE GROUP CALL NUMBER
VGCS_ASS_REQ
Txx
VGCS_ASS_RESULT
CONNECT (to MSC-A)
NOTIFY_REQ (NCH)
NOTIFY_REQ (FACCH)
SEND_GROUP CALL_END_SIGNAL
CONNECT (from MSC-A)
CONNECT
PERIODIC NOTIF_REQ (NCH)
Periodic SACCH Info
UPLINK_RELEASE
UPLINK_RELEASE_IND
PROCESS_GROUP CALL_SIGNAL. (uplink rel
CHAN_RELEASE
CLR_CMD
RELEASE (to MSC-A)
DISC
CLR_COMP

SYS_INFO (NCH allocated): Message used to indicate if the NCH is allocated on the CCCH in the cell.

Initial RACH CHAN_REQ: Standard message.

IMM_ASS: Standard message send on the PCH.

SERV_REQ (voice group call): Modified form of the current call request message L3-MM CM SERVICE REQUEST sent on the allocated channel. Teleservice Voice group call is indicated.

UA (SERV_REQ): This message is used to acknowledge the layer 2 link and provide contention resolution of the service request.

COM_L3_INFO: The MSC is provided with initial information about the voice group call.

NOTE: Messages flows for authentication and ciphering are not represented although performed as normal.

PROC_ACC_REQ: The MAP_PROCESS_ACC_REQ message is sent to the VLR to check the requested VGCS teleservice against the subscription data.

PROC_ACC_ACK: The MAP_PROCESS_ACC_ACK message acknowledges the requested service.

Authentication & Ciphering: Authentication and Ciphering may be performed. Acknowledgement of the service request can also be performed by sending the CM SERVICE ACCEPT.

SETUP: The MSC is provided with details about the voice group call.

NOTE: Alternatively, an IMMEDIATE_SETUP (see Annex) may have been sent as the initial message including all details of the voice group call. In this case no SETUP message must be sent.

SEND_INFO_OUT: The requested group ID is transferred to the VLR in the MAP_SEND_INFO_FOR_OUTGOING_CALL message.

COMPLETE_CALL: The VLR returns the MAP_COMPLETE_CALL message confirming the use of the requested group ID.

ASSIGNMENT_REQUEST: Standard message.

CHAN_MOD_MODFY: Standard message to modify the channel mode in case of very early assignment.

CHAN_MOD_MODFY_ACK: Standard message to acknowledge the modification of the channel mode.

ASSIGNMENT_COMPLETE: Standard message.

NOTE: Alternatively, early assignment or OACSU procedures might be applied with the corresponding assignment messages not presented in figure 3.

VGCS_ATR_REQ: The group call attributes are requested from the GCR.

VGCS_ATR_RES: The requested information (MSC-A address) is returned from the GCR.

SETUP to MSC-A: Based on information received from the GCR the relay MSC shall set-up a dedicated connection for the initiating service subscriber to the anchor MSC.

PREPARE_GROUP CALL: The group call attributes (parts) are received from the anchor MSC.

VGCS_ATR_REQ: The group call attributes are requested from the GCR.

VGCS_ATR_RES: The requested information (cell list) is returned from the GCR.

ALLOCATE GROUP CALL NUMBER: The Group Call number is requested from the VLR.

ALLOCATE GROUP CALL NUMBER ACK: The Group Call number is returned from the VLR.

PREPARE_GROUP_CALL_ACK: The Group Call number is sent to MSC-A.

SETUP from MSC-A: The ISUP connection is set-up between MSC-A and MSC-R.

RELEASE GROUP CALL NUMBER: The VLR is requested to release the Group Call number.

VGCS_ASSIGNMENT_REQ: This message is sent from the MSC to all affected BSCs, [one dedicated message for every requested channel in a cell,] including the group call reference, the channel type and possibly the call priority and details on the ciphering.

NOTE: As an operator option the voice group call channels, the links to them and optionally also the links to dispatchers can already be established and permanently reserved in order to speed up the call set-up for emergency voice group calls.

VGCS_ASSIGNMENT RESULT: Acknowledgement message from the affected BSC in answer to the assignment requests. If the assignment is not successful, a VGCS_ASSIGNMENT_FAILURE message shall be sent instead.

CONNECT to MSC-A: Set-up of the ISUP connection from the anchor MSC is confirmed.

SEND_GROUP CALL_END_SIGNAL: Indicates to the anchor MSC that conversation can start. In addition the IMSI of service subscriber who has established the voice group call and who is allowed to terminate the call is included.

Txx: Timer implemented in the relay MSC which is started with the incoming SETUP message from the anchor MSC and stops with the outgoing paging message. If the timer expires before the MSC receives all of the expected CHAN_REQ_ACK from the BSCs, the VGCS shall be established by the relay MSC to all available parts of the group call area and the anchor MSC shall be informed that conversation can start.

NOTIF_REQ (NCH): Messages for notification which contain the group call reference, the priority of the call if eMLPP is applied, and possibly the channel description of the voice group call channel to which the mobile stations shall listen and the number of the group key used for ciphering.

NOTIF_REQ (FACCH): Message for notification sent on the FACCH to the mobile stations currently involved in other calls. The notification on the FACCH shall include the group call reference, and the priority level and may include also the channel description and the group ciphering key numbers.

Periodic NOTIF_REQ (NCH): The notifications are sent periodically so that mobile stations moving into the area can join the voice group call.

Periodic SACCH Info: Periodic messages sent on the downlink of the SACCH informing mobile stations of:

- information of changes of notifications;
- information used for cell re-selection.

CONNECT (from MSC-A): Call set-up of the dedicated connection for the calling service subscriber is confirmed.

CONNECT: Information to the mobile station of the calling subscriber that the VGCS is established with the related group call reference as the connected number.

UPLINK_RELEASE: When the calling service subscriber wants to become a listening service subscriber for the first time, a message indicating release of the uplink is required to be sent from the MS to the BSS in order to set the uplink free.

UPLINK_RELEASE_INDICATION: The BSS informs the MSC on the uplink release.

PROCESS_GROUP CALL_SIGNALLING (uplink release indication): To indicate to the anchor MSC that the uplink is free.

CLEAR COMMAND: The MSC requests the BSS to clear radio and terrestrial resources associated with originator dedicated link if not already done.

CHAN_RELEASE: The BSS sends a channel release message to the calling service subscriber's mobile station including the channel description of the voice group call channel to which the mobile station shall tune to.

NOTE: Alternatively, if no UPLINK_RELEASE has been sent to the network by the mobile station, the network may transfer the mobile station to the voice group call channel by the channel mode modify procedure or by an assignment procedure or by a handover procedure.

DISC: Two layer 2 disconnect messages shall be sent by the mobile station to the network.

RELEASE to MSC-A: The dedicated connection for the initiating service subscriber is released.

2.2 Messages with Ciphering Parameters

2.2.1 Interface Anchor-MSC - GCR

43068-520, Chapter 12.3

The messages GCR Interrogation and GCR Interrogation Acknowledge are represented in the signalling diagram with VGCS_ATR_REQ and VGCS_ATR_RES respectively.

2.2.1.1 GCR Interrogation

The following information elements are required.

Information element name	Required	Description
Group call reference	C	see clause 9. Must be present if the VGCS call was initiated by a dispatcher or by a service subscriber in the relay MSC area and the receiving GCR is associated to the anchor MSC
Group ID	C	see clause 9. Must be present if the VGCS call was initiated by a service subscriber in the own MSC area
Originating Cell ID	C	see clause 9. Must be present if the VGCS call was initiated by a service subscriber in the own MSC area
CLI	C	Calling Line Identity of the initiating dispatcher, or VGCS prefix plus group call reference in case of service subscriber originated VGCS call in the relay MSC. Must be present if the VGCS call was not initiated by a service subscriber located in the own MSC area
Relay MSC indicator	M	A flag indicating whether the GCR interrogation was triggered from a Prepare Group Call message received from the anchor MSC
IMSI	C	IMSI of the service subscriber who has initiated the VGCS call. Must be present if the VGCS call was initiated by a service subscriber in the own MSC area

2.2.1.2 GCR Interrogation ack

The following information elements are required.

Information element name	**Required**	**Description**
Cell List	C	A list of cells inside the MSC area into which the call is to be sent. Must be present if a) no anchor MSC address is present in the group call reference record, or b) the relay MSC indicator was set in the GCR Interrogation message
Anchor MSC Address	C	E.164 number required to route the call from the relay MSC to the anchor MSC. Must be present if the anchor MSC Address is present in the group call reference record
Relay MSC List	C	A list of relay MSCs into which the call is to be sent. Must be present if a relay MSC list is present in the group call reference record
Group Key and Number	C	Information on the cipher algorithm and the group key to be used. Must be present if Group Key and Number is present in the group call reference record
Codec Information	C	Information on the codecs allowed for the voice broadcast call. Must be present if Codec Info is present in the group call reference record
Establish to Dispatcher List	C	A list of identities of dispatchers to which a dedicated link is

		to be established. Must be present if included in the group call reference record. Note that the CLI possibly received with the GCR interrogation message must not be included
Release from Dispatcher List	C	A list of identities of dispatchers which are allowed to terminate the voice group call. Must be present if included in the group call reference record
Priority	C	The default priority level related to the voice group call if eMLPP applies. Must be present if included in the group call reference record
IMSI	C	IMSI of the service subscriber who has initiated the VGCS call. Must be present if the Relay MSC Indicator was set in the GCR interrogation message and the IMSI is present in the group call reference record
No Activity Time	C	The length of the time over which no activity is detected before the voice group call is automatically terminated

2.2.2 Interface Relay-MSC - Anchor-MSC

29002-620, Chapter 10.4

2.2.2.1 Prepare Group Call

This service is used by the Anchor_MSC to inform the Relay_MSC about a group call set-up.

The MAP_PREPARE_GROUP_CALL service is a confirmed service using the service primitives given in table 10.4/1.

2.2.2.1.1 Service primitives

Parameter name	Request	Indication	Response	Confirm
Invoke Id	M	M(=)	M(=)	M(=)
Teleservice	M	M(=)		
ASCI Call Reference	M	M(=)		
Ciphering Algorithm	M	M(=)		
Group Key Number	C	C(=)		
Group Key	C	C(=)		
Priority	C	C(=)		
CODEC-Information	M	M(=)		
Uplink Free Indicator	M	M(=)		
Group Call Number			M	M(=)
User Error			C	C(=)
Provider Error				O

2.2.2.1.2 Parameter definitions and use

Invoke Id

See definition in clause 7.6.1.

Teleservice

Voice Broadcast Service or Voice Group Call Service.

ASCI Call Reference

Broadcast call reference or group call reference. This item is used to access the VBS-GCR or VGCS-GCR within the Relay_MSC.

Ciphering Algorithm

The ciphering algorithm to be used for the group call.

Group Key Number

This number has to be broadcasted and is used by the mobile station to select the chosen group key.

Shall be present if the ciphering applies.

Group Key

This key is used for ciphering on the radio interface.

Shall be present if the ciphering applies.

Priority

Default priority level related to the call if eMLPP applies.

CODEC-Information

Information on the codecs allowed for this call.

Uplink Free Indicator

A flag indicating whether the call is initiated from a dispatcher.

Group Call Number

This temporary allocated E.164 number is used for routing the call from the Anchor MSC to the Relay MSC.

User Error

For definition of this parameter see clause 7.6.1 The following errors defined in clause 7.6.1 may be used, depending on the nature of the fault:

- No Group Call Number available;
- System Failure;
- Unexpected Data Value.

Provider Error

See definition of provider error in clause 7.6.1.

2.2.3 Interface (Relay- & Anchor-)MSC - BSS

2.2.3.1 Voice group call service and voice broadcast service Assignment procedure

48008-620, Chapter 3.1.22

The purpose of the VGCS/VBS Assignment procedure is to ensure that the correct dedicated radio resources are allocated to the VGCS/VBS call on a per cell basis. In order to support this procedure the MSC sets up a VGCS/VBS resource controlling SCCP connection to the BSS. This connection is then used to support all BSSAP messages related to the dedicated resource(s).

The MSC can command that the radio resources are either allocated immediately or delayed.

The VGCS/VBS call controlling SCCP connection shall be established before the VGCS/VBS Assignment procedure takes place.

The MSC initiates the VGCS/VBS Assignment procedure to the BSS by sending an VGCS/VBS ASSIGNMENT REQUEST on a VGCS/VBS resource controlling SCCP connection.

The BSS will return VGCS/VBS ASSIGNMENT RESULT to the MSC to inform the MSC of the resources allocated by the BSS for the concerned cell.

The BSS shall initiate the radio interface notification procedure on the NCH of the cell in which the call is to take place, this may continue at regular intervals until the call is released. The BSS may on SACCH indicate that a change of notification has occurred and/or initiate notification on FACCH.

In the case where the BSS deallocates/allocates resources to the cell, the BSS sends an VGCS/VBS ASSIGNMENT RESULT message on the VGCS/VBS resource controlling SCCP connection associated to the cell.

In the case of voice group calls, if the MSC has informed the BSS to which voice group call the originator MS belongs to, the BSS may decide to modify the originator dedicated channel into a

voice group call channel relating to the group call reference. If the BSS mode modifies the channel it will send the VGCS/VBS ASSIGNMENT RESULT message on the ressource controlling SCCP connection and then immediately afterwards send a CLEAR REQUEST cause "Joined group call channel" on the originator dedicated connection.

2.2.3.2 VGCS/VBS ASSIGNMENT REQUEST

48008-620, Chapter 3.2.1.53

This message is sent from the MSC to the BSS via the newly created VGCS/VBS resource controlling SCCP connection in order to request the BSS to assign radio resources in a cell to support a VGCS/VBS call.

INFORMATION ELEMENT	REFERENCE	DIRECTION	TYPE	LEN
Message Type	3.2.2.1	MSC-BSS	M	1
Channel Type	3.2.2.11	MSC-BSS	M	5
Assignment Requirement	3.2.2.52	MSC-BSS	M	2
Cell Identifier	3.2.2.17	MSC-BSS	M	3-10
Group Call Reference	3.2.2.55	MSC-BSS	M	3-8
Priority	3.2.2.18	MSC-BSS	O	3
Circuit Identity Code	3.2.2.2	MSC-BSS	O	3
Downlink DTX Flag	3.2.2.26	MSC-BSS	O	2
Encryption Information	3.2.2.10	MSC-BSS	O	3-n

2.2.3.3 Encryption Information

48008-620, Chapter 3.2.2.10

This element contains the user data encryption information used to control any encryption equipment at the BSS.

It is a variable length element.

It is coded as follows:

8	7	6	5	4	3	2	1	
Element identifier								octet 1
Length								octet 2
Permitted algorithms								octet 3
Key								octet 4-n

The length indicator (octet 2) is a binary number indicating the absolute length of the contents after the length indicator octet.

The permitted algorithms octet is a bit map indicating the A5 encryption algorithms and no encryption. From this bit map the BSS may select an A5 algorithm or no encryption to be used.

Bit No	meaning
1	No encryption
2	GSM A5/1
3	GSM A5/2
4	GSM A5/3
5	GSM A5/4
6	GSM A5/5
7	GSM A5/6
8	GSM A5/7

A bit position encoded as 1 indicates that the BSS may use the option repesented by that bit position. A bit position encoded as 0 indicates that the BSS shall not use the option represented by that bit position. A permitted algorithms octet containing all bits encoded as 0 shall not be used.

The key shall be present if at least one of the A5 encryption algorithms is permitted. Over MAP/E interface to 3G_MSC-B the key shall be present if available. When present, the key shall be 8 octets long.

Remark: On the A-interface a list of allowed algorithms is provided, whereas from the anchor MSC a single algorithm to be applied is transmitted only; this leads to the fact, that more information could be provided than is available.

2.2.3.4 Group Call Reference

48008-620, Chapter 3.2.2.55

It is coded as follows:

8	7	6	5	4	3	2	1	
Element identifier								octet 1
Length								octet 2
Descriptive group or broadcast call reference								octets 3-7

Octet 2 is a binary indication of the length of the remainder of the element in octets.

The octets 3-8 are coded in the same way as the octets 2-6 in the Descriptive group or broadcast call reference information element as defined in 3GPP TS 24.008 [6].

2.2.3.5 Descriptive group call reference

24008-610, Chapter 10.5.1.9

The purpose of the *Descriptive Group or Broadcast Call Reference* is to provide information describing a voice group or broadcast call. The IE of the *Descriptive Group or Broadcast Call Reference* is composed of the group or broadcast call reference together with a service flag, an acknowledgement flag, the call priority and the group cipher key number.

The *Descriptive Group or Broadcast Call Reference* information element is coded as shown in figure 10.5.8/3GPP TS 24.008 and Table10.5.8/3GPP TS 24.008

The *Descriptive Group or Broadcast Call Reference* is a type 3 information element with 6 octets length.

8	7	6	5	4	3	2	1	
	Group or broadcast call reference IEI							octet 1
Binary coding of the group or broadcast call reference								octet 2
								octet 3
								octet 4
			SF	AF	call priority			octet 5
Ciphering information				Spare 0	0	0	0	octet 6

Figure 10.5.8/3GPP TS 24.008 Descriptive Group or Broadcast Call Reference

Table 10.5.8/3GPP TS 24.008 Descriptive Group or Broadcast Call Reference

Binary code of the group or broadcast call reference
The length of the binary code has 27 bits which is encoded in the octet 2, 3, 4 and Bits 8,7,6 (octet 5).
The highest bit of the BC is the bit 8 in the octet 2 and the lowest bit is allocated in the bit 6 in the octet 5. (see also 3GPP TS 23.003 [10])
SF Service flag (octet 5)
Bit
5
0 VBS (broadcast call reference)
1 VGCS (group call reference)

AF Acknowledgement flag (octet 5), network to MS direction:
Bit
4
0 acknowledgement is not required
1 acknowledgement is required

Call priority (octet 5)
Bit

3	**2**	**1**	
0	0	0	no priority applied
0	0	1	call priority level 4
0	1	0	call priority level 3
0	1	1	call priority level 2
1	0	0	call priority level 1
1	0	1	call priority level 0
1	1	0	call priority level B
1	1	1	call priority level A

Ciphering information (octet 6)
Bit

8	**7**	**6**	**5**	
0	0	0	0	no ciphering
0	0	0	1	ciphering with cipher key number 1
0	0	1	0	ciphering with cipher key number 2
0	0	1	1	ciphering with cipher key number 3
0	1	0	0	ciphering with cipher key number 4
0	1	0	1	ciphering with cipher key number 5
0	1	1	0	ciphering with cipher key number 6
0	1	1	1	ciphering with cipher key number 7
1	0	0	0	ciphering with cipher key number 8
1	0	0	1	ciphering with cipher key number 9
1	0	1	0	ciphering with cipher key number A
1	0	1	1	ciphering with cipher key number B
1	1	0	0	ciphering with cipher key number C
1	1	0	1	ciphering with cipher key number D
1	1	1	0	ciphering with cipher key number E
1	1	1	1	ciphering with cipher key number F

AF Acknowledgement flag (octet 5), MS to network direction:
Bit 4 is spare and shall be set to "0".

Call priority (octet 5)
Bits 1 to 3 are spare and shall be set to "0".

Ciphering information (octet 6)
Bits 5 to 8 are spare and shall be set to "0".

2.3 Notification procedure

44018-630, chapter 3.3.3

The support of notification procedure is mandatory for mobile stations supporting "VGCS receive" and/or "VBS receive".

The network informs the mobile station of starting or on-going voice broadcast calls and voice group calls with the notification procedure.

In cases where the mobile station has initiated a VGCS call, if the channel mode modify procedure is applied to turn the dedicated channel into a VGCS channel and ciphering may be applied for that call, in this case the network should suspend transmission of notification messages until ciphering with the group cipher key has started on the dedicated channel.

2.3.1 Notification of a call

44018-630, chapter 3.3.3.1

The mobile station may receive a notification that a voice broadcast call or a voice group call is established. Notifications may be sent on the NCH, on the PCH, or on the FACCH when in dedicated mode or group receive mode. The presence of an NCH is indicated on the PCH in the Pi Rest Octets IE. A notification contains the group call reference and possibly other related information. This notification may be contained:

- in a NOTIFICATION/NCH message sent on the NCH to notify mobile stations of VBS or VGCS calls in the current cell, possibly together with a description of the related VBS or VGCS channel;
- in a NOTIFICATION/FACCH message sent in unacknowledged mode on the main DCCH to notify mobile stations in dedicated mode or on the main DCCH of a VGCS or VBS channel, of other VBS or VGCS calls in the current cell, possibly together with a description of the related VBS or VGCS channel;
- in the rest octets part of a PAGING REQUEST TYPE 1 message.

A mobile station supporting neither VGCS listening nor VBS listening may ignore the notifications sent on the NCH or PCH. It may also ignore the notifications sent on the main DCCH except that a RR-STATUS message shall be sent to the network with cause #97, "message not existent or not implemented".

Upon receipt of every notification message a mobile station supporting VGCS listening or VBS listening shall give an indication containing the notified group call reference(s) to upper layers in the mobile station which may then decide:

- not to react on the notification; or
- join the voice broadcast call or the voice group call, if needed after having stopped on going activities.

Remark: The algorithm to be applied in the Voice Group Call is not part of the notification parameters; how is this information given to the Mobile Station?

Alternative 1 - Change of Parameter "Descriptive Group or Broadcast Call Reference"; the bits 1 - 4 of octet 6 are taken for the coding of the algorithm to be applied for the initiated group call.

Ciphering information (octet 6)

Bit 4	3	2	1	
0	0	0	0	no ciphering
0	0	0	1	ciphering with algorithm GSM A5/1
0	0	1	0	ciphering with algorithm GSM A5/2
0	0	1	1	ciphering with algorithm GSM A5/3
0	1	0	0	ciphering with algorithm GSM A5/4
0	1	0	1	ciphering with algorithm GSM A5/5
0	1	1	0	ciphering with algorithm GSM A5/6
0	1	1	1	ciphering with algorithm GSM A5/7
1	0	0	0	spare
1	0	0	1	spare
1	0	1	0	spare
1	0	1	1	spare
1	1	0	0	spare
1	1	0	1	spare
1	1	1	0	spare
1	1	1	1	spare

2.3.2 Notification/FACCH

44018-630, chapter 9.1.21a

The understanding of this message is only required for mobile stations supporting VGCS listening or VBS listening.

This message is sent on the main DCCH, in unacknowledged mode using the RR short protocol discriminator by the network to notify the mobile stations in dedicated mode or in on-going voice broadcast calls or voice group calls on other voice broadcast calls or voice group calls in that cell.

Notification/FACCH messages for VBS or VGCS calls are differentiated by a flag in the call reference.

The message shall not exceed a maximum length of 20 octets.

Mobile stations not supporting VGCS listening or VBS listening shall ignore this message.

See table 9.1.21a.1/3GPP TS 44.018.

Message type: NOTIFICATION/FACCH

Significance: dual

Direction: network to mobile station

Table 9.1.21a.1/3GPP TS 44.018: NOTIFICATION/FACCH message content

```
<NOTIFICATION FACCH>    ::= <RR short PD : bit>                  -- See 3GPP TS 24.007
                            <message type : bit(5)>              -- See 10.4
                        <short layer 2 header : bit(2)>          -- See 3GPP TS 44.006
                       {0 <Group Call information>
                       |1 <Paging Information>}
                            <spare padding> ;
<Group Call information> ::=        <Group Call Reference : bit(36)>
                       {0|1 <Group Channel Description>} ;
```

<Group Call Reference>

This field is syntactically and semantically equivalent to octets 2-5 and bits 5 to 8 of octet 6 of the *Descriptive Group or Broadcast Call Reference* information element.

The <Group Channel Description> field is optionally present. When present only the Channel description is provided in the case of non hopping channels. In the case where the channel is hopping then either a mobile allocation or a frequency short list is provided.

```
<Group Channel Description> : :=        <Channel Description : bit(24)>
                              {0                  -- Non hopping case
                              |1 {0 <Mobile Allocation : <bit string>>
                              |1 <Frequency Short List : bit(64)>}} ;

<bit string> ::= null | bit <bit string> ;
```

<Channel Description>

This field is syntactically and semantically equivalent to octets 2-4 of the *Channel Description* information element. See sub-clause 10.5.2.5.

<Frequency Short List>

This field is syntactically and semantically equivalent to octets 1-8 of the *Frequency Short List 2* information element. See sub-clause 10.5.2.14a.

<Mobile Allocation>

This field is syntactically and semantically equivalent to octet 2 to n+2 of the *Mobile Allocation* information element. See sub-clause 10.5.2.21.

The <Paging Information> field may be used to inform the mobile station in Group Receive or in Group Transmit mode that the corresponding mobile identity is paged in that cell.

```
<Paging Information>    ::= <mobile identity : <bit string>>
                      <channel first: bit(2)>
                      {0|1 <eMLPP priority : bit(3)>} ;

<bit string> ::= null | bit <bit string> ;
```

<mobile identity>

This field is syntactically and semantically equivalent to octet 2-n of the *Mobile Identity* information element. See sub-clause 10.5.1.4.

<channel first>

This field is syntactically and semantically equivalent to bits 1 and 2 of the *Channel Needed* information element. See sub-clause 10.5.2.8.

<eMLPP priority>

This field is coded as the <Priority1> field in the *P1 Rest Octets* information element. See sub-clause 10.5.2.23.

2.3.3 Notification/NCH

44018-630, chapter 9.1.21b

The understanding of this message is only required for mobile stations supporting VGCS listening or VBS listening.

This message is sent on the NCH by the network to notify mobile stations of VBS or VGCS calls in the current cell. The VBS or VGCS calls are identified by their broadcast call reference or group call reference, respectively. For each reference, the corresponding VBS or VGCS call channel may be indicated. See table 9.1.21b.1/3GPP TS 44.018.

Notification/NCH messages for VBS or VGCS calls are differentiated by a flag in the call reference.

The L2 pseudo length of this message has a value one.

Mobile stations not supporting VGCS listening or VBS listening shall ignore this message.

Message type: NOTIFICATION/NCH

Significance: dual

Direction: network to mobile station

Table 9.1.21b.1/3GPP TS 44.018: NOTIFICATION/NCH message content

IEI	Information element	Type / Reference	Presence	Format	length
	L2 Pseudo Length	L2 Pseudo Length 10.5.2.19	M	V	1
	RR management Protocol Discriminator	Protocol Discriminator 10.2	M	V	1/2
	Skip Indicator	Skip Indicator 10.3.1	M	V	1/2
	Notification/NCH Message Type	Message Type 10.4	M	V	1
	NT/N Rest Octets	NT/N Rest Octets 10.5.2.22c	M	V	20

2.3.3.1 NT/N Rest Octets

44018-630, chapter 10.5.2.22c

The *NT/N Rest Octets* information element is a type 5 information element with 20 octets length.

NT/N Rest Octets ::= {0 I 1<NLN(PCH) : bit (2)>} <list of Group Call NCH information> <Spare padding>;
<List of Group Call NCH information> ::= 0 | 1 <Group Call information> <List of Group Call NCH information> ;
NLN(PCH) This field gives the NLN value to be used as specified in 3.3.3
<Group Call information> See sub-clause 9.1.21a

3 Interface ME - SIM

This chapter describes the changes for storage and retrieval of the ciphering key for Voice Group Calls on the SIM-ME Interface in the Recommendation 51011-480; these changes are printed in red.

3.1 Data Files on SIM

3.1.1 EF_{VGCS} (Voice Group Call Service)

51011-480, Chapter 10.3.20

This EF contains a list of those VGCS group identifiers the user has subscribed to. The elementary file is used by the ME for group call establishment and group call reception.

Identifier: '6FB1'	Structure: transparent	Optional
File size: 4n bytes (n <= 50)	Update activity: low	

Access Conditions:

READ	CHV1
UPDATE	ADM
INVALIDATE	ADM
REHABILITATE	ADM

Bytes	Description	M/O	Length
1 to 4	Group ID 1	M	4 bytes
5 to 8	Group ID 2	O	4 bytes
:	:	:	:
(4n-3) to 4n	Group ID n	O	4 bytes

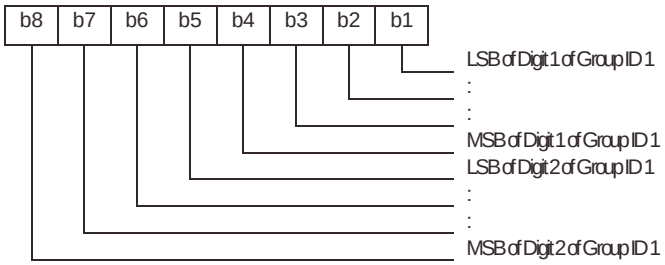
- Group ID

  Contents: VGCS Group ID, according to TS 23.003 [10]

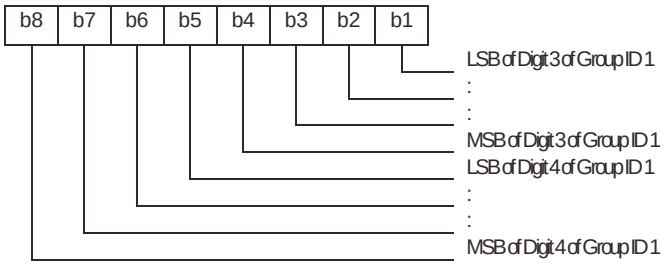
  Coding:

  The VGCS Group ID is of a variable length with a maximum length of 8 digits. Each VGCS Group ID is coded on four bytes, with each digit within the code being coded on four bits corresponding to BCD code. If a VGCS Group ID of less than 8 digits is chosen, then the unused nibbles shall be set to 'F'. VGCS Group ID Digit 1 is the most significant digit of the Group ID.

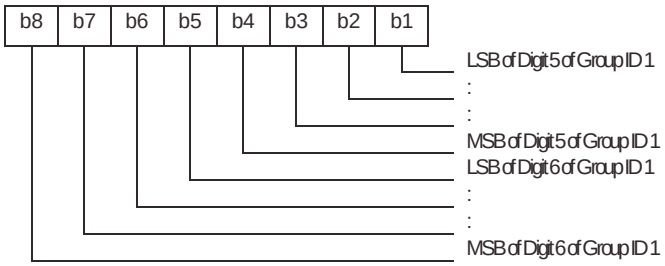
  Byte 1:



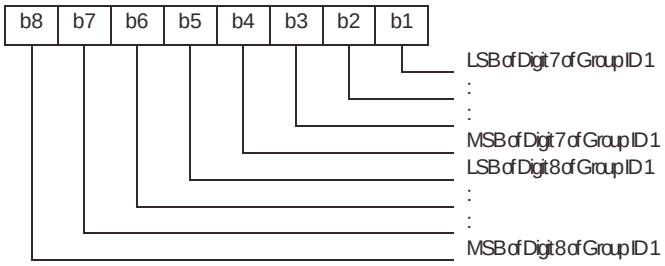
  Byte 2:



  Byte 3:

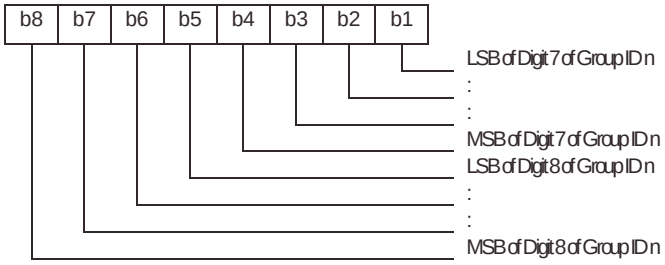


  Byte 4:



  :
  : etc.....

Byte (4n-3) to 4n:



If storage for fewer than the maximum possible number *n* of VGCS Group IDs, is required, the excess bytes shall be set to 'FF'.

3.1.2 EF_{VGCSS} (Voice Group Call Service Status)

51011-480, Chapter 10.3.21

This EF contains the status of activation for the VGCS group identifiers. The elementary file is directly related to the EF_{VGCS}. This EF shall always be allocated if EF_{VGCS} is allocated.

Identifier: '6FB2'	Structure: transparent	Optional
File size: 7 bytes	Update activity: low	

Access Conditions:

READ	CHV1
UPDATE	ADM
INVALIDATE	ADM
REHABILITATE	ADM

Bytes	Description	M/O	Length
1 to 7	Activation/Deactivation Flags	M	7 bytes

- Activation/Deactivation Flags

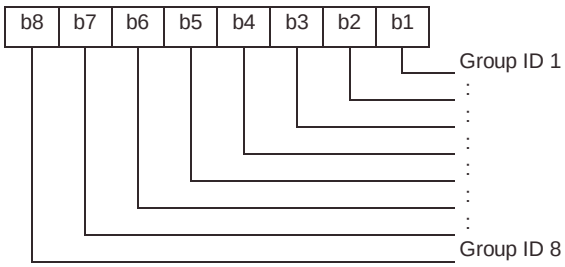
  Contents: Activation/Deactivation Flags of the appropriate Group IDs

  Coding:

  bit = 0 means - Group ID deactivated

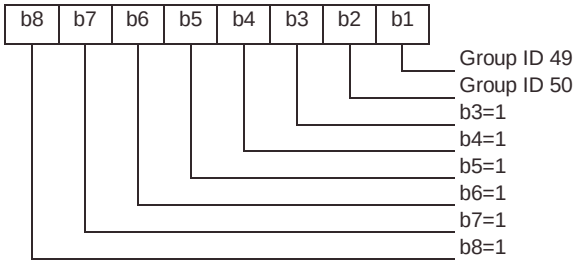
  bit = 1 means - Group ID activated

  Byte 1:



  etc : : : : : : : :

Byte 7:



3.1.3 EF_{VGCGCA} (Voice Group Call Service Group Ciphering Algorithm)

Remark: The algorithm to be applied in the Voice Group Call is not part of the notification parameters; how is this information given to the Mobile Station?

Alternative 2 - Additional Parameter "Voice Group Call Service Group Ciphering Algorithm"; the values are taken for the coding of the algorithm to be applied for the initiated group call.

51011-480, new Chapter 10.3.22

This EF contains the ciphering algorithm which shall be applied for group calls within the specified group. The elementary file is directly related to the EF_{VGCS}. This EF shall always be allocated if EF_{VGCS} is allocated.

Identifier: '6FXX'	Structure: transparent	Optional
File size: 25 bytes	Update activity: low	

Access Conditions:

READ	CHV1
UPDATE	ADM
INVALIDATE	ADM
REHABILITATE	ADM

Bytes	Description	M/O	Length
1 to 7	Activation/Deactivation Flags	M	7 bytes

- Activation/Deactivation Flags

  Contents: Ciphering Algorithm for the specified Group

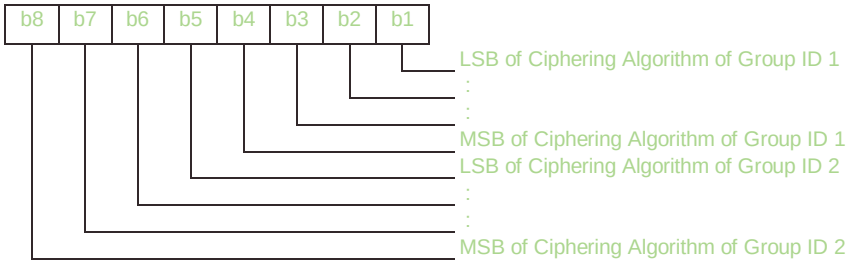
  Coding:

Bit 4	3	2	1	
0	0	0	0	no ciphering
0	0	0	1	ciphering with algorithm GSM A5/1
0	0	1	0	ciphering with algorithm GSM A5/2
0	0	1	1	ciphering with algorithm GSM A5/3
0	1	0	0	ciphering with algorithm GSM A5/4
0	1	0	1	ciphering with algorithm GSM A5/5
0	1	1	0	ciphering with algorithm GSM A5/6
0	1	1	1	ciphering with algorithm GSM A5/7
1	0	0	0	spare
1	0	0	1	spare
1	0	1	0	spare
1	0	1	1	spare
1	1	0	0	spare
1	1	0	1	spare
1	1	1	0	spare
1	1	1	1	spare

bit = 0 means - Group ID deactivated

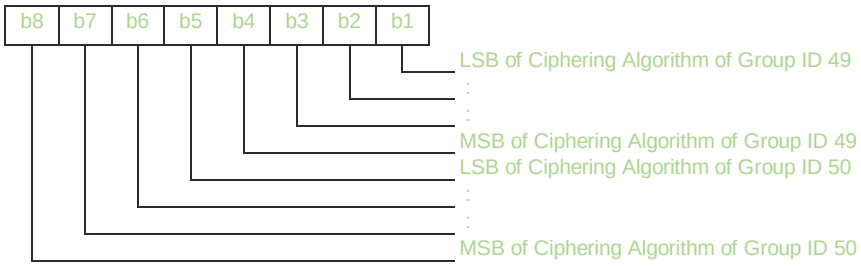
bit = 1 means - Group ID activated

Byte 1:



etc : : : : : : : :

Byte 25:



3.1.4 EF_{VGCSK} (Voice Group Call Service Key)

51011-480, new Chapter 10.3.23)

This EF contains the list of keys for the VGCS group identifiers. The elementary file is directly related to the EF_{VGCS}. This EF shall always be allocated if EF_{VGCS} is allocated.

For each Group Id 15 keys are allocated.

Identifier: '6FXX'	Structure: transparent	Optional
File size: 8 x 15 x n bytes (n <= 50, max. 6.000 bytes)	Update activity: low	

Access Conditions:

READ	CHV1
UPDATE	ADM
INVALIDATE	ADM
REHABILITATE	ADM

Bytes	Description	M/O	Length
1 to 8	Group ID 1, Key 1	M	8 bytes
9 to 16	Group ID 1, Key 2	M	8 bytes
:	:		
113 to 120	Group ID 1, Key 15	M	8 bytes
8 x 15 + 1 to 8 x 15 +8	Group ID 2, Key 1	O	8 bytes
:	:	:	:
8 x 15 + 113 to 8 x 15 + 120	Group ID 2, Key 15	O	8 bytes
:	:	:	:
:	:	:	:
:	:	:	:
(n-1) x 8 x 15 + 1 to (n-1) x 8 x 15 + 8	Group ID n, Key 1	O	8 bytes
:	:	:	:
(n-1) x 8 x 15 + 113 to (n-1) x 8 x 15 + 120	Group ID n, Key 15	O	8 bytes

3.2 Voice Group Call Services

51011-480, Chapter 10.5.10

Requirement: Service n°18 "allocated and activated".

Voice Group Call Service

Request: The ME performs the reading procedure with EF_{VGCS}.

Voice Group Call Service Status

Request: The ME performs the reading procedure with EF_{VGCSS}.

Update: The ME performs the updating procedure with EF_{VGCSS}.

Voice Group Call Service Group Ciphering Algorithm

Request: The ME performs the reading procedure with $EF_{VGCSGCA}$ (e.g. ciphering algorithm of group m)

Voice Group Call Service Key

Request: The ME performs the reading procedure with EF_{VGCSK} (e.g. nth key of group m)

CR-Form-v7

CHANGE REQUEST

⌘ **TS 43.020 CR CRNum** ⌘**rev -** ⌘ Current version: **5.0.0** ⌘

*For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

Proposed change affects: UICC apps⌘ [X] ME [ ] Radio Access Network [X] Core Network [X]

Title:	⌘	Addition of stage 2 concept for VGCS key management
Source:	⌘	Vodafone, Siemens
Work item code:	⌘	???
Date:	⌘	30/09/2003
Category:	⌘	**B**
Release:	⌘	Rel-6

Use one of the following categories:
F *(correction)*
A *(corresponds to a correction in an earlier release)*
B *(addition of feature),*
C *(functional modification of feature)*
D *(editorial modification)*
Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use one of the following releases:

2	*(GSM Phase 2)*
R96	*(Release 1996)*
R97	*(Release 1997)*
R98	*(Release 1998)*
R99	*(Release 1999)*
Rel-4	*(Release 4)*
Rel-5	*(Release 5)*
Rel-6	*(Release 6)*

Reason for change:	⌘	Addition of the Stage 2 description for the feature 'automatic key management for VGCS'
Summary of change:	⌘	
Consequences if not approved:	⌘	The feature cannot be realized. Open issues: It is ffs how to signal to the ME which cipher algorithm is used for the group call. Basically there are two options: • Introduce an appropriate information element in the *Descriptive Group or Broadcast Call Reference* message from the BSS to the ME • or Introduce an field on the USIM which is read out be the ME (together with the group key).

Clauses affected:	⌘	0.1, New annex F			
Other specs affected:	⌘	**Y** [Y] **N** [ ]	Other core specifications	⌘	51.011
		Y [ ] **N** [N]	Test specifications		
		Y [ ] **N** [N]	O&M Specifications		
Other comments:	⌘				

***** Start of change *****

0.1 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document.*

[1] GSM 01.04: "Digital cellular telecommunications system (Phase 2+); Abbreviations and acronyms".

[2] GSM 01.61: "Digital cellular telecommunications system (Phase 2+); General Packet Radio Service (GPRS); GPRS ciphering algorithm requirements".

[3] GSM 02.07: "Digital cellular telecommunications system (Phase 2+); Mobile Station (MS) features".

[4] GSM 02.09: "Digital cellular telecommunications system (Phase 2+); Security aspects".

[5] GSM 02.17: "Digital cellular telecommunications system (Phase 2+); Subscriber Identity Modules (SIM) Functional characteristics".

[6] GSM 02.56: "Digital cellular telecommunications system (Phase 2+); GSM Cordless Telephone System (CTS) Phase 1; Service Description; Stage 1".

[7] GSM 02.60: " Digital cellular telecommunications system (Phase 2+); General Packet Radio Service (GPRS); Service description; Stage 1".

[8] GSM 03.03: "Digital cellular telecommunications system (Phase 2+); Numbering, addressing and identification".

[9] GSM 03.56: "Digital cellular telecommunications system (Phase 2+); GSM Cordless Telephone System (CTS), Phase 1; CTS Architecture Description; Stage 2".

[10] GSM 03.60: " Digital cellular telecommunications system (Phase 2+); General Packet Radio Service (GPRS); Service description; Stage 2".

[11] GSM 04.08: "Digital cellular telecommunications system (Phase 2+); Mobile radio interface layer 3 specification".

[12] GSM 04.64: " Digital cellular telecommunications system (Phase 2+), General Packet Radio Service (GPRS); Logical Link Control (LLC)".

[13] GSM 05.01: "Digital cellular telecommunication system (Phase 2+); Physical layer on the radio path; General description".

[14] GSM 05.02: "Digital cellular telecommunications system (Phase 2+); Multiplexing and multiple access on the radio path".

[15] GSM 05.03: "Digital cellular telecommunications system (Phase 2+); Channel coding".

[16] GSM 09.02: "Digital cellular telecommunications system (Phase 2+); Mobile Application Part (MAP) specification".

[17] GSM 11.11: "Digital cellular telecommunications system (Phase 2+); Specification of the Subscriber Identity Module- Mobile Equipment (SIM-ME) interface".

[18] 3GPP TS 43.068: " 3rd Generation Partnership Project; Technical Specification Group Core Network; Voice Group Call Service (VGCS); Stage 2"

***** End of change *****

***** Start of second change *****

Annex F (normative): Key management for Voice Group Calls

This annex describes the key management of voice group calls. The stage 2 description of voice group calls can be found in [18]. The Key Management Center (KMC) and its interfaces are out of scope of this specification and are given for informational reason only.

Key Management Centre (informative)

Group keys are managed by one or more key management centres (KMC). Each KMC manages GCR only of one network. However it is possible to define voice group areas across several networks. In this case one network shall be identified which manages these international group calls, i.e. the appropriate KMC is obliged to provide the ciphering data to the GCR co-located to the anchor-MSC. If subscribers of a different network shall be member of an international group, an appropriate entry (i.e. group id) in the corresponding HLR is required. However the group keys are only required in the GCR connected to the anchor-MSC and on the USIM.

The KMC and all interfaces to other network elements (e.g. OTA-server, GCR, O&M) are proprietary and not subject of this specification. To have a complete picture of the whole architecture the basic requirements and tasks are described in this section.

The tasks of the KMC are:

1. Generation of group keys: It is up to the policy of the operator and the needs of the respective group how frequently new group keys are generated and old group keys replaced by news ones.

2. Distribution of group keys: The KMC is connected to the

   – OTA-Server in order to send group keys via OTA to the USIM (belonging to the respective group)

   – Group Call Register to store and delete group keys (Note that all those GCRs shall get the group keys which have group call references defined with the specific group)

The transfer of group keys between the KMC and the OTA-server and between the KMC and the GCR shall be confidentiality and integrity protected.

The KMC shall take care that a group key is already distributed to all members (i.e. all USIM) of the group before the group key is delivered to the responsible GCRs. If a new USIM has to be added to an existing group, the KMC has to deliver the group keys to the USIM first before enabling the group call reference (i.e. group-id and group call area) in the GCR.

The picture below gives an overview of the key distribution process:

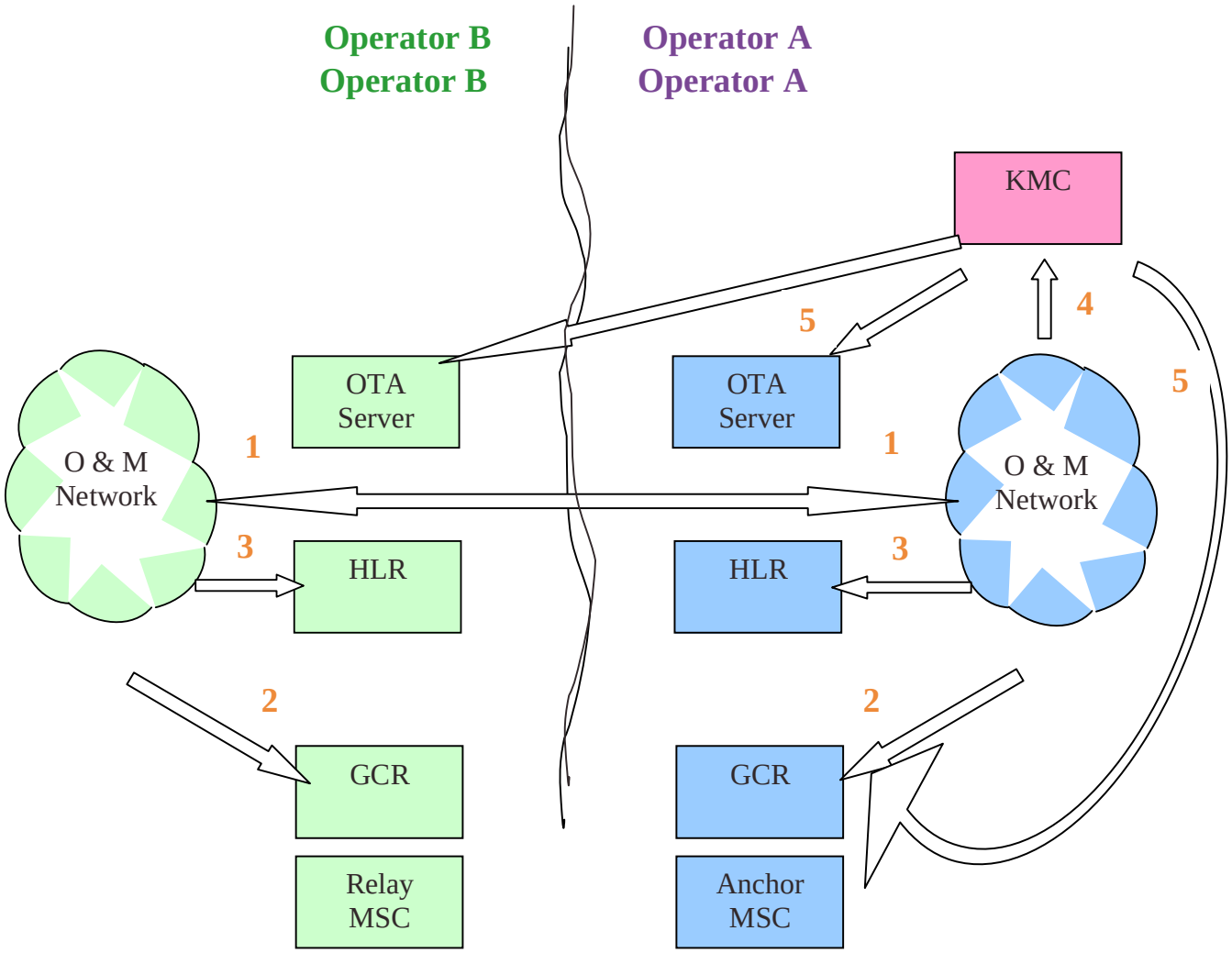


Figure 1: Key management architecture

1. Both networks exchange the group parameters (group name), the MSCs (or numbers relay MSCs); the networks initiate administration tasks.
2. The Group Reference is administered in the GCRs: area definition, group id;
3. The subscriptions are administered in the HLRs: group id, service subscription.
4. The Group Parameters are given to the KMC; these include list of subscribers, group number, group references connected with this group (TBD), anchor MSC.
5. The Key Management Center distributes the keys to the UICC via OTA (the interface to the "foreign" OTA-server is handled from the KMC too) and to the GCR co-located to the anchor -MSC

Storage and transportation of group keys (normative)

In addition to the KMC the groups keys are stored at two locations:

GCR: Beside other information, the GCR stores for each group-id a list of group keys. Each group key is uniquely identified by the group-id and the group key number (1-15).

USIM: The USIM contains a list of 15 group keys for each group id. To have read access to the group keys CHV1 is required. Deletion or changing of group keys are allowed only via OTA (or during the SIM-personalisation process).

1. During the voice group call set-up the anchor-MSC sends a GCR Interrogation to the GCR containing the group id.
2. The GCR selects a key randomly from list of the group keys of the corresponding group id and sends the group key and the group key number back to the anchor-MSC.
3. The Anchor-MSC sends the group key number, the group key and the permitted VGCS ciphering algorithm to the relay-MSC via the "Prepare_Group_Call" MAP-operation.
4. The relay-MSC sends the group key and the permitted algorithm to the BSS using the VGCS Assignment Request.
5. The BSS sends the group id and the group key number to the ME via the Notification/FACCH procedure.
6. The ME fetches the group key from USIM via the "Voice Group Call Service Key"-request.

Ciphering Algorithms

Algorithms: For the ciphering of group calls the same algorithms are used as for the ciphering of normal speech calls (A5/0 – A5/7).

***** End of second change *****