3GPP TSG SA WG3 Security — S3#32 **S3-040117**
09 - 13 February 2004
Edinburgh, Scotland, UK

3GPP TSG GERAN **TSGG#18(04)0566**
Meeting no 18 **Agenda Item: 7.2.5.4.7**
Reykjavík, Iceland
2 – 6 February 2004

Title:	**Draft reply to LS on 'Ciphering for Voice Group Call Services'.**
Response to:	**LS on 'Ciphering for Voice Group Call Services'.**
Release:	**Rel-6**
Source:	**GERAN2**
To:	**SA3**
CC:	**ETSI EP RT, T WG3**

Contact Person:

Name:	Ken Isaacs
Tel. Number:	+44 1794 833531
E-mail Address:	**kenneth.isaacs@roke.co.uk**

Attachments: **GP-040180, GP-040181**

Overall Description:

GERAN 2 would like to thank SA3 for their LS on 'Ciphering for Voice Group Call Services' in Tdoc S3-030804.

GERAN 2 has **considered the provision of the RAND, CGI and the global_count** and the conclusions are summarized below:

A. RAND

The provision of the RAND in the notifications on the NCH, PCH and FACCH has been discussed. The amount of space available for the RAND is dependent on the channel type as described in GP-040180. This paper concludes that **in order to provide a RAND of at least 32 bits** that it would **sometimes be necessary to segment the description for one voice group call over two radio blocks** by using two messages. The following two segmentation schemes are discussed in Tdoc GP-040181:

i. Using two instances of the same message type

With this mechanism it should be possible to provide a RAND of 32 bits in the notifications on the NCH, PCH and the FACCH.

ii. Using one instance of the existing notification message type and a new message to contain additional ciphering parameters.

With this mechanism it should be possible to provide a RAND of 32 bits in the notifications on the NCH and the FACCH. It is not possible to add a new message on the PCH because legacy mobiles will not be able to read their page mode.

However, there is a **concern that these methods may have some issues with legacy mobiles**. It should be noted that a ciphering mechanism has already been specified in 43.068, 43.069 and 44.018 and that the **proposed changes by SA3 are not compatible with the existing procedures**. **GERAN 2 would like more time to consider how voice group calls are administered before confirming that the above solutions are possible.**

B. **CGI**

The provision of the **CGI** as an input parameter to the generation of the group cipher key has been discussed, and is described in GP-040180. This value is **already provided in System Information 3 and 4** messages which are read by the mobile station before it accesses a cell. The value **needs to be also provided** to the MS after handover, **in the Handover Command** message. This message can be segmented over multiple radio blocks so the addition of the CGI should not be an issue.

C. **Global_count**

Two methods for the provision of the global_count were discussed:

i. Cell based, where global_count is common to all group calls in a cell

In this case global_count would need to be provided in the system information on the BCCH and SACCH, and in the Handover Command (FACCH).

ii. Call based, where each group call in a cell has its own global_count.

In this case the global_count would need to be provided in the notifications (NCH,PCH and FACCH) and in the Handover Command(FACCH).

These methods are described in GP-040180. **Option (i) is preferred** at there is a lack of space available in the notifications, as discussed in the provision of the RAND.

GERAN2 also noted that **the name of this variable may not be appropriate** as its value will vary from cell to cell because the TDMA frame numbers are not necessarily synchronized between cells.

GERAN 2 will provide further feedback on the provision of these parameters after further analysis.

However, during GERAN2 discussions the following questions were raised for which GERAN 2 would be grateful if SA3 could answer:

A. Is a UICC/USIM mandatory for the mobile that supports the new VGCS ciphering mechanism?
B. How will a Release 6 MS that supports the new VGCS mechanism react with a SIM card?
C. What happens if a UICC/USIM with voice group id X is inserted into a Release-5 MS and the MS is camped on to a cell where this group call is active?
D. Are the proposed changes also applicable to the VBS service?
E. Are the proposed changes to be applied only from Release-6?
F. Is a cell based global_count as in C(i) an acceptable method for providing this parameter ?

Actions:

SA3: GERAN2 kindly asks SA3 to answer the above questions.

Date of Next GERAN2 Meetings:

GERAN#18 bis	22nd -26th March 2004	Phoenix, USA
GERAN#19	19th -23rd April 2004	Cancun, MEXICO

3GPP TSG GERAN #18 GP-040180
Reykjavik,Iceland Agenda Item 7.2.5.4.7
2nd – 6th February 2004
Source: Siemens

Ciphering for Voice Group Call Services

1 Introduction

SA3 have proposed some security enhancements to the ciphering procedures for Voice Group Calls in order to address the following issues:

- Prevent the same ciphering key being used within different cells
- Prevent the reuse of COUNT with the same ciphering key within the same cell
- VGCS group key shall never leave the USIM

To solve the above issues it has been proposed to make the cipher key generation dependent on the following additional parameters, as shown in Figure 1:-

- RAND – a random number that is allocated when establishing the group call
- Cell Identity – the CGI has been suggested
- GLOBAL_COUNT – this counter is incremented when TDMA number wraps around.

SA3 has asked GERAN 2 to consider the possibility of using the above values in the generation of the short term ciphering key.

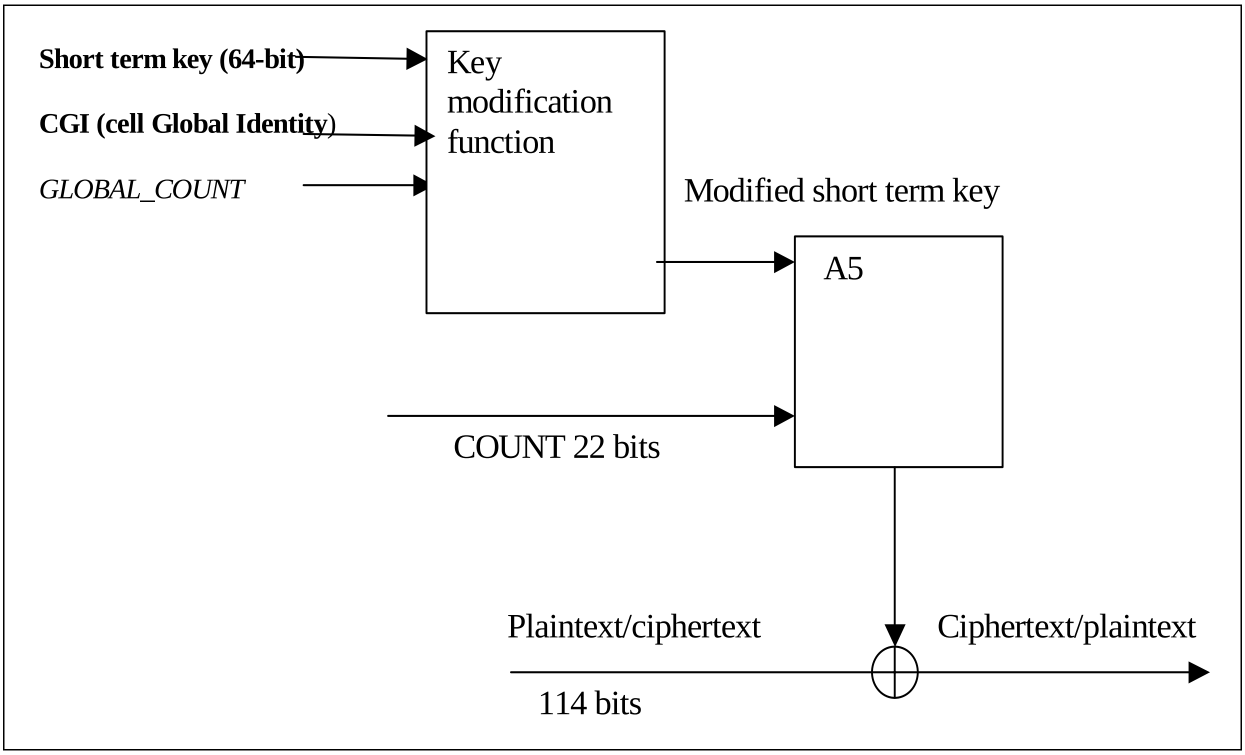

Figure 1: Proposed ciphering for VGCS calls (all requirements addressed)

2 RAND

The RAND is a random number that is to be allocated by the network when establishing a group call. The value needs to be provided to MSs via the Notification messages.
Notification messages may be sent on the NCH, FACCH or the PCH. The RAND needs to be included on all three of these channels as the MS may join a group having been previously in idle mode or dedicated mode.

SA3 have asked GERAN how much space is available for a RAND to be included with the Notification messages.

The amount of space available for the RAND on the NCH, FACCH and the PCH is considered below.

2.1 Notification/NCH

This message is defined in 44.018 sub-clause 9.1.21 as:

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

The restrictions on the space available on the NCH are:

- Each radio block used by the NCH can contain 184 bits (23bytes)
- There is no L2 header (no LAPDm header)
- 3 byte message header (L2 length, PD, skip, message type)
- This leaves 20 bytes available for NT/N Rest octets

NT/N Rest octets is defined to have length of 20 octets, made up of

2.1.1.1 10.5.2.22c NT/N Rest Octets

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

The Group channel description is defined below:

Consider the case where NLN is present ie {0 I 1<NLN(PCH) : bit (2)>} is 3 bits

```
<Group Call information> ::=        <Group Call Reference : bit(36)>
                                      {0|1 <Group Channel Description>} ;
<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> ;

where length of Mobile Allocation is 2 to 9 octets ie 18 to 72 bits

The sizes the fields within NT/N are summarised below:

Field	Size in bits	
1<NLN>	1+2 bits	
Group Call Ref	36 bits	
Channel Description	24 bits	
<Mobile Allocation>	(18 to 72) bits	
<Frequency Short List>	64 bits	
<Group Channel Description>	Non Hopping	(Channel Description)+1 bit
	Mobile Allocation	(Channel Description) +10 (Mobile Allocation) bits
	Frequency Short List	(Channel Description) + 11(Frequency Short List) bits
1<Group call information>	1+(Group Call Ref) + 1(Group Channel Description) bit	
Loop terminator	1	
Total	67 min (non-hopping) to 140 bits	

NOTE: The largest message size is calculated by summing the following: 1<NLN>, 1<Group call information>, Loop terminator for the case when the Mobile Allocation IE is included.

Since the total space available for NT/N is 160 bits, then this leaves at least 20 bits available for the RAND if the notification for one group call is to always fit within one radio block. It should be noted that the notification/NCH can contain notifications for more than one group call and that any additional information would needed to be added as a Rel-6 extension after the current description of the list of group calls. Further, the Group Channel Description is an optional field.

2.2 Notification/FACCH

A notification for one voice group may be contained within the Notification/FACCH message. This message is defined in 44.018 sub-clause 9.1.21a as:

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>} ;
```

Each radio block on the FACCH can contain 23 octets of user data, of which 24 bits are used for a LAPDm header. Each upper layer message may be segmented over many radio blocks.

The sizes of the fields within the Notification/FACCH message are summarised below:

Field	Size in bits	
RR	1 bit	
Message type	5 bits	
L2 header	2 bits	
Group Call Ref	36 bits	
Channel Description	24 bits	
Mobile Allocation	18 to 72 bits	
Frequency Short List	64 bits	
<Group Channel Description>	Non Hopping	(Channel Description) +1 bit
	Mobile Allocation	(Channel Description) + 10 (Mobile Allocation) bits
	Frequency Short List	(Channel Description) + 11 (Frequency Short List) bits
0<Group Call Information>	1+(Group Call Ref) + 1(Group Channel Description) bit	
Total	71 min (non-hopping) to 144 bits	

NOTE: The largest message size is calculated by summing the following: RR, Message Type, L2 header, 0<Group Call information> for Group channel description containing Mobile Allocation IE

If a Notification message is to occupy only one Radio block, then the total space available for the Notification/FACCH message is 160 bits. Thus this leaves at least 16 bits available for the RAND. Thus there is insufficient space available both on the NCH and the FACCH to provide a RAND of 32-64 bits if the Notification message for a particular group call is to always be contained within one Radio Block.

2.3 Notification/PCH

A notification for one voice group may be contained within the P1 Rest octets in a Paging Request Type 1 message on the PCH. This message is defined in 44.018 as follows:

Table 9.1.22.1/3GPP TS 44.018: PAGING REQUEST TYPE 1 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
	Paging Request Type 1 Message Type	Message Type 10.4	M	V	1
	Page Mode	Page Mode 10.5.2.26	M	V	1/2
	Channels Needed for Mobiles 1 and 2	Channel Needed 10.5.2.8	M	V	1/2
	Mobile Identity 1	Mobile Identity 10.5.1.4	M	LV	2-9
17	Mobile Identity 2	Mobile Identity 10.5.1.4	O	TLV	3-10
	P1 Rest Octets	P1 Rest Octets 10.5.2.23	M	V	0-17

P1 Rest Octets is defined in 44.018 as:

```
{        <P1 Rest Octets> ::=
         {L I H <NLN(PCH) : bit (2)> <NLN status : bit>}
         {L I H <Priority1 ::= Priority>}
         {L I H <Priority2 ::= Priority>}
         {L | H <Group Call information>}
         < Packet Page Indication 1 : {L | H} >
         < Packet Page Indication 2 : {L | H} >
         <spare padding>;
}        -- truncation allowed, bits 'L' assumed

<Priority> ::= <bit (3)>;

<Group Call information>
See sub-clause 9.1.21a
```

Each radio block on the PCH can contain 23 octets of user data. The mandatory fields excluding the P1 rest octets occupy 6-13 octets. Thus the available space for the P1 rest octets is 10-17 octets.

The sizes of the fields within the P1 Rest octets message are summarised below:

Field	Size in bits
NLN	1 or 4 bit
Priority 1	1 or 4 bits

Priority 2	1 or 4 bits	
Group Call Ref	36 bits	
Channel Description	24 bits	
Mobile Allocation	18 to 72 bits	
Frequency Short List	64 bits	
<Group Channel Description>	Non Hopping	(Channel Description) +1 bit
	Mobile Allocation	(Channel Description) + 10(Mobile Allocation) bits
	Frequency Short List	(Channel Description) + 11(Frequency Short List) bits
1<Group Call Information>	1 + <Group Call Ref> + 1<Group Channel Description>	
Total	75 min (non-hopping) to 148 bits	

NOTE: The largest message size is calculated by summing the following: NLN, Priority 1, Priority 2, 1<Group Call Information>

Thus there are currently occasions when the radio block is full. Thus it is not possible to include a RAND within this message if this message has to be contained within one radio block.

2.4 Conclusion

It is apparent that there may not always be sufficient space for a notification for a particular group call to be contained within one radio block if a RAND of 32-64 bits is required. If it is required to include the RAND in notifications on the NCH, FACCH and PCH then it cannot be guaranteed that there is any space for this RAND unless it is possible to send the notification for one group call over multiple radio blocks. However, if it were acceptable that the PCH is not used for notifications that are longer than one radio block, then it would be possible to include a RAND of 16 bits (20 bits were available on the NCH whilst 16 bits were available on the FACCH).

If a RAND of 32 – 64 bits is required to be included in each notification then it is necessary that a notification for a particular group call can be spread over more than one radio block on the NCH, PCH and FACCH. This may be achieved by using multiple ‘Notification messages’ for describing one group call. The first block could describe the group call as today, containing group call reference and channel description. This block would also contain an indication that there is further information describing this group call in a subsequent ‘Notification message’. The subsequent message would contain some ciphering parameters (RAND) for the group call identified by its Group Reference (27bits). With this additional block it should be possible to provide a RAND of 64 bits. The likely issues with such a scheme are:

- complexity of scheduling within the BTS

- backward compatibility with existing mobiles, ensuring that the subsequent block is not interpreted by legacy MSs as meaning that there are no ongoing group calls in the cell. A possible solution is to use a different message id for the subsequent block.
- Performance of the Paging Channel

This is analysed in Tdoc GP-040181.

3 Provision of Cell Identifier

SA3 have requested to make the cipher key generation dependent on a cell identifier in order to prevent the same key being used in different cells. The most appropriate cell identifier is the CGI, as it is provides a unique identification of a cell.

The CGI is already provided in System Information 3 and 4 messages and both of these messages are always broadcast (44.018 sub-clause 3.2.2.1). Before the MS camps on a cell after cell reselection it acquires a full set of system information. Thus the MS should have read both of these messages before it accesses a cell (i.e. the VGCS listener), except in the case of handover. For the case that the MS camps on a PBCCH then it will acquire the CGI from the PSI 2 message.

In order for the MS to be able to start ciphering immediately on handover (ie VGCS talker) to the new cell, the CGI of the new cell should be provided in the Handover Command that is sent to the MS in the old cell. The CGI consists of the Cell Identifier (16 bits) and the LAI(40 bits). As the Handover Command may be segmented over multiple radio blocks there is no issue of there being insufficient space in the message for adding this additional field. In order for the source BSC to have access to the CGI of the target cell, it may be necessary for this information to be transported back from the target BSC.

Conclusion: It should be possible to use the CGI as an input parameter to the cipher key generation. The CGI should be added to the Handover Command.

4 Provision of GLOBAL_COUNT

The purpose of providing this value is because COUNT wraps around every 3-4 hours (nb COUNT is derived from the TDMA frame number). Each time that COUNT wraps around then GLOBAL_COUNT would be incremented. Since TDMA frame numbers are not synchronised between cells then GLOBAL_COUNT would need to be maintained for each cell. Hence the name “global_count” may not be appropriate. GLOBAL_COUNT could be either provided as :

A. Cell parameter where GLOBAL_COUNT is the same for all group calls in a given cell
B. Call parameter where GLOBAL_COUNT is maintained for each individual call. The value of GLOBAL_COUNT for a call will still be maintained for each cell that the call is active.

These two alternative means of providing GLOBAL_COUNT are described below.

4.1 GLOBAL_COUNT provided as a cell parameter that is the same for all group calls in a cell

GLOBAL_COUNT value could be potentially provided by the following means

a) Broadcast in system information and included in the Handover Command.
b) Provided in the Notifications and included in the Handover Command

These two options for providing GLOBAL_COUNT on a per cell basis are discussed below:

4.1.1 GLOBAL_COUNT broadcast in system information and included in Handover Command

The value should be provided in system broadcast, both on the BCCH and the SACCH so that MSs in Idle Mode and in Dedicated mode have access to this field.

In addition GLOBAL_COUNT for the target cell should be provided in the Handover Command as GLOBAL_COUNT is not synchronised between cells. The MS can read the TDMA frame number in the new cell from the SCH. It is possible that the TDMA frame number in the target cell has wrapped around between the target cell responding with the Handover Request Ack and the MS accessing the new cell. Thus the target cell should provide GLOBAL_COUNT and TDMA frame number in the Handover Request Ack. On handover, the MS accesses the SCH in the new cell to read the TDMA frame number. If the TDMA frame number that is read from the SCH is less than that provided in the Handover Command, then the GLOBAL_COUNT will need to be incremented.
Once GLOBAL_COUNT has been obtained in a cell there should not be any need to reread it from the system information, as the MS should be aware of the current TDMA frame number and thus know when GLOBAL_COUNT needs to be incremented. GLOBAL_COUNT need not be provided when a cell has no NCH.

4.1.2 GLOBAL_COUNT provided in Notification

GLOBAL_COUNT could be provided to the MS in the Notification messages. Since that parameter is common to all group calls in a cell then it should be only provided once in a radio block that contains notification(s). By providing this parameter in notifications, then this value is not broadcast if the cell does not support group calls. In the event of handover, the GLOBAL_COUNT of the target cell still has to be obtained prior to the MS accessing the target cell. Thus the value still needs to be provided in the handover command.

It has already been shown that there is very little space remaining in the notification messages in certain situations such as when the notification is included in Paging Request Type 1 message and frequency hopping parameters are provided. Thus it cannot be guaranteed that there is always sufficient space for this parameter in a notification if a notification is to be contained within one radio block

4.1.3 Conclusion

In order to prevent reuse of cipher keys within a cell then GLOBAL_COUNT should be incremented each time TDMA frame number wraps around. Thus even if there are no group calls active in a cell the parameter should still be used if the cell supports group calls.

It is recommended that GLOBAL_COUNT is provided in the following:

- System information on BCCH and SACCH
- Handover command (along with TDMA frame number in the target cell)

4.2 GLOBAL_COUNT provided as a call parameter that is maintained for each cell that the call is active

This section considers maintaining the GLOBAL_COUNT on a per call basis. GLOBAL_COUNT still needs to be maintained for each cell as TDMA frame numbers are not synchronised between cells.

It would appear that it is not sufficient for the value to be just broadcast in the system information on the BCCH and SACCH as in 4.1.1 as there would be that danger that the value would not be available to a MS when a new call is setup. Thus it would be more appropriate if the value were provided in a call related message, ie in the Notification message. The only issue with providing this value with the Notification message is the lack of space available in certain configurations (when frequency hopping parameters are included).

In addition to providing GLOBAL_COUNT in the Notification message, the value should also be provided in the Handover Command as the value is still dependent on the cell.

4.2.1 Conclusion

Provision of GLOBAL_COUNT on a call basis is dependent on being able to extend the Notification message as in 2.4. This is analysed in Tdoc GP-040181.

5 Backward Compatibility

The proposed security enhancements (Rel-6) are not backward compatible with the existing ciphering procedures. Thus it is not possible to have a ciphered group call with MSs supporting both the old and new type ciphering procedures in the same group. The following restrictions should be applied when creating a group call that is ciphered:

- A Rel-6 MS shall support the old and new type of ciphering
- A Rel-6 BSS may support the old and new type of ciphering
- A group call that is using Rel-6 type ciphering cannot contain pre Rel-6 members
- A group call that is using pre Rel-6 type ciphering can contain Rel-6 MSs that are using the pre Rel-6 type ciphering and pre Rel-6 members

6 Conclusion

This paper has examined the provision of the RAND, CGI and GLOBAL_COUNT as possible input parameters for the generation of short term cipher keys. It would appear that the main issue in providing these parameters is the amount of space available for these parameters with the notification message. In some cases it is necessary to be able to segment the notification for one group call over two radio blocks.

7 References

GP-040181 Segmentation of notification information for VGCS

3GPP TSG GERAN #18 **GP-040181**
Reykjavik,Iceland **Agenda Item 7.2.5.4.7**
2nd – 6th February 2004
Source: Siemens

Segmentation of notification information for one Voice Group Call over two radio blocks

1.Introduction

At the last Geran2 meeting there was a discussion on the need to be able to segment notifications for one voice group call over multiple radio blocks in order to be able to carry the additional information that is needed for the new cipher key generation procedure that has been proposed by SA3. This contribution examines possible solutions for segmenting notifications over two radio blocks by the following means:

Options

- Use existing message types on NCH (Notification/NCH), PCH (Paging request type 1), FACCH (Notification/FACCH)
- Use new message types NCH, PCH, FACCH to carry the additional information

2. Use existing message types for notifications on NCH, PCH and FACCH

This section considers sending the notifications on the NCH, PCH and FACCH using the existing message types, but with the message definition enhanced to allow the inclusion of additional parameters for the ciphering algorithm.

2.1.NCH (Notification/NCH)

The current message definition of the notification on the NCH is as follows:

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

The Group call information is defined as:

```
<Group Call information> ::=        <Group Call Reference : bit(36)>
                                      {0|1 <Group Channel Description>} ;
```

```
where the Group Channel Decsription is defined as:

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

The following two options are considered for sending the notification for one group call over two radio blocks:

Message option	First message	Second message
Omit Group Call Description from the second message	List of Group Call Information (Group Call Reference, Group Channel Description), Indication that ciphering parameters are in second message	List of Group Call Information containing Group Call References. List of new ciphering parameters for ciphered group calls.
Second message contains empty list of notifications	List of Group Call Information (Group Call Reference and Group Channel Description), Indication that ciphering parameters are in second message	Empty List of Group Call Information. List of Group Call References and new ciphering parameters.

2.1.1. Omit Group Call Description in second message

With this proposal the first message would contain the group call description as currently specified, together with an indication that the call is ciphered (in the broadcast reference as currently specified in 24.008). A flag is set to indicate that additional ciphering parameters follow in a subsequent message.

In the current Notification/NCH message definition the Group Channel Description is optional. Thus it is possible to for the second message to exclude the Group Channel Description. With the space made available by excluding this field the new ciphering parameters could be added.

A Rel-6 MS that was unable to decode the first message would have to read the NCH again to obtain the Group Channel Description from a repetition of the first message.

A legacy MS on reading the second message would read the group call reference and see that the notification is not for it as legacy MS's do not support ciphering on VGCS calls.

2.1.2.Send empty list of group calls in second message

With this proposal the first message would contain the group call description as currently specified, together with an indication that the call is ciphered (in the broadcast reference as currently specified in 24.008). A flag is set to indicate that additional ciphering parameters follow in a subsequent message.

The second message would contain an empty list of group calls and a list of the additional ciphering parameters that could not be contained in the first block.

The problem with this definition is that a legacy MS would interpret the second block as containing an empty list of group calls and thus may think that are no group calls active in the cell.

Conclusion:

It would appear that a notification for one group call could be segmented over two radio blocks on the NCH using the existing message types, with the group channel description omitted from the second message.

2.2.PCH

The Paging Request Type 1 may contain a notification for one group call. The Paging Request Type 1 message is defined as follows:

Table 9.1.22.1/3GPP TS 44.018: PAGING REQUEST TYPE 1 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
	Paging Request Type 1 Message Type	Message Type 10.4	M	V	1
	Page Mode	Page Mode 10.5.2.26	M	V	1/2
	Channels Needed for Mobiles 1 and 2	Channel Needed 10.5.2.8	M	V	1/2
	Mobile Identity 1	Mobile Identity 10.5.1.4	M	LV	2-9
17	Mobile Identity 2	Mobile Identity 10.5.1.4	O	TLV	3-10
	P1 Rest Octets	P1 Rest Octets 10.5.2.23	M	V	0-17

Where P1 test octets is defined as:

```
{           <P1 Rest Octets> ::=
            {L I H <NLN(PCH) : bit (2)> <NLN status : bit>}
            {L I H <Priority1 ::= Priority>}
            {L I H <Priority2 ::= Priority>}
            {L | H <Group Call information>}
            < Packet Page Indication 1 : {L | H} >
            < Packet Page Indication 2 : {L | H} >
            <spare padding>;
}           -- truncation allowed, bits 'L' assumed

<Priority> ::= <bit (3)>;

<Group Call information>
See sub-clause 9.1.21a
```

The following two options are considered for sending the notification for one group call over two radio blocks using Paging Request Type 1 messages:

Message option	First message	Second message
Omit Group Call Description from the second message	Group Call Information (Group Call Reference, Group Channel Description), Indication that ciphering parameters are in second message	Group Call Information containing Group Call Reference. New ciphering parameters for ciphered group call.
Second message contains no Group Call Information notification	Group Call Information (Group Call Reference and Group Channel Description), Indication that ciphering parameters are in second message	Group Call Reference and new ciphering parameters.

2.2.1.Omit Group Channel Description in second message

With this proposal the first message would contain the group call description as currently specified, together with an indication that the call is ciphered (in the broadcast reference as currently specified in 24.008). A flag is set to indicate that additional ciphering parameters follow in a subsequent message.

The second message would contain the Group Call Reference and the additional ciphering parameters that could not be contained in the first block. The additional ciphering parameters would be added in a Rel-6 extension. A pre Rel-6 MS would interpret these fields as “padding”.

A Rel-6 MS that was unable to decode the first message would have to read the NCH to obtain the Group Channel Description.

A legacy MS on reading the second message would read the group call reference and see that the notification is not for it.

2.2.2.Send message contains no Group Call Information

With this proposal the first message would contain the group call description as currently specified, together with an indication that the call is ciphered (in the broadcast reference as currently specified in 24.008). A flag is set to indicate that additional ciphering parameters follow in a subsequent message.

The second message would contain a rel-6 extension that includes the Group Call Reference and the additional ciphering parameters that could not be contained in the first message. A pre Rel-6 MS would interpret these fields as “padding”.

A legacy MS that reads the second message may interpret that the Paging Request Type 1 message contains no notification so the MS would have to go to the NCH to read the notification.

Conclusion:

It would appear that a notification for one group call could be segmented over two radio blocks on the PCH using the existing message types, with the group channel description omitted from the second message.

2.3.FACCH

The Notification/FACCH may contain a notification for one group call, as defined below:

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>} ;
```

The following two options are considered for sending the notification for one group call over two radio blocks using the Notification/FACCH message:

Message option	First message	Second message

Omit Group Call Description from the second message	Group Call Information (Group Call Reference, Group Channel Description), Indication that ciphering parameters are in second message	Group Call Information containing Group Call Reference. New ciphering parameters for ciphered group call.
Second message contains no Group Call Information notification	Group Call Information (Group Call Reference and Group Channel Description), Indication that ciphering parameters are in second message	Group Call Reference and new ciphering parameters.

2.3.1.Omit Group Channel Description in second message

With this proposal the first message would contain the group call description as currently specified, together with an indication that the call is ciphered (in the broadcast reference as currently specified in 24.008). A flag is set to indicate that additional ciphering parameters follow in a subsequent message.

The second message would contain the Group Call Reference and the additional ciphering parameters that could not be contained in the first block. The additional ciphering parameters would be added in a Rel-6 extension. A pre Rel-6 MS would interpret this extension as “padding”.

A Rel-6 MS that was unable to decode the first message may have to read the NCH to obtain the Group Channel Description.

A legacy MS on reading the second message would read the group call reference and see that the notification is not for it.

2.3.2.Send message contains no Group Call Information

With this proposal the first message would contain the group call description as currently specified, together with an indication that the call is ciphered (in the broadcast reference as currently specified in 24.008). A flag is set to indicate that additional ciphering parameters follow in a subsequent message.

The second message would contain a rel-6 extension that includes the Group Call Reference and the additional ciphering parameters that could not be contained in the first message. A pre Rel-6 MS would interpret these fields as “padding”.

A legacy MS would interpret the second message as not containing a notification. A Rel-6 MS that does not read the first message would have to obtain the Group Channel Description from the NCH.

Conclusion:

It would appear that a notification for one group call could be segmented over two radio blocks on the FACCH using the existing message types, with the group channel description omitted from the second message.

3.Use new message types for notification information in second block

This section considers the sending of notification information for one group call on the NCH, PCH and FACCH using two blocks with the following format:

- First message uses existing message type with an indication that the call is ciphered in the Group Call Reference
- Second message uses new message type – contains Group Call Reference and new ciphering parameters.

Using a new message type in the second block should not be an issue with legacy MSs, since according to section 8.4 of 44.018

"If a mobile station receives an RR message with message type not defined for the PD or not implemented by the receiver in unacknowledged mode, it shall ignore the message".

3.1.NCH

With this proposal the first message would contain the group call description as currently specified, together with an indication that the call is ciphered (in the broadcast reference as currently specified in 24.008).

The second message identified by a new message type would contain a list of Group Call References and ciphering parameters (perhaps there may be only one group call in the list).

A legacy MS and a Rel-6 MS that had not read the first message would ignore the second message.

Conclusion:

This mechanism appears to allow the possibility of sending additional ciphering parameters for notifications on the NCH.

3GPP TSG GERAN #18 **GP-040181**
Reykjavik,Iceland **Agenda Item 7.2.5.4.7**
2nd – 6th February 2004
Source: Siemens

3.2.PCH

In order to send a paging message to the MS spread over two radio blocks, the following two options are considered:

- First message indicates extended paging, next but one message on PCH contains new message with ciphering parameters
- First message indicates normal paging, next message on PCH contains new message with ciphering parameters

3.2.1. First message indicates Extended Paging, second message on PCH contains new message with ciphering parameters

The first message that is sent on the PCH uses the existing Paging Request Type 1 message. The Group Call Reference indicates that the call is ciphered. The page mode is set to extended.

The second message that is sent on the next but one block on the PCH contains a new message with the ciphering parameters for the group call. The page mode in the second message would indicate normal paging.

A legacy MS would ignore the second message. It would be unable to read its page mode.

3.2.2. First message indicates normal Paging, next message on PCH contains new message with ciphering parameters

The first message that is sent on the PCH uses the existing Paging Request Type 1 message. The Group Call Reference indicates that the call is ciphered. The page mode is set to normal.

The next message that is sent on the PCH contains a new message with the ciphering parameters for the group call. The page mode in the second message would indicate normal paging. The MS that reads the first block would have to aware that it has to read the next message on the PCH.

A legacy MS would ignore the second message. It would be unable to read its page mode.

Conclusion:

It is not possible to use new message types on the PCH for transporting additional ciphering parameters as legacy MS's would be unable to read the page mode in these messages.

3.3.FACCH

The first message that is sent on the FACCH uses the existing Notification/FACCH message. This message would contain the group call description as currently specified, together with an indication that the call is ciphered.

The next message that is sent on the FACCH contains a new message with the ciphering parameters for the group call.

A legacy MS and a Rel-6 MS that did not read the first message would ignore the second message.

Conclusion:

This mechanism appears to allow the possibility of sending additional ciphering parameters for notifications on the FACCH.

4.Estimation of size available for RAND

4.1.With notification for one group call contained in one message

4.1.1.Without Frequency Hopping

Logical Channel Type	Estimate of amount of space available for ciphering parameters
NCH	93 bits (1)
FACCH	89 bits (2)
PCH	16 bits (3)

Note 1: Assumed that 160 bits available for NT/N – fields included are NLN(2 bits), Channel Description (24 bits), Group Call Reference(36 bits). Only one group call in list
Note 2: Assumed that 160 bits available for Notification/FACCH – fields included are message header (8 bits), Channel Description (24 bits), Group Call Reference (36 bits).
Note 3: Assumed that 80 bits available for P1 rest octets – fields included are NLN, Channel Description (24 bits), Group Call Reference (36 bits).

4.1.2.With Frequency Hopping

Logical Channel Type	Estimate of amount of space available for ciphering parameters
NCH	20 bits (4)

FACCH	16 bits (5)
PCH	0 (6)

Note 4: Assumed that 160 bits available for NT/N – fields included are NLN(2 bits), Group Call Reference(36bits), Channel Description (24 bits), Mobile Allocation (72 bits). Only one group call in list
Note 5: Assumed that 160 bits available for Notification/FACCH – fields included are message header (8 bits), Group Call Reference (36bits), Channel Description (24 bits), Mobile Allocation (72 bits).
Note 6: Assumed that 80 bits available for P1 rest octets – fields included are NLN, Group Call Reference (36bits), Channel Description (24 bits)

With notification for one group call contained in two messages

4.1.1.Using existing message types

Logical Channel Type	Estimate of amount of space available for ciphering parameters
NCH	120 bits (7)
FACCH	114 bits (8)
PCH	38 bits (9)

Note 7: Assumed that 160 bits available for NT/N – fields included are NLN(2 bits), Group Call Reference(36 bits). Only one group call in list
Note 8: Assumed that 160 bits available for Notification/FACCH – fields included are message header (8 bits), Group Call Reference (36 bits).
Note 9: Assumed that 80 bits available for P1 rest octets – fields included are NLN, Group Call Reference (36 bits).

4.1.2.Using new message type for second message

Logical Channel Type	Estimate of amount of space available for ciphering parameters
NCH	120 bits (10)
FACCH	114 bits (11)
PCH	Not Possible

Note 10: Assumed that 160 bits available for notification information – fields included are NLN (2 bits), Group Call Reference (36 bits). Only one group call in message
Note 11: Assumed that 160 bits available for notification information – fields included are message header (8 bits), Group Call Reference (36 bits).

3GPP TSG GERAN #18 **GP-040181**
Reykjavik,Iceland **Agenda Item 7.2.5.4.7**
2nd – 6th February 2004
Source: Siemens

5.Conclusion

This paper has shown that it is possible to provide the additional ciphering parameters for a group call using either:

- Two instances of the existing message types, with second message omitting group channel description. This should be possible on the NCH, PCH and the FACCH
- One instance of the existing message types, with new message type for the second message. This should be possible on the NCH and the FACCH

The option of using the existing messages types is dependent on legacy MS's not supporting ciphered group calls, which is believed to be the case. This is the preferred solution as using new message types on the PCH will cause some degradation in performance of the paging channel as legacy MS will not be able to decode these blocks to read the page mode. The figures in section 4 suggest that by using a two block segmentation approach it should be possible to provide a RAND of 32 bits.