3GPP TSG SA WG3 Security — S3#33 **S3-040366**
10 - 14 May 2004
Beijing, China

3GPP TSG GERAN **TSGG#19(04)1210**
Meeting no 19 **Agenda Item: 7.2.5.4.7**
Cancun, Mexico
19th - 23rd April 2004

Title: **Reply to LS on 'Ciphering for Voice Group Call Services'.**

Response to: **LS on 'Ciphering for Voice Group Call Services'.**

Release: **Rel-6**

Source: **GERAN WG2**

To: **TSG SA WG3**

CC: **ETSI EP RT, TSG T WG3**

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

Attachments: GP-040181

Overall Description:

GERAN2 would like to thank SA3 for their LS on 'Ciphering for Voice Group Call Services' in Tdoc S3-030804.

GERAN2 has **considered the provision of the RAND, CGI and the global_count** and the conclusions are summarized below:

A. RAND

There is some space available in the notification channel (NCH) to carry additional information. However it should be noted that notifications are sent on the NCH, FACCH and PCH and all three cases need to be considered as the available space varies according to channel type. With the current structure of the notification message, the following amount of space (in bits) is available for the RAND:

Channel Type	Available Space (Without frequency hopping)	Available Space(With frequency hopping)
NCH	93	20
FACCH	89	16
PCH	16	0

NOTE: the above figures for the NCH are based on the notification/NCH message containing a description of one group call.

GERAN2 has studied the possibility of segmenting the description for one group call over two messages, as described in GP-040181. With this approach the following amount of space (in bits) is available for the RAND in the second message:

Channel Type	Available Space
NCH	120
FACCH	114
PCH	38

Nb The above figures are not dependent on the use of frequency hopping as the group channel description is not included in the second message.

It should be noted that the **NCH** may contain a **LIST of notifications**. The table below shows how many radio blocks (i.e. number of notification/NCH messages) that are required on the NCH as a function of number of ciphered group calls and size of RAND for the case that frequency hopping is used and that 72 bits are used to describe the frequency list.

	32 bit RAND	48bit RAND	64 bit RAND
1 group call	2 blocks	2 blocks	2 blocks
2 group calls	3 blocks	4 blocks	4 blocks
3 group calls	5 blocks	6 blocks	6 blocks
4 group calls	6 blocks	8 blocks	8 blocks
8 group calls	12 blocks	16 blocks	16 blocks

The above tables show that the number of radio blocks increases when the size of the RAND exceeds a certain threshold. This happens when it is only possible to include one RAND and associated group call reference in the second segment of the notification on the **NCH**. This occurs when the size of the **RAND** exceeds 40 bits.

Thus, with the introduction of this segmentation mechanism it is possible to provide a **RAND of up to 32 bits** in the notifications on the NCH, PCH and FACCH. Although the above tables show that it is possible to provide a 64-bit RAND on the NCH and FACCH, consideration must be given to the additional overhead on the air interface. **Thus GERAN2 recommends that a RAND of 32-bits is provided.**

B. CGI

It is possible to provide the **CGI** as an input parameter to the generation of the group cipher key.

When an MS performs a cell reselection it should read **the System Information 3 and 4** messages before accessing the cell. Both of these messages contain the CGI.

In the case of handover to another cell, the MS needs to be provided with the CGI **in the Handover Command** message. As this message can already be segmented over multiple radio blocks, the addition of the CGI should not be an issue.

C. Global_count

GERAN2 is still investigating mechanisms for providing the Global_Count.

GERAN2 would like to emphasise that the main issue in providing the above parameters is the amount of space available in the notifications, particularly when the notification is included in the Paging Request Type 1 on the PCH. The size of the RAND should be kept to a minimum in order to:

- **Avoid unnecessary segmentation of message and inefficient use of the radio resources**

Actions:

SA3: Please inform GERAN2 about the final decision regarding the provision of the RAND and CGI as VGCS ciphering parameters, such that the necessary CRs can be prepared.

Date of Next GERAN2 Meetings:

GERAN#19 bis	24th – 28th May 2004	Sophia Antipolis, FRANCE
GERAN#20	21st - 25th June 2004	Bilbao, SPAIN
GERAN#21	23rd – 27th August 2004	Montreal, CANADA

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.