3GPP TSG-CN Meeting #25 **NP-040329**
8th – 10th September 2004. Palm Springs, USA.

Source:	**Siemens AG**
Title:	**On CRs for TS 43.068 and 43.069 postponed due to dependencies to other WGs**
Agenda item:	**9.21**
Document for:	**APPROVAL**

CN1 have conditionally agreed two CRs for TS 43.068 and TS 43.069 on the Introduction of USIM based ciphering for VGCS and for VBS in N1-041547 and N1-041548, respectively.

There are dependencies to a CR for TS 43.020, which was conditionally agreed by SA3 and which itself has dependencies to a CR for TS 44.018 in GERAN2.Since the GERAN meeting took place the week after the CN1 meeting, CN1 chose the approval of the GERAN2 CR as condition for its own CRs. The coversheets of the CN1 CRs, however, indicate the relation to the CR to TS 43.020 only.

Now we have the situation that GERAN2 were not able to agree the related CR, but sent an LS to SA3 (GP-042284) that SA3 should go forward with the approval of their CR.

Quotation from GP-042284:

> **To SA3 group.**
>
> **ACTION:** GERAN2 recommends the approval of the SA3 CR in S3-040638.

It seems that GERAN2 do not see a problem if SA3's CR will get approved without having GERAN2's CR approved. Since the CN1 CRs only implement the requirements from SA3's CR in the stage 2 specifications TS 43.068 and TS 43.069, we think that there is no reason for not bringing the CN1 CRs to CN#25.

We would like to ask CN#25 to approve the CRs in N1-041547 and N1-041548 under the condition that the related CR in S3-040638 will be approved by SA#25.

3GPP TSG-GERAN#21 **Tdoc GP-042284**
Montreal, Canada, 23rd –27th August 2004

Title: **[Draft] LS on 'Ciphering for Voice Group Call Services'.**

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

Release: **Release-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: None

1. Overall Description:

GERAN2 would like to thank SA3 for their LSs on 'Ciphering for Voice Group Call Services' in Tdoc S3-030804 and 'Key Management of group keys for Voice Group Call Services' in Tdoc S3-040680. GERAN2 has **considered the provision of the RAND, CGI and the Global_Count** and the conclusions are summarized below:

A **RAND**

GERAN2 has already recommended in GP-041210 that a 32 bit RAND can be provided. However, SA3 has since recommended that a RAND of at least 36 bits and a 2 bit Cell Global Count should be provided (S3-040680). The main points to take into account when considering the provision of a larger RAND are:

- There are less than 40 bits available to provide additional fields in the Paging Request Type 1 message on the PCH even when the notification is segmented over two PCH blocks using extended paging
- The need to make efficient use of the NCH. In order to provide two RAND and two group call references per NCH block puts a restriction of the size of the additional information per call to be no more than 40 bits. These 40 bits have to include bits that are used to make the additional fields optional.
- Need for additional parameters in the notifications that is using the same resource as the RAND (eg 2 bit Cell Global Count)

When taking into account these restrictions, GERAN2 had determined that the size of the RAND can be a maximum of 36 bits. Whilst providing a larger RAND is feasible there would be the following consequences:

- Reduced opportunity for the use of the PCH to send notifications. The use would depend on the mandatory IEs occupying less space than their maximum size.
- On the NCH it may not be possible to include two RAND and two Group Call References per NCH block, thus resulting in greater usage of NCH blocks.

B **CGI**

GERAN2 has already recommended in GP-041210 that the CGI will be used as an input parameter to the generation of the group cipher key.

C **Global_Count**

GERAN2 has shown that it is possible to provide a Global_Count on the NCH, PCH and FACCH, as detailed in GP-041835. Since the resources are scarce on these channels, it is recommended that this field is kept as small as possible. It is suggested that no more than 2 bits are used for the Global_Count. GERAN2 has noted that this is inline with the proposed SA3 CR (S3-040638)

2. Actions:

To SA3 group.

ACTION: GERAN2 recommends the approval of the SA3 CR in S3-040638.

3. Date of Next TSG-GERAN Meetings:

GERAN#21 bis	4th - 8th October 2004 MALTA
GERAN#22	8th - 12th November 2004 South Africa

3GPP TSG-CN1 Meeting #35
Sophia Antipolis, France, 16-20 August 2004

Tdoc N1-041547
(rev of Tdoc N1-041452)

CR-Form-v7

CHANGE REQUEST

⌘ **43.068** **CR** **020** ⌘ **rev** **1** ⌘ Current version: **6.1.0** ⌘

*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 [X] Radio Access Network [X] Core Network [X]

Title:	⌘	Introduction of USIM based ciphering for VGCS
Source:	⌘	Siemens
Work item code:	⌘	TEI6 (SECGKYV)
Date:	⌘	26/07/2004
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:	⌘	Stage 2 requirement for VGCS ciphering is incompletely specified and wrong as it is based on a SIM.
Summary of change:	⌘	Introduce USIM based ciphering. Include the support of the USIM for non-ciphered calls.
Consequences if not approved:	⌘	VGCS Ciphering remains incompletely specified.

Clauses affected:	⌘	4.1, 4.2.5, 6, 7.3, 8.2.3, 8.2.3a, 9.1, 11.2

	Y	N			
Other specs Affected: ⌘	X		Other core specifications	⌘	43.020
		X	Test specifications		
		X	O&M Specifications		

Other comments: ⌘

How to create CRs using this form:
Comprehensive information and tips about how to create CRs can be found at http://www.3gpp.org/specs/CR.htm.
Below is a brief summary:

1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.

2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be

downloaded from the 3GPP server under ftp://ftp.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.

3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause containing the first piece of changed text. Delete those parts of the specification which are not relevant to the change request.

4 Main concepts

4.1 Group definition

Service subscribers can become group members on a PLMN wide basis to one or more groups pre-defined in the network by a corresponding group identification (group ID). The membership enables them to initiate or receive voice group calls associated with that group ID. Certain dispatchers connected to external networks also require the capability to initiate or receive voice group calls.

In addition to subscriber details in the HLR, it is necessary for the mobile station to be aware of its group membership by storing details on the SIM/USIM. This is required because it shall respond to notification messages which include only the group ID (i.e. no IMSI or TMSI details).

Having become a group member, each service subscriber can set to active state or deactive state the group ID or any one out of his several group IDs on the SIM/USIM. In active state the subscriber can initiate voice group calls to that group. When in deactive state the subscriber can not make voice group calls to the group and the mobile station ignores any notification for that group.

If no NCH is defined in the cell, mobiles shall assume VGCS service is not available on that cell.

4.2.5 Acknowledgements

The acknowledgement is an application option.

For voice group calls which are identified by an acknowledgement flag mobile stations which have acknowledgement facilities have to return an acknowledgement message with a predefined content in a predefined manner.

The acknowledgement shall be sent using an appropriate data service, to a predefined address or with a predefined short code stored on the SIM/USIM card. The network may apply geographical routing to a predefined acknowledgement service centre.

6 Compatibility issues

VGCS can not be used with standard Phase 1 or Phase 2 mobile stations. A dedicated mobile station with VGCS capability is required.

A mobile station with VGCS capability shall also provide the complete functionality in order to allow the use of Phase 2 services.

Standard Phase 1 and Phase 2 mobile stations in a network shall not be impacted by the presence of VGCS services in that network due to VGCS signalling, also if the mobile station is operated with a SIM/USIM of a VGCS service subscriber.

7.3 Data confidentiality

Data confidentiality on the radio can be provided as a network option.

If data confidentiality is provided, both the uplink and the downlink of the voice group call channels ~~in each~~ within a cell of the group call area shall be ciphered using voice group ciphering keys derived from the same group key, see 3GPP TS 43.020 [10].

The group key is related to the group ID. For each group ID, there is a number of group keys stored on the ~~SIM~~ USIM which are identified by a group key number. The group key number identifying the group key to be used for a particular

voice group call is provided with the notification to the mobile stations. Mobile stations which have a dedicated connection shall be informed of the group key number before they join the voice group call channel.

~~The distribution of the group keys to the related SIMs shall be done off line.~~

~~NOTE: The distribution of group keys shall be done by the service provider when editing the SIM. Distribution of group keys via the radio interface may be possible with future features as the SIM toolkit. Those distribution schemes are for further study.~~

USIM based VGCS ciphering uses a concept of short term keys where the short term key is derived by the GCR and the USIM from the group key and a RAND (random number) parameter. The actual voice group ciphering key is then derived by the BSS and the ME from the short term key, the cell global identifier, and a Cell Global Count parameter.

To include a subscriber into a voice group the required group data (including the 2 master group keys) shall be stored on the USIM, e.g. during the personalisation process or via OTA (over-the-air). To exclude a subscriber from a voice group the group data shall be deleted from the USIM. If a USIM is lost or stolen, all USIMs of the remaining members of the voice groups that this USIM is a member of need to be changed (e.g. via OTA or manual provisioning).

Details on data confidentiality for voice group calls are provided in 3GPP TS 42.009 [9] and 3GPP TS 43.020 [10].

NOTE: USIM based VGCS ciphering is not compatible with SIM based VGCS ciphering which has not been completely specified. The SIM specifications contain no support for the storage of the group keys. A pre-Rel-6 VGCS capable mobile station will be able to participate in an un-ciphered group call, if it is part of that group.

8 Information storage

8.2 Information managed per subscriber

8.2.3 Stored in the SIM

The information detailed in subclause 8.2.1 also needs to be stored on the SIM. The service subscriber shall be able to deactivate or reactivate a group ID by MMI interaction so that the mobile station ~~does~~ ignores notification messages to this group ID, when the group ID is deactivated.

~~For each group ID where data confidentiality may be applied, the SIM needs to store the cipher algorithm to be used and the possible group keys.~~

8.2.3a Stored in the USIM

The information detailed in subclause 8.2.1 also needs to be stored on the USIM. The service subscriber shall be able to deactivate or reactivate a group ID by MMI interaction so that the mobile station ignores notification messages to this group ID, when the group ID is deactivated.

For each group ID where data confidentiality may be applied, the USIM needs to store the cipher algorithm to be used and the possible group keys.

9 Identities

9.1 Elementary identities for group calls

a) Group ID

The group ID isa sequence of decimal digits with a maximum length depending on the composition of the group call reference defined under c). The length of Group ID shall be in a range of 1 to 6 digits.

The mobile station derives the group ID from the group call reference by identifying the longest group ID amongst those stored in the SIM/USIM and matching the least significant digits of the group call reference. If no group ID is stored in the SIM that matches the least significant digits of the group call reference, the mobile station is not able to derive the group ID from the group call reference.

NOTE 1: The network should use Group IDs matching an initial part of other group IDs with greatest care, if at all.

EXAMPLE: A mobile station storing the group IDs 678, 2 678 and 42 678 (and only those) in the SIM will derive group ID 2 678 from group call reference 13 452 678.

For definition of Group ID on the radio interface, A interface and Abis interface, see 3GPP TS 44.068 [11].

For definition of Group ID coding on MAP protocol interfaces, see 3GPP TS 29.002 [13].

11.2 Group membership management

Once the membership is established, the individual membership of the group can be placed in an active or deactive state on the SIM/USIM by the user. If a subscriber has a group ID in an active state, the subscriber is able to establish voice group calls corresponding to that group ID.

In a deactive state the mobile station prevents the service subscriber from establishing calls using the group ID and the corresponding notifications need to be "ignored" by the mobile station.

The active state and deactive state entries may be password protected as an implementation option.

Group IDs are listed in the subscription data within the network and on the SIM/USIM. The SIM/USIM must be returned to the network operator or service provider for updating if the subscription is to be changed.

NOTE: Updating of subscription data over the radio interface is not considered. However, this shall not preclude future applications if corresponding mechanisms may be implemented.

Users can interrogate their mobile stations to determine to which groups they are members and which subscriptions are currently in an active state.

3GPP TSG-CN1 Meeting #35
Sophia Antipolis, France, 16-20 August 2004

Tdoc N1-041548
(rev of Tdoc N1-041453)

CR-Form-v7.1

CHANGE REQUEST

⌘ **43.069** **CR** **014** ⌘ **rev** **1** ⌘ Current version: **5.3.0** ⌘

*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 [X] Radio Access Network [X] Core Network [X]

Title:	⌘	Introduction of USIM based ciphering for VBS
Source:	⌘	Siemens
Work item code:	⌘	TEI6 (SECGKYV)
Date:	⌘	06/08/2004
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:

Ph2	*(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)*
Rel-7	*(Release 7)*

Reason for change:	⌘	Stage 2 requirement for VBS ciphering is incompletely specified and wrong as it is based on a SIM.
Summary of change:	⌘	Introduce USIM based ciphering. Include the support of the USIM for non-ciphered calls.
Consequences if not approved:	⌘	VBS Ciphering remains incompletely specified.

Clauses affected:	⌘	4.1, 4.2.5, 6, 7.3, 8.2.3, 8.2.3a, 9.1, 11.2

Other specs affected: ⌘	Y	N		⌘	
	X		Other core specifications	⌘	43.020
		X	Test specifications		
		X	O&M Specifications		

Other comments: ⌘

How to create CRs using this form:
Comprehensive information and tips about how to create CRs can be found at http://www.3gpp.org/specs/CR.htm.
Below is a brief summary:

1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.

2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be downloaded from the 3GPP server under ftp://ftp.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.

3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause containing the first piece of changed text. Delete those parts of the specification which are not relevant to the change request.

4.1 Group definition

Service subscribers can become group members on a PLMN wide basis to one or more groups pre-defined in the network by a corresponding group identification (group ID). The membership enables them to receive voice broadcast calls associated with that group ID. In addition, certain group members are entitled by their subscription to initiate voice broadcast calls. Certain dispatchers connected to external networks also require the capability to initiate or receive voice broadcast calls.

In addition to subscriber details in the HLR, it is necessary for the mobile station to be aware of its group membership by storing details on the SIM/USIM. This is required because it shall respond to notification messages which include only the group ID (i.e. no IMSI or TMSI details).

Having become a group member, each service subscriber can set to active state or deactive state the group ID or any one out of his several group IDs on the SIM/USIM. In active state the subscriber can initiate voice broadcast calls to that group ID. When in deactive state the subscriber can not make voice broadcast calls to the group and the mobile station ignores any notification for that group ID.

If no NCH is defined in the cell, mobiles shall assume VBS service is not available on that cell.

4.2.5 Acknowledgements

The acknowledgement is an application option.

For voice broadcast calls which are identified by an acknowledgement flag mobile stations which have acknowledgement facilities have to return an acknowledgement message with a predefined content in a predefined manner.

The acknowledgement shall be sent using an appropriate data service, to a predefined address or with a predefined short code stored on the SIM/USIM card. The network may apply geographical routing to a predefined acknowledgement service centre.

6 Compatibility issues

VBS can not be used with standard Phase 1 or Phase 2 mobile stations. A dedicated mobile station with VBS capability is required.

A mobile station with VBS capability shall also provide the complete functionality in order to allow the use of Phase 2 services.

Standard Phase 1 and Phase 2 mobile stations in a network shall not be impacted by the presence of VBS services in that network due to VBS signalling, also if the mobile station is operated with a SIM/USIM of a VBS service subscriber.

7.3 Data confidentiality

Data confidentiality on the radio link can be provided as a network option.

If data confidentiality is provided, the downlink of the voice broadcast channels ~~in each~~ within a cell of the group call area shall be ciphered using broadcast group ciphering keys derived from the same group key, see 3GPP TS 43.020 [4].

The group key is related to the group ID. For each group ID, there is a number of group keys stored on the SIM which are identified by a group key number. The group key number identifying the group key to be used for a particular voice broadcast call is provided with the notification to the mobile stations. Mobile stations which have a responded to a notification shall be informed of the group key number before they join the voice broadcast channel.

~~The distribution of the group keys to the related SIMs shall be done off-line.~~

~~NOTE: The distribution of group keys shall be done by the service provider when editing the SIM. Distribution of group keys via the radio interface may be possible with future features as the SIM toolkit. Those distribution schemes are for further study.~~

USIM based VBS ciphering uses a concept of short term keys where the short term key is derived by the GCR and the USIM from the group key and a RAND (random number) parameter. The actual broadcast group ciphering key is then derived by the BSS and the ME from the short term key, the cell global identifier, and a Cell Global Count parameter.

To include a subscriber into a voice group the required group data (including the 2 master group keys) shall be stored on the USIM, e.g. during the personalisation process or via OTA (over-the-air). To exclude a subscriber from a voice group the group data shall be deleted from the USIM. If a USIM is lost or stolen, all USIMs of the remaining members of the voice groups that this USIM is a member of need to be changed (e.g. via OTA or manual provisioning).

Details on data confidentiality for voice broadcast calls are provided in 3GPP TS 42.009 [2] and 3GPP TS 43.020 [4].

NOTE: USIM based VBS ciphering is not compatible with SIM based VBS ciphering which has not been completely specified. The SIM specifications contain no support for the storage of the group keys. A pre-Rel-6 VBS capable mobile station will be able to participate in an un-ciphered group call, if it is part of that group.

8.2 Information managed per subscriber

8.2.3 Stored in the SIM

The information detailed in subclause 8.2.1 also needs to be stored on the SIM. The service subscriber shall be able to deactivate or reactivate a group ID by MMI interaction so that the mobile station ~~does~~ ignores notification messages to this group ID, when the group ID is deactivated.

~~For each group ID where data confidentiality may be applied, the SIM needs to store the cipher algorithm to be used and the possible group keys.~~

8.2.3a Stored in the USIM

The information detailed in subclause 8.2.1 also needs to be stored on the USIM. The service subscriber shall be able to deactivate or reactivate a group ID by MMI interaction so that the mobile station ignores notification messages to this group ID, when the group ID is deactivated.

For each group ID where data confidentiality may be applied, the USIM needs to store the cipher algorithm to be used and the possible group keys.

9 Identities

9.1 Elementary identities for broadcast calls

a) Group ID

The group ID is a sequence of decimal digits with a maximumlength depending on the composition of the broadcast call reference defined under c). The length of Group ID shall be in a range of 1 to 6 digits.

The mobile station derives the group ID from the broadcast call reference by identifying the longest group ID amongst those stored in the SIM/USIM and matching the least significant digits of the broadcast call reference. If no group ID is stored in the SIM that matches the least significant digits of the broadcast call reference, the mobile station is not able to derive the group ID from the broadcast call reference.

NOTE 1: The network should use Group IDs matching an initial part of other group IDs with greatest care, if at all.

EXAMPLE: A mobile station storing the group IDs 678, 2 678 and 42 678 (and only those) in the SIM/USIM will derive group ID 2 678 from BROADCAST call reference 13 452 678.

For definition of Group ID on the radio interface, A interface and Abis interface, see 3GPP TS 44.069 [11].

For definition of Group ID coding on MAP protocol interfaces, see 3GPP TS 29.002 [13].

b) Group call area ID

The group call area ID is a sequence of decimal digits uniquely assigned to a group call area in one network and with a maximum lengthdepending on the composition of the broadcast call reference defined under c).

c) Broadcast call reference

Each voice broadcast call in one network is uniquely identified by its broadcast call reference. The broadcast call reference is a concatenated sequence of the group ID (as the least significant part) and the group call area ID (as the most significant part). The broadcast call reference shall have a maximum length of 8 decimal digits. The composition of the group call area ID and the group ID can be specific for each network operator.

Group call area ID	Group ID

For definition of Broadcast Call reference (with leading zeros inserted as necessary) on the radio interface, A interface and Abis interface, see 3GPP TS 24.008 [14], 3GPP TS 44.018[7] and 3GPP TS 44.069 [11].

For definition of Broadcast Call reference coding (also known as ASCI Call Reference, Voice Group Call Reference or Voice Broadcast Call Reference) on MAP protocol interfaces, see 3GPP TS 29.002 [13].

11.2 Group membership management

Once the membership is established, the individual membership of the group can be placed in an active or deactive state on the SIM/USIM by the user. If a subscriber has a group ID in an active state, the subscriber is able to establish voice broadcast calls corresponding to that group ID if he is entitled for it.

In a deactive state the mobile station prevents the service subscriber from establishing calls using the group ID and the corresponding notifications need to be "ignored" by the mobile station.

The active state and deactive state entries may be password protected as an implementation option.

Group IDs are listed in the subscription data within the network and on the SIM/USIM. The SIM/USIM must be returned to the network operator or service provider for updating if the subscription is to be changed.

NOTE: Updating of subscription data over the radio interface is not considered. However, this shall not preclude future applications if corresponding mechanisms may be implemented.

Users can interrogate their mobile stations to determine to which groups they are members and which subscriptions are currently in an active state.