3GPP TSG SA WG3 Security — S3#31 **S3-030804**
18 - 21 November 2003
Munich, Germany

Title: **LS on 'Ciphering for Voice Group Call Services'.**
Response to: **--**
Release: **Rel-6**

Source: **SA3**
To: **GERAN 2**
CC: **ETSI EP RT, T WG3**

Contact Person:
Name: Marc Blommaert
Tel. Number: +32 14 25 3411
E-mail Address: Marc.Blommaert@siemens.com

Attachments: **S3-030692**

Overall Description:

SA3 has discussed a proposal for ciphering of VGCS calls (See attachment). In particular following four requirements were discussed:

REQ-1. Prevent the same ciphering key being used within different cells.

REQ-2. The VGCS Group-key shall never leave the USIM.

REQ-3. Prevent the reuse of COUNT with the same ciphering key within the same cell.

REQ-4. Prevent the same ciphering key being used in uplink and downlink direction.

SA3 have agreed that solutions for REQ-1 and REQ-2 need to be realized and have adopted the concept of a two-step key derivation approach (as described in section 3 of S3-030692) such that the A5 algorithms can be reused for VGCS ciphering without required modifications to input parameters. REQ-4 was already fulfilled by GSM while the A5 algorithms produce two different key streams for uplink and downlink. The acceptance of REQ-3 is pending within SA3.

Inputs on the feasibility of the proposed solutions (see attachment) for the above requirements are requested from GERAN 2.

Actions:

To GERAN 2:

GERAN 2 is kindly asked to provide feedback on

A) Whether the notification channel (which is used to inform the VGCS-mobile of upcoming or ongoing VGCS-calls) can carry additional information i.e. a RAND-value. The length of RAND is estimated as 32 to 64 bits, but its length has not been decided by SA3. SA3 would like to know if there exists a restriction on the amount of bits that can be added to the message on the notification channel which informs the VGCS-mobile of the VGCS-call.

B) Whether potential problems with the use of CGI at handover for the talker and at cell-reselection for the listener can be expected.

C) Impacts and feasibility of the solutions described in section 6 of S3-030692 and in particular on option D where a GLOBAL_COUNT, which length is estimated 4 to 8 bits, can be broadcasted to the VGCS-mobiles participating in a long-lasting VGCS call. It has to be clarified which channels shall be used for this. SACCH or FACCH could be candidates and their use should be evaluated. A requirement on the

solution is that ME and BSS keys shall not get out of synchronisation due to a different ‘modified short term key’.

Date of Next SA3 Meetings:

SA3#32	9 - 13 February 2004	TBC
SA3#33	11-14 May 2004	China (TBC)

3GPP TSG SA WG3 Security — S3#31 **S3-030692**
18 - 21 November 2003
Munich, Germany

Source: **Siemens, Vodafone**

Title: **Securing VGCS calls**

Document for: **Discussion and decision**

Agenda Item: **6.21 (Voice Group Call Services)**

1 Introduction

At the last SA3-meeting (SA3#30, 6.10.-10.10.03, Povoa de Varzim, Portugal) a scheme (S3-030559) was proposed which required minimal changes to existing specification and which based on parameters and messages which were already in place. However some limitations were mentioned during the discussion. This contribution proposes a different concept to secure GSM Voice Group Calls which has some similarities to TETRA. The paper starts with analysing requirements and describes the rationales to come to a stage-2 concept. Section 5, 6 and 7 contain the detailed proposal analysis and Section 8 revisits the working principles that were made by SA3#30.

2 Security requirements for ciphering of VGCS-calls

As also highlighted within contribution S3-030659 to this meeting, the security requirements to develop key management for VGCS are:

REQ-1. **Prevent the same ciphering key being used within different cells.**

This requirement protects an observer of getting more information on the plaintext if different data is enciphered with the same key and COUNT (TDMA-numbers derived) in different cells. A solution for this shall be found. Cell-unique identity information in the ciphering key calculation can be used for this without introduction much complexity. Solutions similar as those known by TETRA-specifications seem possible.

REQ-2. **The VGCS Group-key shall never leave the USIM.**

Even though VGCS users should be trusted, this approach protects the 'root'-key in the most secure way such that it need not be updated very frequently. If the VGCS Group-Key shall never (or only a few times) be updated then this is a must. A solution might be to use a broadcast of RAND-information to derive short-term keys from the master VGCS-key.

REQ-3. **Prevent the reuse of COUNT with the same ciphering key within the same cell.**

The COUNT value is determined by the TDMA frame number. An overflow happens after each 3 hour and 8 minutes period. The lifetime of the used ciphering key shall not be longer than the overflow period. A mechanism is needed to force ciphering key changes more often.

Possible solutions (The evaluation can be found in Section 6):

a. Perform a UE-individual over the air update of information that is used to derive temporary (a short term) keys. (This could be a TETRA-alike Key CCK).

b. Perform a broadcast of RAND-information to derive short-term keys from the master VGCS-key.

c. Switch between VGCS keys during the call and outside the call.

d. Maintain 'hyperframe' numbers for VGCS-calls i.e. maintain overflow counters and use them within the encryption.

It should be noted that this enhancement goes beyond the provided level of security of GSM-calls over a point to point channel (i.e. is not a VGCS-problem) as long standing calls over a dedicated channel have the same characteristic of reusing the COUNT. SA3 should decide if the proposed solutions are worth introducing after evaluating the complexity.

REQ-4. Prevent the same ciphering key being used in uplink and downlink direction (special case of REQ-3).

Solution: This requires a separate bit (either within COUNT or the pre-processing function of REQ-1) such that different ciphering for the uplink and the downlink voice group call channel is ensured.

Similar arguments as with REQ-3 can be brought forward. This goes also beyond the GSM-security.

SA3 should decide if it is worth protecting against REQ-3 if the security of a dedicated channel that is part of the group-call cannot be enhanced (i.e. REQ-4 on a dedicated channel can not be realized). Again the complexity of a solution will play a role in that decision.

3 Rationales and design constraints

A two-step approach is proposed in creating ciphering keys for VGCS channels. An evaluation of the parameters that shall be used is done in further paragraphs.

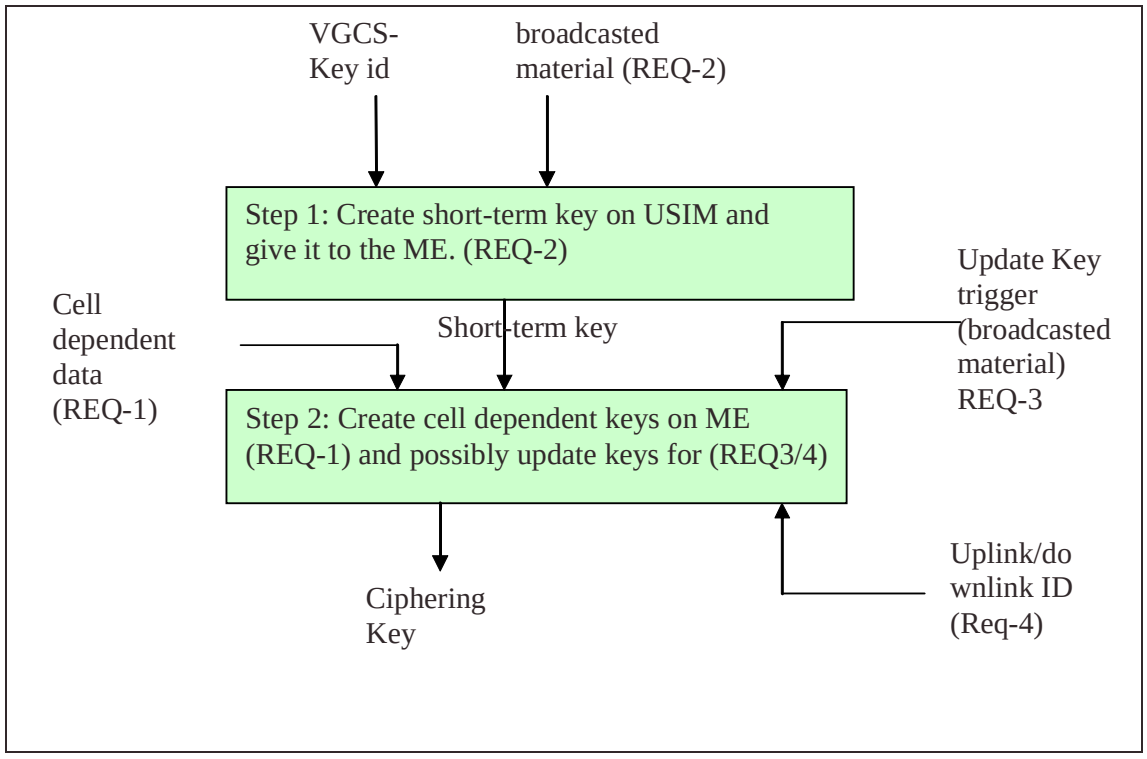

Figure 1:VGCS Key derivation steps from terminal viewpoint

1) A short-term key has to be derived on the USIM and parallel in the GCR (consequence of REQ-2 on group-key secrecy). This key will be modified further on by the ME to create cell dependent ciphering (REQ-1) or to counteract REQ3/4. From the GCR, RAND and short-term key need to be transported to the BSS.

2) The material to derive the short-term key on the ME needs not be secret. Broadcasted information may be used.

3) The short-term key does not need to be stored permanent on the USIM.

4) Late VGCS-entrants shall be allowed to initialise keys based on broadcasted information.

5) The creation of a short-term key on the USIM shall only be done at the moment when the mobile joins the VGCS call. A USIM based key generation takes some time. It might last some hundreds of milliseconds for an ME to get a new session-key. By restricting further key modifications to be applied only on the ME, we try to avoid effects on the received quality of the call during key changes. The second key-modification function on the ME can be executed much faster.

6) The use of OTA for updating VGCS group keys is optional for the operator. By using broadcasted information to derive short term keys on the USIM, the VGCS key value is not revealed to the ME. Therefore we see no requirement to have frequent OTA updates and to standardise interface for updating VGCS-keys to the GCR.

The above figure 1 describes how the solutions for REQ-1/2/3/4 may work together.

Note that the management of several group keys (on the USIM and in the GCR) isn't required any longer but is optional because the group key never leaves the USIM. One advantage of having more than one group key within a group is that the second key may be changed while the first one is being used and the specifications do not need to be touched (regarding this parameter).

4 Ciphering of CS-calls in GERAN A-mode.

This section gives an overview on how ciphering is applied to CS-calls in GSM (as is described in TS 43.020). The copied text has *italic* font.

Synchronization of ciphering between sender and receiver is guaranteed by driving Algorithm A5 by an explicit time variable, COUNT, derived from the TDMA frame number. Therefore each 114-bit block produced by A5 depends only on the TDMA frame numbering and the ciphering key Kc.

Following requirements need also be taken into account when a solution is evaluated.

- **The VGCS ciphering will only apply to voice group call channels (i.e. the pre-processing function is not needed for dedicated channels).**
- **The solution should be modulation agnostic. The concept should work also work in case EDGE modulation has to be applied.**
- **The A5 algorithms should not be modified (avoid requiring changed or added input parameters).**

C.1.1 Purpose

As defined in GSM 03.20, Algorithm A5 realizes the protection of both user data and signalling information elements at the physical layer on the dedicated channels (TCH or DCCH).

C.1.2 Implementation indications

Algorithm A5 is implemented into both the MS and the BSS. On the BSS side description below assumes that one algorithm A5 is implemented for each physical channel (TCH or DCCH).

The ciphering takes place before modulation and after interleaving (see GSM 05.01); the deciphering takes place after demodulation symmetrically. Both enciphering and deciphering need Algorithm A5 and start at different times (see clause 4).

COUNT is expressed in 22 bits as the concatenation of the binary representation of T1, T3 and T2. It is an input parameter of Algorithm A5. The coding of COUNT is shown in figure C.1.

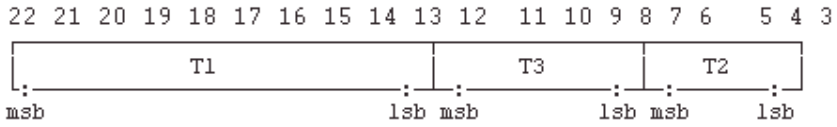

Figure C.1: The coding of COUNT

Binary representation of COUNT. Bit 22 is the most significant bit (msb) and bit 1 the least significant bit (lsb) of COUNT. T1, T3 and T2 are represented in binary. (For definition of T1, T3 and T2, see GSM 05.02).

Figure C.2 summarizes the implementation indications listed above, with only one enciphering/deciphering procedure represented (the second one for deciphering/enciphering is symmetrical).

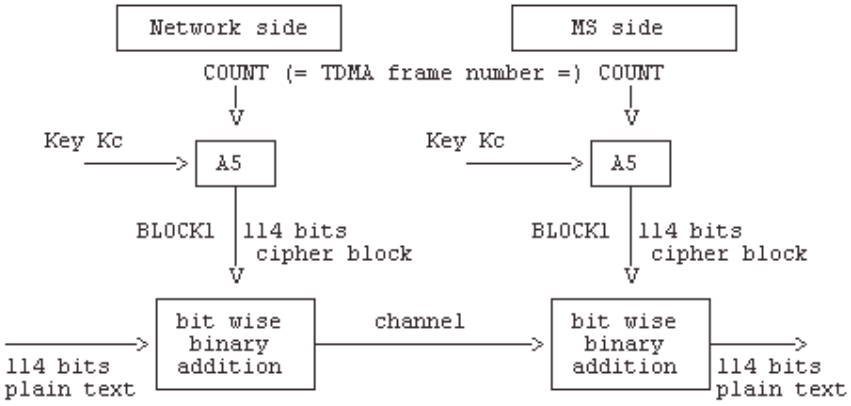

Figure C.2: Deciphering on the MS side

C.1.5 A modification of the usage of A5 for EDGE

In EDGE the block size is greater than 114 bits. With EDGE a modification of the usage of the A5 algorithm is employed which produces BLOCK 1 and BLOCK2 which each contain 348 bits. The other parameters are not modified. The modified algorithm produces both blocks during a TDMA frame duration, i.e. 4.615 ms. The blocks are combined by bitwise modulo 2 addition with the plaintext data as explained in C.1.2.

It is possible in EDGE that the plaintext data block for either uplink or downlink is shorter than 348 bits. In this case only the first part of the corresponding output parameter BLOCK is used in the bit-wise adition and the rest of the bits are discarded.

5 Solutions for REQ-1

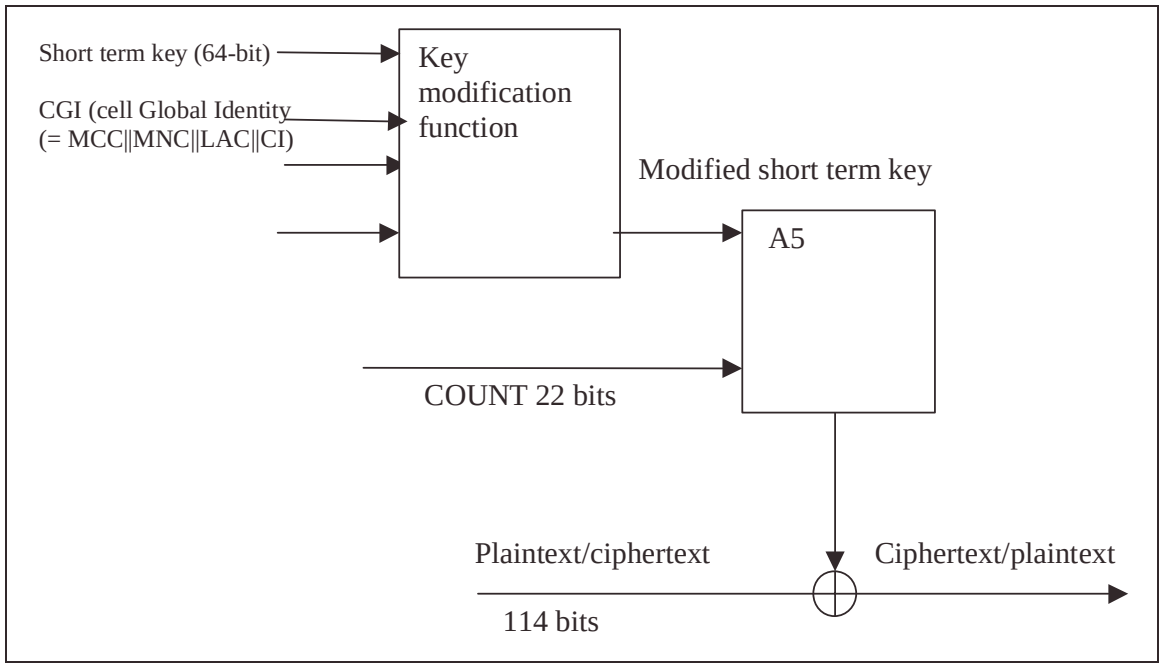

Figure 2: Proposed ciphering for VGCS calls (REQ-1)

The assumption in the above figure is that a 64-bit key is available as input to a key derivation function as currently only 64-bit keys are used for ciphering at the A-interface. But the function could also be designed to support 128 bit keys for use with e.g. A5/4 later on.

The key modification function may be a known Hash algorithm (e.g. HMAC-SHA-1) but also simpler functions might be suitable similarly as used for HSCSD (TS 43.020 section 4.2)

Overview and evaluation of required extra input parameters[1]:

Currently there are two options for suitable input material:

1) CGI (Cell Global Identity) (Preferred Option, since it provides a world-wide unique identifier)

CGI= LAI + CI ; CI is unique within a location area. CGI is a unique world wide identifier

Note: CGI is part of the system info 3 message, a mobile needs to receive system info 3 or 4 before it can enter a Cell, if it changes cell after reception of system info 4 before receiving system info 3. System info 3 is one of the first messages it will receive when it is in the new cell. GERAN 2 may have to confirm if the mobile can determine the CGI (all of its required components) of a cell in time for a ciphering change when switching between cells both for uplink and downlink. If the answer is yes than CGI is a suitable input parameter. Otherwise the choice on input parameters shall be restricted to those that can be uniquely determined.

2) BSIC (= LAC || BCC) (If CGI-solution would not be possible)

– LAC (Location Area Code)

LAC has a fixed length of 2 octets. This is only unique within an operators network. To form a unique location area identification world wide, MCC (Mobile Country Code – three digits) and MNC (Mobile Network Code- two or three digits) shall be added. LAI= MCC+MNC+LAC. Note that MCC and MNC are identities for the network one is roaming in and is not to be distinguished with the MCC and MNC of the own IMSI.

– BCC (Base Station Colour Code)

BCC is 3 bits long. It allows an MS to distinguish between neighbouring base stations. The Base Station Identification Code (BSIC) is formed by adding NCC (3 bits PLMN colour code) to it. In each cell the BSIC is broadcast in each burst sent on the SCH. This allows the mobile to determine the BSIC of a target cell during initial synchronisation.

---

1 Most parameter description can be found within TS 03.03

6 Solutions for REQ-3

Different solutions are possible. This section evaluates the alternatives.

A) Perform a UE-individual over the air update of information that is used to derive temporary (a short term) keys. (This could be a TETRA-alike Key CCK)

Evaluation: This requires that separate procedures to the ME shall be standardized for updating keys over a secure channel. This will cause a lot of impacts.

B) Perform a broadcast of RAND-information to derive short-term keys from the master VGCS-key on the UICC.

Evaluation: There is less impact then alternative A, but frequent UICC access shall be avoided as it would require complex solutions to avoid effects on received voice quality.

C) Switch between VGCS keys during the call and outside the call.

Evaluation: Frequent OTA updates will be needed to refresh the keys in the USIM. The new keys may be sent in batches to reduce the frequency of the required OTA updates. A USIM-access is required for each switch between VGCS-key. Mechanism to trigger frequent key switching, involving the USIM are needed. Ensuring that this switch is co-ordinated between all members of a large geographically spread group of users may be very complex.

D) Maintain 'hyperframe' numbers for VGCS-calls → maintain overflow counters and use them within the encryption.

Several options exist: Overflow counters or global-COUNT need to be inputted into the ciphering key modification function. Overflow counters have to be maintained per cell as they are bound to the TMDA-frame number which is not supposed to be synchronised between the cells. A global-COUNT solution assures that key re-use is prevented when the change is triggered each 3-hours. The global-COUNT can be maintained by the GCR and broadcasted to the mobiles for use as input to the key modification function.

It has to be clarified which channels shall be used for this. SACCH or FACCH are candidates and its use shall be evaluated. The FACCH is fast and steals packets from the voice stream. The SACCH is slower but has no impact on the speech quality. A decision should be made by GERAN 2. In addition the synchronisation of key exchange (in the ME and in the BSS) shall be guaranteed.

E) Stop the call after three hours and perform a new call setup.

Solution D looks most attractive provided that the appropriate channels can be found to broadcast the information in a reliable way such that the chance for wrong decryption at the receivers' side is minimal when GLOBAL-COUNT is updated. Also Solution E seems worth studying when solution D gets too complex.

As noted before, this enhancement goes beyond the provided level of security of GSM-calls over a point to point channel (i.e. is not a VGCS-problem) as long standing calls over a dedicated channel have the same characteristic of reusing the COUNT. SA3 should decide if the proposed solution to REQ-3 is worth introducing after evaluating the complexity. Input from GERAN-2 is needed for this.

7 Solutions for REQ-4

A direction bit need to be introduced: Value 1 for uplink, value 0 for downlink. (this parameter addresses REQ-3). Similar as with REQ-3 this enhancement goes beyond the provided level of security of GSM-calls over a point to point channel.

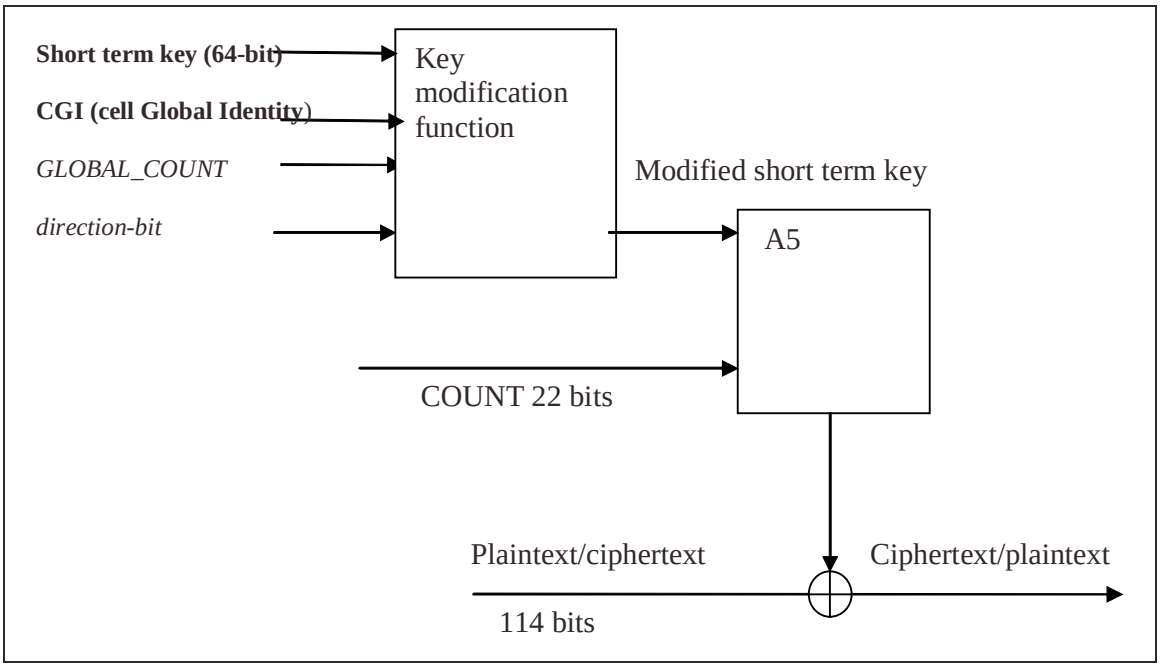

Figure 3: Proposed ciphering for VGCS calls (all requirements addressed)

8 Review of proposed principles from LS 030639

The original text is in blue. Remarks and proposed changes are in black. It is proposed that SA3#31 adopts following changes to the principles (when highlighted with change bars):

Following principles were agreed by SA3#30:

A) For each voice group up to 15 group keys per group can be defined (identified by a group key number).Note: The maximum number of group keys per voice group is determined by the available number of bits in the radio access network to signal a key identifier to the UE.

Comment: No changes required.

B) The group keys are stored in

- the group call register (GCR) on the network side (which is co-located to an MSC),
- USIM application of the UICC on the UE side.

Comment: No changes required.

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

Comment: Changes required as the Group Key will not leave the UICC and GCR.

Proposed new text: On call set-up the GCR selects one group key, generates a temporary key with a RAND and sends the temporary key~~it~~ to the BSS and the group key number and RAND to the UE. The UE then asks the UICC to generate a temporary key based on the group key number and broadcasted information (RAND). ~~which fetches the corresponding key from the USIM.~~

D) A key management centre (KMC) takes care that the group keys are up to date at all locations and are exchanged from time to time (which is up to the operator's policy).
Note: It was recognized that the keys shall be refreshed frequently enough. A study is needed to determine an appropriate key refresh rate.

Comment: In the proposed concept there is no need to have a key management center as the Group-Key will not leave the UICC. The appropriate refresh is achieved by using temporary keys.

It is proposed to delete that principle.

E) The same algorithms are used for encryption of VGCS-calls as for normal GSM-speech calls (i.e. A5/0-A5/7).

Note: It was recognized that the keys shall be refreshed frequently enough. A study is needed to determine an appropriate key refresh rate.

Comment: A key modification concept was proposed such that the GSM speech call ciphering algorithms can still be used without changing the format of input and output values.

It is proposed to delete the note and to add following text: Any requirement for modification of the input parameters to A5 shall be achieved using a separate Key Modification Function (KMF). How this function is realized is currently under study.

Following principles need further investigation:

F) It is for further study whether the KMC is out of scope of 3GPP specification.

Comment: As the concept requires no KMC, the principle is of no relevance any more.

G) It is for further study whether the interface between KMC and the GCRs needs to be standardized.

Comment: As the concept requires no KMC, the principle is of no relevance any more.

H) It is for further study whether the interface between the KMC and the USIM needs to be standardized by 3GPP. The use of OTA techniques has been suggested.

Comment: There is no need to frequently update the VGCS-keys with the current concept. The proposed concept does not exclude the use of OTA.
Proposed principle: The use of OTA for updating VGCS group keys to the UICC is optional for the operator.

I) It is for further study how the UE gets the information which cipher algorithm is used for a group call. One option is to signal the cipher algorithm via the air-interface. Another option may be to store it on the USIM together with the group key.

Comment: the status is unchanged.

9 Conclusion

It is proposed

1) To agree that REQ-1 and REQ-2 need to be realized.
2) To discuss and decide if SA3 wants a solution for realizing REQ-3 and REQ-4 as this enhances VGCS call channel security above dedicated channel security.
3) To wait for agreeing a solution for realizing REQ-3 and REQ-4 as inputs from GERAN 2 are needed to evaluate complexity and feasibility.
4) To adopt the two-step approach and rationales from section 3 as a working assumption.
5) To inform ETSI EP RT (GSM-R) on the progress of the discussions.
6) To ask T3 to realize the needed functions on the USIM.
7) To ask SAGE to select suitable key derivation/modification functions for both ME and UICC after deciding the input and output parameters. Minimal length of RAND should be requested.
8) To decide whether all VGCS network interfaces and key derivation/modification functions shall already be able to support 128-bit cipher keys although no A5 cipher algorithm are yet in the field that support 128-bit keys. At least the key modification/derivation functions should be able to handle 128-bit keys for the input and output parameters.
9) To inform GERAN2 about the above decisions (bullet point 2 and 8) and ask them for commenting a) if potential problems with CGI at handover can be expected and b) to select the right mechanism for broadcasting a RAND, GLOBAL_COUNT to generate the short term key from.

Annex A: Comparison table (TETRA, 3GPP2-MBMS, VGCS) and TETRA solution.

This section is for information and compares roughly the key management solutions for applying protection to multicasted data.

	MBMS- 3GPP2	TETRA	VGCS
Master Key Name	BAK	GCK (Group Call Key)	Group-Key
Where stored	BM-SC, USIM	Network, UE GCK may be updated over the air protected by user individual signalling.	GCR, USIM
Session Key Name	SK	MGCK (Modified Group Cipher Key)	Short Term Key
Purpose of protection	Protect streaming data.	Protect group addressed signalling and traffic.	Protect calls addressed to the VGCS-group.
How to derive a short-term key (or session key)	F(SK_RAND, BAK) = SK	F (CCK, GCK) = MGCK[2]	T.B.D (USIM-proposed key derivation function). A function on the ME for further key modifications
Frequency of Key derivation	SK_RAND is transmitted together with the streaming data.	CCK is updated over the Air. Frequency is determined by the operator.	A cipher key update is required to prevent COUNT-reuse each 3 hours.
Requirement for session key	High frequency of SK_RAND in order to create high workload for fraudsters	Before IV reuse occurs	Prevent the COUNT reuse with the same key within the same cell and the same key in different cells.
Trust model	MBMS users cannot be trusted	TETRA users can be trusted (administrated closed user group)	VGCS users can be trusted (administrated closed user group)
Background documents	S3-030xxx	ETSI EN 300 392-7 V2.1.1 (2001-02)	S3-030559

[2] **Modified Group Cipher Key (MGCK):** cipher key known by the infrastructure and MS to protect group addressed signalling and traffic that is composed algorithmically from either CCK and GCK, or SCK and GCK

The TETRA encryption mechanism works as follows:

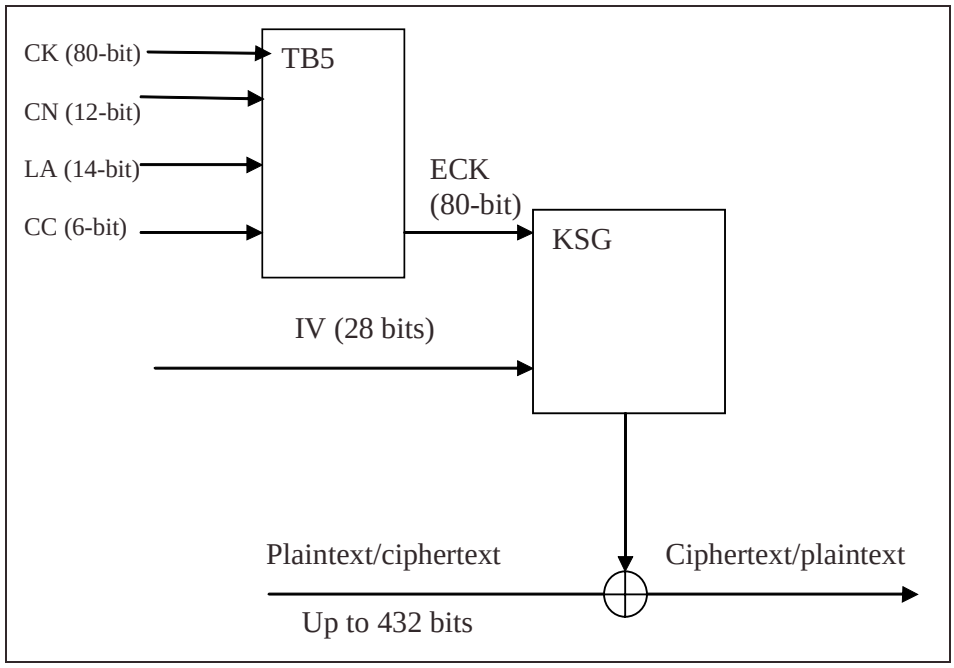

Figure 4: TETRA ciphering According to ETSI EN 300 391-7 v2.1.1 (2001-02) section 6.3

Italic text is a copy from the TETRA-specification:

"CN of the main carrier, CC, LA-id, and initialising values of IV are received at the MS from the BS broadcast signalling messages. After initialization IV is locally generated at the MS. When camped on a cell CN values are received at the MS from downlink MAC-RESOURCE and MAC-END PDUs. IV is locally generated at the BS."

TB5 and KSG are (non-public) TETRA algorithms.

CN is a carrier number (Would correspond with bearer identity ?)

Initialization Value (IV): sequence of symbols that initializes the KSG (key stream generator) inside the encryption unit. IV takes the slot, frame and multiframe and hyperframe number into account. One bit is used to distinguish uplink transmissions from downlink transmissions. The IV as used for TETRA is therefore equivalent with COUNT used for GSM. COUNT in GSM is 22-bits long and derived from the TDMA-frame number. The CK in figure 2 is the Modified Group Call Key of the table in this section. This short life time key is modified frequently.

" The value of hyper-frame (IV(13) to IV(27)) shall be broadcast to a schedule determined by the SwMI with the value of CCK-id on cells of security class 3, and with the value of SCK-VN in cells of security class 2, in the SYSINFO broadcast."