3GPP TSG SA WG3 Security — S3#32 **S3-040181**
9 –13 February 2004
Edinburgh, UK

Title: Reply LS on 'Status of VGCS work in SA3'
Release: 6
Work Items: Key Management of group keys for Voice Group Call Services

Source: 3GPP SA3
To: T3
Cc: ETSI EP RT, GERAN2

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

Attachment: S3-040025

Overall description:

SA3 would like to thank T3 for their response LS on 'Status of VGCS work in SA3' in Tdoc T3-040125 (S3-040173).

SA3 have discussed the T3 questions and can provide following answers:

1/ Is there an SA3 specification that will provide an external description of the algorithm to run in the UICC for derivation of the short-term VGCS key that we could refer to, or is there an assigned name that T3 could use in its specification to refer to this algorithm?

Answer: SA3 may ask ETSI SAGE to select or specify an algorithm to derive the short term VGCS key. ETSI SAGE has not been asked yet as certain parameters lengths have still to be confirmed by GERAN2.

2/ Can SA3 confirm the length of the keys (current understanding is 128 bits) and of the random number (32 bits?) to be used in the VGCS context?

Answer: The 128 bit-length of the VGCS keys (the VGCS group key on the UICC and the short term key that leaves the UICC) can be confirmed. To determine the length of the random number, SA3 is awaiting the analysis results of GERAN 2. Initial GERAN2 analysis indicates certain radio interface impacts to accommodate a 32-bit RAND. SA3 does expect that the RAND will not be longer than 64-bit.

3/ The T3 specification today provides storage for up to 50 VGCS groups that the user may be subscribed to. Can SA3 indicate whether there is any intended relationship between the VGCS Group key identifiers and the VGCS groups that a user is subscribed to? I.e. is it 15 keys for each of the up to 50 groups?

Answer: The voice group keys are voice group specific, i.e. different voice groups will have different sets of group keys. SA3 can confirm that there is no need anymore to store 15 VGCS-keys per VGCS group. Two keys per VGCS group shall be stored.

4/ Can SA3 confirm that the Group keys should preferably be updatable by OTA, while the UICC does not need to provide storage for the derived short-term keys?

Answer: SA3 can confirm that there is not need to store the short-term keys on the UICC. The current SA3 working assumption is that the use of OTA for updating the VGCS group keys is optional.

SA3 would be happy that T3 already starts the analysis based on the above provided information. SA3 will inform T3 of the decisions that will be made at SA3#33.

SA3 would also like to inform T3 that SA3#32 did decide to store the Algorithm Identifier for ciphering VGCS calls on the UICC (solution 1 of the attachment).

ACTION:

3GPP SA3 kindly asks T3 to take into account the above provided answers.

Date of Next SA3 Meetings:

SA3#33	10 - 14 May 2004	Beijing
SA3#34	5 – 9 July 2004	Tbd, NA Friends of 3GPP
SA3#35	4 – 8 October 2004	tbd

3GPP TSG SA WG3 Security — S3#32 **S3-040025**
9.-13. February 2004
Edinburgh, UK

Source:	**Siemens, Vodafone**
Title:	**Securing VGCS calls: signalling the encryption algorithm indicator**
Document for:	**Discussion and decision**
Agenda Item:	**VGCS: 6.21**

1 Introduction

As described within S3-030692 (SA3#31) it is still open how the ME is informed which encryption algorithm should be used (ref. S3-030692 sec. 8 lit I) for securing the VGCS call. This contribution discusses and evaluates two possible solutions after having described the assumptions and requirements.

2 Assumptions and requirements

2.1 Assumptions

Assumption 1: *There shall be no negotiation of encryption capabilities between the network and VGCS listeners*.

Currently for VGCS there is no negotiation of encryption capabilities for pre-rel6 ME. Since an ME can join a voice group call as listener without being recognised by the network, it would add a lot of new functionality (in terms of new protocols, new messages, etc.) to provide a mechanism for negotiation of encryption capabilities. Moreover the situation would get very complicated if an ME with different encryption capabilities enters a cell where a voice group call already takes place.

Assumption 2: *The administrator of a voice group call knows the terminal capabilities of its group. (The administrator of the group has access to GCR and the USIM in order to define a group and administrate some parameters).*

Since the members of a voice group (e.g. police, fire brigade, taxi company) are well known to the administrator of the group and probably equipped with special ME tailored to their special needs, the administrator should know which types of ME are used (or are released for use) and their respective encryption capabilities.

Assumption 3: *The administrator of a group is aware of the encryption algorithm which might or might not be supported within areas of the networks which are relevant for its voice group.*

Since the administrator defines the area in which its voice group shall take place he can ask the network operator which encryption algorithm are supported.

Assumption 4: *Not every BTS within a network might support the same set of encryption algorithm.*

Due to the fact that the roll out of new encryption algorithms (e.g. A5/3) depends on the manufacture and the (hardware) capabilities of the BTS, situations may arise where there exists an heterogeneous supports of ciphering algorithms within the radio network.

2.2 Requirements

Requirement 1: A voice group call should use the strongest possible encryption algorithm and should be able to avoid the use of weak algorithms.

This requirement is not only applicable for VGCS call but also for normal CS calls.

Requirement 2: The standardisation and implementation complexity should be kept as low as possible.

Requirement 3: The mechanism should provide protection against already known attacks like the attack against A5/2.

3 Solutions

Two possible solutions are discussed in this paper:

1. Store the encryption algorithm indicator together with the VGCS-key on the USIM.

Together with the encryption key used for voice group calls exactly one encryption algorithm identifier is stored on the USIM. If a voice group takes place the ME reads the corresponding information from the USIM and uses the indicated algorithm. On the network side the GCR signals the algorithm identifier via the anchor MSC and the relay-MSC to the BSS. To store a set of algorithms make no sense since the ME wouldn’t know which one to select.

2. Signal the encryption algorithm indicator on the air-interface.

The GCR signals the list of encryption algorithm which are supported by the MEs of the voice group via the anchor MSC and the relay-MSC to the BSS. The BSS selects the strongest algorithm which is supported by the BTS and (all members of) the voice group. The BSS signals the selected algorithm to the ME over the air interface. This will require changes to NCH, PCH and NACCH in addition to modifications required to accommodate space for the RAND.

4 Evaluation

1. Strength of selected algorithm

Solution 1: In all cells the same algorithm shall be used since there is exactly one algorithm stored on the USIM. This algorithm can be the strongest one which is supported by all MEs of the group and by **all** BTS in which the voice group may ever take place. As long as there is at least one BTS in the area of the network (in which the group call may take place) which doesn’t support a certain algorithm this algorithm cannot be used by any ME and within any cell. (The same is true for an algorithm which isn’t supported by at least one ME).

Solution 2: The selected algorithm may vary from cell to cell. The algorithm used within a BTS can be the strongest one which is supported by all MEs of the group and by **that** BTS. E.g. if all MEs of the members of a group supports A5/1-A5/3, A5/3 can be used in BTS which has already implemented A5/3. BTS which are not capable of A5/3 can use A5/1.

2. Standardisation and implementation complexity

Solution 1: New mechanism for reading the algorithm-identifier from the USIM shall be specified. However, since the interface between ME and USIM shall be changed anyhow, this is just a minor change with respect to the other required enhancements for VGCS. (See S3-030559 sec 3.1.3 – 3.2 for a proposal).

This solution would be inline with current stage 2 for VGCS (43.068) which already states that the cipher algorithm is stored on the 'SIM' and in the GCR.

Solution 2: The interfaces between anchor-MSC and relay-MSC and between relay-MSC and BSS already contains a transport mechanism of the encryption algorithm identifier. However the message shall be adapted slightly (in order to transport a list of algorithms from the anchor-MSC to the –relay-MSC instead of a single algorithm id (see S3-030559 sec 2 for details).

The cipher mode IE is already present in the Handover Command. However, the specification currently states that this IE is not applicable to VGCS (probably because the algorithm for VGCS is stored on the SIM). Thus some changes are needed to 44.018.

3. Protection against man in the middle attacks

Both solutions provide protection against man-in-the middle attacks since there is no negotiation of the algorithm.

5 Conclusion and proposal

Both solutions seem suitable for the selection process of the encryption algorithm and do not require high implementation efforts. Solution 2 has the advantage that it provides the ability to select a stronger algorithm which is not yet introduced in all group areas of the network, but at the expense of minor extra impacts in the network and on the air interface (i.e. extra changes to NCH, PCH and NACCH in addition to the modifications required to accommodate space for the RAND seems needed).

Therefore it is proposed that

- SA3 selects solution 2 as preferred mechanism for encryption algorithm selection. If GERAN2 identifies problems with solution 2, solution 1 is selected.
- SA3 sends an LS is to GERAN2
  - to ask if the expected extra air interfaces changes are indeed minor
  - to ask if there is still enough space in the messages.