3GPP TSG SA WG3 Security — S3#34 **S3-040496**

July 6 - 9, 2004

Acapulco, Mexico

Source: **Siemens, Vodafone**

Title: **VGCS: Considerations on key generation and key modification.**

Document for: **Discussion and decision**

Agenda Item: **VGCS**

1 Introduction

This contribution takes into account the GERAN2 documents G2-041414 and G2-041415, as well as the SAGE LS to SA3 (S3-040471), and makes a selection between the different alternatives for VSTK_RAND, GLOBAL_CELL_COUNT and KMF. It proposed that the exact construction of VSTK_RAND into a counter and a RAND part is not standardized as this only affects the Core Network Entity that generates the RAND and not the UICC and the Radio network.
Unfortunately, GERAN2 was not able to discuss the above GERAN#2 documents during GERAN#20 (21 – 25 June) due a lack of time. There will be an e-mail discussion on the GERAN#2 reflector on this topic in order to prepare for GERAN2#21-decision, which takes place 24 - 26 Aug 2004.

2 VSTK_RAND[1]

The text in this section assumes that GERAN#2 approves the G2-041415 proposal that results in the availability of 40-bits in total for VSTK_RAND. However also some considerations are included in case only a 38-bit VSTK_RAND could be used.

Looking at following summarized SAGE table (based on the LS) the '**more structured RAND'-proposal** has the interesting property that the total number of calls (under a fixed collision probability) that can be made with the same V_Ki is much higher with a bigger counter part.

Total challenge length	Length of counter	Length of random part	Max collision prob for fixed V_Ki	Corresponding max collision prob for one fixed counter	Number of calls for one fixed counter	Total number of calls for fixed V_Ki
40	0	40	10^{-6}	1.00×10^{-6}	1483	1483
40	16	24	10^{-6}	1.53×10^{-11}	1	65536

The counter part needs only be implemented within the network (at the GCR side) per V_Ki and group-id and does not affect other VGCS-entities. As it was already suggested by SAGE within their analysis of the full random RAND, that a mechanism (e.g. based on counter) would anyhow[2] be needed to warn the operator if a threshold is approached.

[1] In this section it is assumed that no cell_global_count bits are needed. 40 and 38 have to be interpreted as the total amount of available bits.

[2] SAGE quotation: *"**we recommend that implementations include an internal counter to monitor how many calls have been made with a given V_Ki, and to require or at least prompt the operator to update V_Ki when the appropriate threshold is approached**."*

As a future threat assessment might give a different view on the proposed security margins (i.e. the 24-bit) we suggest that the available SAGE information is put into an informal Annex of TS 43.020 and that the structure of the VSTK_RAND is an operator specific decision.

If only 38-bits would be available for VSTK_RAND (in case G2-041415 proposal on GCRef would not be accepted by GERAN#21) this would result in following table

Total challenge length	Length of counter	Length of random part	Max collision prob for fixed V_Ki	Max collision prob for one fixed counter	Number of calls for one fixed counter	Total number of calls for fixed V_Ki
38	0	38	10^{-6}	10^{-6}	741	741
38	14	24	10^{-4}	6.10×10^{-9}	1	16384

Conclusions:

1) The '**more structured RAND'** not only realizes the possibility of checking against a threshold very easily but also allows to safely set-up more ciphered VGCS-calls
2) The table shows that both a VSTK_RAND of 40 and 38 bits provide a sufficient amount of VSTKs (and security) when the VSTK_RAND is generated according the suggested counter scheme.

3 CELL_GLOBAL_COUNT

The text in this section assumes that GERAN#2 approves the G2-041414 proposal on CELL_GLOBAL_COUNT.

The provision of CELL_GLOBAL_COUNT provides a solution to Requirement-3 of S3-040427:

> "*Prevent the reuse of COUNT with the same voice group or broadcast group 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 cipher key shall not be longer than the overflow period.*
>
> *NOTE: This enhancement goes beyond the provided level of security of GSM-calls over a point to point channel (i.e. is not a VGCS/VBS-problem only) as long standing calls over a dedicated channel have the same characteristic of reusing the COUNT."*

The proposed CELL_GLOBAL_COUNT length at SA3#33 [S3-040427] was 4-bit. This would allow extending a group call to 50-hours without repeating the key stream. As was indicated by ETSI SAGE, the more RAND-bits that are available, the more VSTK can be generated before the V_KI needs to be exchanged.

The table below gives the number of VSTK's that can be generated with different CELL_GLOBAL_COUNT length's. This table is based on the assumption that VSTK_RAND length of 40-bits is taken with a minimum random part of 24-bits and a maximum collision probability of 10^{-6}.

	Total number of calls for fixed V_ki	Max call duration before key stream reuse occurs.
No CELL_GLOBAL_COUNT	40= (16+24) → 65536 calls	3 hours
CELL_GLOBAL_COUNT=2-bits	38= (14+24) → 16384 calls	12,5 hours
CELL_GLOBAL_COUNT=3-bits	37= (13+24) → 8192 calls	25 hours

CELL_GLOBAL_COUNT=4-bits	36= (12+24) → 4096 calls	50 hours

The table below is based on the assumption that VSTK_RAND length of 38-bits is taken with a minimum random part of 24-bits and a maximum collision probability of 10^{-6}.

	Total number of calls for fixed V_ki	Max call duration before key stream reuse occurs.
No CELL_GLOBAL_COUNT	38= (14+24) → 16384 calls	3 hours
CELL_GLOBAL_COUNT=2-bits	36= (12+24) → 4096 calls	12,5 hours
CELL_GLOBAL_COUNT=3-bits	35= (11+24) → 2048 calls	25 hours
CELL_GLOBAL_COUNT=4-bits	34= (10+24) → 1024 calls	50 hours

As indicated by document G2-041414 there are some cases where the VGCS-mobile needs to check the CELL_GLOBAL_COUNT value against the TDMA number. One conclusion is that the Requirement-3 can be satisfied but it introduces additional overhead on the air-interface and more complex handling in the radio-network and the VGCS-Mobile. A CELL_GLOBAL_COUNT length of 2 bits should be sufficient for most calls. Longer CELL_GLOBAL_COUNT length would have a disadvantage that the total number of calls is reduced too much such that the operator is forced to changes the V_Ki more frequently. For these usecases where the VGCS-ciphered call-duration would lie anyhow (lets say 99,9%) within the boundary of the 12,5 hours this would even mean a disadvantage.

Conclusion:

Even under the assumption of a maximum of 38-bits and 2 CELL_GLOBAL_COUNT bits, the totals amount of VGCS call with one V_Ki seems to be acceptable.

4 KMF: Key modification function

The options that were suggested by SAGE were: HMAC-SHA-1 (RFC2104), SHA-1 (FIPS180-1) and AES (FIPS197).

It is proposed to choose one of the faster alternatives: SHA-1 or AES-encryption. The preference goes to SHA-1 as from an implementation point of view it is faster and requires less memory than the AES-128 alternative.

5 Conclusions

The LS's from SAGE now provides the required information to make a decision on the VSTK_RAND length.

It is proposed that SA3 approves following parameter lengths and KMF

a) The length of CELL_GLOBAL_COUNT is 2 bits

b) VSTK_RAND has a length of 38 bit. If GERAN prefers or can accommodate only 36 bits (+2 bits for CELL_GLOBAL_COUNT), the length of VSTK_RAND is 36 bits.

c) An informal section on how to avoid colliding VSTK_RAND during the lifetime of V_Ki is included in the specification.

d) The key modification function KMF is based on SHA-1.

Unfortunately, GERAN2 was not able to discuss the GERAN#2 documents which form the basis of this contribution and a companion CR to this meeting.

Still it is proposed that

e) SA3 discusses and conditionally approves the companion CR to 43.020, in order not to delay its approval as a Rel-6 feature at SA#24. If it is found desirable a CR-version with a VSTK_RAND of 36-bits could be made during SA3#34.

This is justified by the fact that the VGCS ciphering-concept has been available since November last year and that no major obstacles have been notified by other groups to SA3 thus far.

Acknowledging that SA3's CR is dependent on GERAN2 decisions, it is proposed that

f) if GERAN2 response would indicate that SA3's CR is not inline with the GERAN2's decision on major points, the CR-presentation would not be done at SA#24 (September). Minor inconsistencies and errors could still be corrected at SA3#35 (November).

g) to inform GERAN2 of the latest CR version and status in SA3.

h) to tell GERAN2 that SA3 wishes to have (38+2)-bits available if possible but can live with 36+2 bits.

It is also proposed

i) to ask SAGE to provide an example algorithm for the key derivation function (e.g. A8_V basing on MILENAGE).