

**Title:** LS on VGCS: Example algorithm A8\_V  
**Response to:**  
**Release:** R6  
**Work Item:** Key Management of group keys for Voice Group Call Services

**Source:** SA3  
**To:** ETSI SAGE  
**Cc:**

**Contact Person:**

**Name:** Benno Tietz  
**Tel. Number:** +49 211 533 2168  
**E-mail Address:** [benno.tietz@vodafone.com](mailto:benno.tietz@vodafone.com)

**Attachments:** S3-040638

---

**1. Overall Description:**

SA3 would like to thank SAGE for their LS on VGCS (S3-040471). The contained advice has been incorporated into the attached CR (S3-040638). The CR will be forwarded to TSG-SA#25 (13th – 16th September 2004, Palm Springs, USA) except if GERAN2 would state that the required numbers of bits (2 bits for CELL\_GLOBAL\_COUNT and 36 bits for VSTK\_RAND) cannot be provided on the air-interface.

SA3 would like to ask SAGE kindly if they would be willing to provide an example for the operator specific algorithm A8\_V (Annex F.4.3.1) and if yes, to do so. It is perfectly acceptable for SA3 if the example algorithm is based on or derived from G\_MILENAGE.

**2. Actions:**

**To ETSI SAGE group.**

**ACTION:** SA3 would like to ask SAGE kindly whether SAGE can provide an example for the operator specific algorithm A8\_V.

**3. Date of Next TSG-SA3 and TSG-SA Meetings:**

TSG-SA3 Meeting #35	5th – 8th October 2004	Malta
TSG-SA3 Meeting #36	23rd – 26th November 2004	Shenzhen, China
TSG-SA Meeting #25	13th – 16th September 2004	Palm Springs, USA
TSG SA Meeting #26	13th – 16th December 2004	Athens, Greece

## CHANGE REQUEST

⌘ **43.020** CR **CRNum** ⌘ rev - ⌘ Current version: **5.0.0** ⌘

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 ⌘  ME  Radio Access Network  Core Network

<b>Title:</b>	⌘ Introducing VGCS/VBS ciphering		
<b>Source:</b>	⌘ Siemens, Vodafone		
<b>Work item code:</b>	⌘ SECGKYV	<b>Date:</b>	⌘ 28/06/2004
<b>Category:</b>	⌘ <b>B</b>	<b>Release:</b>	⌘ Rel-6
	<i>Use <u>one</u> of the following categories:</i> <b>F</b> (correction) <b>A</b> (corresponds to a correction in an earlier release) <b>B</b> (addition of feature), <b>C</b> (functional modification of feature) <b>D</b> (editorial modification) Detailed explanations of the above categories can be found in 3GPP <a href="#">TR 21.900</a> .		<i>Use <u>one</u> of the following releases:</i> <b>2</b> (GSM Phase 2) <b>R96</b> (Release 1996) <b>R97</b> (Release 1997) <b>R98</b> (Release 1998) <b>R99</b> (Release 1999) <b>Rel-4</b> (Release 4) <b>Rel-5</b> (Release 5) <b>Rel-6</b> (Release 6)

<b>Reason for change:</b>	⌘ Introducing a new feature VGCS/VBS ciphering		
<b>Summary of change:</b>	⌘ The new ciphering feature is introduced into Annex F		
<b>Consequences if not approved:</b>	⌘ The feature cannot be realized		

<b>Clauses affected:</b>	⌘ New Annex F										
<b>Other specs affected:</b>	<table border="1" style="display: inline-table; border-collapse: collapse; text-align: center;"> <tr> <td style="width: 20px;">Y</td> <td style="width: 20px;">N</td> </tr> <tr> <td>Y</td> <td></td> </tr> <tr> <td></td> <td>N</td> </tr> <tr> <td></td> <td>N</td> </tr> </table> Other core specifications	Y	N	Y			N		N	⌘	31.102, 42.068, 43.068, 42.069, 43.069, 44.018, 48.008, 29.002
Y	N										
Y											
	N										
	N										
<b>Other comments:</b>	⌘										

---

## Annex F (normative): Ciphering of Voice Group Call Service (VGCS) and Voice Broadcast Service (VBS)

This Annex defines the security related service and functions for VGCS and VBS in order to provide confidentiality protection to the group calls .

---

### F.1 Introduction

#### F.1.1 Scope

In this Annex the ciphering of the voice group call service (VGCS) [1] and voice broadcast service (VBS) [4] is described. The following functions are required:

- Key derivation
- Encryption of voice group/broadcast calls
- The secure storage of the master group keys

VGCS and VBS provide no authentication functions, i.e. authentication is performed implicitly via encryption/decryption since only a legitimate subscriber shall be able to encrypt and decrypt the VGCS/VBS speech call when the group call requires confidentiality protection. 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. In case of a stolen or lost USIM, all USIMs of the remaining members of the voice groups that the USIM is a member of, need to be changed (e.g. via OTA or manual provisioning).

A pre-Rel-6 VGCS/VBS capable mobile shall be able to participate in an un-ciphered group call, if it is part of that group.

NOTE: The only security relevant difference between VBS and VGCS is that in the case of VBS there exists no uplink channel.

#### F.1.2 References

- [1] 3G TS 42.068: 3<sup>rd</sup> Generation Partnership Project; Technical Specification Group Services and system Aspects; Voice Group Call Service (VGCS) - Stage 1
- [2] 3G TS 43.068: 3<sup>rd</sup> Generation Partnership Project; Technical Specification Group Services and system Aspects; Voice Group Call Service (VGCS) - Stage 2
- [3] 3G TS 31.102: 3<sup>rd</sup> Generation Partnership Project; Technical Specification Group Terminals; Characteristics of the USIM application
- [4] 3G TS 42.069: 3<sup>rd</sup> Generation Partnership Project; Technical Specification Group Services and system Aspects; Voice Broadcast Service (VBS) - Stage 1
- [5] 3G TS 43.069: 3<sup>rd</sup> Generation Partnership Project; Technical Specification Group Services and system Aspects; Voice Broadcast Service (VBS) - Stage 2
- [6] 3G TS 23.003: 3<sup>rd</sup> Generation Partnership Project; Technical Specification Group Core Network; Numbering, addressing and identification

[7] FIPS PUB 180-1 Secure Hash Standard

## F.1.3 Definitions and Abbreviations

### F.1.3.1 Definitions

<u>A5 Id</u>	<u>Identifier of the encryption algorithm which shall be used.</u>
<u>CELL_GLOBAL_COUNT</u>	<u>A counter valid for all voice group calls within a cell.</u>
<u>Group_Id</u>	<u>Unique identifier of a voice call group.</u>
<u>KMF</u>	<u>Key Modification Function. KMF derives from the short term key VSTK, the CGI and the CELL_GLOBAL_COUNT the cipher key V_Kc which is valid for that specific cell.</u>
<u>VSTK</u>	<u>Short Term Key provided by the USIM and the GCR. VSTK is derived from VSTK_RAND and V_Ki (128 bit)</u>
<u>VK_Id</u>	<u>Identifier of the Master Group Key (1 bit) of a group. There are up to 2 V_Ki per group</u>
<u>VSTK_RAND</u>	<u>The 36-bit value that is used for derivation of a short term key VSTK.</u>
<u>V_Ki (Group_Id, i)</u>	<u>Voice Group or Broadcast Group Key (128 bit) number i:=VK_Id of group with Group_Id. In short also called Master Group Key or Group Key in this Annex</u>
<u>V_Kc</u>	<u>Voice Group or Broadcast Ciphering Key (128 bit). V_Kc is derived from VSTK</u>

### F.1.3.2 Abbreviations

The following list describes the abbreviations and acronyms used in this Annex.

<u>CGI</u>	<u>Cell Global Identifier</u>
<u>GCR</u>	<u>Group Call Register</u>
<u>VBS</u>	<u>Voice Broadcast Service</u>
<u>VGCS</u>	<u>Voice Group Call Service</u>

---

## F.2 Security Requirements

The ciphering concept for VGCS, VBS fulfils following security requirements

**REQ-1.** Prevent the same Voice group or Broadcast group 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.

**REQ-2.** The master group key shall never leave the USIM and the GCR.

Even though VGCS/VBS users should be trusted, this approach protects the 'root'-key (I.e. Master Group key) in the most secure way such that it need not be updated very frequently.

**REQ-3.** 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.

**REQ-4.** Prevent the same key stream block being used in uplink and downlink direction.

This requirement is fulfilled by Point to Point voice calls already (See Annex C.1.2). By reusing the same mechanisms for uplink/downlink key stream derivation (I.e. reusing A5) the VBS/VGCS ciphering also fulfils this requirement.

---

## F.3 Storage of the Master Group Keys and overview of flows

The master group keys (in short called group keys in this Annex) are securely stored at two locations

- GCR: Beside other information, the GCR stores for each Group\_Id a list of group keys. Each group key is uniquely identified by the Group\_Id and the group key number VK\_Id (1-2).
- USIM: The USIM contains a list of 2 group keys for each Group\_Id. Deletion or changing of group keys are allowed only via OTA or via USIM-personalisation.

The Short Term Key VSTK shall be deleted by the network entities after tearing down the call and by the ME on power down or UICC removal. On each new VGCS/VBS call set up, a new short term key VSTK shall be generated.

The following sequence gives an overview of how the different network entities make use of the group keys (and derived information) during the establishment of a voice group/broadcast call.

1. During the voice group/broadcast call set-up the anchor-MSC sends a GCR Interrogation to the GCR containing the Group\_Id.
2. The GCR provides on the basis of a fresh number VSTK\_RAND (see Annex F.7) the key VSTK as described in Annex F.4. VK\_Id, VSTK\_RAND, VSTK, the permitted ciphering algorithm (A5\_Id) and other voice group/broadcast call related information, are sent from the GCR back to the anchor-MSC.
3. The anchor-MSC sends this information to the relay-MSC's via a MAP-operation.
4. The anchor MSC and relay-MSC's sends this information to the BSS using the VGCS Assignment Request or VBS Assignment Request.
5. The BSS sends the CELL\_GLOBAL\_COUNT, VSTK\_RAND, Group\_Id and the group key number VK\_Id to the ME's via a notification procedure..
6. Each ME generates the VSTK, on the basis of the received information from step 5, as described in Annex F.4.

A late entrant belonging to the right Group\_Id in a cell where a call is active need to pick out the notification parameters from step 5 and executes step 6.

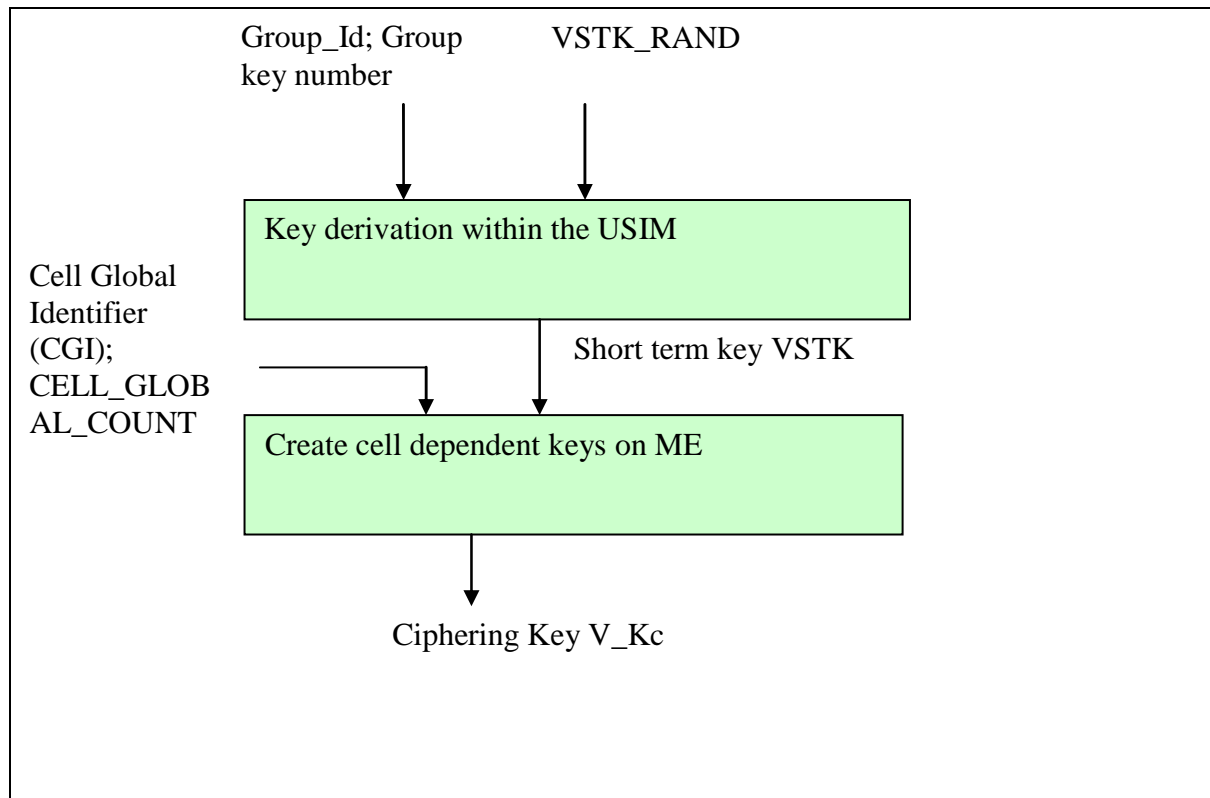
In case of inter-MSC Handover of the talking subscriber the Group\_Id, VSTK\_RAND, VSTK and A5\_Id need to be transferred via MAP Prepare Handover request message from MSC-A to MSC-B.

---

## F.4 Key derivation

The key derivation of the encryption is performed in two steps.

1. Derivation of a short term key VSTK on the GCR-side and USIM; VSTK\_RAND generation on the GCR-side and sending it to the ME via the BSS for use on the USIM.
2. Derivation of the actual encryption key V\_Kc in the BSS and ME.



## F.4.1 Key derivation within the USIM / GCR

This function is performed on

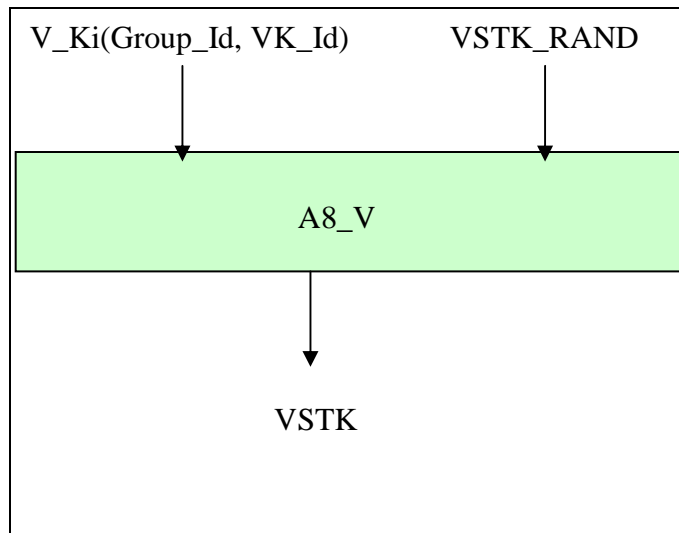
- the set-up of a voice group or broadcast call by the GCR
- entry to a voice group or broadcast call by the USIM

On the set-up of a voice group/broadcast call the GCR generates the VSTK RAND (See Annex F.7). Also an appropriate group key V\_Ki (identified by VK\_Id) is selected by the GCR. Using the function A8\_V a short term key VSTK is derived using as input parameters:

- V\_Ki (Group\_Id, VK\_Id)
- VSTK RAND

Output of A8\_V is

- VSTK



The GCR sends the parameters Group Id, VK Id, VSTK RAND, VSTK, A5 Id via the anchor-MSC and the relay-MSC's to the BSS. The BSS signals the Group Id, VSTK RAND and VK Id to the ME.

On the ME-side, each ME sends the Group Id of the voice group or broadcast call, the identifier of the key VK ID and the VSTK RAND to the USIM. The USIM performs the calculation of the short term key VSTK using the function A8\_V and returns it (together with the encryption algorithm identifier A5 Id).

## F.4.2 Key derivation within the ME/BSS

This function is performed on

- Entry to a voice group/broadcast call
- Cell reselection
- Changing of the value of CELL\_GLOBAL\_COUNT
- Handover

by the ME.

On the network side the function is performed on

- Set-up of a voice group/broadcast call in a cell
- Changing of the value of CELL\_GLOBAL\_COUNT

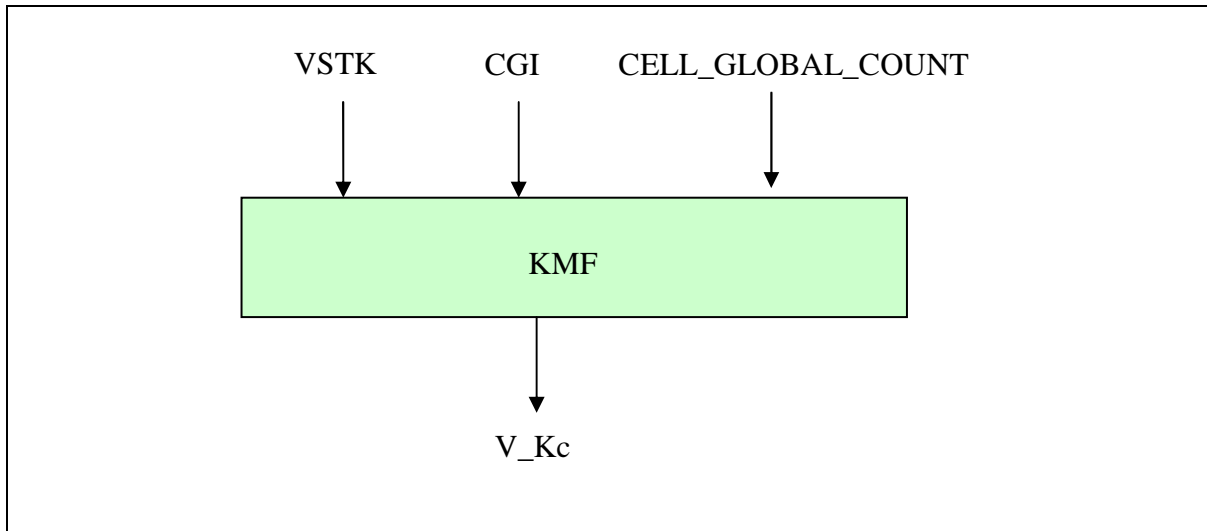
by the BSS.

For each cell the BSS and ME calculate an encryption key V Kc using the key modification function KMF. Input parameter of the KMF are:

- VSTK: the short term key for this voice call group and this call
- CGI: the cell global identifier which identifies a cell world-wide uniquely.
- CELL\_GLOBAL\_COUNT: this parameter shall be incremented by the BSS when the TDMA-frame-number wraps around.

NOTE: The MS and network SHALL be aligned regarding the value of the CELL\_GLOBAL\_COUNT. In case of transmissions on the FACCH, this requires that the network transmits a part of the whole of the TDMA frame number together with the CELL\_GLOBAL\_COUNT

The output of the key modification function is the actually cipher key V Kc.



To provide the required information to the ME the parameters CELL\_GLOBAL\_COUNT and CGI are included in various messages from the BSS to the ME (i.e. CELL\_GLOBAL\_COUNT on the NCH, FACCH and PCH, and the CGI on the BCCH and the FACCH).

### F.4.3 Encryption algorithm selection

The encryption algorithm identifier A5\_Id is stored in the GCR and the USIM. For each group key V\_Ki(Group\_Id, i) there is a unique A5\_Id.

A5\_Id is transmitted from the GCR to the BSS. The ME fetches the A5\_Id together with the VSTK from the USIM.

NOTE: It is possible that different algorithm identifiers are bound to different V\_Ki of the same group.

NOTE: The algorithm identifier A5\_Id stored in the GCR and on the USIM shall match with the encryption capabilities of the ME's used by the group and the BSS where the voice group calls are allowed to take place.

### F.4.4 Algorithm requirements

#### F.4.3.1 A8\_V

The key derivation function A8\_V has the following input and output parameter:

Input Parameter:

VSTK\_RAND: 36 bit value (See Annex F.7)

V\_Ki (Group\_Id, i): 128 bit secret key

Output:

VSTK: 128 bit short term key

A8\_V is an operator specific algorithm. The calculation time for A8\_V shall not exceed 500 ms.

A8\_V is implemented in the GCR and on the USIM

#### F.4.3.1 KMF

The key derivation function KMF has the following input and output parameter:

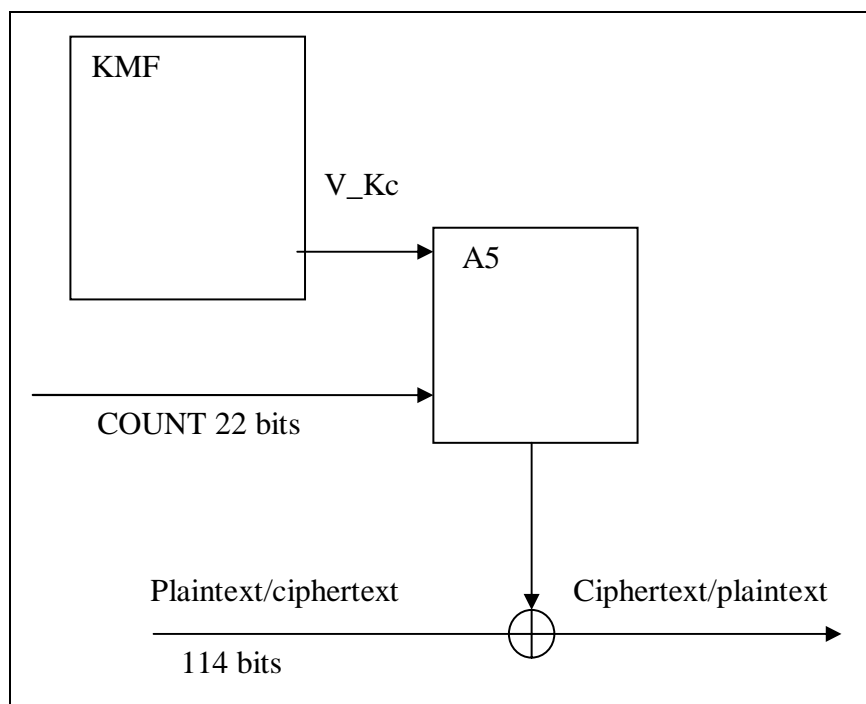


Input Parameter:VSTK: 128 bit short term keyCGI: the cell global identifier: 56 bit ([6] TS 23.003)CELL\_GLOBAL\_COUNT: 2 bitOutput:V\_Kc 128 bit encryption keyThe KMF is implemented in the BSS and in the ME.The specification of KMF can be found in Annex F.6

## F.5 Encryption of voice group calls

For the encryption of a voice group call the same encryption algorithms are used as for a normal GSM speech call. Which algorithm out of the algorithm suite A5/x is used is determined by the identifier A5\_Id, which is stored on the USIM (together with the group key V\_Ki(Group\_Id, i)). The algorithm A5/X is used in the same way as in the GSM (ref. Annex C.1) using the key V\_Kc as encryption/decryption key Kc as input to A5/x.

If the key length KL of the encryption algorithm A5/X is shorter than the length of V\_Kc (128 bit) then only the KL least-significant KL-bits of V\_Kc are used.



## F.6 Specification of the Key Modification Function (KMF)

SHA-1 [7] is used for generating V\_Kc:

$V\_Kc = \text{SHA-1}(\text{VSTK} \parallel \text{CGI} \parallel \text{CELL\_GLOBAL\_COUNT} \parallel \text{VSTK})$

From the 160-bit output of SHA-1, the 128 bit least significant bits are taken as 128-bit  $V\_Kc$ .

## F.7 Generation of VSTK RAND (informative)

Since the length of VSTK RAND (36 bits) is small, care should be taken that a VSTK RAND isn't generated twice (so-called collision) during the lifetime of  $V\_Ki$ . On the other hand, the predictability of VSTK RAND shall be avoided. The following scheme could be used in order to generate 4096 VSTK RAND for each  $V\_Ki$  with a probability  $< 10^{-6}$  that a collision occurs:

NOTE: A collision probability of  $< 10^{-4}$  could still give a sufficient security margin and may allow, depending on the VSTK RAND structure that is chosen, that more VSTK can be generated from one  $V\_Ki$ .

The GCR maintains a COUNTER (12 bits) for each voice group. After each generation of a VSTK RAND for a specific voice group, COUNTER for that voice group is incremented by one.

The left most 12 bits (COUNTER) of VSTK RAND are set to COUNTER. The remaining 24 bits (RANDOM) are generated randomly, i.e. unpredictably for each new VSTK RAND.

Therefore  $\text{VSTK\_RAND} = \text{COUNTER} \parallel \text{RANDOM}$ .

NOTE: The length of RANDOM shall be at least 24 bits.

If COUNTER wraps around, a new  $V\_Ki$  is required for that group.

Following table gives the maximum number of voice group calls that are possible with a with a full random generated VSTK RAND

<u>Length of VSTK RAND</u>	<u>Max collision prob for fixed <math>V\_Ki</math></u>	<u>Number of calls</u>
<u>36</u>	<u><math>10^{-6}</math></u>	<u>TBD</u>
<u>36</u>	<u><math>10^{-4}</math></u>	<u>TBD</u>

Following table give the maximum number of voice group calls that are possible with a VSTK RAND as structured in this informative Annex.

<u>Total challenge length</u>	<u>Length of counter</u>	<u>Length of random part</u>	<u>Max collision prob for fixed <math>V\_Ki</math></u>	<u>Max collision prob for one fixed counter</u>	<u>Number of calls for one fixed counter</u>	<u>Total number of calls for fixed <math>V\_Ki</math></u>
<u>36</u>	<u>14</u>	<u>24</u>	<u><math>10^{-6}</math></u>	<u><math>6.10 \times 10^{-11}</math></u>	<u>1</u>	<u>4096</u>
<u>36</u>	<u>14</u>	<u>24</u>	<u><math>10^{-4}</math></u>	<u><math>6.10 \times 10^{-9}</math></u>	<u>1</u>	<u>4096</u>