3GPP TSG SA WG3 Security — S3#35 **S3-040785**
St Paul's Bay, Malta, 5th – 8th October 2004

CR-Form-v7.1

CHANGE REQUEST

⌘ **43.020** **CR** **002** ⌘ **rev** **-** ⌘ Current version: **6.0.0** ⌘

*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 ☒

Title:	⌘	Clarifications to VGCS/VBS ciphering mechanism
Source:	⌘	Siemens, Vodafone
Work item code:	⌘	SECGKYV
Date:	⌘	28/09/2004
Category:	⌘	**F**
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:	⌘	Annex G contains contradictory text about the VSTK_RAND length and structure. Simplify the use of group key identification i.e. explicitly use VK_id (Annex F)
Summary of change:	⌘	- Correct some contradictory text about the VSTK_RAND length and structure - Align used terminology. - Add some text and enhance the understandability of the used tables in Annex G - Clarify bit numbering
Consequences if not approved:	⌘	Contradictory text will stay in

Clauses affected:	⌘	Annex F, Annex G, new clause 0.3

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

⌘

Other comments: ⌘

*** Begin of change ****

0.3 Conventions

All data variables in this specification are presented with the most significant substring on the left hand side and the least significant substring on the right hand side. A substring may be a bit, byte or other arbitrary length bitstring. Where a variable is broken down into a number of substrings, the leftmost (most significant) substring is numbered 0, the next most significant is numbered 1, and so on through to the least significant.

*** End of change ****

*** Begin of next change ****

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) TS 42.068 [F1] and voice broadcast service (VBS) TS 42.069 [F4] 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

[F1] 3GPP TS 42.068: "3rd Generation Partnership Project; Technical Specification Group Services and system Aspects; Voice Group Call Service (VGCS) - Stage 1".

[F2] 3GPP TS 43.068: "3rd Generation Partnership Project; Technical Specification Group Services and system Aspects; Voice Group Call Service (VGCS) - Stage 2".

[F3] 3GPP TS 31.102: "3rd Generation Partnership Project; Technical Specification Group Terminals; Characteristics of the USIM application".

[F4] 3GPP TS 42.069: "3rd Generation Partnership Project; Technical Specification Group Services and system Aspects; Voice Broadcast Service (VBS) - Stage 1".

[F5] 3GPP TS 43.069: "3rd Generation Partnership Project; Technical Specification Group Services and system Aspects; Voice Broadcast Service (VBS) - Stage 2".

[F6] 3GPP TS 23.003: "3rd Generation Partnership Project; Technical Specification Group Core Network; Numbering, addressing and identification".

[F7] FIPS PUB 180-1 Secure Hash Standard.

F.1.3 Definitions and Abbreviations

F.1.3.1 Definitions

A5_Id: Identifier of the encryption algorithm which shall be used.

CELL_GLOBAL_COUNT: A counter valid for all voice group calls within a cell.

Group_Id: Unique identifier of a voice call group.

KMF: 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.

VSTK: Short Term Key provided by the USIM and the GCR. VSTK is derived from VSTK_RAND and V_Ki (128 bit).

VK_Id: Identifier of the Master Group Key (1 bit) of a group. There are up to 2 V_Ki per group.

VSTK_RAND: The 36-bit value that is used for derivation of a short term key VSTK.

V_Ki (Group_Id, VK_Id~~i~~): Voice Group or Broadcast Group Key (128 bit) number ~~i.:=~~VK_Id of group with Group_Id. This is also called Master Group Key or Group Key in this Annex.

V_Kc: Voice Group or Broadcast Ciphering Key (128 bit). V_Kc is derived from VSTK.

F.1.3.2 Abbreviations

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

CGI	Cell Global Identifier
GCR	Group Call Register
VBS	Voice Broadcast Service
VGCS	Voice Group Call Service

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 clause 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 G) 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 clause 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.

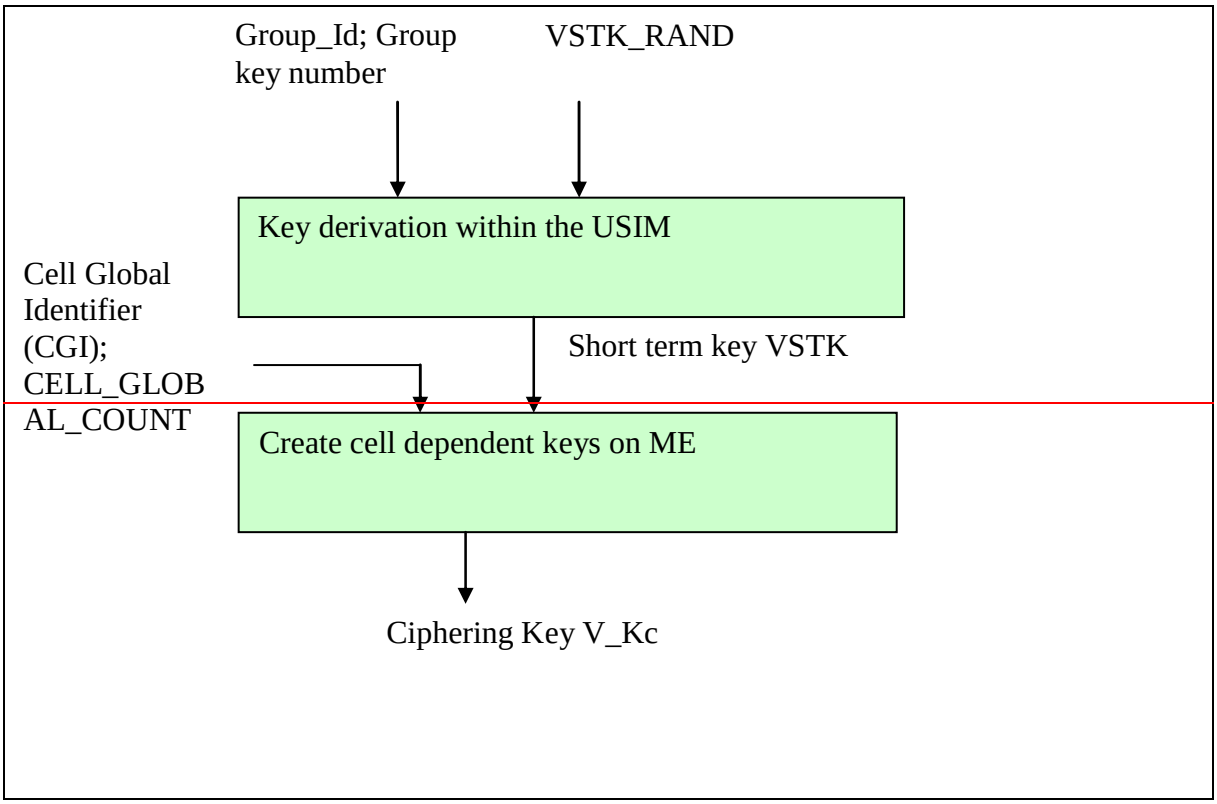
In case of inter-MSC Handover of the talking subscriber the Group_Id, VSTK_RAND, VSTK and A5_Id need to be transferred via MAP Prepare Handover request message from MSC-A to MSC-B.

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.



~~Figure F.1: Key derivation~~

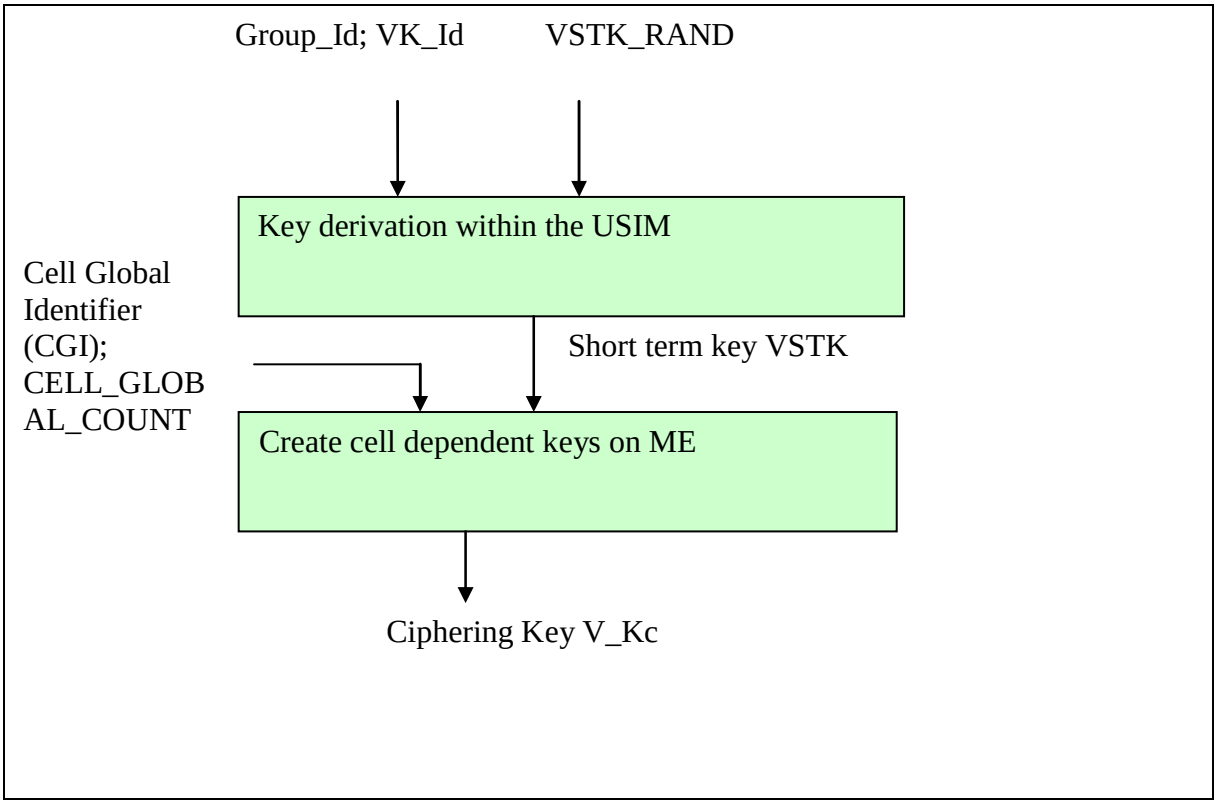


Figure F.1: Key derivation

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 G). 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

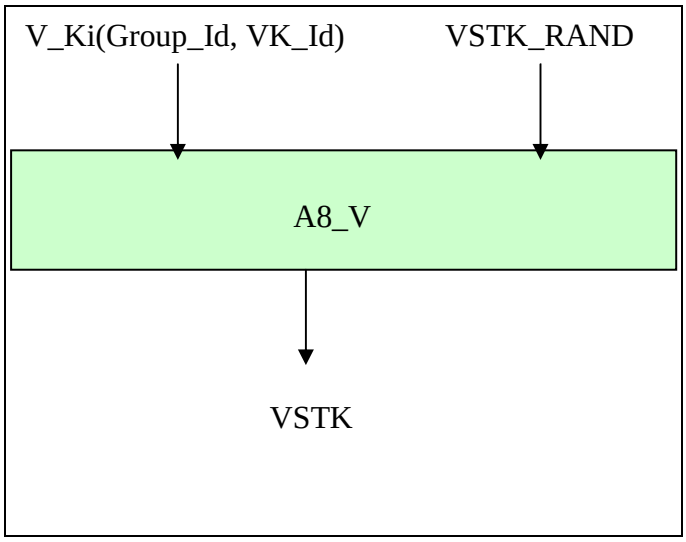


Figure F.2

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 by the ME on:

- entry to a voice group/broadcast call;
- cell reselection;
- changing of the value of CELL_GLOBAL_COUNT;
- Handover.

On the network side the function is performed by the BSS on

- set-up of a voice group/broadcast call in a cell;

- changing of the value of CELL_GLOBAL_COUNT.

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.

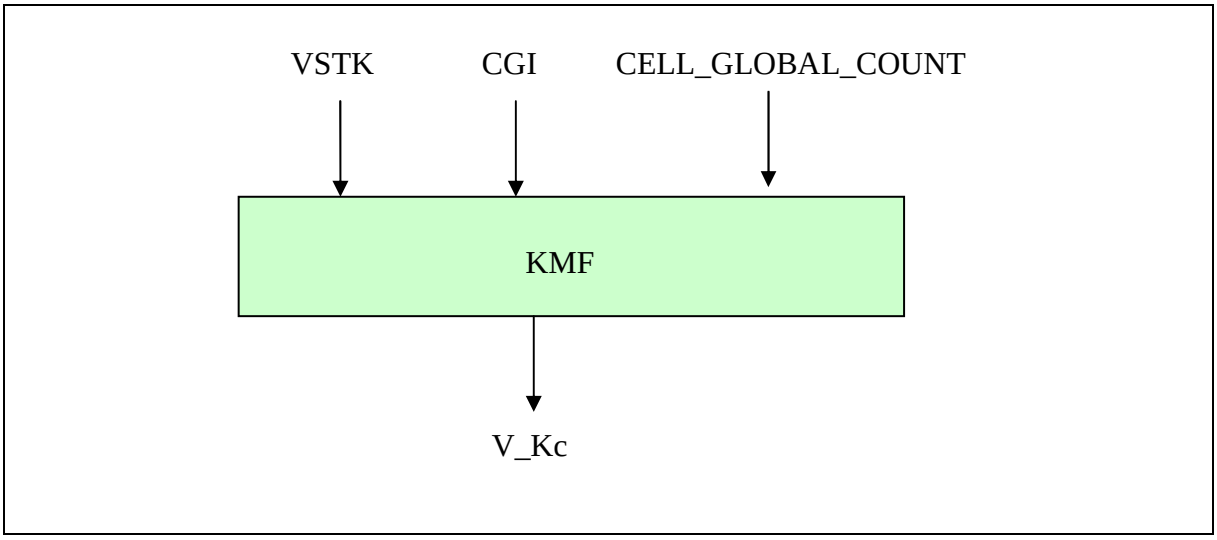


Figure F.3

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, VK_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 1: It is possible that different algorithm identifiers are bound to different V_Ki of the same group.

NOTE 2: 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 G);

V_Ki (Group_Id, VK_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 key;

CGI: the cell global identifier: 56 bit (TS 23.003 [F6]);

CELL_GLOBAL_COUNT: 2 bit.

Output:

V_Kc 128 bit encryption key.

The KMF is implemented in the BSS and in the ME.

The specification of KMF can be found in clause 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, VK_Id~~i~~)). The algorithm A5/X is used in the same way as in the GSM (see clause ~~-~~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 bits [0] to [KL-1] ~~the KL least-significant KL-bits~~ of V_Kc are used.

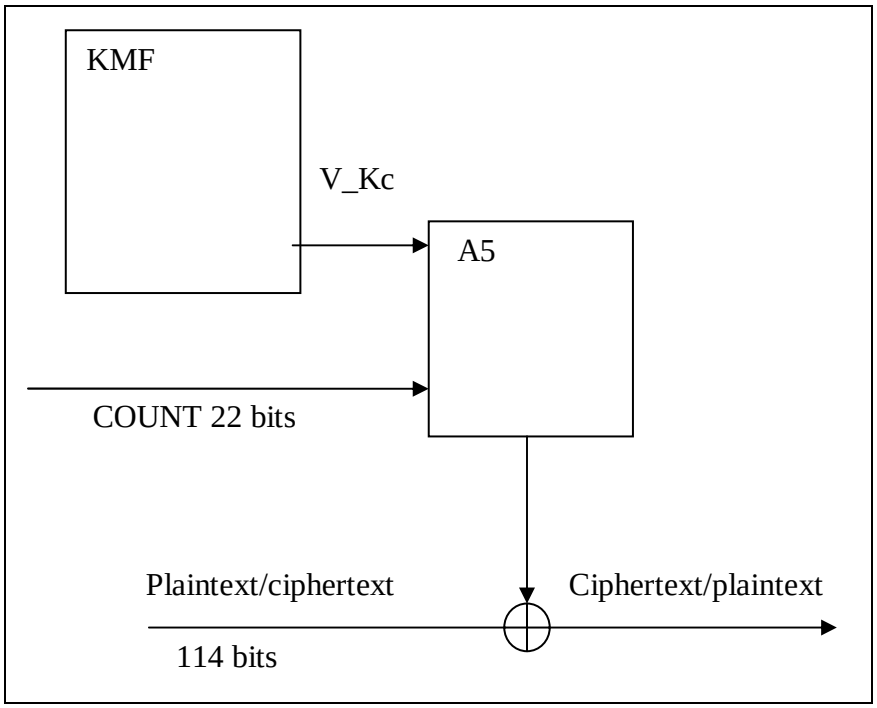


Figure F.4

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

SHA-1 (FIPS PUB 180-1 [F7]) is used for generating V_Kc:

V_Kc= SHA-1(VSTK | CGI | CELL_GLOBAL_COUNT | VSTK)

From the 160 bit output of SHA-1, the ~~128~~ bits numbered as [0] to [127] ~~least significant bits~~ are taken as 128 bit V_Kc.

Annex G (informative): Generation of VSTK_RAND

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 predicta~~i~~bility 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 right most 24 bits (RANDOM) are generated randomly, i.e. unpredictably for each new VSTK_RAND.

Therefore VSTK_RAND = COUNTER | RANDOM.

NOTE: For security reasons, any adopted scheme shall contain at least 24 true random bits. ~~The length of RANDOM shall be at least 24 bits.~~

If COUNTER wraps around, a new V_Ki is required for that group.

Table G.1 gives the maximum number of voice group calls that are possible with ~~a with~~ a full random generated VSTK_RAND:

Table G.1: Maximum number of voice group calls that are possible with a with a full random generated VSTK_RAND

Length of VSTK_RAND	Max collision prob for fixed V_Ki	Number of calls
36	10^{-6}	~~TBD~~371
36	10^{-4}	3707~~TBD~~

Table G.2 gives the maximum number of voice group calls that are possible with a VSTK_RAND, as structured in this annex.

Table G.2: Maximum number of voice group calls that are possible with a VSTK_RAND

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
36	12~~4~~	24	10^{-6}	$2^{6}.44^{10}_{10^{11}} \times 10^{-}$	1	4096
36	12~~4~~	24	10^{-4}	$2^{6}.44^{10}_{8^{9}} \times 10^{-}$	1	4096

Explanation of the columns of table G.2:

Max collision probability for fixed V_Ki: what we have determined, for security reasons, should be the maximum probability that the same value of VSTK_RAND (and hence the same value of VSTK) is used twice before the value of V_Ki is changed. 10^{-6} is a strong security setting; 10^{-4} is not quite so strong, but probably adequate.

Max collision probability for one fixed counter: suppose that VSTK_RAND is made up of N_c counter bits and N_r random bits. We assume that the counter part will take all possible 2^{N_c} values before V_Ki is updated. Having selected our required "Max collision prob for fixed V_Ki", this is the corresponding maximum permitted probability that the same value of the N_r random bits (and hence the same value of VSTK) is used twice for a fixed value of the N_c counter bits.

*** End of change ****