Source: **SA WG3**

Title: **2 CRs to 43.020 (Rel-6)**

Document for: **Approval**

Agenda Item: **7.3.3**

The following CRs have been agreed by SA WG3 and are presented to TSG SA for approval.

TSG SA Doc number	Spec	CR	Rev	Phase	Subject	Cat	Version-Current	SA WG3 Doc number	Work item
SP-040862	43.020	002	2	Rel-6	Clarifications to VGCS/VBS ciphering mechanism	F	6.0.0	S3-040925	SECGKYV
SP-040862	43.020	003	2	Rel-6	Clarifying the mandatory support of A5 algorithms within mobile stations	C	6.0.0	S3-041075	SEC1

3GPP TSG SA WG3 Security ó S3#36 **S3-040925 att2**
Shenzhen, China, 23th ñ 26th October 2004

CR-Form-v7.1

CHANGE REQUEST

⌘ **43.020** **CR** **002** ⌘ **rev** **2** ⌘ 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 [X] Radio Access Network [X] Core Network [X]

Title:	⌘	Clarifications to VGCS/VBS ciphering mechanism
Source:	⌘	SA WG3
Work item code:	⌘	SECGKYV ***Date:*** ⌘ 09/11/2004
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) There are no impacts to the MAP prepare handover command for a talking subscriber. Missing detailed message flows
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 - Remove impacts to inter-MSC handover - Add message flows
Consequences if not approved:	⌘	Contradictory text will stay in or missing information

Clauses affected:	⌘	Annex F, Annex G

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

Other comments:	⌘	

*** Begin of 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.

All data variables in this Annex 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.

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 MSCís via a MAP operation;~~

~~4. the anchor MSC and relay MSCís 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 MEís 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.~~

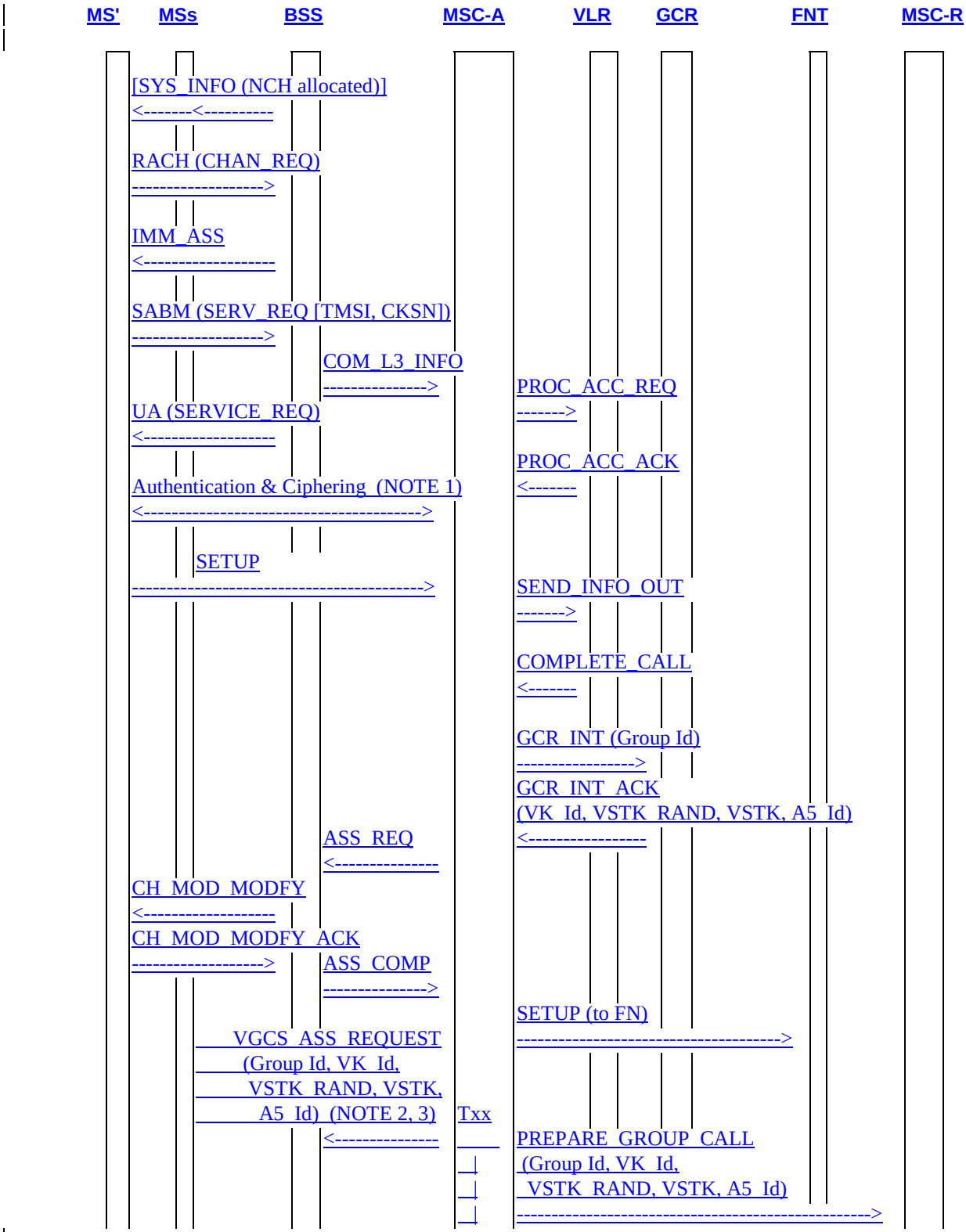
~~A late entrant belonging to the right Group_Id in a cell where a call is active need to pick out the notification parameters from step 5 and executes step 6.~~

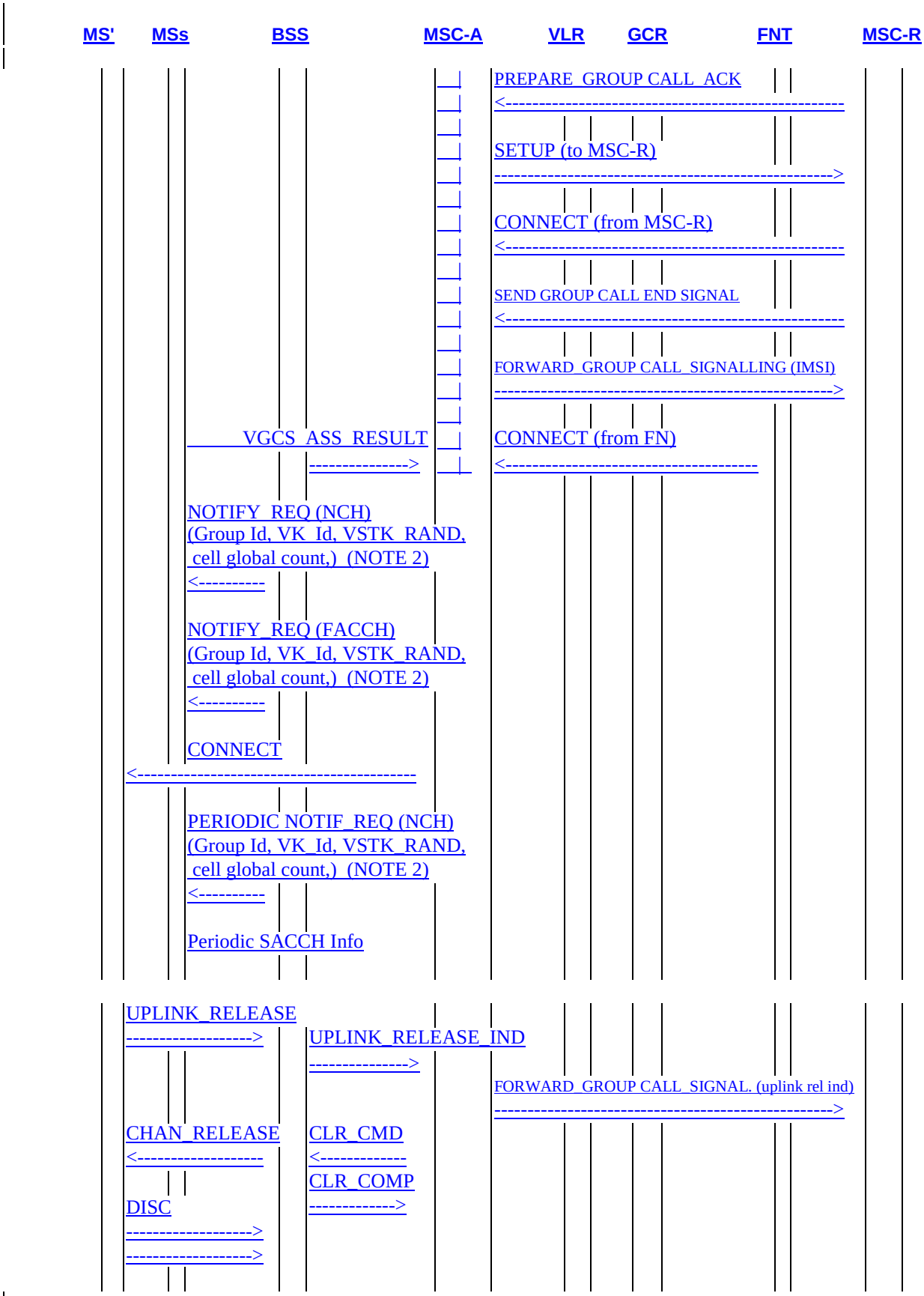
~~In case of inter MSC Handover of the talking subscriber the Group_Id, VSTK_RAND, VSTK and A5_Id need to be transferred via MAP Prepare Handover request message from MSC A to MSC B.~~

F.3.1 Distribution of ciphering data during establishment of a voice/broadcast group call

This signalling flow indicates the distribution of the VGCS parameters during the establishment of a ciphered voice group call. Figure F.3.1-1 shows the distribution of the VSTK_RAND, VSTK, VK_Id, A5_id and Cell_Global_Count between MSC, BSC and MS. The main points are:

- The Notification/NCH and Notification/FACCH are used to transfer the VSTK_RAND, VK_Id and Cell Global Count between the BSS and the MS.
- The PREPARE_GROUP_CALL is used to transfer the VSTK, VSTK_RAND, VK_Id and A5_Id between MSC-A and MSC-B.
- The VGCS/VBS Assignment Request transfers the VSTK, VSTK_RAND, VK_Id and A5_Id between the MSC and the BSC.


MS'
MSs
BSS
MSC-A
VLR
GCR
FNT
MSC-R
[SYS_INFO (NCH allocated)]
RACH (CHAN_REQ)
IMM_ASS
SABM (SERV_REQ [TMSI, CKSN])
COM_L3_INFO
PROC_ACC_REQ
UA (SERVICE_REQ)
PROC_ACC_ACK
Authentication & Ciphering (NOTE 1)
SETUP
SEND_INFO_OUT
COMPLETE_CALL
GCR_INT (Group Id)
GCR_INT_ACK
(VK_Id, VSTK_RAND, VSTK, A5_Id)
ASS_REQ
CH_MOD_MODFY
CH_MOD_MODFY_ACK
ASS_COMP
SETUP (to FN)
VGCS_ASS_REQUEST
(Group Id, VK_Id,
VSTK_RAND, VSTK,
A5_Id) (NOTE 2, 3)
Txx
PREPARE_GROUP_CALL
(Group Id, VK_Id,
VSTK_RAND, VSTK, A5_Id)



NOTE 1: If authentication and ciphering are performed, then the dedicated channel of the originator of the voice group call is ciphered with the cipher key Kc generated during the authentication procedure. If ciphering is started without authentication, the cipher key indicated with CKSN in the Service Request message is used.

NOTE 2: The Group Id and the Group cipher key number (VK_Id) are included in the Descriptive group call reference.

NOTE 3: The permitted ciphering algorithm (A5_Id) is included in the Encryption information.

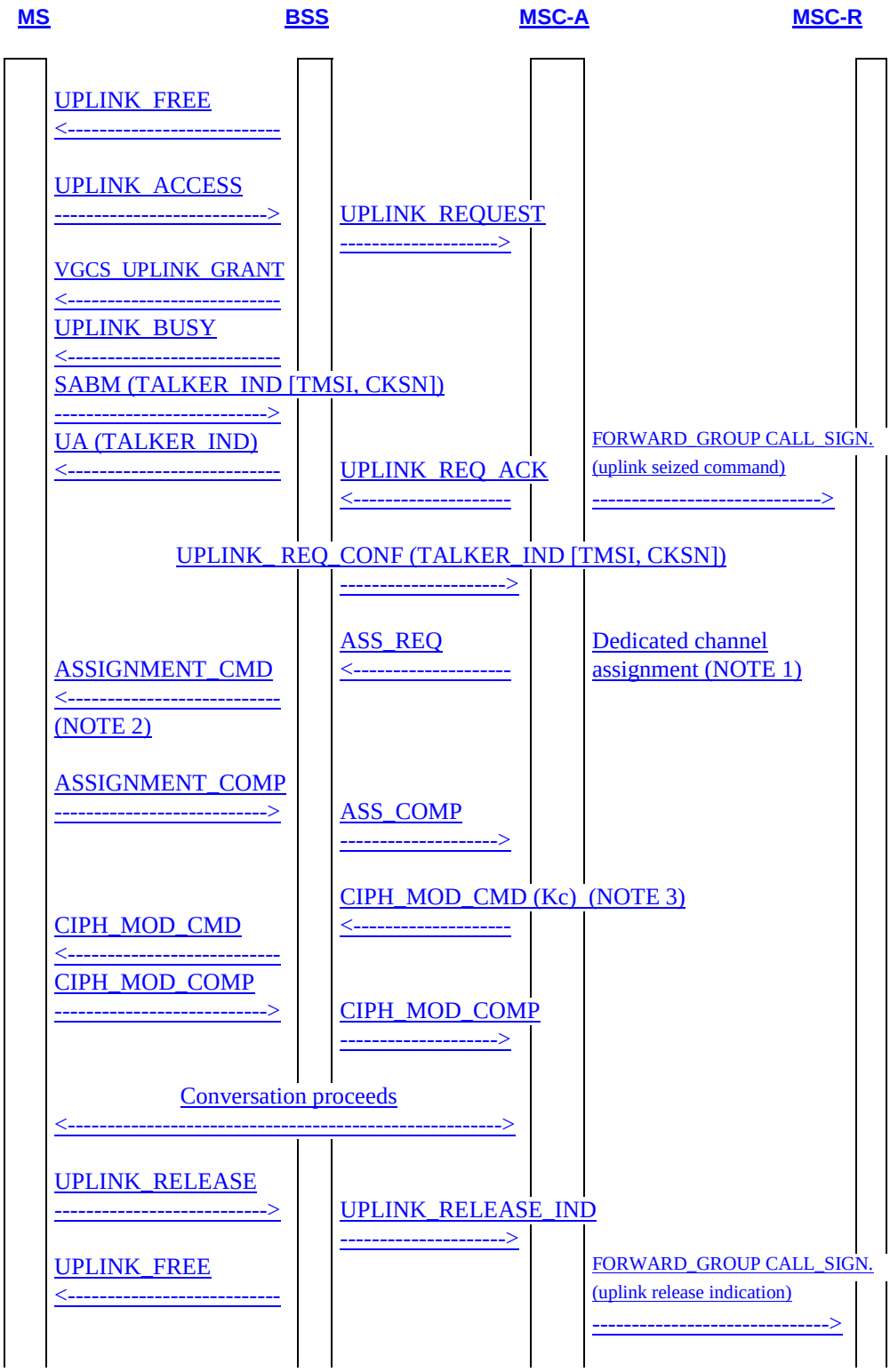
NOTE 4: MS' = calling subscriber mobile station;
MSs = destination subscriber mobile stations;
FNT = fixed network user terminal;
MSC-A = anchor MSC;
MSC-R = relay MSC.

Figure F.3.1-1: Distribution of ciphering data during establishment of a voice group call.

F.3.2 Signalling information required for the voice group call uplink access in the anchor MSC (normal case, subsequent talker on dedicated channel)

Figure F.3.2-1 shows how the MS and the BSC determine the Cipher Key Sequence Number and Ciphering algorithm to use when the VGCS talker is on a dedicated channel. The main points are:

- The MS reads the Cipher Key Sequence Number from the USIM and passes the value to the BSC via the TALKER INDICATION Message
- The Cipher Key Sequence Number is passed from the BSC to the MSC via the UPLINK REQUEST CONFIRMATION message (within Layer 3 information).
- The MS and BSC are informed of the ciphering algorithm identity in the CIPHER MODE COMMAND message.



NOTE 1: In this case the MSC decided to transfer the subsequent talker to a dedicated channel.

NOTE 2: Upon reception of the ASSIGNMENT CMD message which transfers the MS from the group call channel to a dedicated channel, the MS starts transmission and reception on the dedicated channel in unciphered mode.

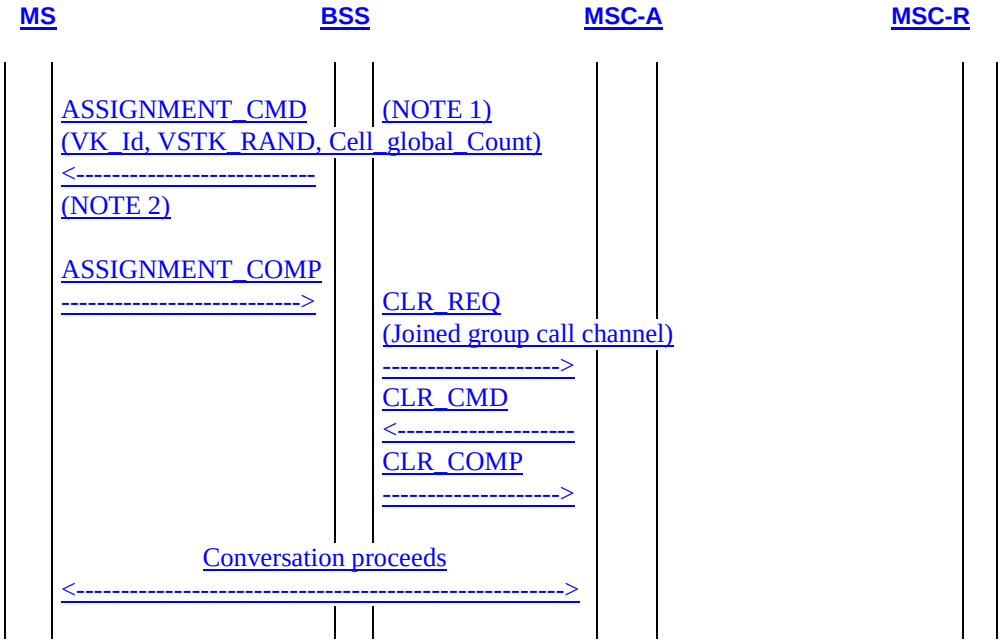
NOTE 3: The dedicated channel of the subsequent talker is ciphered with the cipher key Kc indicated with CKSN in the Talker Indication message.

Figure F.3.2-1: Signalling information required for the voice group call uplink access in the anchor MSC (normal case, subsequent talker on dedicated channel)

F.3.3 Signalling information required to transfer the originator or subsequent talker from a dedicated channel to a group call channel

Figure F.3.3-1 shows the MS being transferred from a dedicated channel to the group channel via the ASSIGNMENT COMMAND message. The main points are:

- The group channel is ciphered with VGCS ciphering
- The VK_Id, VSTK_RAND and Cell_Global_Count are supplied in the ASSIGNMENT COMMAND message in order for the MS to calculate the voice group ciphering keys.



NOTE 1: In this case the BSC decided to transfer the originator or subsequent talker to a group call channel.

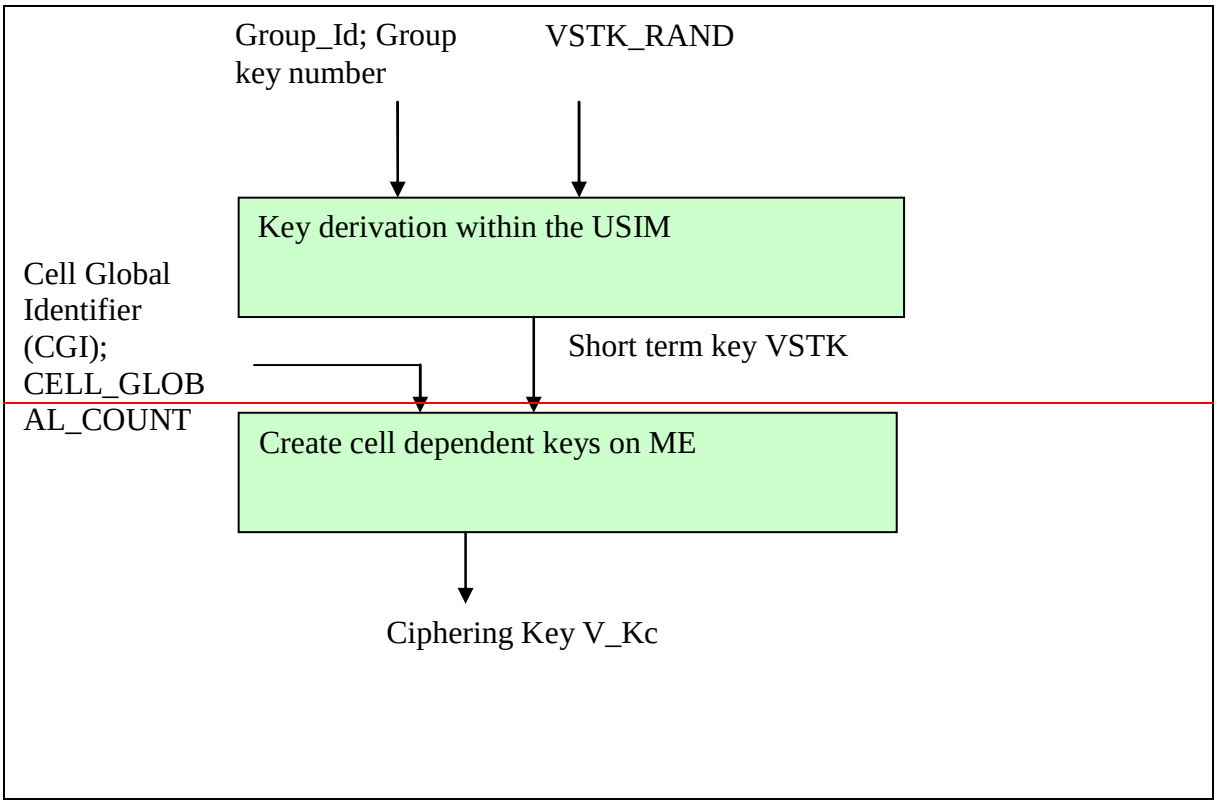
NOTE 2: Upon reception of the ASSIGNMENT CMD message, if the Group cipher key number is different from 'no ciphering', the MS derives the cipher key V_Kc and starts transmission and reception on the group call channel in ciphered mode, using V_Kc.

Figure F.3.3-1: Signalling information required to transfer the originator or subsequent talker from a dedicated channel to a group call channel

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~~

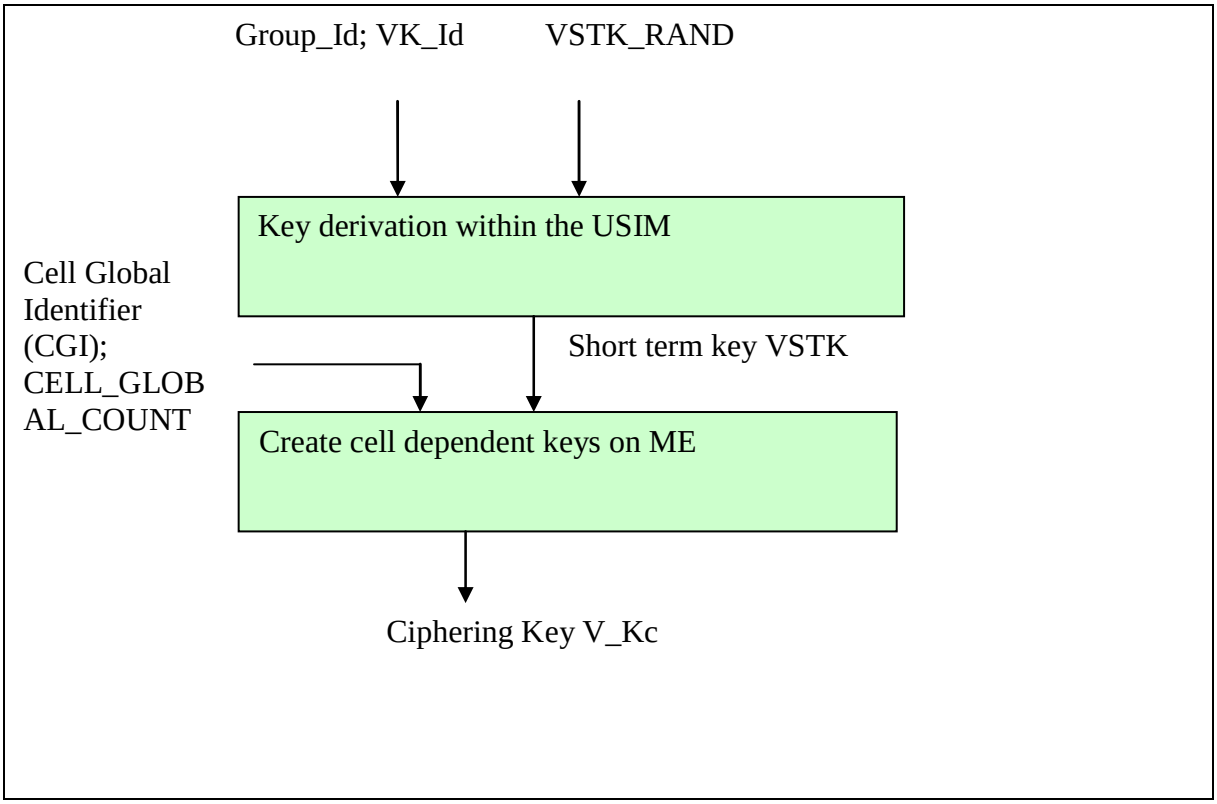


Figure F.1: Key derivation

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

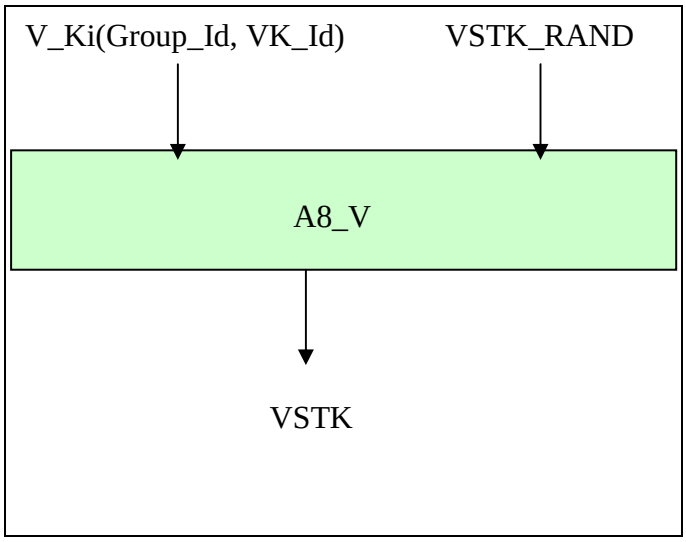


Figure F.2

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.

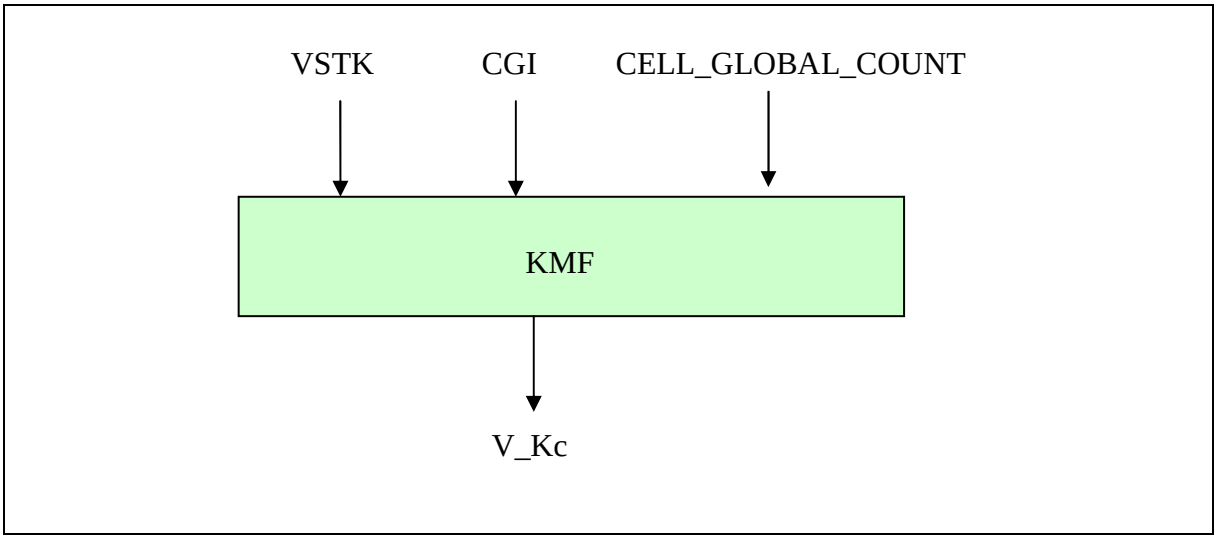


Figure F.3

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 MEís 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.

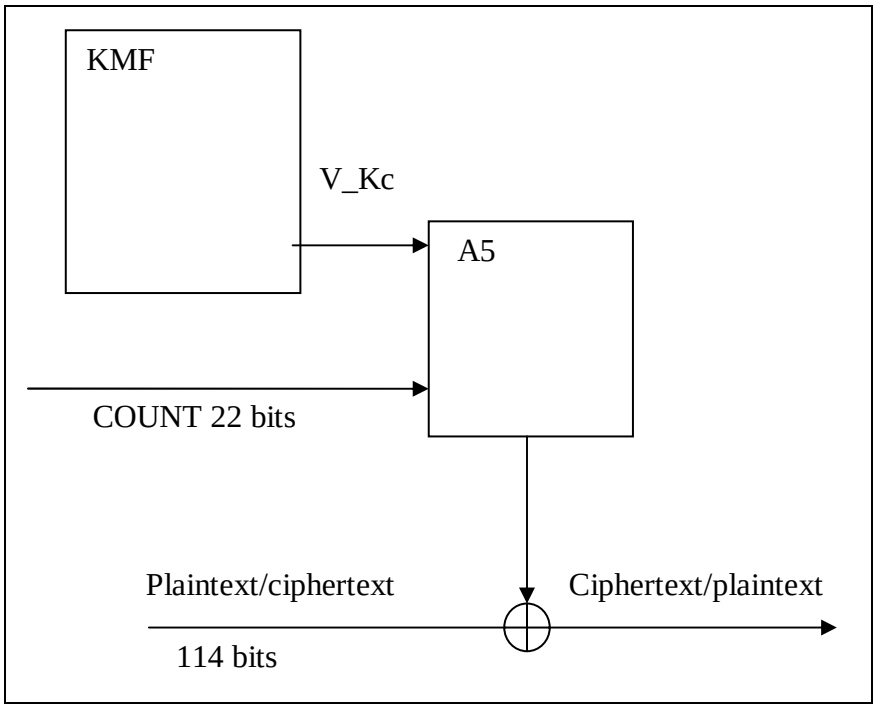


Figure F.4

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

All data variables in this Annex 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.

Since the length of VSTK_RAND (36 bits) is small, care should be taken that a VSTK_RAND isnít 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 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}	TBD371
36	10^{-4}	3707TBD

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	124	24	10^{-6}	$26.44_{10}^{10} \lozenge 10^{-}$	1	4096
36	124	24	10^{-4}	$26.44_{8}^{10} \lozenge 10^{-}$	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 ****

3GPP TSG SA WG3 Security ó S3#36 **S3-0401075**
Shenzhen, China, 23th ñ 26th October 2004

CR-Form-v7.1

CHANGE REQUEST

⌘ **43.020** **CR** **003** ⌘ **rev** **2** ⌘ 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:	⌘	Clarifying the support of algorithms within mobile stations
Source:	⌘	SA WG3
Work item code:	⌘	SEC1
Date:	⌘	17/11/2004
Category:	⌘	**C**
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:	⌘	Since the publication of the Barkan-Biham-Keller attack, the A5/2 algorithm is not considered safe anymore. Therefore it should not be supported in Rel-6 mobile stations. It is also considered appropriate to mandate A5/3 support in Rel-6 mobile stations and to mandate GEA2 and GEA3 support. The mandatory support of other algorithms that are currently implemented in mobile stations is made more explicit. It is also specified that other undefined A5 or GEA algorithms should not be supported since these could open up opportunities for attack.
Summary of change:	⌘	Clarify the support of A5 and GEA algorithms within mobile stations.
Consequences if not approved:	⌘	Attacks which exploit A5/2 weaknesses will persist for Rel-6 UEs. Opportunities are missed to take advantage of new algorithms implemented in networks.

Clauses affected:	⌘	New clause 4.9, new clause D.4.9

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

Other comments:	⌘	The intention is to phase out A5/2 within GSM networks by the end of 2005.

*** Begin of change ****

4 Confidentiality of signalling information elements, connectionless data and user information elements on physical connections

4.1 Generality

In GSM 02.09, some signalling information elements are considered sensitive and must be protected.

To ensure identity confidentiality (see clause 2), the Temporary Subscriber Identity must be transferred in a protected mode at allocation time and at other times when the signalling procedures permit it.

The confidentiality of connection less user data requires at least the protection of the message part pertaining to OSI layers 4 and above.

The user information confidentiality of user information on physical connections concerns the information transmitted on a traffic channel on the MS-BSS interface (e.g. for speech). It is not an end-to-end confidentiality service.

These needs for a protected mode of transmission are fulfilled with the same mechanism where the confidentiality function is a OSI layer 1 function. The scheme described below assumes that the main part of the signalling information elements is transmitted on DCCH (Dedicated Control Channel), and that the CCCH (Common Control Channel) is only used for the allocation of a DCCH.

Four points have to be specified:

- the ciphering method;
- the key setting;
- the starting of the enciphering and deciphering processes;
- the synchronization.

4.2 The ciphering method

The layer 1 data flow (transmitted on DCCH or TCH) is ciphered by a bit per bit or stream cipher, i.e. the data flow on the radio path is obtained by the bit per bit binary addition of the user data flow and a ciphering bit stream, generated by algorithm A5 using a key determined as specified in subclause 4.3. The key is denoted below by Kc, and is called "Ciphering Key".

For multislot configurations (e.g. HSCSD) different ciphering bit streams are used on the different timeslots. On timeslot "n" a ciphering bit stream, generated by algorithm A5, using a key Kcn is used. Kcn is derived from Kc as follows:

> Let BN denote a binary encoding onto 64 bits of the timeslot number "n" (range 0-7). Bit "i" of Kcn, Kcn(i), is then calculated as Kc(i) xor (BN<<32(i)) ("xor" indicates: "bit per bit binary addition" and "<<32" indicates: "32 bit circular shift"), the number convention being such that the lsb of Kc is xored with the lsb of the shifted BN.

Deciphering is performed by exactly the same method.

Algorithm A5 is specified in annex C.

4.3 Key setting

Mutual key setting is the procedure that allows the mobile station and the network to agree on the key Kc to use in the ciphering and deciphering algorithms A5.

A key setting is triggered by the authentication procedure. Key setting may be initiated by the network as often as the network operator wishes.

Key setting must occur on a DCCH not yet encrypted and as soon as the identity of the mobile subscriber (i.e. TMSI or IMSI) is known by the network.

The transmission of Kc to the MS is indirect and uses the authentication RAND value; Kc is derived from RAND by using algorithm A8 and the Subscriber Authentication key Ki, as defined in annex C.

As a consequence, the procedures for the management of Kc are the authentication procedures described in subclause 3.3.

The values Kc are computed together with the SRES values. The security related information (see subclause 3.3.1) consists of RAND, SRES and Kc.

The key Kc is stored by the mobile station until it is updated at the next authentication.

Key setting is schematized in figure 4.1.

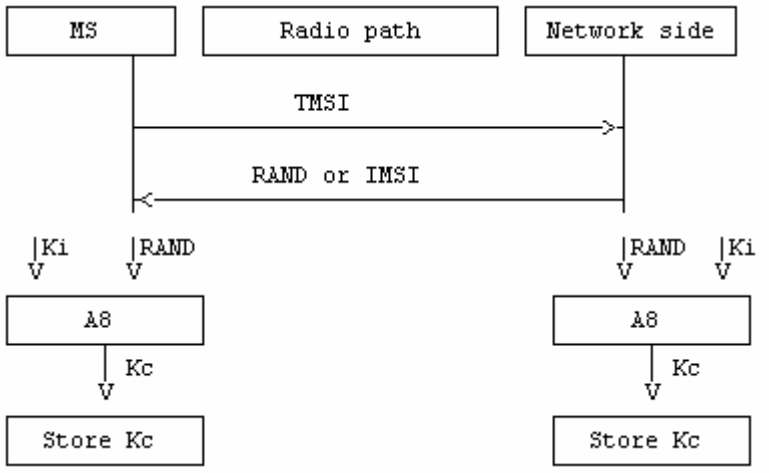


Figure 4.1: Key setting

4.4 Ciphering key sequence number

The ciphering key sequence number is a number which is associated with the ciphering key Kc and they are stored together in the mobile station and in the network.

However since it is not directly involved in any security mechanism, it is not addressed in this specification but in GSM 04.08 instead.

4.5 Starting of the ciphering and deciphering processes

The MS and the BSS must co-ordinate the instants at which the enciphering and deciphering processes start on DCCH and TCH.

On DCCH, this procedure takes place under the control of the network some time after the completion of the authentication procedure (if any), or after the key Kc has been made available at the BSS.

No information elements for which protection is needed must be sent before the ciphering and deciphering processes are operating.

The transition from clear text mode to ciphered mode proceeds as follows: deciphering starts in the BSS, which sends in clear text to the MS a specific message, here called "Start cipher". Both the enciphering and deciphering start on the MS side after the message "Start cipher" has been correctly received by the MS. Finally, enciphering on the BSS side starts as soon as a frame or a message from the MS has been correctly deciphered at the BSS.

The starting of enciphering and deciphering processes is schematized in figure 4.2.

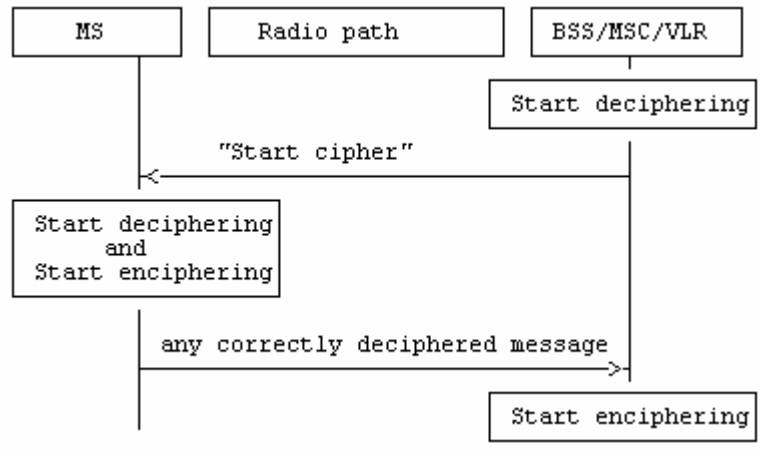


Figure 4.2: Starting of the enciphering and deciphering processes

When a TCH is allocated for user data transmission, the key used is the one set during the preceding DCCH session (Call Set-up). The enciphering and deciphering processes start immediately.

4.6 Synchronization

The enciphering stream at one end and the deciphering stream at the other end must be synchronized, for the enciphering bit stream and the deciphering bit streams to coincide. The underlying Synchronization scheme is described in annex C.

4.7 Handover

When a handover occurs, the necessary information (e.g. key Kc, initialization data) is transmitted within the system infrastructure to enable the communication to proceed from the old BSS to the new one, and the Synchronization procedure is resumed. The key Kc remains unchanged at handover.

4.8 Negotiation of A5 algorithm

Not more then seven versions of the A5 algorithm will be defined.

When an MS wishes to establish a connection with the network, the MS shall indicate to the network which of the seven versions of the A5 algorithm it supports. The network shall not provide service to an MS which indicates that it does not support the ciphering algorithm(s) required by GSM 02.07.

The network shall compare its ciphering capabilities and preferences, and any special requirements of the subscription of the MS, with those indicated by the MS and act according to the following rules:

1) If the MS and the network have no versions of the A5 algorithm in common and the network is not prepared to use an unciphered connection, then the connection shall be released.

2) If the MS and the network have at least one version of the A5 algorithm in common, then the network shall select one of the mutually acceptable versions of the A5 algorithm for use on that connection.

3) If the MS and the network have no versions of the A5 algorithm in common and the network is willing to use an unciphered connection, then an unciphered connection shall be used.

4.9 Support of A5 Algorithms in MS

It is mandatory for A5/1, A5/3 and non encrypted mode (i.e.A5/0) to be implemented in mobile stations. It is prohibited to implement A5/2 in mobile stations. No other A5 algorithms shall be supported in mobile stations.

*** End of change ****

*** Next change ****

D.4 Confidentiality of user information and signalling between MS and SGSN

D.4.1 Generality

In GSM 02.09, some signalling information elements are considered sensitive and must be protected.

To ensure identity confidentiality (see clause 2), the new TLLI must be transferred in a protected mode at allocation time.

The confidentiality of user information concerns the information transmitted on the logical connection between MS and SGSN.

These needs for a protected mode of transmission are fulfilled by a ciphering function in the LLC layer. It is not an end-to-end confidentiality service.

Four points have to be specified:

- the ciphering method;
- the key setting;
- the starting of the enciphering and deciphering processes;
- the synchronisation.

D.4.2 The ciphering method

The LLC layer information flow is ciphered by the algorithm GPRS-A5 as described in GSM 01.61.

D.4.3 Key setting

Mutual key setting is the procedure that allows the mobile station and the network to agree on the key GPRS-Kc to use in the ciphering and deciphering algorithms GPRS-A5. This procedure corresponds to the procedure described in subclause 4.3 besides the different confidential subscriber identity. The GPRS-Kc is handled by the SGSN independently from the MSC. If a MS is using both circuit switched and packet switched, two different ciphering keys will be used independently, one (Kc) in the MSC and one (GPRS-Kc) in the SGSN.

A key setting is triggered by the authentication procedure. Key setting may be initiated by the network as often as the network operator wishes. If an authentication procedure is performed during a data transfer, the new ciphering parameters shall be taken in use immediately at the end of the authentication procedure in both SGSN and MS.

Key setting may not be encrypted and shall be performed as soon as the identity of the mobile subscriber (i.e. TLLI or IMSI) is known by the network.

The transmission of GPRS-Kc to the MS is indirect and uses the authentication RAND value; GPRS-Kc is derived from RAND by using algorithm A8 and the Subscriber Authentication key Ki, in the same way as defined in annex C for Kc.

As a consequence, the procedures for the management of GPRS-Kc are the authentication procedures described in subclause D.3.3.

The values GPRS-Kc are computed together with the SRES values. The security related information (see subclause D.3.3.1) consists of RAND, SRES and GPRS-Kc.

The key GPRS-Kc is stored by the mobile station until it is updated at the next authentication.

Key setting is schematised in figure D.4.1.

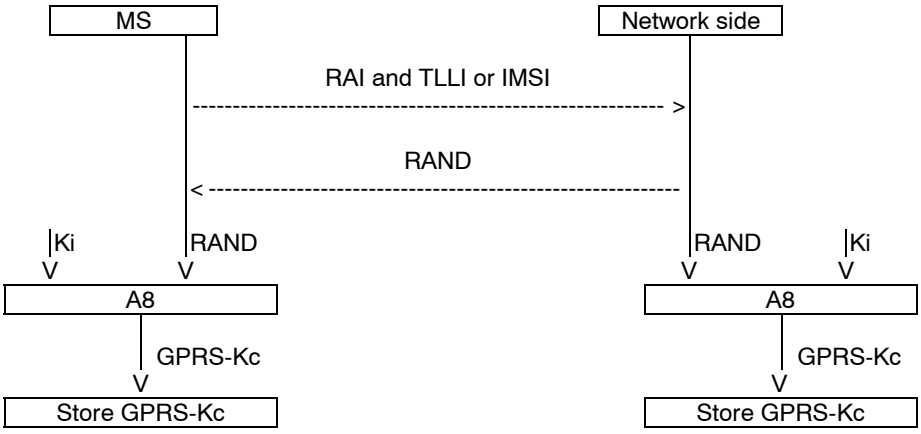


Figure D.4.1: Key setting

D.4.4 Ciphering key sequence number

The GPRS-CKSN (Ciphering Key Sequence Number) is a number which is associated with each ciphering key GPRS-Kc. The GPRS-CKSN and GPRS-Kc are stored together in the mobile station and in the network. It permits the consistency check of the keys stored in the MS and in the network. Two independent pairs, Kc and CKSN (for circuit switched), and GPRS-Kc and GPRS-CKSN (for packet switched) may be stored in the MS simultaneously.

However since it is not directly involved in any security mechanism, it is not addressed in this specification but in GSM 04.08 instead.

D.4.5 Starting of the ciphering and deciphering processes

The MS and the SGSN must co-ordinate the instants at which the ciphering and deciphering processes start. The authentication procedure governs the start of ciphering. The SGSN indicates if ciphering shall be used or not in the Authentication and Ciphering Request message. If ciphering is used, the MS starts ciphering after sending the Authentication and Ciphering Response message. The SGSN starts ciphering when a valid Authentication and Ciphering Response message is received from the MS.

Upon GPRS Attach, if ciphering is to be used, an Authentication and Ciphering Request message shall be sent to the MS to start ciphering.

If the GPRS-CKSN stored in the network does not match the GPRS-CKSN received from the MS in the Attach Request message, then the network should authenticate the MS.

As an option, the network may decide to continue ciphering without authentication after receiving a Routing Area Update Request message with a valid GPRS-CKSN. Both the MS and the network shall use the latest ciphering parameters. The MS starts ciphering after a receiving a valid ciphered Routing Area Update Accept message from the network. The SGSN starts ciphering when sending the ciphered Routing Area Update Accept message to the MS.

Upon delivery of the Authentication and Ciphering Response message or the Routing Area Update Accept message, the GPRS Mobility and Management entity in both SGSN and MS shall be aware if ciphering has started or not. LLC provides the capability to send both ciphered and unciphered PDUs. The synchronisation of ciphering at LLC frames level is done by a bit in the LLC header indicating if the frame is ciphered or not. Only a few identified signalling messages (e.g., Routing Area Update Request message) described in GSM 04.08 may be sent unciphered, any other frames sent unciphered shall be deleted. Once the encryption has been started, neither the MS nor the network shall go to an unciphered session.

D.4.6 Synchronisation

The enciphering stream at one end and the deciphering stream at the other end must be synchronised, for the enciphering bit stream and the deciphering bit streams to coincide. Synchronisation is guaranteed by driving Algorithm GPRS-A5 by an explicit variable INPUT per established LLC and direction.

These initial INPUT values shall not be identical for the different LLC link. The initial INPUT value shall be determined by the network. It may be identical for uplink and downlink value because the direction is given to the ciphering algorithm as described in GSM 01.61 and illustrated on the figure D.4.2. In a given direction, the INPUT value shall be unique for each frame.

The calculation of the INPUT value is described in GSM. The use of the INPUT value is described in GSM 01.61 and illustrated on the figure D.4.2.

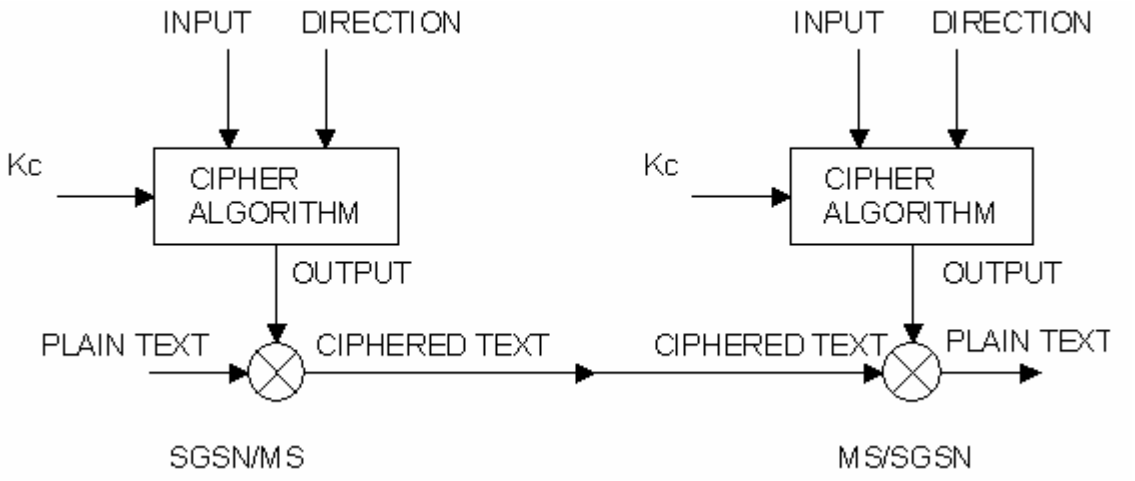


Figure D.4.2: Use of the INPUT parameter

D.4.7 Inter SGSN routing area update

When an Inter SGSN routing area update occurs, the necessary information (e.g. key Kc, INPUT parameters) is transmitted within the system infrastructure to enable the communication to proceed from the old SGSN to the new one, and the Synchronisation procedure is resumed. The key Kc may remains unchanged at Inter SGSN routing area update.

D.4.8 Negotiation of GPRS-A5 algorithm

Not more than seven versions of the GPRS-A5 algorithm will be defined.

When an MS wishes to establish a connection with the network, the MS shall indicate to the network which version(s) of the GPRS-A5 algorithm it supports. The negotiation of GPRS-A5 algorithm happens during the authentication procedure.

The network may renegotiate the version of the GPRS-A5 algorithm in use at inter SGSN routing area update by performing an authentication procedure.

The network shall compare its ciphering capabilities and preferences, and any special requirements of the subscription of the MS, with those indicated by the MS and may take one of the following decisions:

1) If the MS and the network have no versions of the GPRS A5 algorithm in common and the network is not prepared to use an unciphered connections, then the connection is released.

2) If the MS and the network have at least one version of the GPRS A5 algorithm in common, then the network shall select one of the mutually acceptable versions of the GPRS A5 algorithms for use on that connection.

3) ~~3)~~ If the MS and the network have no versions of the GPRS A5 algorithm in common and the network is willing to use an unciphered version, then an unciphered connection shall be used.

D.4.9 Support of GPRS-A5 Algorithms in MS

It is mandatory for GEA1, GEA2, GEA3 and non encrypted mode (i.e. GEA0) to be implemented in mobile stations. No other GPRS encryption algorithms shall be supported in mobile stations.