3GPP TSG CN Plenary Meeting #26 **NP-040534**
8th – 10th December 2004 Athens, Greece.

Source: TSG CN WG4

Title: Corrections on Key Management of group keys for Voice Group Call Services

Agenda item: 9.3

Document for: APPROVAL

Spec	CR	Rev	Doc-2nd-Level N4-040	Phase	Subject	Cat	Ver_C
29.002	746	1	1662	Rel-6	Introducing VGCS/VBS ciphering	B	6.7.0

3GPP TSG-CN WG4 Meeting #25 ***N4-041662***

Seoul, KOREA. 15th to 19th November 2004.

CR-Form-v7.1

CHANGE REQUEST

⌘	**29.002**	**CR**	**746**	⌘ **rev**	**1**	⌘	Current version:	**6.7.0** ⌘

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:	⌘	Introducing VGCS/VBS ciphering		
Source:	⌘	CN4		
Work item code:	⌘	SECGKYV	***Date:*** ⌘	18/11/2004
Category:	⌘	**B**	***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:	⌘	Introducing a new feature VGCS/VBS ciphering
Summary of change:	⌘	Short Term Key and RAND are added to PrepareGroupCall
Consequences if not approved:	⌘	The feature cannot be realized

Clauses affected:	⌘	10.4, 17.7.12				
		Y	**N**			
Other specs affected:	⌘	**X**		Other core specifications	⌘	43.020 CR 001
			X	Test specifications		
			X	O&M Specifications		
Other comments:	⌘					

How to create CRs using this form:

Comprehensive information and tips about how to create CRs can be found at http://www.3gpp.org/specs/CR.htm. Below is a brief summary:

1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.

2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be downloaded from the 3GPP server under ftp://ftp.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.

3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause containing the first piece of changed text. Delete those parts of the specification which are not relevant to the change request.

10.4 MAP_PREPARE_GROUP_CALL service

10.4.1 Definition

This service is used by the Anchor_MSC to inform the Relay_MSC about a group call set-up.

The MAP_PREPARE_GROUP_CALL service is a confirmed service using the service primitives given in table 10.4/1.

10.4.2 Service primitives

Table 10.4/1: MAP_PREPARE_GROUP_CALL service

Parameter name	Request	Indication	Response	Confirm
Invoke Id	M	M(=)	M(=)	M(=)
Teleservice	M	M(=)		
ASCI Call Reference	M	M(=)		
Ciphering Algorithm	M	M(=)		
Group Key Number VK-Id	C	C(=)		
VSTK~~Group~~ Key	C	C(=)		
VSTK-RAND	C	C(=)		
Priority	C	C(=)		
CODEC-Information	M	M(=)		
Uplink Free Indicator	M	M(=)		
Group Call Number			M	M(=)
User Error			C	C(=)
Provider Error				O

10.4.3 Parameter definitions and use

Invoke Id

See definition in clause 7.6.1.

Teleservice

Voice Broadcast Service or Voice Group Call Service.

ASCI Call Reference

Broadcast call reference or group call reference. This item is used to access the VBS-GCR or VGCS-GCR within the Relay_MSC.

Ciphering Algorithm

The ciphering algorithm to be used for the group call.

Group Key Number VK-Id

This Group Key Number~~number~~ has to be broadcast~~ed~~ and is used by the mobile station to derive the key for ciphering on the radio interface (see 3GPP TS 43.020 [24]).~~select the chosen group key.~~ Values 2 to 15 are reserved for future use.

Shall be present if the ciphering applies.

~~Group Key~~

~~This key is used for ciphering on the radio interface.~~

~~Shall be present if the ciphering applies.~~

VSTK

The VGCS/VBS Short Term Key is used to derive the key for ciphering on the radio interface (see 3GPP TS 43.020 [24]).

Shall be present if the ciphering applies.

VSTK-RAND

This random number has to be broadcast and is used by the mobile station to derive the group key for ciphering on the radio interface (see 3GPP TS 43.020 [24]).

Shall be present if the ciphering applies.

Priority

Default priority level related to the call if eMLPP applies.

CODEC-Information

Information on the codecs allowed for this call.

Uplink Free Indicator

A flag indicating whether the call is initiated from a dispatcher.

Group Call Number

This temporary allocated E.164 number is used for routing the call from the Anchor MSC to the Relay MSC.

User Error

For definition of this parameter see clause 7.6.1 The following errors defined in clause 7.6.1 may be used, depending on the nature of the fault:

- No Group Call Number available;
- System Failure;
- Unexpected Data Value.

Provider Error

See definition of provider error in clause 7.6.1.

********next modification*******************

17.7.12 Group Call data types

...

```
PrepareGroupCallArg ::= SEQUENCE {
     teleservice                         Ext-TeleserviceCode,
     asciCallReference                   ASCI-CallReference,
     codec-Info                          CODEC-Info,
     cipheringAlgorithm                  CipheringAlgorithm,
     groupKeyNumber-Vk-Id                [0] GroupKeyNumber                OPTIONAL,
     groupKey                            [1] Kc                            OPTIONAL,
     -- this parameter shall not be sent and shall be discarded if received
     priority                            [2] EMLPP-Priority                OPTIONAL,
     uplinkFree                          [3] NULL                          OPTIONAL,
     extensionContainer                  [4] ExtensionContainer            OPTIONAL,
     ...,
     vstk                                [5] VSTK                          OPTIONAL,
     vstk-rand                           [6] VSTK-RAND                     OPTIONAL}
```

```
VSTK ::= OCTET STRING (SIZE (16))
```

```
VSTK-RAND ::= OCTET STRING (SIZE (5))
     -- The 36 bit value is carried in bit 7 of octet 1 to bit 4 of octet 5
     -- bits 3, 2, 1, and 0 of octet 5 are padded with zeros.
```

...