3GPP TSG_CN **Tdoc NP-000267**
Plenary Meeting #8, Dusseldorf, Germany
21st – 23rd June 2000.

Source: **TSG_N WG "1"**

Title: **Support of GPRS ciphering algorithm GEA2/ R99**

Agenda item: **5.1.2**

Document for: **Discussion**

Introduction:

This document contains **"1"** CRs on **Work Item "Security/QoS",** that have been agreed by **TSG_N WG "1",** with some reservation and are forwarded to **TSG_N Plenary** meeting #8 for approval.

Tdoc	Spec	CR	Rev	CAT	Rel.	Old Ver	New Ver	Subject
N1-000722	24.008	CR211	1	F	R99	3.3.1	3.4.0	Inclusion of PFC Feature Mode in MS Network Capability IE

3GPP-CN1/SMG3WPA Meeting #12
Oahu/Hawaii, USA. 22-26 May, 2000

***Document* N1-000722**
e.g. for 3GPP use the format TP-99xxx
or for SMG, use the format P-99-xxx

CHANGE REQUEST

Please see embedded help file at the bottom of this page for instructions on how to fill in this form correctly.

24.008	CR	211r1	Current Version:	3.3.1

GSM (AA.BB) or 3G (AA.BBB) specification number ↑ *↑ CR number as allocated by MCC support team*

For submission to: TSGN#8 *list expected approval meeting # here ↑*	for approval	X	strategic		*(for SMG use only)*
	for information		non-strategic		

Form: CR cover sheet, version 2 for 3GPP and SMG *The latest version of this form is available from: ftp://ftp.3gpp.org/Information/CR-Form-v2.doc*

Proposed change affects: *(at least one should be marked with an X)*	(U)SIM		ME	X	UTRAN / Radio		Core Network	X

Source: Motorola, Ericsson **Date:** May 25, 2000

Subject: Addition of PFC Feature and Extended GEA in MS Network Capability IE

Work item: QoS & GSM/UMTS Interoperability

Category: *(only one category shall be marked with an X)*				**Release:**	
	F	Correction	X	Phase 2	
	A	Corresponds to a correction in an earlier release		Release 96	
	B	Addition of feature		Release 97	
	C	Functional modification of feature		Release 98	
	D	Editorial modification		Release 99	X
				Release 00	

Reason for change:

1) Stage 3 work has been completed in SMG2 WPA for BSS Involvement in QoS. In order for the MS to receive an SGSN-assigned PFI in the Activate PDP Context Accept message, the MS shall set a "PFC feature" indicator in the MS Network Capabilities IE in the GMM Attach Request. For this reason, the CR proposes the *addition of a PFC Feature indicator in the Network Capabilities IE*.

In addition, the CR proposes to *add support for more GPRS Encryption Algorithms.* This is in line with SA3/SMG10 that suggest the MS Network Capability IE to be extended by a another octet and the additional bits to be used to indicate the capability to support GEA/2, …, GEA/7 (see Tdoc N1-000690). Note that the GEA II ciphering algorithm has already been approved by SMG to be mandatory in R'99 starting after 31st of December 2002.

The proposed additions would increase the total length of the Network Capabilities IE from 3 to 4 octets.

2) During inter-SGSN RAU's the MS Network Capability IE is transferred to another SGSN in the MM Context IE of the SGSN Context Response message (see 3G TS 29.060). Given the different lengths of the MS Network Capability IE expected by 2G- and 3G-SGSN's this may result to incompatibility problems. Consider for instance the case where an MS is attached to a 3G-SGSN and then roams into an area controlled by a 2G-SGSN. The 2G-SGSN will receive the MS Network Capability IE from the 3G-SGSN and it *may* discard the octets after the 3rd since it cannot process them. If afterwards the MS roams again into an area controlled by a 3G-SGSN, the latter will receive the MS Network Capability IE from the 2G-SGSN but with some octets missing. Hence the new features supported by the missing octets will not be visible to the new 3G-SGSN. This can be characterized as a GSM/UMTS Interoperability problem. It must be noted that this problem may be encountered in the future for other IE's as well.

To resolve this problem the CR proposes to include the MS Network Capability IE in the RAU message.

Clauses affected:	9.4.1, 9.4.14, 10.5.5.3, 10.5.5.12			
Other specs affected:	Other 3G core specifications	**X**	→ List of CRs:	
	Other GSM core specifications		→ List of CRs:	
	MS test specifications		→ List of CRs:	
	BSS test specifications		→ List of CRs:	
	O&M specifications		→ List of CRs:	
Other comments:	Note that a PFC_FEATURE_MODE indicator (see GSM 04.60 section 12.24 “GPRS Cell Options”) is specified in the system information to indicate to R99 MSs that the PFC feature is supported by the network and therefore the R99 MS may initiate PFC procedures in the uplink direction by including a PFI in TBF establishment procedures.			


help.doc

<--------- double-click here for help and instructions on how to create a CR.

9.4 GPRS Mobility Management Messages

9.4.1 Attach request

This message is sent by the MS to the network in order to perform a GPRS or combined GPRS attach. See table 9.4.1/TS 24.008.

Message type: ATTACH REQUEST

Significance: dual

Direction: MS to network

Table 9.4.1/TS 24.008: ATTACH REQUEST message content

IEI	Information Element	Type/Reference	Presence	Format	Length
	Protocol discriminator	Protocol discriminator 10.2	M	V	1/2
	Skip indicator	Skip indicator 10.3.1	M	V	½
	Attach request message identity	Message type 10.4	M	V	1
	MS network capability	MS network capability 10.5.5.12	M	LV	~~2~~3-9
	Attach type	Attach type 10.5.5.2	M	V	½
	GPRS ciphering key sequence number	Ciphering key sequence number 10.5.1.2	M	V	½
	DRX parameter	DRX parameter 10.5.5.6	M	V	2
	P-TMSI or IMSI	Mobile identity 10.5.1.4	M	LV	6 - 9
	Old routing area identification	Routing area identification 10.5.5.15	M	V	6
	MS Radio Access capability	MS Radio Access capability 10.5.5.12a	M	LV	6 - 52
19	Old P-TMSI signature	P-TMSI signature 10.5.5.8	O	TV	4
17	Requested READY timer value	GPRS Timer 10.5.7.3	O	TV	2
9-	TMSI status	TMSI status 10.5.5.4	O	TV	1

9.4.1.1 Old P-TMSI signature

This IE is included if a valid P-TMSI and P-TMSI signature are stored in the MS.

9.4.1.2 Requested READY timer value

This IE may be included if the MS wants to indicate a preferred value for the READY timer.

9.4.1.3 TMSI status

This IE shall be included if the MS performs a combined GPRS attach and no valid TMSI is available.

********** Next Modification **********

9.4.14 Routing area update request

This message is sent by the MS to the network either to request an update of its location file or to request an IMSI attach for non-GPRS services. See table 9.4.14/TS 24.008.

Message type: ROUTING AREA UPDATE REQUEST

Significance: dual

Direction: MS to network

Table 9.4.14/TS 24.008: ROUTING AREA UPDATE REQUEST message content

IEI	Information Element	Type/Reference	Presence	Format	Length
	Protocol discriminator	Protocol discriminator 10.2	M	V	1/2
	Skip indicator	Skip indicator 10.3.1	M	V	1/2
	Routing area update request message identity	Message type 10.4	M	V	1
	Update type	Update type 10.5.5.18	M	V	1/2
	GPRS ciphering key sequence number	Ciphering key sequence number 10.5.1.2	M	V	1/2
	Old routing area identification	Routing area identification 10.5.5.15	M	V	6
	MS Radio Access capability	MS Radio Access capability 10.5.5.12a	M	LV	6 - 52
19	Old P-TMSI signature	P-TMSI signature 10.5.5.8	O	TV	4
17	Requested READY timer value	GPRS Timer 10.5.7.3	O	TV	2
27	DRX parameter	DRX parameter 10.5.5.6	O	TV	3
9-	TMSI status	TMSI status 10.5.5.4	O	TV	1
18	P-TMSI	Mobile identity 10.5.1.4	O	TLV	7
31	MS network capability	MS network capability 10.5.5.12	~~O~~O	TLV	~~3~~4-~~9~~10

9.4.14.1 Old P-TMSI signature

This IE is included by the MS if it was received from the network in an ATTACH ACCEPT or ROUTING AREA UPDATE ACCEPT message.

9.4.14.2 Requested READY timer value

This IE may be included if the MS wants to indicate a preferred value for the READY timer.

9.4.14.3 DRX parameter

This IE may be included if the MS wants to indicate new DRX parameters.

9.4.14.4 TMSI status

This IE shall be included if the MS performs a combined routing area update and no valid TMSI is available.

9.4.14.5 P-TMSI (UMTS only)

This IE shall be included by the MS.

9.4.14.x MS network capability

This IE shall be included by the MS to indicate it's capabilities to the network.

********** Next Modification **********

10.5.5.3 Ciphering algorithm

The purpose of the *ciphering algorithm* information element is to specify which ciphering algorithm shall be used.

The *ciphering algorithm* is a type 1 information element.

The *ciphering algorithm* information element is coded as shown in figure 10.5.119/TS 24.008 and table 10.5.136/TS 24.008.

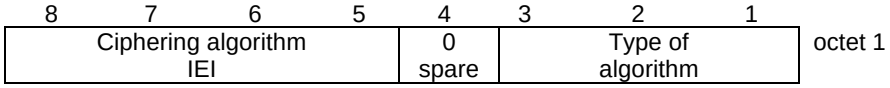

Figure 10.5.119/TS 24.008: *Ciphering algorithm* information element

Table 10.5.136/TS 24.008: *Ciphering algorithm* information element

Type of ciphering algorithm (octet 1)			
Bits			
3	**2**	**1**	
0	0	0	ciphering not used
0	0	1	GPRS Encryption Algorithm GEA/1
0	1	0	GPRS Encryption Algorithm GEA/2
0	1	1	GPRS Encryption Algorithm GEA/3
1	0	0	GPRS Encryption Algorithm GEA/4
1	0	1	GPRS Encryption Algorithm GEA/5
1	1	0	GPRS Encryption Algorithm GEA/6
1	1	1	GPRS Encryption Algorithm GEA/7

~~All other values are interpreted *reserved* by this version of the protocol.~~

********** Next Modification **********

10.5.5.12 MS network capability

The purpose of the *MS network capability* information element is to provide the network with information concerning aspects of the mobile station related to GPRS. The contents might affect the manner in which the network handles the operation of the mobile station. The *MS network capability* information indicates general mobile station characteristics and it shall therefore, except for fields explicitly indicated, be independent of the frequency band of the channel it is sent on.

The *MS network capability* is a type 4 information element with a maximum of ~~3~~ 10 octets length.

The value part of a *MS network capability* information element is coded as shown in figure 10.5.128/TS 24.008 and table 10.5.145/TS 24.008.

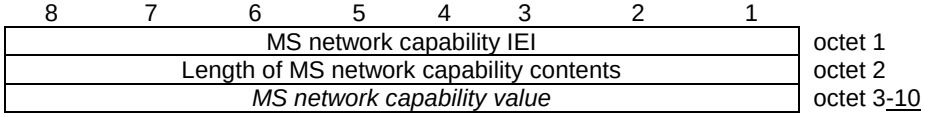

Figure 10.5.128/TS 24.008 MS network capability information element

Table 10.5.145/TS 24.008 *MS network capability* information element

<MS network capability value part> ::=

<**GEA1 bits**>
<**SM capabilities via dedicated channels**: bit>
<**SM capabilities via GPRS channels**: bit>
<**UCS2 support**: bit>
<**SS Screening Indicator**: bit string(2)>
<SoLSA Capability : bit>
<Revision level indicator: bit>
<PFC feature mode: bit>
<Extended GEA bits>
<Spare bits>;

<**GEA1 bits**> ::= < **GEA/1** :bit>;

<Extended GEA bits> ::= <GEA/2:bit><GEA/3:bit>< GEA/4:bit >< GEA/5:bit >< GEA/6:bit ><GEA/7:bit>;

<**Spare bits**> ::= null | {<spare bit> < **Spare bits** >};

SS Screening Indicator

0 0 defined in TS 24.080

0 1 defined in TS 24.080
1 0 defined in TS 24.080
1 1 defined in TS 24.080

SM capabilities via dedicated channels

0 Mobile station does not support mobile terminated point to point SMS via dedicated signalling channels
1 Mobile station supports mobile terminated point to point SMS via dedicated signalling channels

SM capabilities via GPRS channels

0 Mobile station does not support mobile terminated point to point SMS via GPRS packet data channels
1 Mobile station supports mobile terminated point to point SMS via GPRS packet data channels

UCS2 support

This information field indicates the likely treatment by the mobile station of UCS2 encoded character strings.

0 the ME has a preference for the default alphabet (defined in GSM 03.38) over UCS2.
1 the ME has no preference between the use of the default alphabet and the use of UCS2.

GPRS Encryption Algorithm GEA/1

0 encryption algorithm **GEA/1**not available
1 encryption algorithm **GEA/1** available

SoLSA Capability

0 The ME does not support SoLSA.
1 The ME supports SoLSA.

Revision level indicator

0 used by a mobile station supporting earlier versions of the protocol
1 used by a mobile station supporting this version of the protocol

PFC feature mode

0 Mobile station does not support BSS packet flow procedures
1 Mobile station does support BSS packet flow procedures

GEA/2

0 encryption algorithm GEA/2 not available
1 encryption algorithm GEA/2 available

GEA/3

0 encryption algorithm GEA/3 not available

1 encryption algorithm GEA/3 available

GEA/4

0 encryption algorithm GEA/4 not available
1 encryption algorithm GEA/4 available

GEA/5

0 encryption algorithm GEA/5 not available
1 encryption algorithm GEA/5 available

GEA/6

0 encryption algorithm GEA/6 not available
1 encryption algorithm GEA/6 available

GEA/7

0 encryption algorithm GEA/7 not available
1 encryption algorithm GEA/7 available