

<h2 style="margin: 0;">CHANGE REQUEST</h2>		Please see embedded help file at the bottom of this page for instructions on how to fill in this form correctly.
04.08	CR	A1031
		Current Version: 7.7.0
r1		
GSM (AA.BB) or 3G (AA.BBB) specification number ↑	↑ CR number as allocated by MCC support team	
For submission to: TSG CN#8 <small>list expected approval meeting # here ↑</small>	For approval for information: <input checked="" type="checkbox"/>	Strategic non-strategic: <input checked="" type="checkbox"/> (for SMG use only)

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

Source: Ericsson **Date:** 2000-05-26

Subject: Support of GEA/2 Encryption Algorithm

Work item: Security

Category: <small>(only one category shall be marked with an X)</small>	F Correction <input type="checkbox"/> A Corresponds to a correction in an earlier release <input type="checkbox"/> B Addition of feature <input checked="" type="checkbox"/> C Functional modification of feature <input type="checkbox"/> D Editorial modification <input type="checkbox"/>	Release:	Phase 2 <input type="checkbox"/> Release 96 <input type="checkbox"/> Release 97 <input type="checkbox"/> Release 98 <input checked="" type="checkbox"/> Release 99 <input type="checkbox"/> Release 00 <input type="checkbox"/>
--	--	-----------------	--

Reason for change:

The GEA II ciphering algorithm has in SMG been approved to be optional in R'98 starting after the 31st of December 2002.

The possibility to negotiate capabilities for 7 encryption algorithms has been added to R98 (e.g. the MS network capability IE has been extended in order to handle this).

Furthermore the MS Network Capability IE has been added to the Routing Area Update procedure.

Clauses affected: 9.4.1, 9.4.14, 10.5.5.3, 10.5.5.12

Other specs affected:	Other 3G core specifications <input type="checkbox"/> → List of CRs: Other GSM core specifications <input type="checkbox"/> → List of CRs: MS test specifications <input type="checkbox"/> → List of CRs: BSS test specifications <input type="checkbox"/> → List of CRs: O&M specifications <input type="checkbox"/> → List of CRs:	
------------------------------	--	--

Other comments:

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/GSM 04.08.

Message type: ATTACH REQUEST

Significance: dual

Direction: MS to network

Table 9.4.1/GSM 04.08: 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
	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 - 13
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/GSM 04.08.

Message type: ROUTING AREA UPDATE REQUEST

Significance: dual

Direction: MS to network

Table 9.4.14/GSM 04.08: 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 - 13
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
<u>31</u>	<u>MS network capability</u>	<u>MS network capability</u> <u>10.5.5.12</u>	<u>O</u>	<u>TLV</u>	<u>3-4</u>

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.x MS network capability

This IE shall be included by the MS to indicate it's capabilities to the network, if the MS supports at least one of the GPRS Encryption Algorithm GEA/2 to GEA/7.

***** 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/GSM 04.08 and table 10.5.136/GSM 04.08.

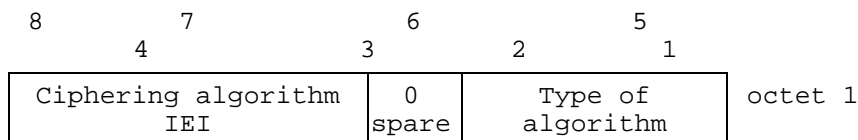


Figure 10.5.119/GSM 04.08: Ciphering algorithm information element

Table 10.5.136/GSM 04.08: Ciphering algorithm information element

<pre> 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. </pre>
--

*** 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 minimum of 3 and maximum of 34 octets length.

Octet 4 shall be included by the MS, if it supports at least one of the GPRS Encryption Algorithm GEA/2 to GEA/7. Support of octet 4 is optional in the network.

The value part of a *MS network capability* information element is coded as shown in figure 10.5.128/GSM 04.08 and table 10.5.145/GSM 04.08.

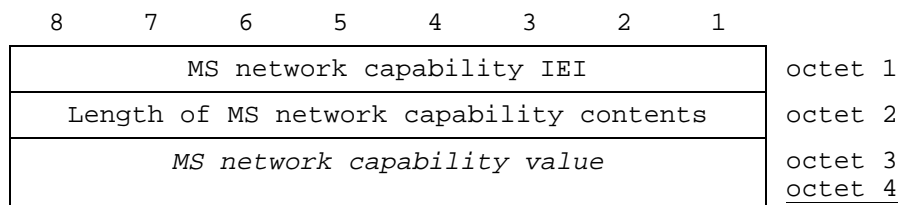


Figure 10.5.128/GSM 04.08: MS network capability information element

Table 10.5.145/GSM 04.08: 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>

<Spare bits>

<Spare bit>

<Extended GEA bits>

<Spare bit>;

<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 GSM 04.80

0 1 defined in GSM 04.80

1 0 defined in GSM 04.80

1 1 defined in GSM 04.80

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.

GPRS Encryption Algorithm GEA/2

0 encryption algorithm GEA/2 not available

1 encryption algorithm GEA/2 available

GPRS Encryption Algorithm GEA/3

0 encryption algorithm GEA/3 not available

1 encryption algorithm GEA/3 available

GPRS Encryption Algorithm GEA/40 encryption algorithm **GEA/4** not available1 encryption algorithm **GEA/4** available**GPRS Encryption Algorithm GEA/5**0 encryption algorithm **GEA/5** not available1 encryption algorithm **GEA/5** available**GPRS Encryption Algorithm GEA/6**0 encryption algorithm **GEA/6** not available1 encryption algorithm **GEA/6** available**GPRS Encryption Algorithm GEA/7**0 encryption algorithm **GEA/7** not available1 encryption algorithm **GEA/7** available