

Agenda Item:

Source: Siemens Atea

Title: Support for multiple GEA in TS 24.008

Document for: Discussion

TS 24.008 version 3.3.0 (March 2000) does not provide the ability for the MS to send the SGSN information of its ciphering capabilities other than whether it supports GEA/1 or not.

The relevant parts of TS 24.008 are attached to this page.

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
	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.

10.5.5.3 Cipherring algorithm

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

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

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

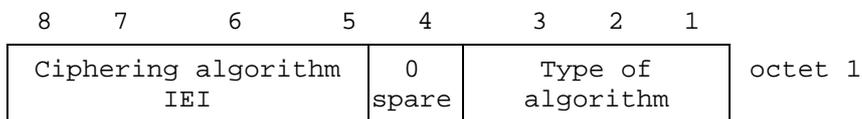


Figure 10.5.119/TS 24.008: Cipherring algorithm information element

Table 10.5.136/TS 24.008: Cipherring algorithm information element

<pre> Type of cipherring algorithm (octet 1) Bits 3 2 1 0 0 0 cipherring not used 0 0 1 GPRS Encryption Algorithm GEA/1 0 1 0 GPRS Encryption Algorithm GEA/2 All other values are interpreted reserved by this version of the protocol. </pre>

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 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.

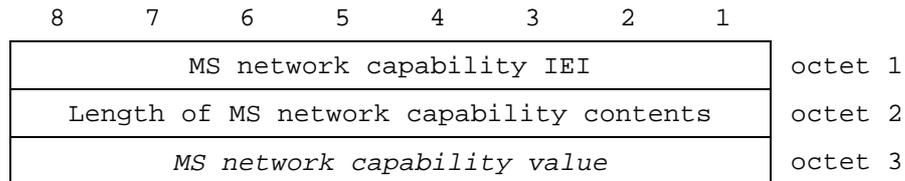


Figure 10.5.128/TS 24.008 MS network capability information element

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

<p><MS network capability value part> ::=</p> <p> <GEA 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>;</p> <p><GEA bits> ::= < GEA/1 :bit>;</p> <p><Spare bits> ::= null {<spare bit> < Spare bits >};</p> <p>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</p> <p>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</p> <p>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</p> <p>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.</p> <p>GPRS Encryption Algorithm GEA/1 0 encryption algorithm GEA/1 not available 1 encryption algorithm GEA/1 available</p> <p>SoLSA Capability 0 The ME does not support SoLSA. 1 The ME supports SoLSA.</p> <p>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</p>
