**3GPP TSG-CN-WG1, Meeting #13** ***Tdoc N1-000971***
**14-18 August, 2000**
**Vancouver/Canada**

| | |
|---|---|
| **Title:** | **Response to LS on Support of additional GPRS ciphering algorithms** |
| **Source:** | **CN WG1** |
| **TO** [1]**:** | **TSG CN, TSG SA2** |
| **Cc:** | **TSG SA, TSG S3, TSG N4** |
| **WI:** | **Security** |

**Contact Person:**

| | |
|---|---|
| **Name:** | **Monica Wifvesson, Ericsson** |
| **E-mail Address:** | **Monica.Wifvesson@ecs.ericsson** |
| **Tel. Number:** | **+46 46 193000** |

| | |
|---|---|
| **Attachments:** | **N1-001028, N1-001029** |
| **Date:** | **18. August 2000** |

TSG CN1 has been informed that TSG CN has been asked by TSG SA to reconsider the matter of introducing the possibility for the MS in Release 97 and R98 to signal it's support of the GEA/2 encryption algorithm.

TSG CN1 would like to inform TSG CN that N1 has agreed CR's to GSM 04.08 R97 and R98 regarding support of additional GPRS ciphering algorithms, which can be found in the attached Tdoc's N1-001028 and N1-001029. With this change, a R97 and R98 MS has the ability to signal its capabilities on 7 GPRS ciphering algorithms (GEA1, GEA 2, GEA3 etc.) to the network in the "MS Network Capability" IE which has been extended with one octet. Notice that a R97 and R98 network does not support the GEA2 Encryption Algorithm and will accordingly ignore the new octet in the extended MS network capability IE in the Attach Request message and also the MS Network Capability IE added as an optional IE to the Routing Area Update Request message.

While studying the issue N1 spotted an related problem which is discussed in a separate LS in N1-001023.

[1] Please write any action required from the groups in a clear way.

**3GPP CN WG1 Meeting #13**
**Vancouver, Canada, 14-18 August 2000**

***Document N1-001028***
***Rev of N1-000994***

# CHANGE REQUEST

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

| | | | | | |
|---|---|---|---|---|---|
| **04.08** | **CR** | **A1045r1** | Current Version: | 6.11.0 | |

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

| | | | | | | |
|---|---|---|---|---|---|---|
| For submission to: | TSG CN#9 | For approval | ☒ | Strategic | ☒ | *(for SMG use only)* |
| *list expected approval meeting # here ↑* | | 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:** (U)SIM □ ME ☒ UTRAN / Radio □ Core Network ☒
*(at least one should be marked with an X)*

| | | | |
|---|---|---|---|
| **Source:** | Ericsson | **Date:** | 2000-08-15 |
| **Subject:** | Optional support of GEA/2 Encryption Algorithm in the MS | | |
| **Work item:** | GPRS | | |

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

**Reason for change:**

The support of GEA2 Encryption Algorithm is optional for the MS in R97.

This CR introduces the possibility for the MS to indicate it's support for 7 encryption algorithms in R97 (e.g. the MS network capability IE has been extended with 1 octet in order to handle this).

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

A R97 network does not support the GEA2 Encryption Algorithm and will accordingly ignore the new octet in the extended MS network capability IE in the Attach Request message and also the MS Network Capability IE added to the Routing Area Update Request message.

**Clauses affected:** 9.4.1, 9.4.14, 10.5.5.3, 10.5.5.12

| | | | |
|---|---|---|---|
| **Other specs Affected:** | Other 3G core specifications | □ | → 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:**

## 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<br>10.2 | M | V | 1/2 |
| | Skip indicator | Skip indicator<br>10.3.1 | M | V | ½ |
| | Attach request message identity | Message type<br>10.4 | M | V | 1 |
| | MS network capability | MS network capability<br>10.5.5.12 | M | LV | 2-3 |
| | Attach type | Attach type<br>10.5.5.2 | M | V | ½ |
| | GPRS ciphering key sequence number | Ciphering key sequence number<br>10.5.1.2 | M | V | ½ |
| | DRX parameter | DRX parameter<br>10.5.5.6 | M | V | 2 |
| | P-TMSI or IMSI | Mobile identity<br>10.5.1.4 | M | LV | 6 - 9 |
| | Old routing area identification | Routing area identification<br>10.5.5.15 | M | V | 6 |
| | MS Radio Access capability | MS Radio Access capability<br>10.5.5.12a | M | LV | 6 – 13 |
| 19 | Old P-TMSI signature | P-TMSI signature<br>10.5.5.8 | O | TV | 4 |
| 17 | Requested READY timer value | GPRS Timer<br>10.5.7.3 | O | TV | 2 |
| 9 | TMSI status | TMSI status<br>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.

***** New 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<br>10.2 | M | V | 1/2 |
| | Skip indicator | Skip indicator<br>10.3.1 | M | V | 1/2 |
| | Routing area update request message identity | Message type<br>10.4 | M | V | 1 |
| | Update type | Update type<br>10.5.5.18 | M | V | 1/2 |
| | GPRS ciphering key sequence number | Ciphering key sequence number<br>10.5.1.2 | M | V | 1/2 |
| | Old routing area identification | Routing area identification<br>10.5.5.15 | M | V | 6 |
| | MS Radio Access capability | MS Radio Access capability<br>10.5.5.12a | M | LV | 6 - 13 |
| 19 | Old P-TMSI signature | P-TMSI signature<br>10.5.5.8 | O | TV | 4 |
| 17 | Requested READY timer value | GPRS Timer<br>10.5.7.3 | O | TV | 2 |
| 27 | DRX parameter | DRX parameter<br>10.5.5.6 | O | TV | 3 |
| 9- | TMSI status | TMSI status<br>10.5.5.4 | O | TV | 1 |
| 31 | MS network capability | MS network capability<br>10.5.5.12 | O | TLV | 3-4 |

### 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 in addition to GEA/1 at least one of the GPRS Encryption Algorithm GEA/2 to GEA/7.

***** New 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.

| 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 | |
|---|---|---|---|---|---|---|---|---|
| Ciphering algorithm IEI | | | | 0<br>spare | Type of algorithm | | | octet 1 |

**Figure 10.5.119/GSM 04.08: *Ciphering algorithm* information element**

**Table 10.5.136/GSM 04.08: *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.~~

In this version of the protocol the network shall not allocate values other than 000 or 001 to the MS.

***** New 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 a maximum of ~~3~~4 octets length.

Octet 4 shall be included by the MS, if it supports in addition to GEA/1 at least one of the GPRS Encryption Algorithm GEA/2 to GEA/7.
In this version of the protocol the network shall ignore octet 4.

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.

| 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 | |
|---|---|---|---|---|---|---|---|---|
| MS network capability IEI | | | | | | | | octet 1 |
| Length of MS network capability contents | | | | | | | | octet 2 |
| *MS network capability value* | | | | | | | | octet 3<br>octet 4 |

**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 bit~~s~~**>
<**SM capabilities via dedicated channels**: bit>
<**SM capabilities via GPRS channels**: bit>
<**UCS2 support**: bit>
<**SS Screening Indicator**: bit string(2)>
<**Spare bit~~s~~**>
<**Spare bit**>
<**Spare bit**>
<Extended GEA bits>
<**Spare bit**>;

<**GEA1 bit~~s~~**> ::= < **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 |

**Table 10.5.145/GSM 04.08: *MS network capability* information element (cont'd)**

**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** |

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

**GPRS Encryption Algorithm GEA/5**
0 encryption algorithm **GEA/5** not available
1 encryption algorithm **GEA/5** available

**GPRS Encryption Algorithm GEA/6**
0 encryption algorithm **GEA/6** not available
1 encryption algorithm **GEA/6** available

**GPRS Encryption Algorithm GEA/7**
0 encryption algorithm GEA/7 not available
1 encryption algorithm GEA/7 available

**3GPP CN WG1 Meeting #13**
**Vancouver, Canada, 14-18 August 2000**

***Document N1-001029***
***Rev of N1-000995***

# CHANGE REQUEST

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

| | | | | |
|---|---|---|---|---|
| **04.08** | **CR** | **A1047r1** | Current Version: | 7.8.0 |

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

| | | | | | | |
|---|---|---|---|---|---|---|
| For submission to: | TSG CN#9 | For approval | X | Strategic | X | *(for SMG* |
| *list expected approval meeting # here ↑* | | for information | | non-strategic | | *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:**<br>*(at least one should be marked with an X)* | (U)SIM | | ME | X | UTRAN / Radio | | Core Network | X |

| | | | |
|---|---|---|---|
| **Source:** | Ericsson | **Date:** | 2000-08-17 |

**Subject:** Optional support of GEA/2 Encryption Algorithm in the MS

**Work item:** GPRS

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

**Reason for change:**

The support of GEA2 Encryption Algorithm is optional for the MS in R98.

This CR introduces the possibility for the MS to indicate it’s support for 7 encryption algorithms in R98 (e.g. the MS network capability IE has been extended with 1 octet in order to handle this).

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

A R98 network does not support the GEA2 Encryption Algorithm and will accordingly ignore the new octet in the extended MS network capability IE in the Attach Request message and also the MS Network Capability IE added to the Routing Area Update Request message.

**Clauses affected:** 9.4.1, 9.4.14, 10.5.5.12

| | | | | |
|---|---|---|---|---|
| **Other specs** | Other 3G core specifications | | → List of CRs: | |
| **Affected:** | 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:**

# 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<br>10.2 | M | V | 1/2 |
| | Skip indicator | Skip indicator<br>10.3.1 | M | V | ½ |
| | Attach request message identity | Message type<br>10.4 | M | V | 1 |
| | MS network capability | MS network capability<br>10.5.5.12 | M | LV | 2-3 |
| | Attach type | Attach type<br>10.5.5.2 | M | V | ½ |
| | GPRS ciphering key sequence number | Ciphering key sequence number<br>10.5.1.2 | M | V | ½ |
| | DRX parameter | DRX parameter<br>10.5.5.6 | M | V | 2 |
| | P-TMSI or IMSI | Mobile identity<br>10.5.1.4 | M | LV | 6 - 9 |
| | Old routing area identification | Routing area identification<br>10.5.5.15 | M | V | 6 |
| | MS Radio Access capability | MS Radio Access capability<br>10.5.5.12a | M | LV | 6 - 13 |
| 19 | Old P-TMSI signature | P-TMSI signature<br>10.5.5.8 | O | TV | 4 |
| 17 | Requested READY timer value | GPRS Timer<br>10.5.7.3 | O | TV | 2 |
| 9- | TMSI status | TMSI status<br>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.

***** New 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<br>10.2 | M | V | 1/2 |
| | Skip indicator | Skip indicator<br>10.3.1 | M | V | 1/2 |
| | Routing area update request message identity | Message type<br>10.4 | M | V | 1 |
| | Update type | Update type<br>10.5.5.18 | M | V | 1/2 |
| | GPRS ciphering key sequence number | Ciphering key sequence number<br>10.5.1.2 | M | V | 1/2 |
| | Old routing area identification | Routing area identification<br>10.5.5.15 | M | V | 6 |
| | MS Radio Access capability | MS Radio Access capability<br>10.5.5.12a | M | LV | 6 - 13 |
| 19 | Old P-TMSI signature | P-TMSI signature<br>10.5.5.8 | O | TV | 4 |
| 17 | Requested READY timer value | GPRS Timer<br>10.5.7.3 | O | TV | 2 |
| 27 | DRX parameter | DRX parameter<br>10.5.5.6 | O | TV | 3 |
| 9- | TMSI status | TMSI status<br>10.5.5.4 | O | TV | 1 |
| 31 | MS network capability | MS network capability<br>10.5.5.12 | O | TLV | 3-4 |

### 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 in addition to GEA/1 at least one of the GPRS Encryption Algorithm GEA/2 to GEA/7.

***** New 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.

| 8 7 6 5 | 4 | 3 2 1 | |
|---|---|---|---|
| Ciphering algorithm IEI | 0<br>spare | Type of algorithm | octet 1 |

**Figure 10.5.119/GSM 04.08: *Ciphering algorithm* information element**

**Table 10.5.136/GSM 04.08: *Ciphering algorithm* information element**

Type of ~~ciphering~~ algorithm (octet 1)

Bits<br>

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.~~

In this version of the protocol the network shall not allocate values other than 000 or 001 to the MS.

## *** New 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 a maximum of ~~3~~4 octets length.

Octet 4 shall be included by the MS, if it supports in addition to GEA/1 at least one of the GPRS Encryption Algorithm GEA/2 to GEA/7.
In this version of the protocol the network shall ignore octet 4.

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.

| 8 7 6 5 4 3 2 1 | |
|---|---|
| MS network capability IEI | Octet 1 |
| Length of MS network capability contents | Octet 2 |
| *MS network capability value* | Octet 3<br>Octet 4 |

**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 bit~~s~~**>
<**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 bit~~s~~**>
<Spare bit>
<Extended GEA bits>
<**Spare bit**>;

<**GEA1 bit~~s~~**> ::= < **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/4**

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

**GPRS Encryption Algorithm GEA/5**
0 encryption algorithm **GEA/5** not available
1 encryption algorithm **GEA/5** available

**GPRS Encryption Algorithm GEA/6**
0 encryption algorithm **GEA/6** not available
1 encryption algorithm **GEA/6** available

**GPRS Encryption Algorithm GEA/7**
0 encryption algorithm GEA/7 not available
1 encryption algorithm GEA/7 available