3GPP TSG CN Plenary Meeting #14 **NP-010660**
Kyoto, Japan, 12th –14th December 2001

Source: TSG CN WG 1

Title: CRs to Rel-5 on Work Item TEI5 towards 24.008

Agenda item: 9.13

Document for: APPROVAL

Introduction:

This document contains **3** CRs on **Rel-5 to** Work Item **"TEI5"**, that have been agreed by **TSG CN WG1**, and are forwarded to TSG CN Plenary meeting #14 for approval.

Spec	CR	Rev	Phase	Subject	Cat	Version-Current	Version-New	Doc-2nd-Level
24.008	458	3	Rel-5	Introduction of Source Statistics Descriptor	B	5.1.0	5.2.0	N1-011620
24.008	488		Rel-5	Correction of missing actions on RAND and T3218, T3316	F	5.1.0	5.2.0	N1-011469
24.008	510	2	Rel-5	Clarification on the EDGE parameters in the Mobile Station Classmark 3 IE	F	5.1.0	5.2.0	N1-011995

3GPP TSG-CN1 Meeting #20
Brighton, England, 15.-19. October 2001

Tdoc N1-011620

CR-Form-v4

CHANGE REQUEST

⌘ **24.008** **CR** **458** ⌘ ev **3** ⌘ Current version: **5.1.0** ⌘

*For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

Proposed change affects: ⌘ (U)SIM □ ME/UE ☒ Radio Access Network ☒ Core Network ☒

Title:	⌘	Introduction of Source Statistics Descriptor
Source:	⌘	Nokia
Work item code:	⌘	TEI5
Date:	⌘	18.10.2001
Category:	⌘	**B**
Release:	⌘	REL-5

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:

2	*(GSM Phase 2)*
R96	*(Release 1996)*
R97	*(Release 1997)*
R98	*(Release 1998)*
R99	*(Release 1999)*
REL-4	*(Release 4)*
REL-5	*(Release 5)*

Reason for change:	⌘	3GPP TSG-SA2 QoS group agreed the introduction of the Source Statistics Descriptor as a new QoS parameter to 23.107 (S2-010006). It was also agreed that 29.060 and 24.008 should be updated accordingly.
Summary of change:	⌘	Chapter 10.5.6.5, QoS IE has been updated. Due to ongoing discussions in GERAN and SA2 groups about the possible addition of new values to the Source Statistics Descriptor, 4 bits are reserved for this parameter.
Consequences if not approved:	⌘	Requirements from SA2 are not fulfilled.

Clauses affected:	⌘	10.5.6.5, 9.5.1, 9.5.2, 9.5.4, 9.5.5, 9.5.9, 9.5.10, 9.5.12.		
Other specs Affected:	⌘	☒ Other core specifications	⌘	29.060, 23.107
		□ Test specifications		
		□ 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/3G_Specs/CRs.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.

****First Modified Section ****

10.5.6.5 Quality of service

The purpose of the *quality of service* information element is to specify the QoS parameters for a PDP context.

The QoS IE is defined to allow backward compatibility to earlier version of Session Management Protocol.

The *quality of service* is a type 4 information element with a length of 14 ~~3~~ octets.

The *quality of service* information element is coded as shown in figure 10.5.138/3GPP TS 24.008 and table 10.5.156/3GPP TS 24.008.

<table>
<tr><td>8</td><td>7</td><td>6</td><td>5</td><td>4</td><td>3</td><td>2</td><td>1</td><td></td></tr>
<tr><td colspan="8">Quality of service IEI</td><td>Octet 1</td></tr>
<tr><td colspan="8">Length of quality of service IE</td><td>Octet 2</td></tr>
<tr><td colspan="2">0 0
spare</td><td colspan="3">Delay
class</td><td colspan="3">Reliability
class</td><td>Octet 3</td></tr>
<tr><td colspan="4">Peak
throughput</td><td>0
spare</td><td colspan="3">Precedence
class</td><td>Octet 4</td></tr>
<tr><td colspan="3">0 0 0
spare</td><td colspan="5">Mean
throughput</td><td>Octet 5</td></tr>
<tr><td colspan="3">Traffic Class</td><td colspan="2">Delivery order</td><td colspan="3">Delivery of erroneous SDU</td><td>Octet 6</td></tr>
<tr><td colspan="8">Maximum SDU size</td><td>Octet 7</td></tr>
<tr><td colspan="8">Maximum bit rate for uplink</td><td>Octet 8</td></tr>
<tr><td colspan="8">Maximum bit rate for downlink</td><td>Octet 9</td></tr>
<tr><td colspan="4">Residual BER</td><td colspan="4">SDU error ratio</td><td>Octet 10</td></tr>
<tr><td colspan="6">Transfer delay</td><td colspan="2">Traffic Handling priority</td><td>Octet 11</td></tr>
<tr><td colspan="8">Guaranteed bit rate for uplink</td><td>Octet 12</td></tr>
<tr><td colspan="8">Guaranteed bit rate for downlink</td><td>Octet 13</td></tr>
<tr><td colspan="4">0 0 0 0
Spare</td><td colspan="4">Source Statistics Descriptor</td><td>Octet 14</td></tr>
</table>

Figure 10.5.138/3GPP TS 24.008: *Quality of service* information element

Table 10.5.156/3GPP TS 24.008: *Quality of service* information element

Reliability class, octet 3 (see 3GPP TS 23.107)
Bits
3 2 1
In MS to network direction:
0 0 0 Subscribed reliability class
In network to MS direction:
0 0 0 Reserved
In MS to network direction and in network to MS direction :
0 0 1 Acknowledged GTP, LLC, and RLC; Protected data
0 1 0 Unacknowledged GTP; Acknowledged LLC and RLC, Protected data
0 1 1 Unacknowledged GTP and LLC; Acknowledged RLC, Protected data
1 0 0 Unacknowledged GTP, LLC, and RLC, Protected data
1 0 1 Unacknowledged GTP, LLC, and RLC, Unprotected data
1 1 1 Reserved

All other values are interpreted as *Unacknowledged GTP and LLC; Acknowledged RLC, Protected data* in this version of the protocol.

Delay class, octet 3 (see 3GPP TS 22.060 and 3GPP TS 23.107)
Bits
6 5 4
In MS to network direction:
0 0 0 Subscribed delay class
In network to MS direction:

0 0 0 Reserved
In MS to network direction and in network to MS direction :
0 0 1 Delay class 1
0 1 0 Delay class 2
0 1 1 Delay class 3
1 0 0 Delay class 4 (best effort)
1 1 1 Reserved

All other values are interpreted as *Delay class 4 (best effort)* in this version of the protocol.
Bit 7 and 8 of octet 3 are spare and shall be coded all 0.
Precedence class, octet 4 (see 3GPP TS 23.107)
Bits
3 2 1
In MS to network direction:
0 0 0 Subscribed precedence
In network to MS direction:
0 0 0 Reserved
In MS to network direction and in network to MS direction :
0 0 1 High priority
0 1 0 Normal priority
0 1 1 Low priority
1 1 1 Reserved

All other values are interpreted as *Normal priority* in this version of the protocol.

Bit 4 of octet 4 is spare and shall be coded as 0.

Peak throughput, octet 4 (see 3GPP TS 23.107)
Bits
8 7 6 5
In MS to network direction:
0 0 0 0 Subscribed peak throughput
In network to MS direction:
0 0 0 0 Reserved
In MS to network direction and in network to MS direction :
0 0 0 1 Up to 1 000 octet/s
0 0 1 0 Up to 2 000 octet/s
0 0 1 1 Up to 4 000 octet/s
0 1 0 0 Up to 8 000 octet/s
0 1 0 1 Up to 16 000 octet/s
0 1 1 0 Up to 32 000 octet/s
0 1 1 1 Up to 64 000 octet/s
1 0 0 0 Up to 128 000 octet/s
1 0 0 1 Up to 256 000 octet/s
1 1 1 1 Reserved

All other values are interpreted as *Up to 1 000 octet/s* in this version of the protocol.
Mean throughput, octet 5 (see 3GPP TS 23.107)
Bits
5 4 3 2 1

In MS to network direction:
0 0 0 0 0 Subscribed mean throughput
In network to MS direction:
0 0 0 0 0 Reserved
In MS to network direction and in network to MS direction :
0 0 0 0 1 100 octet/h
0 0 0 1 0 200 octet/h
0 0 0 1 1 500 octet/h
0 0 1 0 0 1 000 octet/h
0 0 1 0 1 2 000 octet/h
0 0 1 1 0 5 000 octet/h
0 0 1 1 1 10 000 octet/h
0 1 0 0 0 20 000 octet/h
0 1 0 0 1 50 000 octet/h
0 1 0 1 0 100 000 octet/h
0 1 0 1 1 200 000 octet/h
0 1 1 0 0 500 000 octet/h
0 1 1 0 1 1 000 000 octet/h
0 1 1 1 0 2 000 000 octet/h
0 1 1 1 1 5 000 000 octet/h
1 0 0 0 0 10 000 000 octet/h
1 0 0 0 1 20 000 000 octet/h
1 0 0 1 0 50 000 000 octet/h
1 1 1 1 0 Reserved
1 1 1 1 1 Best effort
The value Best effort indicates that throughput shall be made available to the MS on a per need and availability basis.
All other values are interpreted as *Best effort* in this
version of the protocol.

Bits 8 to 6 of octet 5 are spare and shall be coded all 0.

Delivery of erroneous SDUs, octet 6 (see 3GPP TS 23.107)
Bits
3 2 1
In MS to network direction:
0 0 0 Subscribed delivery of erroneous SDUs
In network to MS direction:
0 0 0 Reserved
In MS to network direction and in network to MS direction :
0 0 1 No detect ('-')
0 1 0 Erroneous SDUs are delivered ('yes')
0 1 1 Erroneous SDUs are not delivered ('no')
1 1 1 Reserved

The network shall map all other values not explicitly defined onto one of the values defined in this version of the protocol. The network shall return a negotiated value which is explicitly defined in this version of this protocol.

The MS shall consider all other values as reserved.

Delivery order, octet 6 (see 3GPP TS 23.107)
Bits
5 4 3
In MS to network direction:
0 0 Subscribed delivery order
In network to MS direction:
0 0 Reserved
In MS to network direction and in network to MS direction :
0 1 With delivery order ('yes')
1 0 Without delivery order ('no')
1 1 Reserved

Traffic class, octet 6 (see 3GPP TS 23.107)
Bits
8 7 6
In MS to network direction:
0 0 0 Subscribed traffic class
In network to MS direction:
0 0 0 Reserved
In MS to network direction and in network to MS direction :
0 0 1 Conversational class
0 1 0 Streaming class
0 1 1 Interactive class
1 0 0 Background class
1 1 1 Reserved

The network shall map all other values not explicitly defined onto one of the values defined in this version of the protocol. The network shall return a negotiated value which is explicitly defined in this version of this protocol.

The MS shall consider all other values as reserved.

Maximum SDU size, octet 7 (see 3GPP TS 23.107)
In MS to network direction:
0 0 0 0 0 0 0 0 Subscribed maximum SDU size
1 1 1 1 1 1 1 1 Reserved
In network to MS direction:
0 0 0 0 0 0 0 0 Reserved
1 1 1 1 1 1 1 1 Reserved
In MS to network direction and in network to MS direction :

For values in the range 00000001 to 10010110 the Maximum SDU size value is binary coded in 8 bits, using a granularity of 10 octets, giving a range of values from 10 octets to 1500 octets.
Values above 10010110 are as below:
1 0 0 1 0 1 1 1 1502 octets
1 0 0 1 1 0 0 0 1510 octets
1 0 0 1 1 0 0 1 1520 octets

The network shall map all other values not explicitly defined onto one of the values defined in this version of the protocol. The network shall return a negotiated value which is explicitly defined in this version of this protocol.

The MS shall consider all other values as reserved.

Maximum bit rate for uplink, octet 8
Bits
8 7 6 5 4 3 2 1
In MS to network direction:
0 0 0 0 0 0 0 0 Subscribed maximum bit rate for uplink
In network to MS direction:
0 0 0 0 0 0 0 0 Reserved
In MS to network direction and in network to MS direction :
0 0 0 0 0 0 0 1 The maximum bit rate is binary coded in 8 bits, using a granularity of 1 kbps
0 0 1 1 1 1 1 1 giving a range of values from 1 kbps to 63 kbps in 1 kbps increments.

0 1 0 0 0 0 0 0 The maximum bit rate is 64 kbps + ((the binary coded value in 8 bits –01000000) * 8 kbps)
0 1 1 1 1 1 1 1 giving a range of values from 64 kbps to 568 kbps in 8 kbps increments.

1 0 0 0 0 0 0 0 The maximum bit rate is 576 kbps + ((the binary coded value in 8 bits –10000000) * 64 kbps)
1 1 1 1 1 1 1 0 giving a range of values from 576 kbps to 8640 kbps in 64 kbps increments.

1 1 1 1 1 1 1 1 0kbps

Maximum bit rate for downlink, octet 9 (see 3GPP TS 23.107)

Coding is identical to that of Maximum bit rate for uplink.

Residual Bit Error Rate (BER), octet 10 (see 3GPP TS 23.107)
Bits
8 7 6 5
In MS to network direction:
0 0 0 0 Subscribed residual BER
In network to MS direction:
0 0 0 0 Reserved
In MS to network direction and in network to MS direction :
The Residual BER value consists of 4 bits. The range is from $5*10^{-2}$ to $6*10^{-8}$.
0 0 0 1 $5*10^{-2}$
0 0 1 0 $1*10^{-2}$
0 0 1 1 $5*10^{-3}$
0 1 0 0 $4*10^{-3}$
0 1 0 1 $1*10^{-3}$
0 1 1 0 $1*10^{-4}$
0 1 1 1 $1*10^{-5}$
1 0 0 0 $1*10^{-6}$
1 0 0 1 $6*10^{-8}$
1 1 1 1 Reserved

The network shall map all other values not explicitly defined onto one of the values defined in this version of the protocol. The network shall return a negotiated value which is explicitly defined in this version of the protocol.

The MS shall consider all other values as reserved.

SDU error ratio, octet 10 (see 3GPP TS 23.107)
Bits
4 3 2 1
In MS to network direction:
0 0 0 0 Subscribed SDU error ratio
In network to MS direction:
0 0 0 0 Reserved
In MS to network direction and in network to MS direction :
The SDU error ratio value consists of 4 bits. The range is is from $1*10^{-1}$ to $1*10^{-6}$.
0 0 0 1 $1*10^{-2}$
0 0 1 0 $7*10^{-3}$
0 0 1 1 $1*10^{-3}$
0 1 0 0 $1*10^{-4}$
0 1 0 1 $1*10^{-5}$
0 1 1 0 $1*10^{-6}$
0 1 1 1 $1*10^{-1}$
1 1 1 1 Reserved

The network shall map all other values not explicitly defined onto one of the values defined in this version of the protocol. The network shall return a negotiated value which is explicitly defined in this version of the protocol.

The MS shall consider all other values as reserved.

Traffic handling priority, octet 11 (see 3GPP TS 23.107)
Bits
2 1
In MS to network direction:
0 0 Subscribed traffic handling priority
In network to MS direction:
0 0 Reserved
In MS to network direction and in network to MS direction :
0 1 Priority level 1
1 0 Priority level 2
1 1 Priority level 3

The Traffic handling priority value is ignored if the Traffic Class is Conversation class, Streaming class or Background class.

Transfer delay, octet 11 (See 3GPP TS 23.107)
Bits
8 7 6 5 4 3

In MS to network direction:
0 0 0 0 0 0 Subscribed transfer delay
In network to MS direction:
0 0 0 0 0 0 Reserved
In MS to network direction and in network to MS direction :

0 0 0 0 0 1 The Transfer delay is binary coded in 6 bits, using a granularity of 10 ms
0 0 1 1 1 1giving a range of values from 10 ms to 150 ms in 10 ms increments

0 1 0 0 0 0 The transfer delay is 200 ms + ((the binary coded value in 6 bits – 010000) * 50 ms)
0 1 1 1 1 1 giving a range of values from 200 ms to 950 ms in 50ms increments

1 0 0 0 0 0 The transfer delay is 1000 ms + ((the binary coded value in 6 bits – 100000) * 100 ms)
1 1 1 1 1 0 giving a range of values from 1000 ms to 4100 ms in 100ms increments

1 1 1 1 1 1 Reserved
.
The Transfer delay value is ignored if the Traffic Class is Interactive class or Background class.
Guaranteed bit rate for uplink, octet 12 (See 3GPP TS 23.107)

Coding is identical to that of Maximum bit rate for uplink.

The Guaranteed bit rate for uplink value is ignored if the Traffic Class is Interactive class or Background class, or Maximum bit rate for uplink is set to 0 kbps.
Guaranteed bit rate for downlink, octet 13(See 3GPP TS 23.107)

Coding is identical to that of Maximum bit rate for uplink.

The Guaranteed bit rate for downlink value is ignored if the Traffic Class is Interactive class or Background class, or Maximum bit rate for downlink is set to 0 kbps.

Source Statistics Descriptor, octet 14 (see 3GPP TS 23.107)
Bits

4 3 2 1

In MS to network direction
0 0 0 0 unknown
0 0 0 1 speech

The MS shall consider all other values as unknown.
Bits 8 to 5 of octet 14 are spare and shall be coded all 0.

******Next Modified Section ******

9.5.1 Activate PDP context request

This message is sent by the MS to the network to request activation of a PDP context.
See table 9.5.1/3GPP TS 24.008.

Message type:	ACTIVATE PDP CONTEXT REQUEST
Significance:	global
Direction:	MS to network

Table 9.5.1/3GPP TS 24.008: ACTIVATE PDP CONTEXT REQUEST message content

IEI	Information Element	Type/Reference	Presence	Format	Length
	Protocol discriminator	Protocol discriminator 10.2	M	V	1/2
	Transaction identifier	Transaction identifier 10.3.2	M	V	1/2– 3/2
	Activate PDP context request message identity	Message type 10.4	M	V	1
	Requested NSAPI	Network service access point identifier 10.5.6.2	M	V	1
	Requested LLC SAPI	LLC service access point identifier 10.5.6.9	M	V	1
	Requested QoS	Quality of service 10.5.6.5	M	LV	13~~2~~
	Requested PDP address	Packet data protocol address 10.5.6.4	M	LV	3 - 19
28	Access point name	Access point name 10.5.6.1	O	TLV	3 - 102
27	Protocol configuration options	Protocol configuration options 10.5.6.3	O	TLV	3 - 253

******Next Modified Section ******

9.5.2 Activate PDP context accept

This message is sent by the network to the MS to acknowledge activation of a PDP context.
See table 9.5.2/3GPP TS 24.008.

Message type: ACTIVATE PDP CONTEXT ACCEPT

Significance: global

Direction: network to MS

Table 9.5.2/3GPP TS 24.008: ACTIVATE PDP CONTEXT ACCEPT message content

IEI	Information Element	Type/Reference	Presence	Format	Length
	Protocol discriminator	Protocol discriminator 10.2	M	V	1/2
	Transaction identifier	Transaction identifier 10.3.2	M	V	1/2– 3/2
	Activate PDP context accept message identity	Message type 10.4	M	V	1
	Negotiated LLC SAPI	LLC service access point identifier 10.5.6.9	M	V	1
	Negotiated QoS	Quality of service 10.5.6.5	M	LV	13~~2~~
	Radio priority	Radio priority 10.5.7.2	M	V	1/2
	Spare half octet	Spare half octet 10.5.1.8	M	V	1/2
2B	PDP address	Packet data protocol address 10.5.6.4	O	TLV	4 - 20
27	Protocol configuration options	Protocol configuration options 10.5.6.3	O	TLV	3 - 253
34	Packet Flow Identifier	Packet Flow Identifier 10.5.6.11	O	TLV	3

******Next Modified Section ******

9.5.4 Activate Secondary PDP Context Request

This message is sent by the MS to the network to request activation of an additional PDP context associated with the same PDP address and APN as an already active PDP context. See Table 9.5.4/3GPP TS 24.008.

Message type: ACTIVATE SECONDARY PDP CONTEXT REQUEST

Significance: global

Direction: MS to network

Table 9.5.4/3GPP TS 24.008: Activate SECONDARY PDP context request message content

IEI	Information Element	Type/Reference	Presence	Format	Length
	Protocol discriminator	Protocol discriminator 10.2	M	V	½
	Transaction identifier	Transaction identifier 10.3.2	M	V	½– 3/2
	Activate secondary PDP context request message identity	Message type 10.4	M	V	1
	Requested NSAPI	Network service access point identifier 10.5.6.2	M	V	1
	Requested LLC SAPI	LLC service access point identifier 10.5.6.9	M	V	1
	Requested QoS	Quality of service 10.5.6.5	M	LV	13~~2~~
	Linked TI	Linked TI 10.5.6.7	M	LV	2-3
36	TFT	Traffic Flow Template 10.5.6.12	O	TLV	257

******Next Modified Section ******

9.5.5 Activate Secondary PDP Context Accept

This message is sent by the network to the MS to acknowledge activation of an additional PDP context associated with the same PDP address and APN as an already active PDP context. See Table 9.5.5/3GPP TS 24.008.

Message type: ACTIVATE SECONDARY PDP CONTEXT ACCEPT

Significance: global

Direction: network to MS

Table 9.5.5/3GPP TS 24.008: ACTIVATE SECONDARY PDP CONTEXT ACCEPT message content

IEI	Information Element	Type/Reference	Presence	Format	Length
	Protocol discriminator	Protocol discriminator 10.2	M	V	1/2
	Transaction identifier	Transaction identifier 10.3.2	M	V	1/2– 3/2
	Activate secondary PDP context accept message identity	Message type 10.4	M	V	1
	Negotiated LLC SAPI	LLC service access point identifier 10.5.6.9	M	V	1
	Negotiated QoS	Quality of service 10.5.6.5	M	LV	13~~2~~
	Radio priority	Radio priority	M	V	1/2
	Spare half octet	Spare half octet 10.5.1.8	M	V	1/2
34	Packet Flow Identifier	Packet Flow Identifier 10.5.6.11	O	TLV	3

******Next Modified Section ******

9.5.9 Modify PDP context request (Network to MS direction)

This message is sent by the network to the MS to request modification of an active PDP context. See table 9.5.9/3GPP TS 24.008.

Message type: MODIFY PDP CONTEXT REQUEST (NETWORK TO MS DIRECTION)

Significance: global

Direction: network to MS

Table 9.5.9/3GPP TS 24.008: MODIFY PDP CONTEXT REQUEST (NETWORK TO MS DIRECTION) message content

IEI	Information Element	Type/Reference	Presence	Format	Length
	Protocol discriminator	Protocol discriminator 10.2	M	V	1/2
	Transaction identifier	Transaction identifier 10.3.2	M	V	1/2– 3/2
	Modify PDP context request message identity	Message type 10.4	M	V	1
	Radio priority	Radio priority 10.5.7.2	M	V	1/2
	Spare half octet	Spare half octet 10.5.1.8	M	V	1/2
	Requested LLC SAPI	LLC service access point identifier 10.5.6.9	M	V	1
	New QoS	Quality of service 10.5.6.5	M	LV	13~~2~~
2B	PDP address	Packet data protocol address 10.5.6.4	O	TLV	4-20
34	Packet Flow Identifier	Packet Flow Identifier 10.5.6.11	O	TLV	3

******Next Modified Section ******

9.5.10 Modify PDP context request (MS to network direction)

This message is sent by the MS to the network to request modification of an active PDP context. See table 9.5.10/3GPP TS 24.008.

Message type: MODIFY PDP CONTEXT REQUEST (MS TO NETWORK DIRECTION)

Significance: global

Direction: MS to network

Table 9.5.10/3GPP TS 24.008: modify PDP context request (MS to network direction) message content

IEI	Information Element	Type/Reference	Presence	Format	Length
	Protocol discriminator	Protocol discriminator 10.2	M	V	1/2
	Transaction identifier	Transaction identifier 10.3.2	M	V	1/2– 3/2
	Modify PDP context request message identity	Message type 10.4	M	V	1
32	Requested LLC SAPI	LLC service access point identifier 10.5.6.9	O	TV	2
30	Requested new QoS	Quality of service 10.5.6.5	O	TLV	14~~3~~
31	New TFT	Traffic Flow Template 10.5.6.12	O	TLV	257

******Last Modified Section ******

9.5.12 Modify PDP context accept (Network to MS direction)

This message is sent by the network to the MS to acknowledge the modification of an active PDP context. See table 9.5.12/3GPP TS 24.008.

Message type: MODIFY PDP CONTEXT ACCEPT (NETWORK TO MS DIRECTION)

Significance: global

Direction: Network to MS

Table 9.5.12/3GPP TS 24.008: modify PDP context accept (NETWORK to ms direction) message content

IEI	Information Element	Type/Reference	Presence	Format	Length
	Protocol discriminator	Protocol discriminator 10.2	M	V	½
	Transaction identifier	Transaction identifier 10.3.2	M	V	½– 3/2
	Modify PDP context accept message identity	Message type 10.4	M	V	1
30	Negotiated QoS	Quality of service 10.5.6.5	O	TLV	14~~3~~
32	Negotiated LLC SAPI	LLC service access point identifier 10.5.6.9	O	TV	2
8	New radio priority	Radio priority 10.5.7.2	O	TV	1
34	Packet Flow Identifier	Packet Flow Identifier 10.5.6.11	O	TLV	3

3GPP TSG-CN1 Meeting #20
Brighton, England, 15.-19. October 2001

Tdoc N1-011469

CR-Form-v4

CHANGE REQUEST

⌘ **24.008 CR 488** ⌘ rev **-** ⌘ Current version: **5.1.0.** ⌘

For ***HELP*** *on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

Proposed change affects: ⌘ (U)SIM □ ME/UE ☒ Radio Access Network □ Core Network □

Title: ⌘	Correction of missing actions on RAND and T3218, T3316		
Source: ⌘	Ericsson		
Work item code: ⌘	TEI 5	***Date:*** ⌘	15th Oct 2001
Category: ⌘	**F**	***Release:*** ⌘	Rel 5

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:

2	*(GSM Phase 2)*
R96	*(Release 1996)*
R97	*(Release 1997)*
R98	*(Release 1998)*
R99	*(Release 1999)*
REL-4	*(Release 4)*
REL-5	*(Release 5)*

Reason for change: ⌘ T3218 and T3316 were introduced as guard timers when RAND and RES areto be stored at completion of an authentication challenge. However the full extent of starting and stopping T3218 and T3316 as well as all the occasions whereupon the stored RAND (and RES) has to be deleted have not been fully covered, namely:-

1. The procedure description parts only mentions the restart of timers T3218 and T3316 and not the start of these timers.
2. In sec. 11.2 it is ambigious when T3218, T3316 is to be started.
3. The case of MS deciding on authentication failure is not covered. If the mobile decides that an authentication has failed, there is no need to keep the stored RAND and there is no need to start T3218 or T3316.
4. In case CM_SERVICE_ACCEPT, CM_SERVICE_REJECT, LOCATION_UPDATING_ACCEPT or SERVICE_ACCEPT (Iu mode only), SERVICE_REJECT (Iu mode only), ROUTING_AREA_UPDATE_ACCEPT (Iu mode only) is received, the RAND and RES should have to be deleted too, along with stopping of T3218 and T3316.

Summary of change: ⌘

a) To clearly state in the procedure description parts when the timers T3218 and T3316 should be started and stopped.

b) To clarify in the procedural descriptions, sec. 11.2. and sec. 11.2.2. the actions on timer T3218, T3316 and the stored RAND when mobile concludes that authentication has failed.

c) Include in sec. 11.2 and sec. 11.2.2., stopping of T3216 or T3316 if CM_SERVICE_ACCEPT or SERVICE_ACCEPT (respectively) is received.

Consequences if not approved: ⌘ Firstly, misalignment will remain between the procedural parts and section on system parameters regarding timers T3218 and T3316.

Secondly, there is a risk that should the second AUTHENTICATION_REQUEST -

	(from the network) after an AUTHENTICATION_FAILURE (by the mobile) - carry the same RAND, the present specifications is unclear whether the mobile may immediately respond with a AUTHENTICATION_FAILURE or ask the SIM to run the Authentication again.. Consequently cell barring (resulting from failure of Authentication procdure) could occur more frequently than need be. Thirdly, the stored RAND and RES might be kept longer than should be, thereby increasing security risks.

Clauses affected:	⌘	4.3.2.2., 4.3.2.5.1., 4.7.7.2., 4.7.7.5.1., 11.2, 11.2.2.			
Other specs affected:	⌘	□	Other core specifications	⌘	
		□	Test specifications		
		□	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/3G_Specs/CRs.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.

****************************** NEXT SECTION MODIFIED *************************************

4.3.2.2 Authentication response by the mobile station

The mobile station shall be ready to respond upon an AUTHENTICATION REQUEST message at any time whilst a RR connection exists. With exception of the cases described in 4.3.2.5.1, it shall process the challenge information and send back an AUTHENTICATION RESPONSE message to the network.

A MS which does not support the UMTS authentication algorithm shall ignore the Authentication Parameter AUTN IE if included in the AUTHENTICATION REQUEST message and shall proceed as in case of a GSM authentication challenge. It shall not perform the authentication of the network described in 4.3.2.5.1.

In a GSM authentication challenge, the new GSM ciphering key calculated from the challenge information shall overwrite the previous GSM ciphering key and any previously stored UMTS ciphering key and UMTS integrity key shall be deleted. The new GSM ciphering key shall be stored on the SIM together with the ciphering key sequence number.

In a UMTS authentication challenge, the new UMTS ciphering key, the new GSM ciphering key and the new UMTS integrity key calculated from the challenge information shall overwrite the previous UMTS ciphering key, GSM ciphering key and UMTS integrity key. The new UMTS ciphering key, GSM ciphering key and UMTS integrity key are stored on the SIM together with the ciphering key sequence number.

The SIM will provide the mobile station with the authentication response, based upon the authentication challenge given from the ME. A UMTS authentication challenge will result in the SIM passing a RES to the ME. A GSM authentication challenge will result in the SIM passing a SRES to the ME.

A ME ~~mobile station~~ supporting UMTS authentication challenge may support the following procedure.

In order to avoid a synchronisation failure, if the same RAND is received twice, the mobile station shall store the received RAND together with ~~and~~ the RES returned from the SIM in the volatile memory and compare it with any subsequently received RAND values, until the RAND value stored in the mobile station is deleted. If the stored RAND value is equal to the new received value in the AUTHENTICATION REQUEST message, then the mobile station shall not pass the RAND to the SIM, but shall immediately send the AUTHENTICATION RESPONSE message with the stored RES. If there is no valid stored RAND in the mobile station or the stored RAND is different from the new received value in the AUTHENTICATION REQUEST message, the mobile station shall pass the RAND to the SIM, shall override any previously stored RAND and RES with the new ones and start , or reset and restart timer T3218.

The RAND and RES values stored in the mobile station shall be deleted and timer T3218, if running, shall be stopped:

- upon receipt of a SECURITY MODE COMMAND (Iu mode only),
  CIPHERING MODE COMMAND (A/Gb mode only),
  CM_SERVICE_ACCEPT,
  CM_SERVICE_REJECT,
  LOCATION_UPDATING_ACCEPT
  or AUTHENTICATION REJECT message;
- upon expiry of timer T3218; or
- if the mobile station enters the MM state MM IDLE or NULL.

4.3.2.3 Authentication processing in the network

Upon receipt of the AUTHENTICATION RESPONSE message, the network stops the timer T3260 and checks the validity of the response (see GSM 03.20 in case of a GSM authentication challenge respective 3GPP TS 33.102 in case of an UMTS authentication challenge).

Upon receipt of the AUTHENTICATION FAILURE message, the network stops the timer T3260. In Synch failure case, the core network may renegotiate with the HLR/AuC and provide the MS with new authentication parameters.

****************************** NEXT SECTION MODIFIED *************************************

The mobile station stores the ciphering key sequence number with the GSM ciphering key (in case of a GSM authentication challenge) and the UMTS ciphering key and the UMTS integrity key (in case of a UMTS authentication challenge) and indicates to the network in the first message (LOCATION UPDATING REQUEST, CM SERVICE REQUEST, PAGING RESPONSE, CM RE-ESTABLISHMENT REQUEST) which ciphering key sequence number the stored GSM ciphering key (in case of a GSM authentication challenge) or set of UMTS ciphering, UMTS integrity and derived GSM ciphering keys (in case of a UMTS authentication challenge) has.

When the deletion of the ciphering key sequence number is described this also means that the associated GSM ciphering key, the UMTS ciphering key and the UMTS integrity key shall be considered as invalid (i.e. the established GSM security context or the UMTS security context is no longer valid).

In GSM, the network may choose to start ciphering with the stored GSM ciphering key (under the restrictions given in GSM 02.09) if the stored ciphering key sequence number and the one given from the mobile station are equal.

In UMTS, the network may choose to start ciphering and integrity with the stored UMTS ciphering key and UMTS integrity key (under the restrictions given in GSM 02.09 and 3GPP TS 33.102) if the stored ciphering key sequence number and the one given from the mobile station are equal.

NOTE: In some specifications the term KSI (Key Set Identifier) might be used instead of the term ciphering key sequence number.

4.3.2.5 Authentication not accepted by the network

If authentication fails, i.e. if the response is not valid, the network may distinguish between the two different ways of identification used by the mobile station:

- the TMSI was used;
- the IMSI was used.

If the TMSI has been used, the network may decide to initiate the identification procedure. If the IMSI given by the mobile station then differs from the one the network had associated with the TMSI, the authentication should be restarted with the correct parameters. If the IMSI provided by the MS is the expected one (i.e. authentication has really failed), the network should proceed as described below.

If the IMSI has been used, or the network decides not to try the identification procedure, an AUTHENTICATION REJECT message should be transferred to the mobile station.

After having sent this message, all MM connections in progress (if any) are released and the network should initiate the RR connection release procedure described in clause 3.5.of 04.18 (GSM) or in 3GPP TS 25.331 (UMTS).

Upon receipt of an AUTHENTICATION REJECT message, the mobile station shall set the update status in the SIM to U3 ROAMING NOT ALLOWED, delete from the SIM the stored TMSI, LAI and ciphering key sequence number. The SIM shall be considered as invalid until switching off or the SIM is removed.

If the AUTHENTICATION REJECT message is received in the state IMSI DETACH INITIATED the mobile station shall follow clause 4.3.4.3.

If the AUTHENTICATION REJECT message is received in any other state the mobile station shall abort any MM specific, MM connection establishment or call re-establishment procedure, stop any of the timers T3210 or T3230 (if running), release all MM connections (if any), start timer T3240 and enter the state WAIT FOR NETWORK COMMAND, expecting the release of the RR connection. If the RR connection is not released within a given time controlled by the timer T3240, the mobile station shall abort the RR connection. In both cases, either after a RR connection release triggered from the network side or after a RR connection abort requested by the MS-side, the MS enters state MM IDLE, substate NO IMSI. If the MS has a separate ongoing RR connection to a different core network node, it shall consider this separate connection as still being good.

4.3.2.5.1 Authentication not accepted by the MS

In a UMTS authentication challenge, the authentication procedure is extended to allow the MS to check the authenticity of the core network. Thus allowing, for instance, detection of false base station.

Following a UMTS authentication challenge, the MS may reject the core network, on the grounds of an incorrect AUTN parameter (see 3GPP TS 33.102). This parameter contains two possible causes for authentication failure:

a) MAC code failure

If the MS considers the MAC code (supplied by the core network in the AUTN parameter) to be invalid, it shall send an AUTHENTICATION FAILURE message to the network, with the reject cause 'MAC failure'. The MS shall then follow the procedure described in clause 4.3.2.6 (c).

b) SQN failure

If the MS considers the SQN (supplied by the core network in the AUTN parameter) to be out of range, it shall send a AUTHENTICATION FAILURE message to the network, with the reject cause 'Synch failure' and a re-synchronization token AUTS provided by the SIM (see 3GPP TS 33.102). The MS shall then follow the procedure described in clause 4.3.2.6 (d).

In UMTS, an MS which supports the UMTS authentication algorithm shall reject the authentication challenge if no Authentication Parameter AUTN IE was present in the AUTHENTICATION REQUEST message (i.e. a GSM authentication challenge has been received when the MS expects a UMTS authentication challenge). In such a case, the MS shall send the AUTHENTICATION FAILURE message to the network, with the reject cause ‘GSM authentication unacceptable. The MS shall then follow the procedure described in section 4.3.2.6 (c).

If the MS returns an AUTHENTICATION_FAILURE message to the network, the MS shall delete any previously stored RAND and RES and shall stop timer T3218, if running.

4.3.2.6 Abnormal cases

(a) RR connection failure:

Upon detection of a RR connection failure before the AUTHENTICATION RESPONSE is received, the network shall release all MM connections (if any) and abort any ongoing MM specific procedure.

(b) Expiry of timer T3260:

The authentication procedure is supervised on the network side by the timer T3260. At expiry of this timer the network may release the RR connection. In this case the network shall abort the authentication procedure and any ongoing MM specific procedure, release all MM connections if any, and initiate the RR connection release procedure described in clause 3.5.

(c) Authentication failure (reject cause 'MAC failure' or ‘GSM authentication unacceptable’):

The MS shall send an AUTHENTICATION FAILURE message, with reject cause 'MAC failure' or ‘GSM authentication unacceptable’ according to section 4.3.2.5.1, to the network and start timer T3214. Upon receipt of an AUTHENTICATION FAILURE message from the MS, with reject cause 'MAC failure' or ‘GSM authentication unacceptable’ the network may initiate the identification procedure described in clause 4.3.3. This is to allow the network to obtain the IMSI from the MS. The network may then check that the TMSI originally used in the authentication challenge corresponded to the correct IMSI. Upon receipt of the IDENTITY REQUEST message from the network, the MS shall send the IDENTITY RESPONSE message.

If the TMSI/IMSI mapping in the network was incorrect, the network should respond by sending a new AUTHENTICATION REQUEST message to the MS. Upon receiving the second AUTHENTICATION REQUEST message from the network, the MS shall stop the timer T3214, if running, and then process the challenge information as normal.

When the first AUTHENTICATION REQUEST message containing an invalid MAC has been received by the MS from the network, the MS shall stop any of the retransmission timers that are running (i.e. T3210, T3220 or T3230).

Upon successfully validating the network (an AUTHENTICATION REQUEST that contains a valid MAC is received), the MS shall send the AUTHENTICATION RESPONSE message to the network and shall start any retransmission timers (e.g. T3210, T3220 or T3230) , if they were running and stopped when the MS received the first AUTHENTICATION REQUEST message containing an invalid MAC.

It can be assumed that the source of the authentication challenge is not genuine (authentication not accepted by the MS) if any of the following occur:

GSM authentication challenge. After a successful GSM authentication challenge, the GPRS GSM ciphering key and the GPRS ciphering key sequence number, are stored both in the network and the MS.

******************************* NEXT SECTION MODIFIED ***************************************

4.7.7.1 Authentication and ciphering initiation by the network

The network initiates the authentication and ciphering procedure by transferring an AUTHENTICATION AND CIPHERING REQUEST message across the radio interface and starts timer T3360. The AUTHENTICATION AND CIPHERING REQUEST message shall contain all parameters necessary to calculate the response parameters when authentication is performed (see GSM 03.20 [13] and 3GPP TS 33.102).

If authentication is requested, then the AUTHENTICATION AND CIPHERING REQUEST message shall contain either:

- In a GSM authentication challenge, the GPRS ciphering key sequence number, allocated to the GPRS GSM ciphering key and the RAND, or
- In a UMTS authentication challenge, the GPRS ciphering key sequence number, allocated to the GPRS UMTS ciphering and GPRS UMTS integrity keys, the RAND and the AUTN.

In GSM, if authentication is not requested, then the AUTHENTICATION AND CIPHERING REQUEST message shall not contain neither the GPRS ciphering key sequence number, the RAND nor the AUTN.

In GSM, if ciphering is requested, in a GSM authentication challenge or in a UMTS authentication challenge, then the AUTHENTICATION AND CIPHERING REQUEST message shall indicate the GPRS GSM ciphering algorithm.

The network includes the A&C reference number information element in the AUTHENTICATION AND CIPHERING REQUEST message. Its value is chosen in order to link an AUTHENTICATION AND CIPHERING REQUEST in a RA with its RESPONSE. The A&C reference number value might be based on the RA Colour Code value.

Additionally, the network may request the MS to include its IMEISV in the AUTHENTICATION AND CIPHERING RESPONSE message.

4.7.7.2 Authentication and ciphering response by the MS

In GSM, a MS that is attached to GPRS shall be ready to respond upon an AUTHENTICATION AND CIPHERING REQUEST message at any time.

In UMTS, an MS that is attached to GPRS shall be ready to respond upon an AUTHENTICATION AND CIPHERING REQUEST message at any time whilst a PS signalling connection exists.

A MS which does not support the UMTS authentication algorithm shall ignore the Authentication Parameter AUTN IE if included in the AUTHENTICATION AND CIPHERING REQUEST message and perform the GSM authentication challenge. It shall not perform the authentication of the network described in 4.7.7.5.1.

In a GSM authentication challenge, if the AUTHENTICATION AND CIPHERING REQUEST message includes the authentication parameters RAND and GPRS CKSN, then upon receipt of the message, the MS processes the challenge information and sends an AUTHENTICATION AND CIPHERING RESPONSE message to the network. The value of the received A&C reference number information element shall be copied into the A&C reference number information element in the AUTHENTICATION AND CIPHERING RESPONSE message. A GSM authentication challenge will result in the SIM passing a SRES and a GPRS GSM ciphering key to the ME. The new GPRS GSM ciphering key calculated from the challenge information shall overwrite the previous one and any previously stored GPRS UMTS ciphering and GPRS UMTS integrity keys shall be deleted. The calculated GSM ciphering key shall be stored on the SIM together with the GPRS ciphering key sequence number before the AUTHENTICATION AND CIPHERING RESPONSE message is transmitted.

In a UMTS authentication challenge, if the AUTHENTICATION AND CIPHERING REQUEST message includes the UMTS authentication parameters GPRS CKSN, RAND and AUTN, then upon receipt of the message, the MS verifies the AUTN parameter and if this is accepted, the MS processes the challenge information and sends an AUTHENTICATION AND CIPHERING RESPONSE message to the network. The value of the received A&C reference number information element shall be copied into the A&C reference number information element in the AUTHENTICATION AND CIPHERING RESPONSE message. A UMTS authentication challenge will result in the

SIM passing a RES, a GPRS UMTS ciphering key, a GPRS UMTS integrity key and a GPRS GSM ciphering key to the ME. The new GPRS UMTS ciphering key, GPRS UMTS integrity key and GPRS GSM ciphering key calculated from the challenge information shall overwrite the previous ones. The new GPRS UMTS ciphering key, GPRS UMTS integrity key and GPRS GSM ciphering key shall be stored on the SIM together with the GPRS ciphering key sequence number before the AUTHENTICATION AND CIPHERING RESPONSE message is transmitted.

In UMTS, an MS capable of UMTS only shall ignore the Ciphering Algorithm IE in the AUTHENTICATION AND CIPHERING REQUEST message. An MS capable of both UMTS and GSM shall store the received value in the Ciphering Algorithm IE in the AUTHENTICATION AND CIPHERING REQUEST message in order to use it at an inter system change from UMTS to GSM.

If the AUTHENTICATION AND CIPHERING REQUEST message does not include neither the GSM authentication parameters (RAND and GPRS CKSN) nor the UMTS authentication parameters (RAND, AUTN and GPRS CKSN), then upon receipt of the message, the MS replies by sending an AUTHENTICATION AND CIPHERING RESPONSE message to the network.

In GSM, the GMM layer shall notify the LLC layer if ciphering shall be used or not and if yes which GSM ciphering algorithm and GPRS GSM ciphering key that shall be used (see GSM 04.64 [76]).

A ME ~~mobile station~~ supporting UMTS authentication challenge shall support the following procedure:

In order to avoid a synchronisation failure, if the same RAND is received twice, the mobile station shall store the received RAND together with ~~and~~ the RES returned from the SIM in the volatile memory and compare it with any subsequently received RAND values, until the RAND value stored in the mobile station is deleted. If the stored RAND value is equal to the new received value in the AUTHENTICATION ~~&~~ AND CIPHERING REQUEST message, then the mobile station shall not pass the RAND to the SIM, but shall immediately send the AUTHENTICATION ~~&~~ AND CIPHERING RESPONSE message with the stored RES. If there is no valid stored RAND in the mobile station or the stored RAND is different from the new received value in the AUTHENTICATION ~~&~~ AND CIPHERING REQUEST message, the mobile station shall pass the RAND to the SIM, shall override any previously stored RAND and RES with the new ones and start , or reset and restart timer T3316.

The RAND and RES values stored in the mobile station shall be deleted and timer T3316, if running, shall be stopped:

- upon receipt of a SECURITY MODE COMMAND (Iu mode only),
  SERVICE ACCEPT (Iu mode only),
  SERVICE REJECT (Iu mode only),
  ROUTING AREA UPDATE ACCEPT
  or AUTHENTICATION ~~&~~ AND CIPHERING REJECT message;
- upon expiry of timer T3316; or
- if the mobile station enters the GMM states GMM-DEREGISTERED or GMM-NULL.

4.7.7.3 Authentication and ciphering completion by the network

Upon receipt of the AUTHENTICATION AND CIPHERING RESPONSE message, the network stops the timer T3360 and checks the validity of the response (see GSM 03.20 [13] and 3GPP TS 33.102). For this, it may use the A&C reference number information element within the AUTHENTICATION AND CIPHERING RESPONSE message to determine whether the response is correlating to the last request that was sent.

In GSM, the GMM layer shall notify the LLC sublayer if ciphering shall be used or not and if yes which algorithm and GPRS GSM ciphering key that shall be used (see GSM 04.64 [76]).

Upon receipt of the AUTHENTICATION AND CIPHERING FAILURE message, the network stops the timer T3360. In Synch failure case, the core network may renegotiate with the HLR/AuC and provide the MS with new authentication parameters.

4.7.7.4 GPRS ciphering key sequence number

The security parameters for authentication and ciphering are tied together in sets. In a GSM authentication challenge, from a challenge parameter RAND both the authentication response parameter SRES and the GPRS GSM ciphering key can be computed given the secret key associated to the IMSI. In a UMTS authentication challenge, from a challenge parameter RAND, the authentication response parameter RES and the GPRS UMTS ciphering key and the GPRS UMTS integrity key can be computed given the secret key associated to the IMSI.

If the AUTHENTICATION AND CIPHERING REJECT message is received, the MS shall abort any GMM procedure, shall stop the timers T3310, T3317 and T3330 (if running) and shall enter state GMM-DEREGISTERED.

***************************** NEXT SECTION MODIFIED ************************************

4.7.7.5.1 Authentication not accepted by the MS

In a UMTS authentication challenge, the authentication procedure is extended to allow the MS to check the authenticity of the core network. Thus allowing, for instance, detection of false base station.

Following a UMTS authentication challenge, the MS may reject the core network, on the grounds of an incorrect AUTN parameter (see 3GPP TS 33.102). This parameter contains two possible causes for authentication failure:

a) MAC code failure

If the MS considers the MAC code (supplied by the core network in the AUTN parameter) to be invalid, it shall send a AUTHENTICATION AND CIPHERING FAILURE message to the network, with the GMM cause 'MAC failure'. The MS shall then follow the procedure described in clause 4.7.7.6 (f).

b) SQN failure

If the MS considers the SQN (supplied by the core network in the AUTN parameter) to be out of range, it shall send a AUTHENTICATION AND CIPHERING FAILURE message to the network, with the GMM cause 'Synch failure' and the re-synchronization token AUTS provided by the SIM (see 3GPP TS 33.102). The MS shall then follow the procedure described in clause 4.7.7.6 (g).

In UMTS, an MS which supports the UMTS authentication algorithm shall reject the authentication challenge if no Authentication Parameter AUTN IE was present in the AUTHENTICATION REQUEST message (i.e. a GSM authentication challenge has been received when the MS expects a UMTS authentication challenge). In such a case, the MS shall send the AUTHENTICATION AND CIPHERING FAILURE message to the network with the GMM cause ‘GSM authentication unacceptable’. The MS shall then follow the procedure described in section 4.7.7.6 (f).

If the MS returns an AUTHENTICATION_AND_CIPHERING_FAILURE message to the network, the MS shall delete any previously stored RAND and RES and shall stop timer T3316, if running.

4.7.7.6 Abnormal cases on the network side

The following abnormal cases can be identified:

a) Lower layer failure

Upon detection of a lower layer failure before the AUTHENTICATION AND CIPHERING RESPONSE is received, the network shall abort the procedure.

b) Expiry of timer T3360

The network shall, on the first expiry of the timer T3360, retransmit the AUTHENTICATION AND CIPHERING REQUEST and shall reset and start timer T3360. This retransmission is repeated four times, i.e. on the fifth expiry of timer T3360, the procedure shall be aborted.

c) Collision of an authentication and ciphering procedure with a GPRS attach procedure

If the network receives an ATTACH REQUEST message before the ongoing authentication procedure has been completed and no GPRS attach procedure is pending on the network (i.e. no ATTACH ACCEPT/REJECT message has to be sent as an answer to an ATTACH REQUEST message), the network shall abort the authentication and ciphering procedure and proceed with the new GPRS attach procedure.

d) Collision of an authentication and ciphering procedure with a GPRS attach procedure when the authentication and ciphering procedure has been caused by a previous GPRS attach procedure

If the network receives an ATTACH REQUEST message before the ongoing authentication procedure has been completed and a GPRS attach procedure is pending (i.e. an ATTACH ACCEPT/REJECT message has still to be sent as an answer to an earlier ATTACH REQUEST message), then:

******************************** NEXT SECTION MODIFIED **

11.2 Timers of mobility management

Table 11.1/3GPP TS 24.008: Mobility management timers - MS-side

TIMER NUM.	MM STAT	TIME OUT VAL.	CAUSE FOR START	NORMAL STOP	AT THE EXPIRY
T3210	3	20s	- LOC_UPD_REQ sent	- LOC_UPD_ACC - LOC_UPD_REJ - AUTH_REJ - Lower layer failure	Start T3211
T3211	1 2	15s	- LOC_UPD_REJ with cause#17 netw. failure - lower layer failure or RR conn. released after RR conn. abort during loc. updating	- Time out - cell change - request for MM connection establishment - change of LA	Restart the Location update proc.
T3212	1, 2	Note 1	- termination of MM service or MM signalling	- initiation of MM service or MM signalling	initiate periodic updating
T3213	1 2 11	4s	- location updating failure	- expiry - change of BCCH parameter	new random attempt
T3214	3 5 7	20s	AUTHENT FAILURE Cause = 'MAC failure' or 'GSM authentication unacceptable' sent	AUTHENT REQ - received	Consider the network as 'false' (see 4.3.2.6.1)
T3216	3 5 7	15s	AUTHENT FAILURE Cause = Synch failure sent	AUTHENT REQ received	Consider the network as 'false' (see 4.3.2.6.1)
T3218	3 5 7	20s	RAND and RES stored as a result of ~~after receipt of~~ a UMTS authentication challenge	- Cipher mode setting (A/Gb mode only) - Security mode setting (Iu mode only) - CM_SERV_ ACCEPT received - CM SERVICE REJECT received - LOCATION UPDATING ACCEPT received - AUTHENT REJ received - AUTHENT FAIL sent - enter MM IDLE or NULL	Delete the stored RAND and RES
T3220	7	5s	- IMSI DETACH	- release from RM-sublayer	enter Null or Idle, ATTEMPTING TO UPDATE

T3230	5	15s	- CM SERV REQ CM REEST REQ	- Cipher mode setting - CM SERV REJ - CM SERV ACC	provide release ind.
T3240	9 10	10s	see clause 11.2.1	see clause 11.2.1	abort the RR connection
T3241	25	300s	see section 11.2.1	See section 11.2.1	abort the RR connection

****************************** NEXT SECTION MODIFIED **************************************

11.2.2 Timers of GPRS mobility management

Table 11.3/3GPP TS 24.008: GPRS Mobility management timers - MS side

TIMER NUM.	TIMER VALUE	STATE	CAUSE OF START	NORMAL STOP	ON THE 1st , 2nd, 3rd , 4th EXPIRY Note 3
T3310	15s	GMM-REG-INIT	ATTACH REQ sent	ATTACH ACCEPT received ATTACH REJECT received	Retransmission of ATTACH REQ
T3311	15s	GMM-DEREG ATTEMPTING TO ATTACH or GMM-REG ATTEMPTING TO UPDATE	ATTACH REJ with other cause values as described in chapter 'GPRS Attach' ROUTING AREA UPDATE REJ with other cause values as described in chapter 'Routing Area Update' Low layer failure	Change of the routing area	Restart of the Attach or the RAU procedure with updating of the relevant attempt counter
T3316	30s	GMM-REG-INIT GMM-REG GMM-DEREG-INIT GMM-RA-UPDATING-INT GMM-SERV-REQ-INIT (Iu mode only)	RAND and RES stored as a result of ~~after receipt of~~ a UMTS authentication challenge	Security mode setting (Iu mode only) SERVICE ACCEPT received. (Iu mode only) SERVICE REJECT received (Iu mode only) ROUTING AREA UPDATE ACCEPT received AUTHENTICATION & CIPHERING REJECT received AUTHENTICATION & CIPHERING FAILURE sent Enter GMM-DEREG or GMM-NULL	Delete the stored RAND and RES
T3318	20s	GMM-REG-INIT GMM-REG GMM-DEREG-INIT GMM-RA-UPDATING-INT GMM-SERV-REQ-INIT (UMTS only)	AUTHENTICATION & CIPHERING FAILURE (cause='MAC failure' or 'GSM authentication unacceptable') sent	AUTHENTICATION & CIPHERING REQUEST received	On first expiry, the MS should consider the network as false (see 4.7.7.6.1)

T3320	15s	GMM-REG-INIT GMM-REG GMM-DEREG-INIT GMM-RA-UPDATING-INT GMM-SERV-REQ-INIT (UMTS only)	AUTHENTICATION & CIPHERING FAILURE (cause=synch failure) sent	AUTHENTICATION & CIPHERING REQUEST received	On first expiry, the MS should consider the network as false (see 4.7.7.6.1)

3GPP TSG-CN1 Meeting #21
Cancun, Mexico, 26.- 30. November 2001

Tdoc N1-011995
revision of Tdoc N1-011980
revision of Tdoc N1-011850

CR-Form-v4

CHANGE REQUEST

⌘ **24.008 CR 510** ⌘ ev **2** ⌘ Current version: **5.1.0** ⌘

For ***HELP*** *on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

Proposed change affects: ⌘ (U)SIM □ ME/UE ☒ Radio Access Network ☒ Core Network ☒

Title: ⌘	Clarification on the EDGE parameters in the Mobile Station Classmark 3 IE
Source: ⌘	Siemens AG
Work item code: ⌘	TEI5
Date: ⌘	29.11.01
Category: ⌘	**F**
Release: ⌘	REL-5

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:

2	*(GSM Phase 2)*
R96	*(Release 1996)*
R97	*(Release 1997)*
R98	*(Release 1998)*
R99	*(Release 1999)*
REL-4	*(Release 4)*
REL-5	*(Release 5)*

Reason for change: ⌘	As the EDGE technology and multiple timeslots can be used for both CS dedicated and PS TBF connections, and as the Mobile Station Classmark 3 IE does not only contain CS related, but also PS related parameters (like, e.g., DTM GPRS Multi Slot Sub-Class or MS EXT UTBF), it should be clarified which of the EDGE related parameters and multi-slot related parameters in the IE are applicable to CS connections or to PS connections.
Summary of change: ⌘	For the EDGE specific parameters defined in the MS CM3 IE that are applicable only to CS connections, the term ECSD is used instead of EDGE. For the multi-slot related parameters defined in the MS CM3 IE that are applicable only to CS connections, the term HSCSD is added. Furthermore, various editorial and syntactical corrections are proposed.
Consequences if not approved: ⌘	Possible misinterpretation that the EDGE and multi-slot parameters are also applicable for the PS domain.

Clauses affected: ⌘	10.5.1.7
Other specs affected: ⌘	□ Other core specifications ⌘ □ Test specifications □ O&M Specifications
Other comments: ⌘	

10.5.1.7 Mobile Station Classmark 3

The purpose of the *Mobile Station Classmark 3* information element is to provide the network with information concerning aspects of the mobile station. The contents might affect the manner in which the network handles the operation of the mobile station. The Mobile Station Classmark 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 Classmark 3* is a type 4 information element with a maximum of 14 octets length.

The value part of a *MS Classmark 3* information element is coded as shown in figure 10.5.7/3GPP TS 24.008 and table 10.5.7/3GPP TS 24.008.

NOTE: The 14 octet limit is so that the CLASSMARK CHANGE message will fit in one layer 2 frame.

SEMANTIC RULE : a multiband mobile station shall provide information about all frequency bands it can support. A single band mobile station shall not indicate the band it supports in the *Multiband Supported*, *GSM 400 Bands Supported*, *GSM 700 Associated Radio Capability*, *GSM 850 Associated Radio Capability* or PCS *1900 Associated Radio Capability* fields in the MS Classmark 3. Due to shared radio frequency channel numbers between DCS 1800 and PCS 1900, the mobile should indicate support for either DCS 1800 band OR PCS 1900 band.

SEMANTIC RULE : a mobile station shall include the MS Measurement Capability field if the *Multi Slot Class* field contains a value of 19 or greater (see 3GPP TS 05.02).

Typically, the number of spare bits at the end is the minimum to reach an octet boundary. The receiver may add any number of bits set to "0" at the end of the received string if needed for correct decoding.

```
<Classmark 3 Value part> ::=
    < spare bit >
    {    < Multiband supported : { 000 } >
            < A5 bits >
    |    < Multiband supported : { 101 | 110 } >
            < A5 bits >
            < Associated Radio Capability 2 : bit(4) >
            < Associated Radio Capability 1 : bit(4) >
    |    < Multiband supported : { 001 | 010 | 100 } >
            < A5 bits >
            < spare bit >(4)
            < Associated Radio Capability 1 : bit(4) > }
    { 0 | 1 < R Support > }
    { 0 | 1 < HSCSD Multi Slot Capability > }
    < UCS2 treatment: bit >
    < Extended Measurement Capability : bit >
    { 0 | 1 < MS measurement capability > }
    { 0 | 1 < MS Positioning Method Capability > }
    { 0 | 1 < ECSD~~EDGE~~ Multi Slot Capability > }
    { 0 | 1 < ECSD~~EDGE~~ Struct > }
    { 0 | 1 < GSM 400 Bands Supported : { 01 | 10 | 11 } >
            < GSM 400 Associated Radio Capability: bit(4) > }

    { 0 | 1 <GSM 850 Associated Radio Capability : bit(4) > }
    { 0 | 1 <PCS 1900 Associated Radio Capability : bit(4) > }
    < UMTS FDD Radio Access Technology Capability : bit >
    < UMTS 3.84 Mcps TDD Radio Access Technology Capability : bit >
    < CDMA 2000 Radio Access Technology Capability : bit >

    { 0 | 1  < DTM GPRS Multi Slot Sub-Class : bit(2) >
            < MAC Mode Support : bit >
            {0 | 1< DTM EGPRS Multi Slot Sub-Class : bit(2) > } }
    { 0 | 1 < Single Band Support > } -- Release 4 starts here:
    { 0 | 1 <GSM 700 Associated Radio Capability : bit(4)>}

    < UMTS 1.28 Mcps TDD Radio Access Technology Capability : bit >
    < MS_EXT_UTBF : bit >
    < spare bit > ;

< A5 bits > ::=
    < A5/7 : bit > < A5/6 : bit > < A5/5 : bit > < A5/4 : bit >  ;

<R Support>::=
    < R-GSM band Associated Radio Capability : bit(3) > ;

< HSCSD Multi Slot Capability > ::=
    < HSCSD Multi Slot Class : bit(5) >  ;

< MS Measurement capability > ::=
    < SMS_VALUE : bit (4) >
    < SM_VALUE : bit (4) > ;

< MS Positioning Method Capability > ::=
    < MS Positioning Method : bit(5) > ;

< ~~EDGE~~ ECSD Multi Slot Capability > ::=
    < ~~EDGE~~ ECSD Multi Slot Class : bit(5) > ;

 <~~EDGE~~ ECSD Struct> : :=
    < Modulation Capability : bit >
    { 0 | 1 < ~~EDGE~~ ECSD RF Power Capability 1: bit(2) > }
    { 0 | 1 < ~~EDGE~~ ECSD RF Power Capability 2: bit(2) > };

< Single Band Support > ::=
    < GSM Band : bit (4) > ;
```

Figure 10.5.7/3GPP TS 24.008 *Mobile Station Classmark 3* information element

Table 10.5.7/3GPP TS 24.008: *Mobile Station Classmark 3* information element

Multiband Supported (3 bit field)

Band 1 supported (third bit of the field)
Bit 3
~~Bit 3~~
0 P-GSM not supported
1 P-GSM supported

Band 2 supported (second bit of the field)
Bit 2
~~BIT 2~~
0 E-GSM or R-GSM not supported
1 E-GSM or R-GSM supported

Band 3 supported (first bit of the field)
Bit 1
~~Bit 1~~
0 DCS 1800 not supported
1 DCS 1800 supported

The indication of support of P-GSM band or E-GSM or R-GSM band is mutually exclusive.

When the 'Band 2 supported' bit indicates support of E-GSM or R-GSM, the presence of the <R Support> field, see below, indicates if the E-GSM or R-GSM band is supported.

In this version of the protocol, the sender indicates in this field either none, one or two of these 3 bands supported.

For single band mobile station or a mobile station supporting none of the GSM 900 bands(P-GSM, E-GSM and R-GSM) and DCS 1800 bands, all bits are set to 0.

A5/4
~~Bit 1~~
0 Encryption algorithm A5/4 not available
1 Encryption algorithm A5/4 available

A5/5
~~Bit 1~~
0 Encryption algorithm A5/5 not available
1 Encryption algorithm A5/5 available

A5/6
~~Bit 1~~
0 Encryption algorithm A5/6 not available
1 Encryption algorithm A5/6 available

A5/7
0 Encryption algorithm A5/7 not available
1 Encryption algorithm A5/7 available

Associated Radio capability 1 and 2 (4 bit fields)

If either of P-GSM or E-GSM or R-GSM is supported, the radio capability 1 field indicates the radio capability for P-GSM, E-GSM or R-GSM, and the radio capability 2 field indicates the radio capability for DCS1800 if supported, and is spare otherwise.

If none of P-GSM or E-GSM or R-GSM are supported, the radio capability 1 field indicates the radio capability for DCS1800, and the radio capability 2 field is spare.

The radio capability contains the binary coding of the power class associated with the band indicated in multiband support bits (see GSMß05.05).

(continued...)

Table 10.5.1.7/3GPP TS 24.008 (continued): *MS Classmark 3* information element

~~R Support~~ R-GSM band Associated Radio Capability (3 bit field)

In case where the R-GSM band is supported the R-GSM band associated radio capability field contains the binary coding of the power class associated (see GSM 45.005) (regardless of the number of GSM bands supported). A mobile station supporting the R-GSM band shall also when appropriate, (see 10.5.1.6) indicate its support in the 'FC' bit in the Mobile Station Classmark 2 information element.

Note: the coding of the power class for P-GSM, E-GSM, R-GSM and DCS 1800 in radio capability 1 and/or 2 is different to that used in the Mobile Station Classmark 1 and Mobile Station Classmark 2 information elements.

HSCSD Multi Slot Class (5 bit field)
~~Multi Slot Class (5 bit field)~~

In case the MS supports the use of multiple timeslots for HSCSD then the HSCSD Multi Slot Class field is coded as the binary representation of the multislot class defined in TS GSM 05.02.

UCS2 treatment (1 bit field)

This information field indicates the likely treatment by the mobile station of UCS2 encoded character strings. If not included, the value 0 shall be assumed by the receiver.
~~Bit 1~~
0 the ME has a preference for the default alphabet (defined in 3GPP TS 03.38) over UCS2.
~~0 the ME has a preference for the default alphabet (defined in 3GPP TS 03.38) over UCS2.~~
1 the ME has no preference between the use of the default alphabet and the use of UCS2.
~~1 the ME has no preference between the use of the default alphabet and the use of UCS2.~~

Extended Measurement Capability (1 bit field)

This bit indicates whether the mobile station supports 'Extended Measurements' or not
~~Bit 1~~
0 the MS does not support Extended Measurements
1 the MS supports Extended Measurements

SMS_VALUE (Switch-Measure-Switch) (4 bit field)
The SMS field indicates the time needed for the mobile station to switch from one radio channel to another, perform a neighbour cell power measurement, and the switch from that radio channel to another radio channel.
Bits

4 3 2 1	
0 0 0 0	1/4 timeslot (~144 microseconds)
0 0 0 1	2/4 timeslot (~288 microseconds)
0 0 1 0	3/4 timeslot (~433 microseconds)
. . .	
1 1 1 1	16/4 timeslot (~2307 microseconds)

SM_VALUE (Switch-Measure) (4 bit field)
The SM field indicates the time needed for the mobile station to switch from one radio channel to another and perform a neighbour cell power measurement.
Bits

4 3 2 1	
0 0 0 0	1/4 timeslot (~144 microseconds)
0 0 0 1	2/4 timeslot (~288 microseconds)
0 0 1 0	3/4 timeslot (~433 microseconds)
. . .	
1 1 1 1	16/4 timeslot (~2307 microseconds)

MS Positioning Method Capability (1 bit field)
This bit indicates whether the MS supports Positioning Method or not for the provision of Location Services.

MS Positioning Method (5 bit field)
This field indicates the Positioning Method(s) supported by the mobile station.
MS assisted E-OTD
Bit 5

~~Bit 5~~

0 MS assisted E-OTD not supported

1 MS assisted E-OTD supported

Table 10.5.1.7/3GPP TS 24.008 (continued): *MS Classmark 3* information element

MS based E-OTD

4

~~Bit 4~~

0 MS based E-OTD not supported

1 MS based E-OTD supported

MS assisted GPS

3

~~Bit 3~~

0 MS assisted GPS not supported

1 MS assisted GPS supported

MS based GPS

2

~~Bit 2~~

0 MS based GPS not supported

1 MS based GPS supported

MS conventional GPS

1

~~Bit 1~~

0 conventional GPS not supported

1 conventional GPS supported

~~1 conventional GPS supported~~

~~EDGE~~ ECSD Multi Slot class (5 bit field)

In case the ~~EDGE~~ **ECSD** MS supports the use of multiple timeslots and the number of supported time slots is different from number of time slots supported for GMSK then the ~~EDGE~~ Multi Slot class field is included and is coded as the binary representation of the multislot class defined in TS GSM 05.02.

Modulation Capability

Modulation Capability field indicates the ~~supported~~ modulation scheme- ~~by~~ MS in addition to GMSK.

~~Bit 1~~

0 8-PSK supported for downlink reception only

1 8-PSK supported for uplink transmission and downlink reception

EDGE RF Power Capability 1 (2 bit field)

If 8-PSK is supported for both uplink and downlink, the **EDGE RF Power Capability 1** field indicates the radio capability for GSM700, GSM850 or GSM900.

The radio capability contains the binary coding of the EDGE power class~~(see GSMß05.05)~~(see 3GPP TS 45.005).

EDGE RF Power Capability 2 (2 bit field)

If 8-PSK is supported for both uplink and downlink, the ~~-~~**EDGE RF Power Capability 2** field indicates the radio capability for DCS1800 or PCS1900 if supported, and is not included otherwise.

The radio capability contains the binary coding of the EDGE power class (see 3GPP TS ~~0~~45.005).

Table 10.5.1.7/3GPP TS 24.008 (continued): *MS Classmark 3* information element

GSM 400 Bands Supported (2 bit field) See the semantic rule for the sending of this field. Bits 2 1 0 1 GSM 480 supported, GSM 450 not supported 1 0 GSM 450 supported, GSM 480 not supported 1 1 GSM 450 supported, GSM 480 supported **GSM 400 Associated Radio Capability (4 bit field)** If either GSM 450 or GSM 480 or both is supported, the GSM 400 Associated Radio Capability field indicates the radio capability for GSM 450 and/or GSM 480. The radio capability contains the binary coding of the power class associated with the band indicated in GSM 400 Bands Supported bits (see 3GPP TS 05.05). Note: the coding of the power class for GSM 450 and GSM 480 in GSM 400 Associated Radio Capability is different to that used in the Mobile Station Classmark 1 and Mobile Station Classmark 2 information elements. **GSM 850 Associated Radio Capability (4 bit field)** See the semantic rule for the sending of this field. This field indicates whether GSM 850 band is supported and its associated radio capability. The radio capability contains the binary coding of the power class associated with the GSM 850 band (see 3GPP TS 05.05). Note: the coding of the power class for GSM 850 in GSM 850 Associated Radio Capability is different to that used in the Mobile Station Classmark 1 and Mobile Station Classmark 2 information elements. **PCS 1900 Associated Radio Capability (4 bit field)** See the semantic rule for the sending of this field. This field indicates whether PCS 1900 band is supported and its associated radio capability. The radio capability contains the binary coding of the power class associated with the PCS 1900 band (see 3GPP TS 05.05). Note: the coding of the power class for PCS 1900 in PCS 1900 Associated Radio Capability is different to that used in the Mobile Station Classmark 1 and Mobile Station Classmark 2 information elements.

Table 10.5.1.7/3GPP TS 24.008 (continued): ***MS Classmark 3*** **information element**

UMTS FDD Radio Access Technology Capability (1 bit field)
~~Bit 1~~
0 UMTS FDD not supported
1 UMTS FDD supported

UMTS 3.84 Mcps TDD Radio Access Technology Capability (1 bit field)
~~Bit 1~~
0 UMTS 3.84 Mcps TDD not supported
1 UMTS 3.84 Mcps TDD supported

CDMA 2000 Radio Access Technology Capability (1 bit field)
~~CDMA 2000 Radio Access Technology Capability (1 bit field)~~
~~Bit 1~~
0 CDMA2000 not supported
1 CDMA2000 supported
~~0 CDMA2000 not supported~~
~~1 CDMA2000 supported~~

DTM GPRS Multi Slot Sub-Class (2 bit field)
This field indicates the GPRS DTM capabilities of the MS. The DTM GPRS ~~DTM~~ Multi Slot Sub-Class is independent from the HSCSD Multi Slot Capabilities field. It is coded as follows:
Bit
2 1
~~Bit 2 1~~

0 0	Sub-Class 1 supported
0 1	Sub-Class 5 supported
1 0	Sub-Class 9 supported
1 1	Reserved for future extension. If received, the network shall interpret this as '00'

DTM EGPRS Multi Slot Sub-Class (2 bit field)
This field indicates the EGPRS DTM capabilities of the MS.~~-~~ The DTM EGPRS Multi Slot Sub-Class is independent from the HSCSD Multi Slot Capabilities field. This field shall be included only if the mobile station supports EGPRS DTM. This field is coded as the DTM GPRS Multi Slot Sub-Class field.

MAC Mode Support (1 bit field)
This field indicates whether the MS supports Dynamic and Fixed Allocation or only supports Exclusive Allocation. It is coded as follows:
~~Bit 1~~
0 Dynamic and Fixed Allocation not supported
1 Dynamic and Fixed allocation supported

Single Band Support
This field shall be sent if the mobile station supports UMTS and one and only one GSM band with the exception of R-GSM; this field shall not be sent otherwise

GSM Band (4 bit field)
Bits

4 3 2 1	
0 0 0 0	E-GSM is supported
0 0 0 1	P-GSM is supported
0 0 1 0	DCS 1800 is supported
0 0 1 1	GSM 450 is supported
0 1 0 0	GSM 480 is supported
0 1 0 1	GSM 850 is supported
0 1 1 0	PCS 1900 is supported
0 1 1 1	GSM 700 is supported

All other values are reserved for future use.

NOTE: When this field is received, the associated RF power capability is found in Classmark 1 or 2.
~~NOTE: When this field is received, the associated RF power capability is found in Classmark 1 or 2.~~

GSM 700 Associated Radio Capability (4 bit field)

See the semantic rule for the sending of this field.
This field indicates whether GSM 700 band is supported and its associated radio capability.

The radio capability contains the binary coding of the power class associated with the GSM 700 band (see 3GPP TS 05.05).

Note: the coding of the power class for GSM 700 in GSM 700 Associated Radio Capability is different to that used in the Mobile Station Classmark 1 and Mobile Station Classmark 2 information elements.

UMTS 1.28 Mcps TDD Radio Access Technology Capability (1 bit field)~~**(1 bit field)**~~

~~Bit 1~~
0 UMTS 1.28 Mcps TDD not supported
1 UMTS 1.28 Mcps TDD supported

MS_EXT_UTBF (1 bit field)

~~Bit~~
0 Extended uplink TBF not supported
1 Extended uplink TBF supported