3GPP TSG-CN Meeting #24 **NP-040190**
2nd – 4th June 2004. Seoul, Korea.

Source: **TSG CN WG 1**

Title: **CRs to Rel-5 (with mirror CR) on Work Item TEI5 towards 24.008**

Agenda item: **8.8**

Document for: **APPROVAL**

Introduction:

This document contains **3** CRs, **Rel-5** Work Item **"TEI5"**, that have been agreed by **TSG CN WG1 in CN1#34 meeting**, and are forwarded to TSG CN Plenary meeting #24 for approval.

Spec	CR	Rev	Phase	Subject	Cat	Version-Current	Doc-2nd-Level
24.008	868		Rel-5	GERAN Iu mode capability and future Iu mode-specific extensions	F	5.11.0	N1-040828
24.008	880	1	Rel-5	Handling of key sets at inter-system change	F	5.11.0	N1-041074
24.008	881	1	Rel-6	Handling of key sets at inter-system change	A	6.4.0	N1-041075

3GPP TSG-CN1 Meeting #34 **Tdoc N1-040828**
Zagreb, Croatia 10 – 14 May 2004

CR-Form-v7

CHANGE REQUEST

⌘ **24.008 CR 868** ⌘**rev** **-** ⌘ Current version: **5.11.0** ⌘

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

Proposed change affects: UICC apps⌘ □ ME ☒ Radio Access Network ☒ Core Network □

Title:	⌘	GERAN Iu mode capability and future Iu mode-specific extensions		
Source:	⌘	NOKIA, Siemens AG, Infineon AG		
Work item code:	⌘	TEI-5	***Date:*** ⌘	10/05/2004
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)*
Rel-6	*(Release 6)*

Reason for change:	⌘	In order to save bits in MS RAC IE and Classmark 3 so as not to force a non-Iu mode capable MS to indicate its non-support for Iu mode specific features, it is proposed to indicate Iu mode specific features conditionally to the GERAN Iu mode support
Summary of change:	⌘	The GERAN Iu mode capability bit is replaced by a {0|1} indication, within which the Iu mode specific capabilities can be added
Consequences if not approved:	⌘	Bits may be wasted in MS RAC and CM3 in case of non-Iu mode capable MSs. CSN.1 error leading to the impossibility to decode Rel-6 capabilities

Clauses affected:	⌘	10.5.1.7; 10.5.5.12a				
		Y	N			
Other specs affected:	⌘		X	Other core specifications	⌘	
			X	Test specifications		
			X	O&M Specifications		
Other comments:	⌘	No mirror CR to Rel-6 is provided. A separate CR for introducing the Iu mode FLO capability in Rel-6 is provided assuming this Rel-5 proposal would be agreed				

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 GSM 1900 Associated Radio Capability* fields in the MS Classmark 3. Due to shared radio frequency channel numbers between GSM 1800 and GSM 1900, the mobile should indicate support for either GSM 1800 band OR GSM 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 45.002 [32]).

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 Multi Slot Capability > }
    { 0 | 1 < ECSD 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 <GSM 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 Class : bit(2) >
            < MAC Mode Support : bit >
            {0 | 1< DTM EGPRS Multi Slot 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 >
    < GERAN Feature Package 1 : bit >

    { 0 | 1 < Extended DTM GPRS Multi Slot Class : bit(2) >
            < Extended DTM EGPRS Multi Slot Class : bit(2) > }

    { 0 | 1 < High Multislot Capability : bit(2) > }---Release 5 starts here.

    { 0 | 1 < GERAN Iu Mode Capabilities > }        -- '1' also means support of GERAN Iu mode
~~< GERAN Iu Mode Capability : bit >~~
    < GERAN Feature Package 2 : 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) > ;
< ECSD Multi Slot Capability > ::=
     < ECSD Multi Slot Class : bit(5) > ;

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

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

< GERAN Iu Mode Capabilities > ::=
     < Length : bit (4) >          -- Length in bits of Iu mode only capabilities and spare bits
     < spare bits > **;            -- expands to the indicated length
                                   -- may be used for future enhancements
```

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
Bit 1
0 P-GSM not supported
1 P-GSM supported

Band 2 supported
Bit 2
0 E-GSM or R-GSM not supported
1 E-GSM or R-GSM supported

Band 3 supported
Bit 3
0 GSM 1800 not supported
1 GSM 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 GSM 1800 bands, all bits are set to 0.

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

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

A5/6
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 GSM 1800 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 GSM 1800, 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 3GPP TS 45.005 [33]).

(continued...)

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

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 3GPP TS 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 GSM 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)

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 3GPP TS 45.002 [32].

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.

0 the ME has a preference for the default alphabet (defined in 3GPP TS 23.038 [8b]) over 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

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 (5 bit field)
This field indicates the Positioning Method(s) supported by the mobile station for the provision of location services (LCS) via the CS domain in A-mode.
MS assisted E-OTD
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

<u>MS based E-OTD</u>
<u>Bit 4</u>
0 MS based E-OTD not supported
1 MS based E-OTD supported

<u>MS assisted GPS</u>
<u>Bit 3</u>
0 MS assisted GPS not supported
1 MS assisted GPS supported

<u>MS based GPS</u>
<u>Bit 2</u>
0 MS based GPS not supported
1 MS based GPS supported

<u>MS Conventional GPS</u>
<u>Bit 1</u>
0 conventional GPS not supported
1 conventional GPS supported

ECSD Multi Slot class (5 bit field)

In case the **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 **ECSD** Multi Slot class field is included and is coded as the binary representation of the multislot class defined in 3GPP TS 45.002 [32].

Modulation Capability

The Modulation Capability field indicates the modulation scheme the MS supports in addition to GMSK.
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 modulation is supported for both uplink and downlink, the **EDGE RF Power Capability 1** field indicates the radio capability for 8-PSK modulation in GSM 400, GSM 700, GSM 850 or GSM 900.

EDGE RF Power Capability 2 (2 bit field)
If 8-PSK modulation is supported for both uplink and downlink, the **EDGE RF Power Capability 2** field indicates the radio capability for 8-PSK modulation in GSM 1800 or GSM 1900 if supported, and is not included otherwise.

The respective **EDGE RF Power Capability 1** and **EDGE RF Power Capability 2** fields contain the following coding of the 8-PSK modulation power class (see 3GPP TS 45.005 [33]):

Bits 2 1	
0 0	Reserved
0 1	Power class E1
1 0	Power class E2
1 1	Power class E3

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 45.005 [33]).

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 45.005 [33]).

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.

GSM 1900 Associated Radio Capability (4 bit field)
See the semantic rule for the sending of this field.
This field indicates whether GSM 1900 band is supported and its associated radio capability.

The radio capability contains the binary coding of the power class associated with the GSM 1900 band (see 3GPP TS 45.005 [33]).

Note: the coding of the power class for GSM 1900 in GSM 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)

0	UMTS FDD not supported
1	UMTS FDD supported

UMTS 3.84 Mcps TDD Radio Access Technology Capability (1 bit field)

0	UMTS 3.84 Mcps TDD not supported
1	UMTS 3.84 Mcps TDD supported

CDMA 2000 Radio Access Technology Capability (1 bit field)

0	CDMA2000 not supported
1	CDMA2000 supported

DTM GPRS Multi Slot Class (2 bit field)
This field indicates the DTM GPRS multislot capabilities of the MS. It is coded as follows:
Bit

2 1	
0 0	Multislot class 1 supported
0 1	Multislot class 5 supported
1 0	Multislot class 9 supported
1 1	Reserved for future extension. If received, the network shall interpret this as ‘00’

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:

0	Dynamic and Fixed Allocation not supported
1	Dynamic and Fixed allocation supported

DTM EGPRS Multi Slot Class (2 bit field)
This field indicates the DTM EGPRS multislot capabilities of the MS. This field shall be included only if the mobile station supports EGPRS DTM. This field is coded as the DTM GPRS Multi Slot Class field.

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	GSM 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	GSM 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.

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 45.005 [33]).

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)

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

GERAN Feature Package 1 (1 bit field)
This field indicates whether the MS supports the GERAN Feature Package 1 (see 3GPP TS 44.060). It is coded as follows:

0 GERAN feature package 1 not supported.
1 GERAN feature package 1 supported.

Extended DTM GPRS Multi Slot Class (2 bit field)
This field indicates the extended DTM GPRS multislot capabilities of the MS and shall be interpreted in conjunction with the DTM GPRS Multi Slot Class field. It is coded as follows, where 'DGMSC' denotes the DTM GPRS Multi Slot Class field:

DGMSC Bit 2 1	Bit 2 1	
0 0	0 0	Multislot class 2 supported
0 0	0 1	Multislot class 3 supported
0 0	1 0	Multislot class 4 supported
0 0	1 1	Multislot class 8 supported
0 1	0 0	Multislot class 5 supported
0 1	0 1	Multislot class 6 supported
0 1	1 0	Multislot class 7 supported
0 1	1 1	Not used. If received, the network shall interpret it as '(01) 00'.
1 0	0 0	Multislot class 9 supported
1 0	0 1	Multislot class 10 supported
1 0	1 0	Multislot class 11 supported
1 0	1 1	Multislot class 12 supported

The presence of this field indicates that the MS supports combined fullrate and halfrate GPRS channels in the downlink.When this field is not present, the MS supports the multislot class indicated by the *DTM GPRS Multi Slot Class field*.

Extended DTM EGPRS Multi Slot Class (2 bit field)
This field is not considered when the DTM EGPRS Multi Slot Class field is not included. This field indicates the extended DTM EGPRS multislot capabilities of the MS and shall be interpreted in conjunction with the DTM EGPRS Multi Slot Class field. This field is coded as the Extended DTM GPRS Multi Slot Class field. The presence of this field indicates that the MS supports combined fullrate and halfrate GPRS channels in the downlink. When this field is not present, the MS supports the multislot class indicated by the *DTM GPRS Multi Slot Class* field.

High Multislot Capability (2 bit field)
This field indicates the support of multislot classes 30 to 45, see 3GPP TS 45.002.
The High Multislot Capability is individually combined with each multislot class field sent by the MS (the possible multislot class fields are: HSCSD multislot class, ECSD multislot class, GPRS multislot class, EGPRS multislot class, DTM GPRS multislot class, DTM EGPRS multislot class, extended DTM GPRS multislot class and extended DTM EGPRS multislot class) to extend the related multislot class with the rule described in the MS Radio Access Capability IE.

GERAN Iu Mode Capabilities~~y~~ ~~(1 bit field)~~
This field indicates if the mobile station supports GERAN Iu mode. Furthermore, it indicates the GERAN Iu mode-only capabilities of the mobile station. The field shall be included if the mobile station supports GERAN Iu mode. If the field is not present, the mobile station does not support GERAN Iu mode.
~~Bit~~
~~0 GERAN Iu mode not supported~~
~~1 GERAN Iu mode supported~~

GERAN Feature Package 2 (1 bit field)
This field indicates the MS support of the GERAN Feature Package 2. The GERAN Feature Package 2 includes **Enhanced Power Control (EPC)** (see 3GPP TS 45.008).

0 GERAN feature package 2 not supported.
1 GERAN feature package 2 supported.

**** NEXT MODIFIED SECTION ****

10.5.5.12a MS Radio Access capability

The purpose of the *MS RA capability* information element is to provide the radio part of the network with information concerning radio aspects of the mobile station. The contents might affect the manner in which the network handles the operation of the mobile station.

The *MS RA capability* is a type 4 information element, with a maximum length of 52 octets.

The value part of a *MS RA capability* information element is coded a shown table 10.5.146/3GPP TS 24.008.

For the indication of the Access Technology Types the following conditions shall apply:

- Among the three Access Type Technologies GSM 900-P, GSM 900-E and GSM 900-R only one shall be present.

- Due to shared radio frequency channel numbers between GSM 1800 and GSM 1900, the mobile station should provide the relevant radio access capability for either GSM 1800 band OR GSM 1900 band, not both.

- The MS shall indicate its supported Access Technology Types during a single MM procedure.

- If the alternative coding by using the Additional access technologies struct is chosen by the mobile station, the mobile station shall indicate its radio access capability for the serving BCCH frequency band in the first included Access capabilities struct.

- The first Access Technology Type shall not be set to "1111".

For error handling the following shall apply:

- If a received Access Technology Type is unknown to the receiver, it shall ignore all the corresponding fields.

- If within a known Access Technology Type a receiver recognizes an unknown field it shall ignore it.

- For more details about error handling of MS radio access capability see 3GPP TS 48.018 [86].

Table 10.5.146/3GPP TS 24.008: *Mobile Station Radio Access Capability* Information Element

<**MS RA capability value part** : < MS RA capability value part struct >>
<spare bits>**; -- *may be used for future enhancements*

<MS RA capability value part struct >::= --*recursive structure allows any number of Access technologies*
{ { < **Access Technology Type**: bit (4) > exclude 1111
< **Access capabilities** : <Access capabilities struct> > }

| { < **Access Technology Type**: bit (4) == 1111 > -- *structure adding Access technologies with same capabilities*
< **Length** : bit (7) > -- *length in bits of list of Additional access technologies and spare bits*
{ 1 < **Additional access technologies**: < Additional access technologies struct > > } ** 0
<spare bits>** } }

{ 0 | 1 <MS RA capability value part struct> } ;

< Additional access technologies struct > ::=
< **Access Technology Type** : bit (4) >
< **GMSK Power Class** : bit (3) >
< **8PSK Power Class** : bit (2) > ;

< Access capabilities struct > ::=
< **Length** : bit (7) > -- length in bits of Content and spare bits
<Access capabilities : <Content>>
<spare bits>** ; -- expands to the indicated length
-- may be used for future enhancements

< Content > ::=
< **RF Power Capability** : bit (3) >
{ 0 | 1 <**A5 bits** : <A5 bits> > } -- *zero means that the same values apply for parameters as in the immediately preceding Access capabilities field within this IE*
< **ES IND** : bit >
< **PS** : bit >
< **VGCS** : bit >
< **VBS** : bit >
{ 0 | 1 < **Multislot capability** : Multislot capability struct > } -- *zero means that the same values for multislot parameters as given in an earlier Access capabilities field within this IE apply also here*
-- *Additions in release 99*
{ 0 | 1 < **8PSK Power Capability** : bit(2) >} -- *'1' also means 8PSK modulation capability in uplink.*
< **COMPACT Interference Measurement Capability : bit >**
< **Revision Level Indicator** : bit >
< **UMTS FDD Radio Access Technology Capability** : bit > -- *3G RAT*
< **UMTS 3.84 Mcps TDD Radio Access Technology Capability** : bit > -- *3G RAT*
< **CDMA 2000 Radio Access Technology Capability** : bit > -- *3G RAT*
-- *Additions in release 4*
< **UMTS 1.28 Mcps TDD Radio Access Technology Capability**: bit > -- *3G RAT*
< **GERAN Feature Package 1** : bit >
{ 0 | 1 < **Extended DTM GPRS Multi Slot Class** : bit(2) >
< **Extended DTM EGPRS Multi Slot Class** : bit(2) > }
< Modulation based multislot class support : bit >
-- *Additions in release 5*
{ 0 | 1 < **High Multislot Capability** : bit(2) > }
{ 0 | 1 < **GERAN Iu Mode Capabilities** > } -- *'1' also means support of GERAN Iu mode*
~~< **GERAN Iu Mode Capability** : bit >~~
< **GMSK Multislot Power Profile** : bit (2) >
< **8-PSK Multislot Power Profile** : bit (2) > ;
-- error: struct too short, assume features do not exist
-- error: struct too long, ignore data and jump to next Access technology

Table 10.5.146/3GPP TS 24.008 (continued): ***Mobile Station Radio Access Capability*** **IE**

```
< Multislot capability struct > ::=
    { 0 | 1 < HSCSD multislot class : bit (5) > }
    { 0 | 1 < GPRS multislot class : bit (5) > < GPRS Extended Dynamic Allocation Capability : bit > }
    { 0 | 1 < SMS_VALUE : bit (4)  > < SM_VALUE : bit (4)  > }
-- Additions in release 99
    { 0 | 1 < ECSD multislot class : bit (5) > }
    { 0 | 1 < EGPRS multislot class : bit (5) > < EGPRS Extended Dynamic Allocation   Capability : bit > }
    {0 | 1   < DTM GPRS Multi Slot Class: bit(2)>
             <Single Slot DTM : bit>
             {0 | 1 <DTM EGPRS Multi Slot Class : bit(2)> } } ;
    -- error: struct too short, assume features do not exist

< GERAN Iu Mode Capabilities > ::=
    < Length : bit (4) >        -- length in bits of Iu mode-only capabilities and spare bits
    < spare bits > ** ;         -- expands to the indicated length
                                -- may be used for future enhancements
```

<A5 bits> ::= < A5/1 : bit> <A5/2 : bit> <A5/3 : bit> <A5/4 : bit> <A5/5 : bit> <A5/6 : bit> <A5/7 : bit>; -- bits for circuit mode ciphering algorithms. These fields are not used by the network and may be excluded by the MS.

Access Technology Type
This field indicates the access technology type to be associated with the following access capabilities.

Bits	
4 3 2 1	
0 0 0 0	GSM P
0 0 0 1	GSM E *--note that GSM E covers GSM P*
0 0 1 0	GSM R *--note that GSM R covers GSM E and GSM P*
0 0 1 1	GSM 1800
0 1 0 0	GSM 1900
0 1 0 1	GSM 450
0 1 1 0	GSM 480
0 1 1 1	GSM 850
1 0 0 0	GSM 700
1 0 0 1	GSM T 380
1 0 1 0	GSM T 410
1 0 1 1	GSM T 900
1 1 1 1	Indicates the presence of a list of Additional access technologies

All other values are treated as unknown by the receiver.

A MS which does not support any GSM access technology type shall set this field to '0000'.

RF Power Capability, GMSK Power Class (3 bit field)
This field contains the binary coding of the power class used for GMSK associated with the indicated Access Technology Type (see 3GPP TS 45.005).

A MS which does not support any GSM access technology type shall set this field to '000'.

8PSK Power Capability (2 bit field)
If 8-PSK modulation is supported for uplink, this field indicates the radio capability for 8-PSK modulation. The following coding is used (see 3GPP TS 45.005 [33]):

Bits	2 1	
	0 0	Reserved
	0 1	Power class E1
	1 0	Power class E2
	1 1	Power class E3

8PSK Power Class (2 bit field)
This field indicates the radio capability for 8-PSK modulation. The following coding is used (see 3GPP TS 45.005):

Bits	2 1	
	0 0	8PSK modulation not supported for uplink
	0 1	Power class E1
	1 0	Power class E2

1 1 Power class E3

Additional access technologies struct
This structure contains the GMSK Power Class and 8PSK Power Class for an additional Access Technology. All other capabilities for this indicated Access Technology are the same as the capabilities indicated by the preceding Access capabilities struct.

A5/1
0 encryption algorithm A5/1 not available
1 encryption algorithm A5/1 available
A5/2
0 encryption algorithm A5/2 not available
1 encryption algorithm A5/2 available
A5/3
0 encryption algorithm A5/3 not available
1 encryption algorithm A5/3 available
A5/4
0 encryption algorithm A5/4 not available
1 encryption algorithm A5/4 available
A5/5
0 encryption algorithm A5/5 not available
1 encryption algorithm A5/5 available
A5/6
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

ES IND – (Controlled early Classmark Sending)
0 "controlled early Classmark Sending" option is not implemented
1 "controlled early Classmark Sending" option is implemented

Table 10.5.146/3GPP TS 24.008 (concluded): *Mobile Station Radio Access Capability* IE

PS – (Pseudo Synchronisation)
0 PS capability not present
1 PS capability present

VGCS – (Voice Group Call Service)
0 no VGCS capability or no notifications wanted
1 VGCS capability and notifications wanted.

VBS – (Voice Broadcast Service)
0 no VBS capability or no notifications wanted
1 VBS capability and notifications wanted

HSCSD Multi Slot Class
The Multi Slot Class field is coded as the binary representation of the multislot class defined in 3GPP TS 45.002 [32].
This field is not used by the network and may be excluded by the MS.
Range 1 to 18, all other values are reserved.

GPRS Multi Slot Class
The GPRS Multi Slot Class field is coded as the binary representation of the multislot class defined in 3GPP TS 45.002 [32].

ECSD Multi Slot Class
The presence of this field indicates ECSD capability. Whether the MS is capable of 8-PSK modulation in uplink is indicated by the presence of 8-PSK Power Capability field. The Multi Slot Class field is coded as the binary representation of the multislot class defined in 3GPP TS 45.002 [32]. This field is not used by the network and may be excluded by the MS.
Range 1 to 18, all other values are reserved.

EGPRS Multi Slot Class
The presence of this field indicates EGPRS capability. Whether the MS is capable of 8-PSK modulation in uplink is indicated by the presence of 8-PSK Power Capability field. The EGPRS Multi Slot Class field is coded as the binary representation of the multislot class defined in 3GPP TS 45.002 [32].

GPRS Extended Dynamic Allocation Capability
0 Extended Dynamic Allocation Capability for GPRS is not implemented
1 Extended Dynamic Allocation Capability for GPRS is implemented

EGPRS Extended Dynamic Allocation Capability
0 Extended Dynamic Allocation Capability for EGPRS is not implemented
1 Extended Dynamic Allocation Capability for EGPRS is implemented

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 neighbor cell power measurement, and the switch from that radio channel to another radio channel. This field is not used by the network and may be excluded by the MS.
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. This field is not used by the network and may be excluded by the MS.
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)

DTM GPRS Multi Slot Class (2 bit field)
This field indicates the DTM GPRS multislot capabilities of the MS. It is coded as follows:
Bits
2 1
0 0 Unused. If received, the network shall interpret this as ‘01’
0 1 Multislot class 5 supported
1 0 Multislot class 9 supported
1 1 Multislot class 11 supported

Single Slot DTM (1 bit field)
This field indicates whether the MS supports single slot DTM operation (see 3GPP TS 43.055 [87]).
Bit
0 Single Slot DTM not supported
1 Single Slot DTM supported

An MS indicating support for Extended DTM GPRS multislot class or Extended DTM EGPRS multislot class shall set this bit to ‘1’. The network may ignore the bit in this case.

DTM EGPRS Multi Slot Class (2 bit field)
This field indicates the DTM EGPRS multislot capabilities of the MS. This field shall be included only if the mobile station supports EGPRS DTM. This field is coded as the DTM GPRS multislot Class field.

COMPACT Interference Measurement Capability (1 bit field)
0 COMPACT Interference Measurement Capability is not implemented
1 COMPACT Interference Measurement Capability is implemented

Revision Level Indicator (1 bit field)
Bit
0 The ME is Release ’98 or older
1 The ME is Release ’99 onwards

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

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

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

UMTS 1.28 Mcps TDD Radio Access Technology Capability (1 bit field)
Bit
0 UMTS 1.28 Mcps TDD not supported
1 UMTS 1.28 Mcps TDD supported

GERAN Feature Package 1 (1 bit field)
This field indicates whether the MS supports the GERAN Feature Package 1 (see 3GPP TS 44.060). It is coded as follows:

0 GERAN feature package 1 not supported.
1 GERAN feature package 1 supported.

Extended DTM GPRS Multi Slot Class (2 bit field)
This field indicates the extended DTM GPRS capabilities of the MS and shall be interpreted in conjunction with the DTM GPRS Multi Slot Class field. It is coded as follows, where ‘DGMSC’ denotes the DTM GPRS multislot class field:

DGMSC Bit 2 1	**Bit 2 1**	
0 0	**0 0**	Unused. If received, it shall be interpreted as ‘01 00’
0 0	**0 1**	Unused. If received, it shall be interpreted as ‘01 00’

0 0	**1 0**	Unused. If received, it shall be interpreted as ‘01 00’
0 0	**1 1**	Unused. If received, it shall be interpreted as ‘01 00’
0 1	**0 0**	Multislot class 5 supported
0 1	**0 1**	Multislot class 6 supported
0 1	**1 0**	Unused. If received, it shall be interpreted as ‘01 00’
0 1	**1 1**	Unused. If received, it shall be interpreted as ‘01 00’
1 0	**0 0**	Multislot class 9 supported
1 0	**0 1**	Multislot class 10 supported
1 0	**1 0**	Unused. If received, it shall be interpreted as ’10 00’
1 0	**1 1**	Unused. If received, it shall be interpreted as ’10 00’
1 1	**0 0**	Multislot class 11 supported
1 1	**0 1**	Unused. If received, it shall be interpreted as ’11 00’
1 1	**1 0**	Unused. If received, it shall be interpreted as ’11 00’
1 1	**1 1**	Unused. If received, it shall be interpreted as ’11 00’

The presence of this field indicates that the MS supports combined fullrate and halfrate GPRS channels in the downlink. When this field is not present, the MS supports the multislot class indicated by the *DTM GPRS Multi Slot Class* field.

Extended DTM EGPRS Multislot Class (2 bit field)
This field is not considered when the DTM EGPRS Multislot Class field is not included. This field indicates the extended DTM EGPRS multislot capabilities of the MS and shall be interpreted in conjunction with the DTM EGPRS Multislot Class field. This field is coded as the Extended DTM GPRS Multislot Class field. The presence of this field indicates that the MS supports combined fullrate and halfrate GPRS channels in the downlink. When this field is not present, the MS supports the multislot class indicated by the DTM EGPRS Multi Slot Class field.

Modulation based multislot class support (1 bit field)
Bit

0	"Modulation based multislot class" not supported
1	"Modulation based multislot class" supported

High Multislot Capability (2 bit field)
The High Multislot Capability is individually combined with each multislot class field sent by the MS (the possible multislot class fields are: HSCSD multislot class, ECSD multislot class, GPRS multislot class, EGPRS multislot class, DTM GPRS multislot class, DTM EGPRS multislot class, extended DTM GPRS multislot class and extended DTM EGPRS multislot class) to extend the related multislot class to multislot classes 30 to 45, see
3GPP TS 45.002.
For each multislot class, the following mapping is done:
Bits

2 1	coded multislot class field	actual multislot class
0 0	8	30
0 0	10, 23, 28, 29	39
0 0	11, 20, 25	32
0 0	12, 21, 22, 26, 27	33
0 0	Any other	Multislot Class field value
0 1	8	35
0 1	10, 19, 24	36
0 1	11, 23, 28, 29	45
0 1	12, 21, 22, 26, 27	38
0 1	Any other	Multislot Class field value
1 0	8	40
1 0	10, 19, 24	41
1 0	11, 20, 25	42
1 0	12, 23, 28, 29	44
1 0	Any other	Multislot Class field value
1 1	12, 21, 22, 26, 27	43
1 1	11, 20, 25	37
1 1	10, 19, 24	31
1 1	9, 23, 28, 29	34
1 1	Any other	Multislot Class field value

~~**GERAN Iu Mode Capability** (1 bit field)~~
~~Bit~~
~~0 GERAN Iu mode not supported~~
~~1 GERAN Iu mode supported~~
GERAN Iu Mode Capabilities
This field indicates if the mobile station supports GERAN Iu mode. Furthermore, it indicates the GERAN Iu mode-

only capabilities of the mobile station. the field shall be included if the mobile station supports GERAN Iu mode. If the field is not present, the mobile station does not support GERAN Iu mode.

3GPP TSG-CN1 Meeting #34 **Tdoc N1-041074**
Zagreb, Croatia 10 – 14 May 2004 **Revision of N1-040906**

CR-Form-v7

CHANGE REQUEST

⌘ **24.008 CR 880** ⌘**rev 1** ⌘ Current version: **5.11.0** ⌘

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

Proposed change affects: UICC apps⌘ □ ME ☒ Radio Access Network □ Core Network ☒

Title: ⌘	Handling of key sets at inter-system change			
Source: ⌘	Ericsson, Siemens			
Work item code: ⌘	TEI5		***Date:*** ⌘	13/05/2004
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)*
Rel-6	*(Release 6)*

Reason for change: ⌘ At TSG-CN#23 CRs on ‘Handling of key sets’ were approved (i.e. NP-040099, NP-040030) and implemented in TS 24.008 from Rel-5 onwards. However, the tables that specify the handling of key sets at intersystem change from/to GSM to/from UMTS in case of CS and PS domains remained being incorrect.

In addition, the stage 2 specification on security (i.e. TS 33.102) in the sub-clause 6.8.5 states:

> The integrity protection of signalling messages shall be started immediately after that the intersystem handover from GSM BSS to UTRAN is completed. The serving RNC will do this initiating the RRC Security mode procedure when the first message (i.e. the Handover to UTRAN complete message) has been received from the MS.

Furthermore, TS 25.331 in the sub-clause 8.3.6.3 states the following:

> If ciphering has been activated and ongoing in the radio access technology from which inter RAT handover is performed, UTRAN should not include the IE "Ciphering mode info" in the SECURITY MODE COMMAND message that starts Integrity protection, and should not send a SECURITY MODE COMMAND including IE "Ciphering mode info" and IE "CN domain identity" set to the same value as UE variable LATEST_CONFIGURED_CN_DOMAIN until all pending ciphering activation times have been reached for the radio bearers using RLC-TM.

According to this, the UTRAN starts ‘always’ integrity protection when inter-system change to UMTS occurs, so the security mode control procedure in UTRAN is always triggered when the HANDOVER TO UTRAN COMMAND COMPLETE message is received from the MS. This first SECURITY MODE COMMAND message triggered immediately after inter-system handover is not

		triggered by a RANAP security mode control procedure. Furthermore, this SECURITY MODE COMMAND message is sent in order to start integrity only, if the RR connection was already ciphered.
Summary of change:	⌘	The text in the tables that specify the handling of key sets at inter-system change from/to UMTS to/from GSM is clarified and corrected. Finally, it is stated that in case of inter-system handover to UMTS the MS and the network shall continue to use the keys from the old key set until the second valid SECURITY MODE COMMAND message indicating CS domain is received. Two informative notes are also added to explain the reason for the ‘first’ and ‘second’ SECURITY MODE COMMAND messages.
Consequences if not approved:	⌘	The inter-system change scenarios after re-authentication can be misinterpreted which might lead to different implementations in terminals and networks. This results in undesirable effects, i.e. ciphering and/or integrity protection will fail; in the CS domain, the call will be dropped and in the PS domain, data based services will not be possible. Misalignment among different specifications remains, so the inter-system change scenario to UMTS will fail.

Clauses affected:	⌘	4.3.2.7, 4.3.2.7a, 4.3.2.8, 4.7.7.8, 4.7.7.9				
		Y	**N**			
Other specs affected:	⌘		**X**	Other core specifications	⌘	
			X	Test specifications		
			X	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/specs/CR.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 CHANGE

4.3.2.7 Handling of keys at intersystem change from UMTS to GSM

At inter-system change from UMTS to GSM, ciphering may be started (see 3GPP TS 44.018 [86]) without any new authentication procedure. Deduction of the appropriate security key for ciphering in GSM, depends on the current GSM/UMTS security context stored in the MS and the network.

The ME shall handle the GSM ciphering key according to table 4.3.2.7.1.

Table 4.3.2.7.1/3GPP TS 24.008: Inter-system change from UMTS to GSM

Security context established in MS and network in UMTS	At inter-system change to GSM:
GSM security context	An ME shall apply the stored GSM cipher key that was received from the GSM security context residing in the SIM/USIM during the latest successful ciphering mode setting or security mode control procedure before the inter-system change.
UMTS security context	An ME shall apply the stored GSM cipher key that was derived by the USIM from the UMTS cipher key and the UMTS integrity key and provided by the USIM during the latest successful ciphering mode setting or security mode control procedure before the inter-sytem change.

NOTE: A USIM with UMTS security context, passes the UMTS cipher key, the UMTS integrity key and the derived GSM cipher key to the ME independent on the current radio access being UMTS or GSM.

4.3.2.7a Use of established security contexts

In GSM, in the case of an established GSM security context, the GSM ciphering key shall be loaded from the SIM/USIM and taken into use by the ME when any valid CIPHERING MODE COMMAND is received during an RR connection (the definition of a valid CIPHERING MODE COMMAND message is given in 3GPP TS 44.018 [84] subclause 3.4.7.2).

In GSM, in the case of an established UMTS security context, the GSM ciphering key shall be loaded from the USIM and taken into use by the MS when a valid CIPHERING MODE COMMAND is received during an RR connection (the definition of a valid CIPHERING MODE COMMAND message is given in 3GPP TS 44.018 [84] subclause 3.4.7.2). The network shall derive a GSM ciphering key from the UMTS ciphering key and the UMTS integrity key by using the conversion function named "c3" defined in 3GPP TS 33.102 [5a].

In UMTS, in the case of an established GSM security context, the ME shall derive a UMTS ciphering key and a UMTS integrity key from the GSM ciphering key by using the conversion functions named "c4" and "c5" defined in 3GPP TS 33.102 [5a]. The GSM ciphering key shall be loaded from the SIM/USIM and the derived UMTS ciphering key and UMTS integrity key shall be taken into use by the MS when a valid SECURITY MODE COMMAND indicating CS domain is received during an RR connection (the definition of a valid SECURITY MODE COMMAND message is given in 3GPP TS 25.331 [23c]). The network shall derive a UMTS ciphering key and a UMTS integrity key from the GSM ciphering key by using the conversion functions named "c4" and "c5" defined in 3GPP TS 33.102 [5a].

In UMTS, in the case of an established UMTS security context, the UMTS ciphering key and UMTS integrity key shall be loaded from the USIM and taken into use by the MS when a valid SECURITY MODE COMMAND indicating CS domain is received during a RR connection (the definition of a valid SECURITY MODE COMMAND message is given in 3GPP TS 25.331 [23c]).

In UMTS and GSM, if the MS received a valid SECURITY MODE COMMAND indicating CS domain in UMTS or a valid CIPHERING MODE COMMAND in GSM before~~if during an ongoing, already ciphering and/or integrity protected RR connection,~~ the network initiates a new Authentication procedure and establishes a new GSM/UMTS security context, the new keys are taken into use in the MS when a new valid SECURITY MODE COMMAND indicating CS domain in UMTS, or a new valid CIPHERING MODE COMMAND in GSM, is received during the RR connection. In case of UMTS to UMTS handover, GSM to GSM handover, ~~to UMTS~~ or inter-system change to~~or~~ GSM the MS and the network shall continue to use the key from the old key set until a new valid SECURITY MODE

COMMAND indicating CS domain in UMTS, or a new valid CIPHERING MODE COMMAND in GSM, is received during the RR connection. In case of inter-system change to UMTS, the MS and the network shall continue to use the keys from the old key set until the second valid SECURITY MODE COMMAND indicating CS domain is received during the RR connection.

NOTE 1: If the MS received a valid SECURITY MODE COMMAND indicating CS domain in UMTS or a valid CIPHERING MODE COMMAND in GSM before the inter-system change to UMTS occurs, the first SECURITY MODE COMMAND message after the inter-system change, which indicates CS domain and includes only an Integrity protection mode IE, is initiated by the UTRAN without receipt of a corresponding RANAP security mode control procedure from the MSC/VLR. The only purpose of this SECURITY MODE COMMAND message is to activate the integrity protection, but not to load a new key set from the SIM/USIM (see 3GPP TS 25.331 [23c]).

NOTE 2: If the MS did not receive any valid SECURITY MODE COMMAND indicating CS domain in UMTS or any valid CIPHERING MODE COMMAND in GSM before the inter-system change to UMTS occurs, the first SECURITY MODE COMMAND message after the inter-system change, which indicates CS domain, is initiated by the UTRAN on receipt of a RANAP security mode control procedure from the MSC/VLR. The purpose of this SECURITY MODE COMMAND message is to load a key set from the SIM/USIM and to activate either integrity protection or ciphering and integrity protection (see 3GPP TS 25.331 [23c]).

4.3.2.8 Handling of keys at intersystem change from GSM to UMTS

At inter-system change from GSM to UMTS, ciphering and integrity may be started (see 3GPP TS 25.331 [23c]) without any new authentication procedure. Deduction of the appropriate security keys for ciphering and integrity check in UMTS, depends on the current GSM/UMTS security context stored in the MS and the network.

The ME shall handle the UMTS cipher key and the UMTS integrity key according to table 4.3.2.8.1.

Table 4.3.2.8.1/3GPP TS 24.008: Inter-system change from GSM to UMTS

Security context established in MS and network in GSM	At inter-system change to UMTS:
GSM security context	An ME shall derive the UMTS cipher key and the UMTS integrity key from the stored GSM cipher key that was provided by the SIM/USIM during the latest successful ciphering mode setting or security mode control procedure before the inter-system change. The conversion functions named "c4" and "c5" in 3GPP TS 33.102 [5a] are used for this purpose.
UMTS security context	An ME shall apply the stored UMTS ciphering key and the stored UMTS integrity key that were received from the UMTS security context residing in the USIM during the latest successful ciphering mode setting or security mode control procedure before the inter-system change.

NOTE: A USIM with UMTS security context, passes the UMTS cipher key, the UMTS integrity key and the derived GSM cipher key to the ME independent on the current radio access being UMTS or GSM.

SECOND CHANGE

4.7.7.7 Use of established security contexts

In GSM, in the case of an established GSM security context, the GPRS GSM ciphering key shall be taken into use by the MS before the AUTHENTICATION AND CIPHERING RESPONSE message is transmitted.

In GSM, in the case of an established UMTS security context, the GPRS GSM ciphering key shall be taken into use by the MS before the AUTHENTICATION AND CIPHERING RESPONSE message is transmitted. The network shall derive a GPRS GSM ciphering key from the GPRS UMTS ciphering key and the GPRS UMTS integrity key, by using the conversion function named "c3" defined in 3GPP TS 33.102 [5a].

In GSM, if during an ongoing, already ciphering protected RR connection, the network initiates a new Authentication and ciphering procedure, the new GPRS GSM ciphering key shall be taken into use by the MS before the AUTHENTICATION AND CIPHERING RESPONSE message is transmitted. In case of inter-system change to UMTS after receipt of the AUTHENTICATION AND CIPHERING REQUEST message, the MS and the network shall take the new keys into use immediately after the inter-system change.

In UMTS, in the case of an established GSM security context, the ME shall derive a GPRS UMTS ciphering key and a GPRS UMTS integrity key from the GPRS GSM ciphering key by using the conversion functions named "c4" and "c5" defined in 3GPP TS 33.102 [5a]. The derived GPRS UMTS ciphering key and GPRS UMTS integrity key shall be taken into use by the MS when a valid SECURITY MODE COMMAND indicating PS domain is received during an RR connection (the definition of a valid SECURITY MODE COMMAND message is given in 3GPP TS 25.331 [23c]). The network shall derive a GPRS UMTS ciphering key and a GPRS UMTS integrity key from the GPRS GSM ciphering key by using the conversion functions named "c4" and "c5" defined in 3GPP TS 33.102 [5a].

In UMTS, in the case of an established UMTS security context, the GPRS UMTS ciphering key and the GPRS UMTS integrity key shall be taken into use by the MS when a valid SECURITY MODE COMMAND indicating PS domain is received during an PS signalling connection (the definition of a valid SECURITY MODE COMMAND message is given in 3GPP TS 25.331[23c]).

In UMTS, if the MS received a valid SECURITY MODE COMMAND indicating PS domain in UMTS or a valid AUTHENTICATION AND CIPHERING REQUEST in GSM before ~~if during an ongoing, already ciphering/integrity protected PS signalling connection,~~ the network initiates a new Authentication and ciphering procedure and establishes a new GSM/UMTS security context, the new GPRS UMTS ciphering key and GPRS UMTS integrity key are taken into use by the MS, when a new valid SECURITY MODE COMMAND indicating PS domain is received during the PS signalling connection. In case of inter-system change to GSM, the MS and the network shall take the new keys into use immediately after the inter-system change.

4.7.7.8 Handling of keys at intersystem change from UMTS to GSM

At an inter-system change from UMTS to GSM, ciphering may be started (see 3GPP TS 44.064 [78a]) without any new authentication and ciphering procedure. Deduction of the appropriate security key for ciphering in GSM, depends on the current GSM/UMTS security context stored in the MS and the network.

The ME shall handle the GPRS GSM ciphering key according to table 4.7.7.8.1.

Before any initial GMM message is sent in the new cell in GSM, the GMM layer in the MS shall notify the LLC layer if ciphering shall be used or not. If yes, the GPRS GSM ciphering key and the applicable ciphering algorithm according to the stored *Ciphering Algorithm IE* in the MS shall also be indicated to the LLC layer (see 3GPP TS 44.064 [78a]).

Table 4.7.7.8.1/3GPP TS 24.008: Inter-system change from UMTS to GSM

Security context established in MS and network in UMTS	At inter-system change to GSM:
GSM security context	An ME shall apply the ~~latest~~ GPRS GSM cipher key that was received from the GSM security context created~~residing~~ in the SIM/USIM during the latest successful authentication procedure.
UMTS security context	An ME shall apply the GPRS GSM cipher key that was derived by the USIM from the GPRS UMTS cipher key and the GPRS UMTS integrity key during the latest successful authentication procedure.

NOTE: A USIM with UMTS security context, passes the GPRS UMTS ciphering key, the GPRS UMTS integrity key and the derived GPRS GSM ciphering key to the ME independent on the current radio access being UMTS or GSM.

4.7.7.9 Handling of keys at intersystem change from GSM to UMTS

At an inter-system change from GSM to UMTS, ciphering and integrity may be started (see 3GPP TS 25.331) without any new authentication and ciphering procedure. Deduction of the appropriate security keys for ciphering and integrity check in UMTS, depend on the current GSM/UMTS security context stored in the MS and the network.

The ME shall handle the GPRS UMTS cipher key and the GPRS UMTS integrity key according to table 4.7.7.9.1.

Table 4.7.7.9.1/3GPP TS 24.008: Inter-system change from GSM to UMTS

Security context established in MS and network in GSM	At inter-system change to UMTS:
GSM security context	An ME shall derive the GPRS UMTS cipher key and the GPRS UMTS integrity key from the GPRS GSM cipher key that was provided by the SIM/USIM during the latest successful authentication procedure. The conversion functions named "c4" and "c5" in 3GPP TS 33.102 [5a] are used for this purpose.
UMTS security context	An ME shall apply the ~~latest~~ GPRS UMTS ciphering key and the GPRS UMTS integrity key that were received from the UMTS security context created~~residing~~ in the USIM during the latest successful authentication procedure.

NOTE: A USIM with UMTS security context, passes the GPRS UMTS ciphering key, the GPRS UMTS integrity key and the derived GPRS GSM ciphering key to the ME independent on the current radio access being UMTS or GSM.

3GPP TSG-CN1 Meeting #34 **Tdoc N1-041075**

Revision of N1-040907

Zagreb, Croatia 10 – 14 May 2004

CR-Form-v7

CHANGE REQUEST

⌘	**24.008**	**CR**	**881**	⌘**rev**	**1**	⌘	Current version:	**6.4.0** ⌘

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

Proposed change affects: UICC apps⌘ □ ME ☒ Radio Access Network □ Core Network ☒

Title:	⌘	Handling of key sets at inter-system change		
Source:	⌘	Ericsson, Siemens		
Work item code:	⌘	TEI5	***Date:*** ⌘	13/05/2004
Category:	⌘	**A**	***Release:*** ⌘	Rel-6
		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)* *Rel-6 (Release 6)*	

Reason for change: ⌘

At TSG-CN#23 CRs on 'Handling of key sets' were approved (i.e. NP-040099, NP-040030) and implemented in TS 24.008 from Rel-5 onwards. However, the tables that specify the handling of key sets at intersystem change from/to GSM to/from UMTS in case of CS and PS domains remained being incorrect.

In addition, the stage 2 specification on security (i.e. TS 33.102) in the sub-clause 6.8.5 states:

> The integrity protection of signalling messages shall be started immediately after that the intersystem handover from GSM BSS to UTRAN is completed. The serving RNC will do this initiating the RRC Security mode procedure when the first message (i.e. the Handover to UTRAN complete message) has been received from the MS.

Furthermore, TS 25.331 in the sub-clause 8.3.6.3 states the following:

> If ciphering has been activated and ongoing in the radio access technology from which inter RAT handover is performed, UTRAN should not include the IE "Ciphering mode info" in the SECURITY MODE COMMAND message that starts Integrity protection, and should not send a SECURITY MODE COMMAND including IE "Ciphering mode info" and IE "CN domain identity" set to the same value as UE variable LATEST_CONFIGURED_CN_DOMAIN until all pending ciphering activation times have been reached for the radio bearers using RLC-TM.

According to this, the UTRAN starts 'always' integrity protection when inter-system change to UMTS occurs, so the security mode control procedure in UTRAN is always triggered when the HANDOVER TO UTRAN COMMAND COMPLETE message is received from the MS. This first SECURITY MODE

		COMMAND message triggered immediately after inter-system handover is not triggered by a RANAP security mode control procedure. Furthermore, this SECURITY MODE COMMAND message is sent in order to start integrity only, if the RR connection was already ciphered.
Summary of change:	⌘	The text in the tables that specify the handling of key sets at inter-system change from/to UMTS to/from GSM is clarified and corrected. Finally, it is stated that in case of inter-system handover to UMTS the MS and the network shall continue to use the keys from the old key set until the second valid SECURITY MODE COMMAND message indicating CS domain is received. Two informative notes are also added to explain the reason for the 'first' and 'second' SECURITY MODE COMMAND messages.
Consequences if not approved:	⌘	The inter-system change scenarios after re-authentication can be misinterpreted which might lead to different implementations in terminals and networks. This results in undesirable effects, i.e. ciphering and/or integrity protection will fail; in the CS domain, the call will be dropped and in the PS domain, data based services will not be possible. Misalignment among different specifications remains, so the inter-system change scenario to UMTS will fail.

Clauses affected:	⌘	4.3.2.7, 4.3.2.7a, 4.3.2.8, 4.7.7.8, 4.7.7.9				
		Y	**N**			
Other specs affected:	⌘		**X**	Other core specifications	⌘	
			X	Test specifications		
			X	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/specs/CR.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 CHANGE

4.3.2.7 Handling of keys at intersystem change from UMTS to GSM

At inter-system change from UMTS to GSM, ciphering may be started (see 3GPP TS 44.018 [86]) without any new authentication procedure. Deduction of the appropriate security key for ciphering in GSM, depends on the current GSM/UMTS security context stored in the MS and the network.

The ME shall handle the GSM ciphering key according to table 4.3.2.7.1.

Table 4.3.2.7.1/3GPP TS 24.008: Inter-system change from UMTS to GSM

Security context established in MS and network in UMTS	At inter-system change to GSM:
GSM security context	An ME shall apply the stored GSM cipher key that was received from the GSM security context residing in the SIM/USIM during the latest successful ciphering mode setting or security mode control procedure before the inter-system change.
UMTS security context	An ME shall apply the stored GSM cipher key that was derived by the USIM from the UMTS cipher key and the UMTS integrity key and provided by the USIM during the latest successful ciphering mode setting or security mode control procedure before the inter-sytem change.

NOTE: A USIM with UMTS security context, passes the UMTS cipher key, the UMTS integrity key and the derived GSM cipher key to the ME independent on the current radio access being UMTS or GSM.

4.3.2.7a Use of established security contexts

In GSM, in the case of an established GSM security context, the GSM ciphering key shall be loaded from the SIM/USIM and taken into use by the ME when any valid CIPHERING MODE COMMAND is received during an RR connection (the definition of a valid CIPHERING MODE COMMAND message is given in 3GPP TS 44.018 [84] subclause 3.4.7.2).

In GSM, in the case of an established UMTS security context, the GSM ciphering key shall be loaded from the USIM and taken into use by the MS when a valid CIPHERING MODE COMMAND is received during an RR connection (the definition of a valid CIPHERING MODE COMMAND message is given in 3GPP TS 44.018 [84] subclause 3.4.7.2). The network shall derive a GSM ciphering key from the UMTS ciphering key and the UMTS integrity key by using the conversion function named "c3" defined in 3GPP TS 33.102 [5a].

In UMTS, in the case of an established GSM security context, the ME shall derive a UMTS ciphering key and a UMTS integrity key from the GSM ciphering key by using the conversion functions named "c4" and "c5" defined in 3GPP TS 33.102 [5a]. The GSM ciphering key shall be loaded from the SIM/USIM and the derived UMTS ciphering key and UMTS integrity key shall be taken into use by the MS when a valid SECURITY MODE COMMAND indicating CS domain is received during an RR connection (the definition of a valid SECURITY MODE COMMAND message is given in 3GPP TS 25.331 [23c]). The network shall derive a UMTS ciphering key and a UMTS integrity key from the GSM ciphering key by using the conversion functions named "c4" and "c5" defined in 3GPP TS 33.102 [5a].

In UMTS, in the case of an established UMTS security context, the UMTS ciphering key and UMTS integrity key shall be loaded from the USIM and taken into use by the MS when a valid SECURITY MODE COMMAND indicating CS domain is received during a RR connection (the definition of a valid SECURITY MODE COMMAND message is given in 3GPP TS 25.331 [23c]).

In UMTS and GSM, if the MS received a valid SECURITY MODE COMMAND indicating CS domain in UMTS or a valid CIPHERING MODE COMMAND in GSM before~~if during an ongoing, already ciphering and/or integrity protected RR connection,~~ the network initiates a new Authentication procedure and establishes a new GSM/UMTS security context, the new keys are taken into use in the MS when a new valid SECURITY MODE COMMAND indicating CS domain in UMTS, or a new valid CIPHERING MODE COMMAND in GSM, is received during the RR connection. In case of UMTS to UMTS handover, GSM to GSM handover, ~~to UMTS~~ or inter-system change to~~or~~ GSM the MS and the network shall continue to use the key from the old key set until a new valid SECURITY MODE

COMMAND indicating CS domain in UMTS, or a new valid CIPHERING MODE COMMAND in GSM, is received during the RR connection. In case of inter-system change to UMTS, the MS and the network shall continue to use the keys from the old key set until the second valid SECURITY MODE COMMAND indicating CS domain is received during the RR connection.

NOTE 1: If the MS received a valid SECURITY MODE COMMAND indicating CS domain in UMTS or a valid CIPHERING MODE COMMAND in GSM before the inter-system change to UMTS occurs, the first SECURITY MODE COMMAND message after the inter-system change, which indicates CS domain and includes only an Integrity protection mode IE, is initiated by the UTRAN without receipt of a corresponding RANAP security mode control procedure from the MSC/VLR. The only purpose of this SECURITY MODE COMMAND message is to activate the integrity protection, but not to load a new key set from the SIM/USIM (see 3GPP TS 25.331 [23c]).

NOTE 2: If the MS received a valid SECURITY MODE COMMAND indicating CS domain in UMTS or a valid CIPHERING MODE COMMAND in GSM before the inter-system change to UMTS occurs, the first SECURITY MODE COMMAND message after the inter-system change, which indicates CS domain, is initiated by the UTRAN on receipt of a RANAP security mode control procedure from the MSC/VLR. The purpose of this SECURITY MODE COMMAND message is to load a key set from the SIM/USIM and to activate either integrity protection or ciphering and integrity protection (see 3GPP TS 25.331 [23c]).

4.3.2.8 Handling of keys at intersystem change from GSM to UMTS

At inter-system change from GSM to UMTS, ciphering and integrity may be started (see 3GPP TS 25.331 [23c]) without any new authentication procedure. Deduction of the appropriate security keys for ciphering and integrity check in UMTS, depends on the current GSM/UMTS security context stored in the MS and the network.

The ME shall handle the UMTS cipher key and the UMTS integrity key according to table 4.3.2.8.1.

Table 4.3.2.8.1/3GPP TS 24.008: Inter-system change from GSM to UMTS

Security context established in MS and network in GSM	At inter-system change to UMTS:
GSM security context	An ME shall derive the UMTS cipher key and the UMTS integrity key from the stored GSM cipher key that was provided by the SIM/USIM during the latest successful ciphering mode setting or security mode control procedure before the inter-system change. The conversion functions named "c4" and "c5" in 3GPP TS 33.102 [5a] are used for this purpose.
UMTS security context	An ME shall apply the stored UMTS ciphering key and the stored UMTS integrity key that were received from the UMTS security context residing in the USIM during the latest successful ciphering mode setting or security mode control procedure before the inter-system change.

NOTE: A USIM with UMTS security context, passes the UMTS cipher key, the UMTS integrity key and the derived GSM cipher key to the ME independent on the current radio access being UMTS or GSM.

SECOND CHANGE

4.7.7.7 Use of established security contexts

In GSM, in the case of an established GSM security context, the GPRS GSM ciphering key shall be taken into use by the MS before the AUTHENTICATION AND CIPHERING RESPONSE message is transmitted.

In GSM, in the case of an established UMTS security context, the GPRS GSM ciphering key shall be taken into use by the MS before the AUTHENTICATION AND CIPHERING RESPONSE message is transmitted. The network shall derive a GPRS GSM ciphering key from the GPRS UMTS ciphering key and the GPRS UMTS integrity key, by using the conversion function named "c3" defined in 3GPP TS 33.102 [5a].

In GSM, if during an ongoing, already ciphering protected RR connection, the network initiates a new Authentication and ciphering procedure, the new GPRS GSM ciphering key shall be taken into use by the MS before the AUTHENTICATION AND CIPHERING RESPONSE message is transmitted. In case of inter-system change to UMTS after receipt of the AUTHENTICATION AND CIPHERING REQUEST message, the MS and the network shall take the new keys into use immediately after the inter-system change.

In UMTS, in the case of an established GSM security context, the ME shall derive a GPRS UMTS ciphering key and a GPRS UMTS integrity key from the GPRS GSM ciphering key by using the conversion functions named "c4" and "c5" defined in 3GPP TS 33.102 [5a]. The derived GPRS UMTS ciphering key and GPRS UMTS integrity key shall be taken into use by the MS when a valid SECURITY MODE COMMAND indicating PS domain is received during an RR connection (the definition of a valid SECURITY MODE COMMAND message is given in 3GPP TS 25.331 [23c]). The network shall derive a GPRS UMTS ciphering key and a GPRS UMTS integrity key from the GPRS GSM ciphering key by using the conversion functions named "c4" and "c5" defined in 3GPP TS 33.102 [5a].

In UMTS, in the case of an established UMTS security context, the GPRS UMTS ciphering key and the GPRS UMTS integrity key shall be taken into use by the MS when a valid SECURITY MODE COMMAND indicating PS domain is received during an PS signalling connection (the definition of a valid SECURITY MODE COMMAND message is given in 3GPP TS 25.331[23c]).

In UMTS, if the MS received a valid SECURITY MODE COMMAND indicating PS domain in UMTS or a valid AUTHENTICATION AND CIPHERING REQUEST in GSM before ~~if during an ongoing, already ciphering/integrity protected PS signalling connection,~~ the network initiates a new Authentication and ciphering procedure and establishes a new GSM/UMTS security context, the new GPRS UMTS ciphering key and GPRS UMTS integrity key are taken into use by the MS, when a new valid SECURITY MODE COMMAND indicating PS domain is received during the PS signalling connection. In case of inter-system change to GSM, the MS and the network shall take the new keys into use immediately after the inter-system change.

4.7.7.8 Handling of keys at intersystem change from UMTS to GSM

At an inter-system change from UMTS to GSM, ciphering may be started (see 3GPP TS 44.064 [78a]) without any new authentication and ciphering procedure. Deduction of the appropriate security key for ciphering in GSM, depends on the current GSM/UMTS security context stored in the MS and the network.

The ME shall handle the GPRS GSM ciphering key according to table 4.7.7.8.1.

Before any initial GMM message is sent in the new cell in GSM, the GMM layer in the MS shall notify the LLC layer if ciphering shall be used or not. If yes, the GPRS GSM ciphering key and the applicable ciphering algorithm according to the stored *Ciphering Algorithm IE* in the MS shall also be indicated to the LLC layer (see 3GPP TS 44.064 [78a]).

Table 4.7.7.8.1/3GPP TS 24.008: Inter-system change from UMTS to GSM

Security context established in MS and network in UMTS	At inter-system change to GSM:
GSM security context	An ME shall apply the ~~latest~~ GPRS GSM cipher key that was received from the GSM security context created~~residing~~ in the SIM/USIM during the latest successful authentication procedure.
UMTS security context	An ME shall apply the GPRS GSM cipher key that was derived by the USIM from the GPRS UMTS cipher key and the GPRS UMTS integrity key during the latest successful authentication procedure.

NOTE: A USIM with UMTS security context, passes the GPRS UMTS ciphering key, the GPRS UMTS integrity key and the derived GPRS GSM ciphering key to the ME independent on the current radio access being UMTS or GSM.

4.7.7.9 Handling of keys at intersystem change from GSM to UMTS

At an inter-system change from GSM to UMTS, ciphering and integrity may be started (see 3GPP TS 25.331) without any new authentication and ciphering procedure. Deduction of the appropriate security keys for ciphering and integrity check in UMTS, depend on the current GSM/UMTS security context stored in the MS and the network.

The ME shall handle the GPRS UMTS cipher key and the GPRS UMTS integrity key according to table 4.7.7.9.1.

Table 4.7.7.9.1/3GPP TS 24.008: Inter-system change from GSM to UMTS

Security context established in MS and network in GSM	At inter-system change to UMTS:
GSM security context	An ME shall derive the GPRS UMTS cipher key and the GPRS UMTS integrity key from the GPRS GSM cipher key that was provided by the SIM/USIM during the latest successful authentication procedure. The conversion functions named "c4" and "c5" in 3GPP TS 33.102 [5a] are used for this purpose.
UMTS security context	An ME shall apply the ~~latest~~ GPRS UMTS ciphering key and the GPRS UMTS integrity key that were received from the UMTS security context created~~residing~~ in the USIM during the latest successful authentication procedure.

NOTE: A USIM with UMTS security context, passes the GPRS UMTS ciphering key, the GPRS UMTS integrity key and the derived GPRS GSM ciphering key to the ME independent on the current radio access being UMTS or GSM.