3GPP TSG CN Plenary Meeting #25 **NP-040408**
8th – 10th August 2004 Palm Springs, US.

Source: TSG CN WG4

Title: Corrections on TEI6 GTP enhancements

Agenda item: 9.21

Document for: APPROVAL

Spec	CR	Rev	Doc-2nd-Level N4-04	Phase	Subject	Cat	Ver_C
29.060	501		0946	Rel-6	Alignment and enhancement of the "RAT Type" IE	C	6.5.0
29.060	502		0961	Rel-6	Corrections to charging information IEs	F	6.5.0
29.060	511		1065	Rel-6	Handling of ciphering and integrity keys at inter-SGSN RAU	F	6.5.0
29.060	507	1	1132	Rel-6	RIM transparent routing	F	6.5.0

3GPP TSG-CN WG4 Meeting #24 **N4-040946**
Sophia Antipolis, France, 16th – 20th August 2004

CR-Form-v7.1

CHANGE REQUEST

⌘ **29.060** **CR** **501** ⌘ **rev** **-** ⌘ Current version: **6.5.0** ⌘

*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 **X**

Title:	⌘	Alignment and enhancement of the "RAT Type" IE
Source:	⌘	CN4
Work item code:	⌘	CH
Date:	⌘	02/08/2004
Category:	⌘	**C**
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:
Ph2 (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)
Rel-7 (Release 7)

Reason for change:	⌘	1. Alignment with 3GPP TS 32.215 ("Telecommunication Management; Charging Management; Charging data description for the Packet Switched (PS) domain") "System Type" S-CDR IE. Also, an enumerated field allows for many more new, future RATs to be conveyed in the one byte field than the amount that could be conveyed using a one byte bit field (maximum of 256 different RATs as opposed to only 8). 2. An SGSN (or at least, an entity emulating SGSN functionality to a GGSN) needs to be able to convey to the GGSN that the RAT currently being used is WLAN. This is needed for 3GPP WLAN-I scenario 3.
Summary of change:	⌘	1. "RAT Type" IE is changed from a bit field to an enumerated type. 2. Additional value to convey a RAT of WLAN being used is also added.
Consequences if not approved:	⌘	N/A

Clauses affected:	⌘	7.7.50

Other specs affected:	⌘	Y	N		⌘
			X	Other core specifications	
			X	Test specifications	
			X	O&M Specifications	

Other comments: ⌘ The "RAT Type" value of 0 is marked as reserved as this value is not used in the

	PS domain according to 3GPP TS 32.215. A CR adding the capability to convey WLAN as the current RAT being used by a subscriber in S-CDRs is also being submitted (to SA5), however, neither this CR or the CR to the charging spec rely upon each other being approved for being approved themselves.

7.7.50 RAT Type

The 'RAT Type' information element is used to indicate which Radio Access Technology is currently serving the UE. ~~If the UE is currently being served by a GPRS/EDGE Radio Access Network (GERAN) then bit 1 of octet 4 shall be set to 1, otherwise it shall be set to 0. If the UE is currently being served by a UMTS Terrestrial Radio Access Network (UTRAN) then bit 2 of octet 4 shall be set to 1, otherwise it shall be set to 0.~~

Octets	Bits 8	7	6	5	4	3	2	1
1	Type = 151 (Decimal)							
2-3	Length							
~~4~~	~~Spare~~	~~Spare~~	~~Spare~~	~~Spare~~	~~Spare~~	~~Spare~~	~~UTRAN~~	~~GERAN~~
4	RAT Type value							

Figure 7.7.50.1: RAT Type Information Element

Table XX: RAT Type values

RAT Type values	Value(s) (Decimal)
<reserved>	0
UTRAN	1
GERAN	2
WLAN	3
<spare>	4-255

NOTE: Currently it is only possible to detect the difference between GERAN and UTRAN when GERAN Gb mode is used. If GERAN Iu mode is used, then an SGSN may not be able to detect the difference between GERAN and UTRAN.

3GPP TSG-CN WG4 Meeting #24 **N4-040961**
Sophia Antipolis, France, 16th – 20th August 2004

CR-Form-v7.1

CHANGE REQUEST

⌘ **29.060** **CR** **502** ⌘ **rev** **-** ⌘ Current version: **6.5.0** ⌘

*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:	⌘	Corrections to charging information IEs
Source:	⌘	CN4
Work item code:	⌘	CH
Date:	⌘	02/08/2004
Category:	⌘	**F**
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:

Ph2	*(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)*
Rel-7	*(Release 7)*

Reason for change:	⌘	1. Mis-alignment with the stage 2 of the presence conditions of the IEs included for Flow Based Charging. 2. Remnants of an early version of CR 29060-478 exist where the new IEs were part of one compound IE.
Summary of change:	⌘	1. Change of presence conditions for IEs used for Flow Based Charging to make them in-line with those provided in the stage 2 (see 3GPP TS 23.060 sub-section 15.1.1a). 2. Removal of the presence information for User Location Information IE in section 7.7.51 which was originally specified due to when this IE was aactually a field of a compound IE in an early version of CR 29.060-478.
Consequences if not approved:	⌘	Mis-alignment with stage 2 and confusion over the values used for the "Geographic Location Type" field in the "User Location Information" IE.

Clauses affected:	⌘	7.7.51, 7.3.1, 7.3.3			
Other specs affected:	⌘	**Y**	**N**		⌘
			X	Other core specifications	
			X	Test specifications	
			X	O&M Specifications	
Other comments:	⌘	Please note: in order to maintain backwards compatibility with previous versions			

	of GTP, the newly included IEs must be stated in the stage 3 to be *optionally* included. However, they can be *mandated* for inclusion at the stage 2 just like other IEs within GTP e.g. RAI in Create PDP Context Req and Update PDP Context Req.

****** First Modified Section ******

7.3 Tunnel Management Messages

7.3.1 Create PDP Context Request

A Create PDP Context Request shall be sent from a SGSN node to a GGSN node as a part of the GPRS PDP Context Activation procedure. After sending the Create PDP Context Request message, the SGSN marks the PDP context as 'waiting for response'. In this state the SGSN shall accept G-PDUs from the GGSN but shall not send these G-PDUs to the MS. A valid request initiates the creation of a tunnel between a PDP Context in a SGSN and a PDP Context in a GGSN. If the procedure is not successfully completed, the SGSN repeats the Create PDP Context Request message to the next GGSN address in the list of IP addresses, if there is one. If the list is exhausted the activation procedure fails.

The Tunnel Endpoint Identifier Data I field specifies a downlink Tunnel Endpoint Identifier for G-PDUs which is chosen by the SGSN. The GGSN shall include this Tunnel Endpoint Identifier in the GTP header of all subsequent downlink G-PDUs which are related to the requested PDP context.

The Tunnel Endpoint Identifier Control Plane field specifies a downlink Tunnel Endpoint Identifier for control plane messages which is chosen by the SGSN. The GGSN shall include this Tunnel Endpoint Identifier in the GTP header of all subsequent downlink control plane messages which are related to the requested PDP context. If the SGSN has already confirmed successful assignment of its Tunnel Endpoint Identifier Control Plane to the peer GGSN, this field shall not be present. The SGSN confirms successful assignment of its Tunnel Endpoint Identifier Control Plane the GGSN when it receives any message with its assigned Tunnel Endpoint Identifier Control Plane in the GTP header from the GGSN.

The MSISDN of the MS is passed to the GGSN inside the Create PDP Context Request; This additional information can be used when a secure access to a remote application residing on a server is needed. The GGSN would be in fact able to provide the user identity (i.e. the MSISDN) to the remote application server, providing it with the level of trust granted to users through successfully performing the GPRS authentication procedures, without having to re-authenticate the user at the application level.

If the MS requests a dynamic PDP address and a dynamic PDP address is allowed, then the PDP Address field in the End User Address information element shall be empty. If the MS requests a static PDP Address then the PDP Address field in the End User Address information element shall contain the static PDP Address. In case the PDP addresses carried in the End User Address and optionally in the Protocol Configuration Option information element contain contradicting information, the PDP address carried in the End User Address information element takes the higher precedence. The Quality of Service Profile information element shall be the QoS values to be negotiated between the MS and the SGSN at PDP Context activation.

The SGSN shall include an SGSN Address for control plane and an SGSN address for user traffic, which may differ from that provided by the underlying network service (e.g. IP). The GGSN shall store these SGSN Addresses and use them when sending control plane on this GTP tunnel or G-PDUs to the SGSN for the MS.

The SGSN shall include a Recovery information element into the Create PDP Context Request if the SGSN is in contact with the GGSN for the very first time or if the SGSN has restarted recently and the new Restart Counter value has not yet been indicated to the GGSN or if the SGSN has noticed that the path between itself and the GGSN has failed at some point and has deleted all the active PDP contexts associated with the GGSN as a result and the new Restart Counter value has not yet been indicated to the GGSN. The GGSN that receives a Recovery information element in the Create PDP Context Request message element shall handle it in the same way as when receiving an Echo Response message. The Create PDP Context Request message shall be considered as a valid activation request for the PDP context included in the message.

The SGSN shall include either the MS provided APN, a subscribed APN or an SGSN selected APN in the message; the Access Point Name may be used by the GGSN to differentiate accesses to different external networks.

The Selection Mode information element shall indicate the origin of the APN in the message.

For contexts created by the Secondary PDP Context Activation Procedure the SGSN shall include the linked NSAPI. Linked NSAPI indicates the NSAPI assigned to any one of the already activated PDP contexts for this PDP address and APN.

The Secondary PDP Context Activation Procedure may be executed without providing a Traffic Flow Template (TFT) to the newly activated PDP context if all other active PDP contexts for this PDP address and APN already have an associated TFT, otherwise a TFT shall be provided. TFT is used for packet filtering in the GGSN.

When using the Secondary PDP Context Activation Procedure, the Selection mode, IMSI, MSISDN, End User Address, Access Point Name and APN Restriction information elements shall not be included in the message.

The Protocol Configuration Options (PCO) information element may be included in the request when the MS provides the GGSN with application specific parameters. The SGSN includes this IE in the Create PDP Context Request if the associated Activate PDP Context Request or Activate Secondary PDP Context Request from the MS includes protocol configuration options. The SGSN shall copy the content of this IE transparently from the content of the PCO IE in the Activate PDP Context Request message or Activate Secondary PDP Context Request.

The SGSN shall select one GGSN based on the user provided or SGSN selected APN. The GGSN may have a logical name that is converted to an address. The conversion may be performed with any name-to-address function. The converted address shall be stored in the "GGSN Address in Use" field in the PDP context and be used during the entire lifetime of the PDP context.

NOTE: A DNS query may be used as the name-to-IP address mapping of the GGSN. The IP address returned in the DNS response is then stored in the "GGSN Address in Use" field in the PDP context.

The IMSI information element together with the NSAPI information element uniquely identifies the PDP context to be created.

The SGSN shall not send a Create PDP Context Request for an already active context.

If a new Create PDP Context Request is incoming on TEID 0 for an already active PDP context, this Create PDP Context Request must be considered related to a new session. The existing PDP context shall be torn down locally, and the associated PDP contexts deleted locally, before the new session is created. If a new Create PDP Context Request is incoming on a TEID which is different from 0 and this TEID is already allocated to one or more activated PDP contexts, and the NSAPI IE value in this message matches the NSAPI value of an active PDP context, the GGSN shall send back a Create PDP Context Response with a rejection cause code. It is implementation dependent deciding whether to teardown or keep the existing PDP context.

If the GGSN uses the MNRG flag and the flag is set, the GGSN should treat the Create PDP Context Request as a Note MS Present Request and clear the MNRG flag.

The SGSN shall determine Charging Characteristics from the Subscribed Charging Characteristics and/or PDP Context Charging Characteristics depending on the presence of the information in the Packet Domain Subscription Data as defined in 3GPP TS 23.060 [4]. The requirements for the presence of the Charging Characteristics IE are defined in 3GPP TS 23.060 [4]. The contents of the Charging Characteristics IE are defined in 3GPP TS 32.215 [18].

The SGSN shall include Trace Reference, Trace Type, Trigger Id, and OMC Identity in the message if GGSN trace is activated. The SGSN shall copy Trace Reference, Trace Type, and OMC Identity from the trace request received from the HLR or OMC.

The SGSN may include the Routeing Area Identity (RAI) of the SGSN where the MS is registered. The MCC and MNC components shall be populated with the MCC and MNC, respectively, of the SGSN where the MS is registered. The LAC and RAC components shall be populated by the SGSN with the value of 'FFFE' and 'FF', respectively.

The APN Restriction is an optional information element. In this instance it is used by the SGSN to convey to the GGSN the highest restriction type out of all the currently active PDP Contexts for a particular subscriber.

~~If charging is to be performed in the GGSN, t~~The SGSN ~~shall~~ may include the User Location Information IE, MS Time Zone IE, RAT Type IE, IMEI(SV) IE and the CAMEL Charging Information Container IE if they are available (see sub-clause 15.1.1a of 3GPP TS 23.060 [4] for more information). If the User Location Information IE is included then ~~T~~the SGSN shall include the CGI or SAI in the 'Geographic Location' field depending on whether the MS is in a cell or a service area respectively.

The optional Private Extension contains vendor or operator specific information.

Table 5: Information Elements in a Create PDP Context Request

Information element	Presence requirement	Reference
IMSI	Conditional	7.7.2
Routeing Area Identity (RAI)	Optional	7.7.3
Recovery	Optional	7.7.11
Selection mode	Conditional	7.7.12
Tunnel Endpoint Identifier Data I	Mandatory	7.7.13
Tunnel Endpoint Identifier Control Plane	Conditional	7.7.14
NSAPI	Mandatory	7.7.17
Linked NSAPI	Conditional	7.7.17
Charging Characteristics	Conditional	7.7.23
Trace Reference	Optional	7.7.24
Trace Type	Optional	7.7.25
End User Address	Conditional	7.7.27
Access Point Name	Conditional	7.7.30
Protocol Configuration Options	Optional	7.7.31
SGSN Address for signalling	Mandatory	GSN Address 7.7.32
SGSN Address for user traffic	Mandatory	GSN Address 7.7.32
MSISDN	Conditional	7.7.33
Quality of Service Profile	Mandatory	7.7.34
TFT	Conditional	7.7.36
Trigger Id	Optional	7.7.41
OMC Identity	Optional	7.7.42
APN Restriction	Optional	7.7.49
RAT Type	Optional	7.7.50
User Location Information	Optional	7.7.51
MS Time Zone	Optional	7.7.52
IMEI(SV)	Optional	7.7.53
CAMEL Charging Information Container	Optional	7.7.54
Private Extension	Optional	7.7.46

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

7.3.3 Update PDP Context Request

An Update PDP Context Request message shall be sent from a SGSN to a GGSN as part of the GPRS Inter SGSN Routeing Update procedure or the PDP Context Modification procedure or to redistribute contexts due to load sharing. It shall be used to change the QoS and the path. In addition it shall be used if it is necessary to change the GTP version of a tunnel to a GGSN from GTP v0 to GTP v1. The message shall be sent by the new SGSN at the Inter SGSN Routeing Update procedure.

The NSAPI information element together with the Tunnel Endpoint Identifier in the GTP header unambiguously identifies a PDP Context in the GGSN.

The IMSI shall be included if the message is sent during an Inter SGSN change when changing the GTP version from GTP v0 to GTP v1; this is required, as the TEID in the header of the message is set to all zeros in this case.

The Tunnel Endpoint Identifier Data field specifies a downlink Tunnel Endpoint Identifier for G-PDUs which is chosen by the SGSN. The GGSN shall include this Tunnel Endpoint Identifier in the GTP header of all subsequent downlink G-PDUs that are related to the requested PDP context.

The Tunnel Endpoint Identifier Control Plane field specifies a downlink Tunnel Endpoint Identifier Control Plane messages which is chosen by the SGSN. The GGSN shall include this Tunnel Endpoint Identifier in the GTP header of all subsequent downlink control plane messages that are related to the requested PDP context. If the SGSN has already confirmed successful assignment of its Tunnel Endpoint Identifier Control Plane to the peer GGSN, this field shall not be present. The SGSN confirms successful assignment of its Tunnel Endpoint Identifier Control Plane to the GGSN when it receives any message with its assigned Tunnel Endpoint Identifier Control Plane in the GTP header from the GGSN.

The Quality of Service Profile information element shall include the QoS negotiated between the MS and SGSN at PDP Context activation or the new QoS negotiated in the PDP Context Modification procedure.

The SGSN shall include an SGSN Address for control plane and an SGSN address for user traffic, which may differ from that provided by the underlying network service (e.g. IP).

If an IPv4/IPv6 capable SGSN received IPv4 GGSN addresses from the old SGSN, it shall include IPv4 addresses in the fields SGSN Address for Control Plane and SGSN Address for User Traffic and IPv6 addresses in the fields Alternative SGSN Address for Control Plane and Alternative SGSN Address for User Traffic. Otherwise, an IPv4/IPv6 capable SGSN shall use only SGSN IPv6 addresses if it has GGSN IPv6 addresses available. If the GGSN supports IPv6 below GTP, it shall store and use the IPv6 SGSN addresses for communication with the SGSN and ignore the IPv4 SGSN addresses. If the GGSN supports only IPv4 below GTP, it shall store and use the IPv4 SGSN addresses for communication with the SGSN and ignore the IPv6 SGSN addresses. When active contexts are being redistributed due to load sharing, G-PDUs that are in transit across the Gn-interface are in an undetermined state and may be lost.

The SGSN shall include a Recovery information element into the Update PDP Context Request if the SGSN is in contact with the GGSN for the very first time or if the SGSN has restarted recently and the new Restart Counter value has not yet been indicated to the GGSN or if the SGSN has noticed that the path between itself and the GGSN has failed at some point and has deleted all the active PDP contexts associated with the GGSN as a result and the new Restart Counter value has not yet been indicated to the GGSN. The GGSN that receives a Recovery information element in the Update PDP Context Request message element shall handle it in the same way as when receiving an Echo Response message. The Update PDP Context Request message shall be considered as a valid update request for the PDP context indicated in the message.

The Traffic Flow Template (TFT) is used to distinguish between different user traffic flows.

The SGSN shall include Trace Reference, Trace Type, Trigger Id, and OMC Identity in the message if GGSN trace is activated while the PDP context is active. The SGSN shall copy Trace Reference, Trace Type, and OMC Identity from the trace request received from the HLR or OMC.

The SGSN may include the Routeing Area Identity (RAI) of the SGSN where the MS is registered. The MCC and MNC components shall be populated with the MCC and MNC, respectively, of the SGSN where the MS is registered. The LAC and RAC components shall be populated by the SGSN with the value of 'FFFE' and 'FF', respectively.

The optional Private Extension contains vendor or operator specific information.

The MS includes the Protocol Configuration Options (PCO) information element in the request if the MS wishes to provide the GGSN with application specific parameters. The SGSN includes this IE in the Update PDP Context Request if the associated Modify PDP Context Request from the MS includes protocol configuration options. The SGSN shall copy the content of this IE transparently from the content of the PCO IE in the Modify PDP Context Request message.

~~If charging is to be performed in the GGSN, t~~The SGSN ~~shall~~ may include the User Location Information IE, RAT Type IE and MS Time Zone IE if they are available. However, the RAT Type IE shall not be included for the MS-initiated PDP Context Modification procedure (see sub-clause 15.1.1a of 3GPP TS 23.060 [4] for more information). If the User Location Information IE is included then ~~T~~the SGSN shall include the CGI or SAI in the 'Geographic Location' field depending on whether the MS is in a cell or a service area respectively.

Table 7: Information Elements in an SGSN-Initiated Update PDP Context Request

Information element	Presence requirement	Reference
IMSI	Conditional	7.7.2
Routeing Area Identity (RAI)	Optional	7.7.3
Recovery	Optional	7.7.11
Tunnel Endpoint Identifier Data I	Mandatory	7.7.13
Tunnel Endpoint Identifier Control Plane	Conditional	7.7.14
NSAPI	Mandatory	7.7.17
Trace Reference	Optional	7.7.24
Trace Type	Optional	7.7.25
Protocol Configuration Options	Optional	7.7.31
SGSN Address for Control Plane	Mandatory	GSN Address 7.7.32
SGSN Address for User Traffic	Mandatory	GSN Address 7.7.32
Alternative SGSN Address for Control Plane	Conditional	GSN Address 7.7.32
Alternative SGSN Address for User Traffic	Conditional	GSN Address 7.7.32
Quality of Service Profile	Mandatory	7.7.34
TFT	Optional	7.7.36
Trigger Id	Optional	7.7.41
OMC Identity	Optional	7.7.42
RAT Type	Optional	7.7.50
User Location Information	Optional	7.7.51
MS Time Zone	Optional	7.7.52
Private Extension	Optional	7.7.46

An Update PDP Context Request may also be sent from a GGSN to a SGSN to re-negotiate the QoS of a PDP context. The GGSN-initiated Update PDP Context Request can also be used to provide a PDP address to the SGSN (and MS). The latter shall be used by GGSN when it acts as a DHCP Relay Agent or Mobil IP Foreign Agent. A GGSN may send an update PDP context to a SGSN to check that the PDP context is still active at the SGSN. In such a case, the GGSN shall include the optional IMSI IE, to add robustness against the case the SGSN has re-assigned the TEID to another PDP context (this may happen when the PDP context is dangling at the GGSN). Also, the "Quality of service profile" IE and the "End user Address" IE shall not be included in this case.

The Quality of Service Profile information element shall include the GGSN requested QoS.

The End User Address information element shall contain a valid IPv4 or IPv6 address.

The GGSN shall include a Recovery information element into the Update PDP Context Request if the GGSN has restarted recently and the new Restart Counter value has not yet been indicated to the SGSN or if the GGSN has noticed that the path between itself and the SGSN has failed at some point and has deleted all the active PDP contexts associated with the SGSN as a result and the new Restart Counter value has not yet been indicated to the SGSN. The SGSN that receives a Recovery information element in the Update PDP Context Request message element shall handle it in the same way as when receiving an Echo Response message. The Update PDP Context Request message shall be considered as a valid update request for the PDP context indicated in the message.

The NSAPI information element together with the Tunnel Endpoint Identifier in the GTP header unambiguously identifies a PDP Context in the SGSN.

The GGSN includes the Protocol Configuration Options (PCO) information element in the request if the GGSN wishes to provide the MS with application specific parameters. The SGSN includes this IE in the Modify PDP Context Request message if the associated Update PDP Context Request message from the GGSN includes protocol configuration options. The SGSN shall copy the content of this IE transparently from the content of the PCO IE in the Update PDP Context Request message.

The optional Private Extension contains vendor or operator specific information.

The APN Restriction is an optional information element. In this instance it is used by the GGSN to convey to the SGSN the restriction type of the associated PDP Context being updated.

Table 8: Information Elements in a GGSN-Initiated Update PDP Context Request

Information element	Presence requirement	Reference
IMSI	optional	7.7.2
Recovery	Optional	7.7.11
NSAPI	Mandatory	7.7.17
End User Address	Optional	7.7.27
Protocol Configuration Options	Optional	7.7.31
Quality of Service Profile	Optional	7.7.34
APN Restriction	Optional	7.7.49
Private Extension	Optional	7.7.46

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

7.7.51 User Location Information

The 'User Location Information' IE is used to indicate CGI/SAI of where the MS is currently located.

The 'Geographic Location Type' field is used to convey ~~whether or not location field is included, and if so,~~ what type of location information is present in the 'Geographic Location field'. The types of locations that can be conveyed are defined in table 7.7.51A.

The 'Geographic Location' field is used to convey the actual geographic information as indicated in the 'Geographic Location Type' field. ~~This field shall not be present if the value of the 'Geographic Location Type' field is 0.~~

Octets	Bits 8	7	6	5	4	3	2	1
1	Type = 152 (Decimal)							
2-3	Length							
4	Geographic Location Type							
5 - m	Geographic Location							

Figure 7.7.51.1: User Location Information IE

Table 7.7.51A: Geographic Location Type values and their meanings

Value (Decimal)	Definition	Encoding Definition
0	Geographic Location field included and it holds the Cell Global Identification (CGI) of where the user currently is registered. CGI is defined in sub-clause 4.3.1 of 3GPP TS 23.003 [2].	Figure 7.7.51.2.
1	Geographic Location field included and it holds the Service Area Identity (SAI) of where the user currently is registered. SAI is defined in sub-clause 9.2.3.9 of 3GPP TS 25.413 [7].	Figure 7.7.51.3.

NOTE: The decimal values 3 to 255 are reserved for future use.

Octets	Bits 8	7	6	5	4	3	2	1
5	MCC digit 2				MCC digit 1			
6	MNC digit 3				MCC digit 3			
7	MNC digit 2				MNC digit 1			
8-9	LAC							
10-11	CI							

Figure 7.7.51.2: Geographic Location field for CGI

If only two digits are included in the MNC, then bits 5 to 8 of octet 6 are coded as "1111".

The location area code consists of 2 octets and is found in octet 8 and octet 9. Bit 8 of octet 8 is the most significant bit and bit 1 of octet 9 the least significant bit. The coding of the location area code is the responsibility of each administration. Coding using full hexadecimal representation shall be used.

The cell identity consists of 2 octets and is found in octet 10 and octet 11. Bit 8 of octet 10 is the most significant bit and bit 1 of octet 11 the least significant bit. The coding of the cell identity is the responsibility of each administration. Coding using full hexadecimal representation shall be used.

	Bits							
Octets	**8**	**7**	**6**	**5**	**4**	**3**	**2**	**1**
5	MCC digit 2				MCC digit 1			
6	MNC digit 3				MCC digit 3			
7	MNC digit 2				MNC digit 1			
8-9	LAC							
10-11	SAC							

Figure 7.7.51.3: Geographic Location field for SAI

If only two digits are included in the MNC, then bits 5 to 8 of octet 6 are coded as "1111".

The location area code consists of 2 octets and is found in octet 8 and octet 9. Bit 8 of octet 8 is the most significant bit and bit 1 of octet 9 the least significant bit. The coding of the location area code is the responsibility of each administration. Coding using full hexadecimal representation shall be used. See 3GPP TS 24.008 [5] for more information.

The service area code consists of 2 octets and is found in octet 10 and octet 11. Bit 8 of octet 10 is the most significant bit and bit 1 of octet 11 the least significant bit. The SAC is defined by the operator. See 3GPP TS 23.003 [2] section 12.5 for more information.

3GPP TSG-CN WG4 Meeting #24 ***N4-041065***

Sophia Antipolis, France. 16th to 20th August 2004.

CR-Form-v7.1

CHANGE REQUEST

⌘ **29.060** **CR** **511** ⌘ **rev** **-** ⌘ Current version: **6.5.0** ⌘

*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 ciphering and integrity keys at inter-SGSN RAU
Source:	⌘	CN4
Work item code:	⌘	TEI6
Date:	⌘	06.08.2004
Category:	⌘	**F**
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:

Ph2	*(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)*
Rel-7	*(Release 7)*

Reason for change: ⌘ Recently, SA3 and CN1 agreed CRs to TS 33.102 (SP-040370) and TS 24.008 (NP-040190) which clarify the handling of ciphering keys and integrity keys during an inter-system change for the rare case that an Authentication and Ciphering procedure is performed on an already ciphering and/or integrity protected connection, i.e. a new security context is created, and the MS performs an inter-system change before the new key set has been taken into use.

For the PS domain the following principles apply for the re-authentication scenario (without inter-system change):

- In GERAN A/Gb mode the new GSM or UMTS security context is taken into use immediately after the Authentication and Ciphering procedure creating the new context.

- In UTRAN or GERAN Iu mode an explicit Security Mode Command procedure initiated by the SGSN is necessary to take the new keys into use.

In the scenario with inter-system change after the re-authentication, the behaviour is now specified as follows:

(*) If an inter-system change from UTRAN/GERAN Iu mode to GERAN A/Gb mode occurs before the SGSN initiated a Security Mode Command procedure, the new keys will be taken into use immediately after the inter-system change. The same applies if an inter-system change from GERAN A/Gb mode to UTRAN/GERAN Iu mode occurs, before an Authentication and Ciphering procedure initiated in GERAN A/Gb mode could be completed.

	According to TS 29.060, however, during an inter-SGSN routing area update or inter-SGSN relocation only one security context ((CKSN, Kc) or (KSI, CK, IK)) can be transferred from the old SGSN to the new SGSN, and this is the context 'currently used' by the old SGSN, i.e. the 'old' security context. In order to align with the principle (*) stated above, this needs to be changed. Otherwise, the MS will indicate in the Routing Area Update Request message after the inter-system inter-SGSN change the **new** CKSN/KSI, whereas the new SGSN only has the security context belonging to the **old** CKSN/KSI. Because of the mismatch the new SGSN will then need to perform another re-authentication. (Note: During a 3G-3G inter-SGSN routing area update, the new SGSN will always initiate a Security Mode Command procedure and thereby take the new keys into use. During a 3G-3G inter-SGSN handover, the old keys currently in use are transferred from the old RNC to the new RNC within the RANAP signalling, whereas the new security context is provided to the new SGSN via GTP.)
Summary of change: ⌘	Instead of the keys currently in use, the old SGSN shall pass the keys belonging to the security context agreed with the MS during the latest successful authentication and ciphering procedure to the new SGSN.
Consequences if not approved: ⌘	Misalignment with TS 33.102 and TS 24.008, with the consequence that in the scenario described above, an additional re-authentication is necessary: If the wrong ciphering and integrity keys are passed to the new SGSN, the CKSN or KSI indicated by the MS in the Routing Area Update Request message to the new SGSN will deviate from the one the new SGSN receives from the old SGSN via GTP. Consequently, the new SGSN has to perform a new Authentication and Ciphering procedure

Clauses affected:	⌘	7.7.28			
Other specs affected:	⌘	**Y**	**N**		⌘
			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.

7.7.28 MM Context

The MM Context information element contains the Mobility Management, MS and security parameters that are necessary to transfer between SGSNs at the Inter SGSN Routeing Area Update procedure.

Security Mode indicates the type of security keys (GSM/UMTS) and Authentication Vectors (quintuplets/triplets) that are passed to the new SGSN.

Ciphering Key Sequence Number (CKSN) is described in 3GPP TS 24.008 [5]. Possible values are integers in the range [0; 6]. The value 7 is reserved. CKSN identifies Kc. During the Intersystem Change to 3G-SGSN, the KSI shall be assigned the value of CKSN.

Key Set Identifier (KSI) identifies CK and IK. During the Intersystem Change to 2G-SGSN, the CKSN shall be assigned the value of KSI.

Used Cipher indicates the GSM ciphering algorithm that is in use.

Kc is the GSM ciphering key of the GSM security context to be~~currently~~ used by the new~~old~~ SGSN. This is the GSM security context agreed with the MS during the latest successful authentication procedure. Kc shall be present if GSM key is indicated in the Security Mode.

CK is the UMTS ciphering key of the UMTS security context to be~~currently~~ used by the new~~old~~ SGSN. This is the UMTS security context agreed with the MS during the latest successful authentication procedure. CK shall be present if UMTS keys are indicated in the Security Mode.

IK is the UMTS integrity key of the UMTS security context to be~~currently~~ used by the new~~old~~ SGSN. This is the UMTS security context agreed with the MS during the latest successful authentication procedure. IK shall be present if UMTS keys are indicated in the Security Mode.

The Triplet array contains triplets encoded as the value in the Authentication Triplet information element The Triplet array shall be present if indicated in the Security Mode.

The Quintuplet array contains Quintuplets encoded as the value in the Authentication Quintuplet information element. The Quintuplet array shall be present if indicated in the Security Mode. If the quintuplet array is present, the Quintuplet length field indicates its length.

DRX parameter indicates whether the MS uses DRX mode or not.

MS Network Capability provides the network with information concerning aspects of the MS related to GPRS. MS Network Capability and MS Network Capability Length are coded as in the value part described in 3GPP TS 24.008 [5].

DRX parameter is coded as described in 3GPP TS 24.008 [5], the value part only.

The two octets Container Length holds the length of the Container, excluding the Container Length octets.

Container contains one or several optional information elements as described in the clause 'Overview', from the clause 'General message format and information elements coding' in 3GPP TS 24.008 [5]. An SGSN supporting the 'PUESBINE' feature (see 3GPP TS 23.195 [25] for more information) or the ADD feature (see 3GPP TS 22.101 [29] for more information) shall include the IMEISV in the Container.

	Bits							
Octets	**8**	**7**	**6**	**5**	**4**	**3**	**2**	**1**
1	Type = 129 (Decimal)							
2-3	Length							
4	Spare 1111					CKSN		
5	Security Mode		No of Vectors			Used Cipher		
6-13	Kc							
14-m	Triplet [0..4]							
(m+1)-(m+2)	DRX parameter							
(m+3)	MS Network Capability Length							
(m+4)-n	MS Network Capability							
(n+1)-(n+2)	Container length							
(n+3)-o	Container							

Figure 40: MM Context Information Element with GSM Key and Triplets

Octets	Bits 8	7	6	5	4	3	2	1
1	Type = 129 (Decimal)							
2-3	Length							
4	Spare 1111					KSI		
5	Security Mode		No of Vectors			Spare 111		
6-21	CK							
22-37	IK							
38-39	Quintuplet Length							
40-m	Quintuplet [0..4]							
(m+1)-(m+2)	DRX parameter							
(m+3)	MS Network Capability Length							
(m+4)-n	MS Network Capability							
(n+1)-(n+2)	Container length							
(n+3)-o	Container							

Figure 41: MM Context Information Element with UMTS Keys and Quintuplets

Octets	Bits 8	7	6	5	4	3	2	1
1	Type = 129 (Decimal)							
2-3	Length							
4	Spare 1111					CKSN		
5	Security Mode		No of Vectors			Used Cipher		
6-13	Kc							
14-15	Quintuplet Length							
16-m	Quintuplet [0..4]							
(m+1)-(m+2)	DRX parameter							
(m+3)	MS Network Capability Length							
(m+4)-n	MS Network Capability							
n+1-n+2	Container length							
n+3-o	Container							

Figure 42: MM Context Information Element with GSM Keys and UMTS Quintuplets

Octets	Bits 8	7	6	5	4	3	2	1
1	Type = 129 (Decimal)							
2-3	Length							
4	Spare 1111					CKSN/KSI		
5	Security Mode		No of Vectors			Used Cipher		
6-21	CK							
22-37	IK							
38-39	Quintuplet Length							
40-m	Quintuplet [0..4]							
(m+1)-(m+2)	DRX parameter							
(m+3)	MS Network Capability length							
(m+4)-n	MS Network Capability							
(n+1)-(n+2)	Container length							
(n+3)-n	Container							

Figure 42A: MM Context Information Element with Used Cipher value, UMTS Keys and Quintuplets

Table 46: Used Cipher Values

Cipher Algorithm	Value (Decimal)
No ciphering	0
GEA/1	1
GEA/2	2
GEA/3	3
GEA/4	4
GEA/5	5
GEA/6	6
GEA/7	7

Table 47: Security Mode Values

Security Type	Value (Decimal)
GSM key and triplets	1
GSM key and quintuplets	3
UMTS key and quintuplets	2
Used cipher value, UMTS Keys and Quintuplets	0

3GPP TSG-CN4 Meeting #24
Sophia Antipolis, France, 16th to 20th August

Tdoc ⌘ N4-041132

CR-Form-v7.1

CHANGE REQUEST

⌘ **29.060** **CR** **507** ⌘ **rev** **1** ⌘ Current version: **6.5.0** ⌘

*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 **X**

Title:	⌘	RIM transparent routing
Source:	⌘	CN4
Work item code:	⌘	TEI6
Date:	⌘	19/08/2004
Category:	⌘	**F**
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:
Ph2 (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)
Rel-7 (Release 7)

Reason for change: ⌘

In 3GPP Rel-5, 'RAN Information Management' (RIM) messages (defined in 3GPP TS 48.018) are used for GERAN to GERAN information exchange via CN. SGSN's sole function is to read the destination identity from the RIM message and make a routing decision whether to forward the message to one of its BSCs or tunnel the encapsulated RIM message through Gn interface towards target SGSN hosting the destination. The 3GPP TS 29.060 defines 'RAN Information Relay' procedure for the latter case.

In 3GPP Rel-6, TR 25.901 v6.0.0 describes the Network Assisted Cell Change feature between UTRAN and GERAN. This feature utilizes 'RAN Information Management' procedures and in the section 7 of the TR 25.901 it has been agreed the following:

"7.2 Format of RIM messages
GERAN does not adapt RIM messages to the target system and are routed via the CN without interpretation. The RNC alone needs to send and receive BSSGP messages within a container within the RANAP message."

To align relevant RANAP messages with the principles mentioned above, TSG RAN meeting #24 has approved CR 668 against TS 25.413 introducing destination identity for the encapsulated RIM message on the RANAP protocol level.

However in the Gn interface, the way how 'RAN Information Relay' procedure is currently defined does not make it possible to fullfill the requirement of transparency for the CN since, in order to determine the target RNC to which

		RIM message is to be forwarded, 3G SGSN would have to decode the destination identity from the encapsulated RIM message. To align also GTP with the agreed principles and to prevent introduction of BSSGP protocol decoding capabilities to 3G SGSN, destination identity for the RIM message has to be added to 'RAN Information Relay' message.
Summary of change:	⌘	'RIM Routing Address' is introduced as a new conditional IE to 'RAN Information Relay' message. It is included when the target for the RIM message is RNC (in UTRAN/GERAN to GERAN direction 2G SGSN has no difficulties to decode the destination identity from RIM PDU).
Consequences if not approved:	⌘	The 3G SGSN has to decode BSSGP RIM message in order to route it towards radio access network. This violates the principles agreed in RAN3 and furthermore requires termination of 2G access protocol to 3G SGSN.

Clauses affected:	⌘	7.5.14; 7.5.14.1; 7.7 and 7.7.xx as a new clause			
Other specs affected:	⌘	**Y**	**N**		
			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.

START of first modification

7.5.14 RAN Information Management Messages

The RAN Information Relay is used over the Gn interface to tunnel RAN INFORMATION messages received by an SGSN from a BSS or from RNS. The procedures are specified in 3GPP TS 23.060 [4] and the RAN INFORMATION messages are specified in 3GPP TS 48.018 [20].

7.5.14.1 RAN Information Relay

All information elements from the RAN INFORMATION messages, starting from and including the BSSGP 'PDU type', shall be contained within the RAN Transparent Container and forwarded to the destination SGSN in the RAN Information Relay message. For handling of protocol errors the RAN Information Relay message is treated as a Response message.

RIM Routing Address contains the destination RNC Identity from the RAN INFORMATION message when the source is GERAN and the target is UTRAN.

The optional Private Extension contains vendor or operator specific information.

Table 7.5.14.1: Information Elements in a RAN Information Relay

Information element	Presence requirement	Reference
RAN Transparent Container	Mandatory	7.7.43
RIM Routing Address	Optional~~Conditional~~	7.7.xx
Private Extension	Optional	7.7.46

END of first modification

START of second modification

7.7 Information Elements

A GTP Signalling message may contain several information elements. The TLV (Type, Length, Value) or TV (Type, Value) encoding format shall be used for the GTP information elements. The information elements shall be sorted, with the Type fields in ascending order, in the signalling messages. The Length field contains the length of the information element excluding the Type and Length field.

For all the length fields, bit 8 of the lowest numbered octet is the most significant bit and bit 1 of the highest numbered octet is the least significant bit.

Within information elements, certain fields may be described as spare. These bits shall be transmitted with the value defined for them. To allow for future features, the receiver shall not evaluate these bits.

The most significant bit in the Type field is set to 0 when the TV format is used and set to 1 for the TLV format.

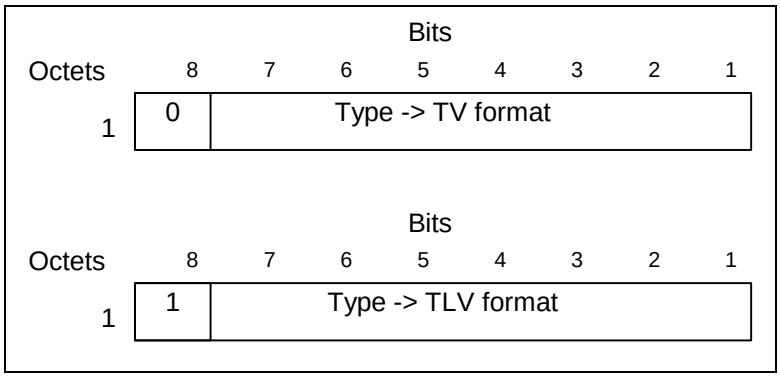

Figure 8: Type field for TV and TLV format

Table 37: Information Elements

IE Type Value	Format	Information Element	Reference
1	TV	Cause	7.7.1
2	TV	International Mobile Subscriber Identity (IMSI)	7.7.2
3	TV	Routeing Area Identity (RAI)	7.7.3
4	TV	Temporary Logical Link Identity (TLLI)	7.7.4
5	TV	Packet TMSI (P-TMSI)	7.7.5
6-7	Spare		
8	TV	Reordering Required	7.7.6
9	TV	Authentication Triplet	7.7.7
10	Spare		
11	TV	MAP Cause	7.7.8
12	TV	P-TMSI Signature	7.7.9
13	TV	MS Validated	7.7.10
14	TV	Recovery	7.7.11
15	TV	Selection Mode	7.7.12
16	TV	Tunnel Endpoint Identifier Data I	7.7.13
17	TV	Tunnel Endpoint Identifier Control Plane	7.7.14
18	TV	Tunnel Endpoint Identifier Data II	7.7.15
19	TV	Teardown Ind	7.7.16
20	TV	NSAPI	7.7.17
21	TV	RANAP Cause	7.7.18
22	TV	RAB Context	7.7.19
23	TV	Radio Priority SMS	7.7.20
24	TV	Radio Priority	7.7.21
25	TV	Packet Flow Id	7.7.22
26	TV	Charging Characteristics	7.7.23
27	TV	Trace Reference	7.7.24
28	TV	Trace Type	7.7.25
29	TV	MS Not Reachable Reason	7.7.25A
30	TV	Radio Priority LCS	7.7.25B
117-126	Reserved for the GPRS charging protocol (see GTP' in 3GPP TS 32.215 [18])		
127	TV	Charging ID	7.7.26
128	TLV	End User Address	7.7.27
129	TLV	MM Context	7.7.28
130	TLV	PDP Context	7.7.29
131	TLV	Access Point Name	7.7.30
132	TLV	Protocol Configuration Options	7.7.31
133	TLV	GSN Address	7.7.32
134	TLV	MS International PSTN/ISDN Number (MSISDN)	7.7.33
135	TLV	Quality of Service Profile	7.7.34
136	TLV	Authentication Quintuplet	7.7.35
137	TLV	Traffic Flow Template	7.7.36
138	TLV	Target Identification	7.7.37
139	TLV	UTRAN Transparent Container	7.7.38

IE Type Value	Format	Information Element	Reference
140	TLV	RAB Setup Information	7.7.39
141	TLV	Extension Header Type List	7.7.40
142	TLV	Trigger Id	7.7.41
143	TLV	OMC Identity	7.7.42
144	TLV	RAN Transparent Container	7.7.43
145	TLV	PDP Context Prioritization	7.7.45
146	TLV	Additional RAB Setup Information	7.7.45A
147	TLV	SGSN Number	7.7.47
148	TLV	Common Flags	7.7.48
149	TLV	APN Restriction	7.7.49
150	TLV	Radio Priority LCS	7.7.25B
151	TLV	RAT Type	7.7.50
152	TLV	User Location Information	7.7.51
153	TLV	MS Time Zone	7.7.52
154	TLV	IMEI(SV)	7.7.53
155	TLV	CAMEL Charging Information Container	7.7.54
156	TLV	MBMS UE Context	7.7.55
157	TLV	Temporary Mobile Group Identity (TMGI)	7.7.56
XXX	TLV	RIM Routing Address	7.7.xx
239-250	Reserved for the GPRS charging protocol (see GTP' in 3GPP TS 32.215 [18])		
251	TLV	Charging Gateway Address	7.7.44
252-254	Reserved for the GPRS charging protocol (see GTP' in 3GPP TS 32.215 [18])		
255	TLV	Private Extension	7.7.46

END of second modification

START of third modification

7.7.xx RIM Routing Address

Octets 4-n are coded according to 3GPP TS 48.018 [20] RIM Routing Information IE octets 4-n.

	Bits							
Octets	8	7	6	5	4	3	2	1
1	Type = xxx (Decimal)							
2-3	Length							
4-n	RIM Routing Address							

END of third modification