3GPP TSG CN Plenary Meeting #20 **NP-030284**
4th - 6th June 2003. HÄMEENLINNA, Finland.

Source: **TSG CN WG 1**

Title: **CRs to Rel-6 on Work Item TEI6 towards 24.008 and 44.065**

Agenda item: **9.18**

Document for: **APPROVAL**

Introduction:

This document contains **4** CRs, **Rel-5 to** Work Item **"TEI6"**, that have been agreed by **TSG CN WG1**, and are forwarded to TSG CN Plenary meeting #20 for approval.

Spec	CR	Rev	Cat	Phase	Subject	Version-Current	Version-New	Meeting-2nd-Level	Doc-2nd-Level
24.008	750		F	Rel-6	MS RAC encoding	6.0.0	6.1.0	N1-29	N1-030390
24.008	768		F	Rel-6	Wrong references in SETUP and redirected number/subaddress IEs	6.0.0	6.1.0	N1-30	N1-030626
44.065	004	4	B	Rel-6	Additional support of ROHC in SNDCP	5.0.0	6.0.0	N1-30	N1-030934
44.065	005	1	C	Rel-6	Multiple header compression algorithms handling	5.0.0	6.0.0	N1-30	N1-030833

CR-Form-v7

CHANGE REQUEST

⌘ **44.065** **CR** **004** ⌘ **rev** **4** ⌘ Current version: **5.0.0** ⌘

*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 [X] Radio Access Network [ ] Core Network [X]

Title:	⌘	Additional support of ROHC in SNDCP
Source:	⌘	Ericsson L.M.
Work item code:	⌘	TEI-6
Date:	⌘	21/05/2003
Category:	⌘	**B**
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:	⌘	SNDCP has currently support for two header compression schemes (RFC 1144 and RFC 2507) compressing the headers of UDP/IP and TCP/IP. However, the current state-of-the-art header compression platform, ROHC (RObust Header Compression), is not supported. Also, currently there is no support for compression of RTP traffic in SNDCP, but as new RTP based IMS services are introduced, it is important to have a scheme that efficiently compresses the RTP/UDP/IP headers, in order not to waste valuable radio resources. Today there are five ROHC profiles defined: Uncompressed, RTP/UDP/IP, UDP/IP only, ESP/IP and LLA RTP. The IETF ROHC WG is currently in the process of creating three new profiles: IP only, TCP/IP and UDP-Lite. According to the IETF ROHC charter these are expected to be ready in the first half of 2003. Based on the above it is proposed to include ROHC as a new option in SNDCP from Release 6.
Summary of change:	⌘	Appropriate text to incorporate the support of ROHC into SNDCP as a new option are added to sub-clause 6.5. Also, references to the appropriate ROHC RFCs are included in sub-clause 2.
Consequences if not approved:	⌘	The current state-of-the-art header compression platform would not be supported and there would be no header compression support for RTP traffic at all.

Clauses affected:	⌘	Clauses 2, 3.2 and 6.5.
Other specs	⌘	Y [ ] N [X] Other core specifications ⌘

affected:		
	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 *****

2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document.*

[1] 3GPP TS 01.04: "Digital cellular telecommunications system (Phase 2+); Abbreviations and acronyms".

[2] 3GPP TS 02.60: "Digital cellular telecommunication system (Phase 2+); General Packet Radio Service (GPRS); Service Description; Stage 1".

[3] 3GPP TS 03.60: "Digital cellular telecommunication system (Phase 2+); General Packet Radio Service (GPRS); Service Description; Stage 2".

[4] 3GPP TS 04.07: "Digital cellular telecommunications system (Phase 2+); Mobile radio interface signalling layer 3; General aspects".

[5] 3GPP TS 04.08: "Digital cellular telecommunications system (Phase 2+), Mobile radio interface; Layer 3 specification".

[6] 3GPP TS 04.64: "Digital cellular telecommunications system (Phase 2+); General Packet Radio Service (GPRS); Mobile Station - Serving GPRS Support Node (MS-SGSN) Logical Link Control (LLC) layer specification".

[7] 3GPP TS 09.60: "Digital cellular telecommunications system (Phase 2+), General Packet Radio Service (GPRS); GPRS Tunnelling Protocol (GTP) across the Gn and Gp Interface".

[8] ITU-T Recommendation V.42 bis: "Data compression procedures for data circuit-terminating equipment (DCE) using error correcting procedures".

[9] IETF RFC 1144: "Compressing TCP/IP headers for low-speed serial links", V. Jacobson.

[10] IETF RFC 2507: "IP Header Compression", M. Degermark, B. Nordgren, S. Pink.

[11] ITU-T Recommendation V.44: "Data compression procedures".

[12] IETF RFC 3095: "RObust Header Compression (ROHC): Framework and four profiles: RTP, UDP, ESP, and uncompressed". C. Bormann et al.

[13] IETF RFC 3241: "Robust Header Compression (ROHC) over PPP". C. Bormann.

[14] "RObust Header Compression (ROHC) Profile Identifiers". IANA registry at: *http://www.iana.org/assignments/rohc-pro-ids*

***** Next change *****

3.2 Abbreviations

For the purposes of the present document, the abbreviations given in 3GPP TS 01.04 [1], 3GPP TS 02.60 [2], and 3GPP TS 03.60 [3], and the following apply:

CID	Context Identifier
DCOMP	Identifier of the user data compression algorithm used for the N-PDU
ESP	Encapsulating Security Payload
F	First segment indicator bit
GMM	GPRS Mobility Management
IP	Internet Protocol
LLC	Logical Link Control
LSB	Least Significant Bits
M	More bit used to indicate the last segment of N-PDU
MRRU	Maximum Reconstructed Reception Unit
MSB	Most Significant Bits
N-PDU	Network Protocol Data Unit
NSAPI	Network Layer Service Access Point Identifier
P	Propose bit
PCOMP	Identifier of the protocol control information compression algorithm used for the N-PDU
PDP	Packet Data Protocol (e.g. IPv4 or IPv6)
PDU	Protocol Data Unit
PID	Protocol Identifier
PTP	Point to Point
QoS	Quality of Service
ROHC	RObust Header Compression
RTP	Real Time Protocol
SAPI	Service Access Point Identifier
SDU	Service Data Unit
SGSN	Serving GPRS Support Node
SM	Session Management
SNDCP	Subnetwork Dependent Convergence Protocol
SNSM	SNDCP-SM
TCP	Transmission Control Protocol
TLLI	Temporary Logical Link Identifier
X	Spare bit

***** Next change *****

6.5.1.1.4 Algorithm type

Table 4 show the list of protocol control information compression algorithms supported by the SNDCP layer. When new compression algorithms are needed for SNDCP, table 4 shall be updated.

Table 4: List of protocol control information compression algorithms supported by SNDCP

Compression algorithm	Algorithm type (Range 0 to 31)
RFC 1144	0
RFC 2507	1
ROHC	2
-	Other values Reserved

***** Next change *****

6.5.4 Robust Header Compression (ROHC)

Robust Header Compression (ROHC) is a framework for header compression, on top of which compression schemes can be defined for the compression of various protocol headers. Both the SNDCP ROHC negotiation mechanisms and

the SN-PDU ROHC identifiers are generally defined for the ROHC framework, and therefore capable of handling both existing and future ROHC compression protocols (profiles). RFC 3095 [12] defines the ROHC framework, as well as the compression schemes and profiles for RTP/UDP/IP, UDP/IP, ESP/IP and uncompressed.

6.5.4.1 Parameters

Table 8 contains the parameters defined for a compression entity using ROHC. They may be negotiated during SNDCP XID negotiation.

Table 8: Robust Header Compression (ROHC) parameters

Algorithm Name	Algorithm Type	Length	Parameter Name	Format	Range	Sense of Negotiation	Default Value
ROHC	2	0, 2, 4, 6, 8, 8+n*2 if P bit is 0, 2, 4, 6, 8, 10, 10+n*2 if P bit is 1. (where n is the number of profiles, the max. number of profiles is 16)	Applicable NSAPIs	bbbbbbbb bbb00000	0, 32, 64, … , 65504	down (each bit separately)	0
			MAX_CID	00bbbbbb bbbbbbbb	0-16383	down	15
			MAX_HEADER	00000000 bbbbbbbb	60-255	down	168
			MRRU	bbbbbbbb bbbbbbbb	0-65535	down	0
			PROFILE 1	bbbbbbbb bbbbbbbb	0-65535	(see 6.5.4.1.5)	0
			PROFILE 2	bbbbbbbb bbbbbbbb	0-65535	(see 6.5.4.1.5)	0
			...	...	...	...	...
			PROFILE 16	bbbbbbbb bbbbbbbb	0-65535	(see 6.5.4.1.5)	0

6.5.4.1.1 Applicable NSAPIs

See subclause 7.1.3.

6.5.4.1.2 MAX_CID

The MAX_CID parameter indicates the maximum number of context identifiers. A value N means N+1 context, e.g. 0 means 1 context.

6.5.4.1.3 MAX_HEADER

The MAX_HEADER parameter indicates the maximum number of octets of the protocol control information that may be compressed.

6.5.4.1.4 MRRU

If ROHC segmentation is used, the maximum reconstructed reception unit (MRRU) indicates the number of octets that the decompressor is expected to reassemble from the segments. If MRRU is negotiated to 0, ROHC segmentation is disabled.

6.5.4.1.5 PROFILE~~S~~

The PROFILE parameter indicates the profile identifier. A list of up to 16 PROFILEs, indicating which ROHC profiles [14] are supported may be included. The negotiated list which is used for compression consists of the list of profiles supported by both peer entities, reduced to include at most ONE profile identifier with the same 8-bit LSB part. If both peer entities support more than one profile with the same 8-bit LSB part in its profile identifier, the set of these profiles shall be reduced to the profile with the highest MSB-value in its profile identifier.

Note: The reason for this is that the 8-bit MSB part of the profile identifier indicates the "variant" of the profile, and since only the 8-bit LSB part is sent in compressed headers, the set of available profiles must not include two profiles with the same 8-bit LSB part of the profile identifier.

6.5.4.2 Assignment of PCOMP values for ROHC

As opposed to other header compression schemes, the whole ROHC framework has only one packet type that has to be identified by the PDU format, and this packet type can be used by any ROHC compression profile. However, ROHC has two different context identification (CID) sizes. To avoid having to negotiate and potentially re-negotiate CID size, the mechanism from ROHC-over-PPP [13] is adopted in SNDCP, i.e. as shown in table 9, two packet types are defined for ROHC, one for small and one for large CIDs.

This implies that all CIDs within one ROHC packet shall be of the same size as indicated by the PID value, either small or large. In particular, embedded feedback shall have a CID of the same size as indicated by the PID value. For piggybacking feedback, a compressor must be able to control the feedback CID size used by the associated decompressor, ensure that all CIDs are of the same size, and indicate this size with the appropriate PID value. To make CID interpretation unambiguous when ROHC segmentation is used, all packets that contribute to a segment shall be sent with the same PID value, either PCOMP1 or PCOMP2, which then also applies to the CID size in the reconstructed unit. A unit reconstructed out of packets with PID values that differ shall be discarded.

Table 9: PCOMP values assigned to Robust Header Compression (ROHC)

PID value	Packet type
PCOMP1	ROHC small-CIDs
PCOMP2	ROHC large-CIDs

6.5.4.3 Error Recovery and other feedback

ROHC has built-in robustness mechanisms to avoid error events, as well as error recovery mechanisms using decompressor to compressor feedback. Such ROHC feedback is carried according to alternative 6) in section 5.2.1 of RFC 3095 [12].

***** Last change *****

CR-Form-v7

CHANGE REQUEST

⌘ **44.065** **CR** **005** ⌘ **rev** **1** ⌘ Current version: **5.0.0** ⌘

*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:	⌘	Multiple header compression algorithms handling
Source:	⌘	Siemens AG
Work item code:	⌘	TEI-6
Date:	⌘	20.05.2003
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:

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:	⌘	For header compression the two algorithms RFC1144 and RFC2507 are defined in the SNDCP protocol. With RFC1144 TCP and IPv4 header will be compressed. With RFC2507 UDP / TCP with IPv4/IPv6 will be compressed. From the functional point of view RFC2507 is covering the functionality of RFC1144. For data compression the two algorithms V42bis and V44 are defined in the SNDCP protocol. There is no technical reason to activate two data compression algorithms on one NSAPI, as they are not content specific. If the originator (MS or SGSN) of the XID negotiation is supporting two algorithms for either header or data compression, then he will offer for each NSAPI the parameters of both algorithms. If the peer entity also supports both algorithms then there is the risk that both algorithms are accepted, even if only one is used. The creation of a compression instance causes significant allocation of RAM which is a limited resource in both the MS and the SGSN. Such a unnecessary waste of resources should be avoided.
Summary of change:	⌘	The peer entity of the XID negotiation shall accept only one header compression algorithm and one data compression algorithm for an NSAPI.
Consequences if not approved:	⌘	As only one header/data compression algorithm is used, all the other offered compression algorithm which are unnecessarily activated are causing a waste of resources(especially RAM) and will in consequence either limiting the overall amount of PDP contexts which could be compressed by the MS and the SGSN or increase the costs of the MS and the SGSN.

Clauses affected:	⌘	6.5.1, 6.6.1

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

Other comments:	⌘	

6.5 Protocol control information compression

Protocol control information compression is an optional SNDCP feature.

Negotiation of the supported algorithms and their parameters is carried out between MS and SGSN using the SNDCP XID parameters (see clause 8).

6.5.1 Negotiation of multiple protocol control information compression types

Each SNDCP entity that supports protocol control information compression shall be able to negotiate one or several protocol control information compression entities with the compression field format shown in figure 7. The negotiation shall be carried out using the XID parameter negotiation specified in subclause 6.8. The initiating entity defines a set of requested compression entities, together with the algorithm and parameters for each compression entity. The set of entities and their algorithms and parameters shall be transmitted to the peer entity. The peer entity responds with the set of negotiated entities and their algorithms and parameters. The peer entity shall select the proposed parameter values or other appropriate values for the negotiated entities. If more than one protocol control information compression algorithm for a specific NSAPI is proposed during the XID negotiation then the receiving peer entity shall only choose one algorithm for that NSAPI.

6.5.1.1 Format of the protocol control information compression field

Bit	8	7	6	5	4	3	2	1
Octet 1	P	X	X	Entity number				
Octet 2	X	X	X	Algorithm type				
Octet 3	Length=n-3							
Octet 4	PCOMP1				PCOMP2			
…	…				…			
Octet x	High-order octet							
…	…							
Octet n	Low-order octet							

Figure 7: Protocol control information compression field format for SNDCP XID negotiation

6.5.1.1.1 Spare bit (X)

The X bit shall be set to 0 by the transmitting SNDCP entity and shall be ignored by the receiving SNDCP entity.

6.5.1.1.2 Propose bit (P)

The P bit shall be set to 1 if a new compression entity is being proposed, otherwise it shall be set to 0. If the P bit is set to 1, then all octets shall be included, otherwise octet 2 and octets 4 to x-1 shall not be included. If the P bit is set to 1, then only enough number of octets shall be included to contain the number of PCOMP values needed by the corresponding compression algorithm (e.g. PCOMP3 and PCOMP4 shall not be included if the number of PCOMP values needed by a compression algorithm is one or two). If an odd number of PCOMP values are used by a compression algorithm, then the last PCOMP value shall be set to 0 in the compression field by the transmitting SNDCP entity, and it shall be ignored by the receiving SNDCP entity.

6.5.1.1.3 Entity number

The entity number shall be used to identify a protocol control information compression entity on a SAPI. The entity number shall be assigned using the following rules:

- The entity number shall be an integer from 0 to 31.

- The entity number shall be assigned independently on each of the SAPIs.
- An entity number shall be in one of the three states: unassigned, selected, or assigned.
- When a new compression entity is to be proposed, an unassigned entity number shall become selected. If there is no unassigned entity number left, the compression entity shall not be proposed.
- A selected entity number shall become assigned if the corresponding proposed compression entity is created as a result of the XID negotiation, otherwise it shall become unassigned.
- An assigned entity number shall become unassigned when the corresponding compression entity is deleted as a result of an XID negotiation, or upon the receipt of the LL-RESET.indication primitive.
- In the case of a collision (see subclause 6.2.1.4) in which an entity number is currently selected:
    - If the selected entity number is included with the P bit set to 0 in the incoming SNDCP XID block, then it shall be assumed that the peer SNDCP entity agreed to the creation of the proposed entity but the response was lost. Therefore the selected entity number shall become assigned, any selected PCOMP and DCOMP values for the algorithm of the entity shall become assigned, and the compression entity shall be created, before the incoming SNDCP XID block is processed. After the incoming SNDCP XID block is processed, the compression entity shall be negotiated again if necessary, as defined in subclause 6.2.1.4.
    - Otherwise (i.e. if the selected entity number is not included, or is included with the P bit set to 1 in the incoming SNDCP XID block), the selected entity number shall become unassigned, and any selected PCOMP and DCOMP values for the algorithm of the entity shall become unassigned, before the incoming SNDCP XID block, if any, is processed. Following the collision resolution procedure, the originally-proposed compression entity shall be proposed again (i.e. the originally-proposed compression entity shall not be considered created even if the originally-selected entity number is proposed in the incoming SNDCP XID block) by sending the appropriate primitive (LL-ESTABLISH.request or LL-XID.request). The originally-selected entity number, PCOMP and DCOMP values shall be used for the compression entity being re-proposed if they are unassigned, otherwise a new entity number, PCOMP or DCOMP value shall be selected.
- In the case of a collision in which an entity number is currently assigned:
    - If the peer SNDCP entity proposes a new compression entity with the same entity number, then it shall be assumed that the peer SNDCP entity negotiated the deletion of the entity but the response was lost, and the entity number is being reused. Therefore the original compression entity shall be deleted, the entity number shall become unassigned, PCOMP and DCOMP values shall be unassigned if necessary (see subclause 6.5.1.1.5), and then the proposed compression entity shall be responded to as usual.
    - Otherwise (i.e. if the assigned entity number is not included, or is included with the P bit set to 0 in the incoming SNDCP XID block), the usual rules regarding collision handling shall apply.
- In the case of a collision in which a PCOMP or DCOMP value is currently assigned to a compression algorithm:
    - If the peer SNDCP entity proposes a new compression entity with the same PCOMP or DCOMP assigned to a different algorithm, then it shall be assumed that the peer SNDCP entity negotiated the deletion of all entities using the algorithm to which the PCOMP or DCOMP value was assigned, but the response was lost, and the PCOMP or DCOMP value is being reused. Therefore, all compression entities using that algorithm shall be deleted, all corresponding entity numbers shall become unassigned, and all PCOMP or DCOMP values assigned to the algorithm shall become unassigned, and then the proposed compression entity shall be responded to as usual.
    - Otherwise (i.e. if the assigned PCOMP or DCOMP is not included, or is included and assigned to the same algorithm), the usual rules regarding collision handling shall apply.

6.5.1.1.4 Algorithm type

Table 4 show the list of protocol control information compression algorithms supported by the SNDCP layer. When new compression algorithms are needed for SNDCP, table 4 shall be updated.

Table 4: List of protocol control information compression algorithms supported by SNDCP

Compression algorithm	Algorithm type (Range 0 to 31)
RFC 1144	0
RFC 2507	1
-	Other values Reserved

6.5.1.1.5 PCOMP

One or more PCOMP values shall be assigned dynamically to a compression algorithm, based on the negotiation of the XID parameters for protocol control information compression. Each of the assigned PCOMP values denotes one compressed frame type of that compression algorithm.

The assignment of the PCOMP values follows the following general rules:

- PCOMP shall be an integer from 0 to 15.
- PCOMP value 0 is reserved permanently for no compression.
- PCOMP shall be assigned independently on each of the SAPIs.
- An assigned PCOMP value applies to all NSAPIs mapped to the same SAPI.
- PCOMP values shall be assigned to compression algorithms, not to compression entities (i.e. the same PCOMP value(s) shall be used by different compression entities on the same SAPI using the same compression algorithm).
- A PCOMP value shall be in one of the three states: unassigned, selected, or assigned.
- When a new compression entity is to be proposed, and if PCOMP values have not yet been assigned to the corresponding compression algorithm, then the appropriate number of unassigned PCOMP values shall be selected. If there is not enough unassigned PCOMP values left, the compression entity shall not be proposed.
- A selected PCOMP value shall become assigned if the corresponding proposed compression entity is created as a result of the XID negotiation, otherwise it shall become unassigned.
- An assigned PCOMP value shall become unassigned when the corresponding compression algorithm is no longer in use by any compression entity, or upon the receipt of the LL-RESET.indication primitive.
- In the case of a collision (see subclause 6.2.1.4), the handling of PCOMP values shall be in accordance with subclause 6.5.1.1.3.

While transferring data, the compressed frame type for an N-PDU is conveyed in the PCOMP field of the SNDCP header of the first SN-PDU belonging to the N-PDU. Any successfully negotiated algorithm may be used for compression of an N-PDU.

6.5.1.2 Resetting compression entities following SNDCP XID negotiation

The LL-Establish primitives shall be used for the negotiation of protocol control information compression if:

- one or more parameters, excluding the applicable NSAPIs, of existing compression entities used with acknowledged peer-to-peer LLC operation are changed by the originator of the negotiation; or
- one or more NSAPIs are removed, by the originator of the negotiation, from existing compression entities used with acknowledged peer-to-peer LLC operation, except when all NSAPIs using the compression entity are removed, or when LLC is already in ADM.

Otherwise, either the LL-Establish primitives or the LL-XID primitives may be used.

If the LL-XID primitives are used for XID negotiation, then in addition to restrictions specified elsewhere in the present document, the following parameters of the protocol control information compression entities are non-negotiable by the responding SNDCP entity:

- any parameter of existing compression entities used with acknowledged peer-to-peer LLC operation.

If one or more parameters, other than the applicable NSAPIs, of a compression entity used with unacknowledged peer-to-peer LLC operation are changed, the compression entity shall be reset locally upon completion of the SNDCP XID negotiation.

6.5.1.3 Parameters for compression entities

On negotiating a compression entity, not all the parameters of the entity have to be specified. If a parameter is to be included, all the preceding parameters shall also be specified, and the length field shall be set to the sum of the lengths of all the parameters specified. If any of the parameters is not specified, the rules in subclause 6.8.2 shall apply.

6.6 Data compression

Data compression is an optional SNDCP feature. Data compression applies to both SN-DATA and SN-UNITDATA primitives.

Data compression, if used, shall be performed on the entire N-PDU, including the possibly compressed protocol control information.

Figure 8 shows an example how the SNDCP functions may be used. Several NSAPIs may use a common data compression entity, i.e. the same compression algorithm and the same dictionary. Separate data compression entities shall be used for acknowledged (SN-DATA) and unacknowledged (SN-UNITDATA) data transfer. Several NSAPIs may be associated with one SAPI, i.e. they may use the same QoS profile.

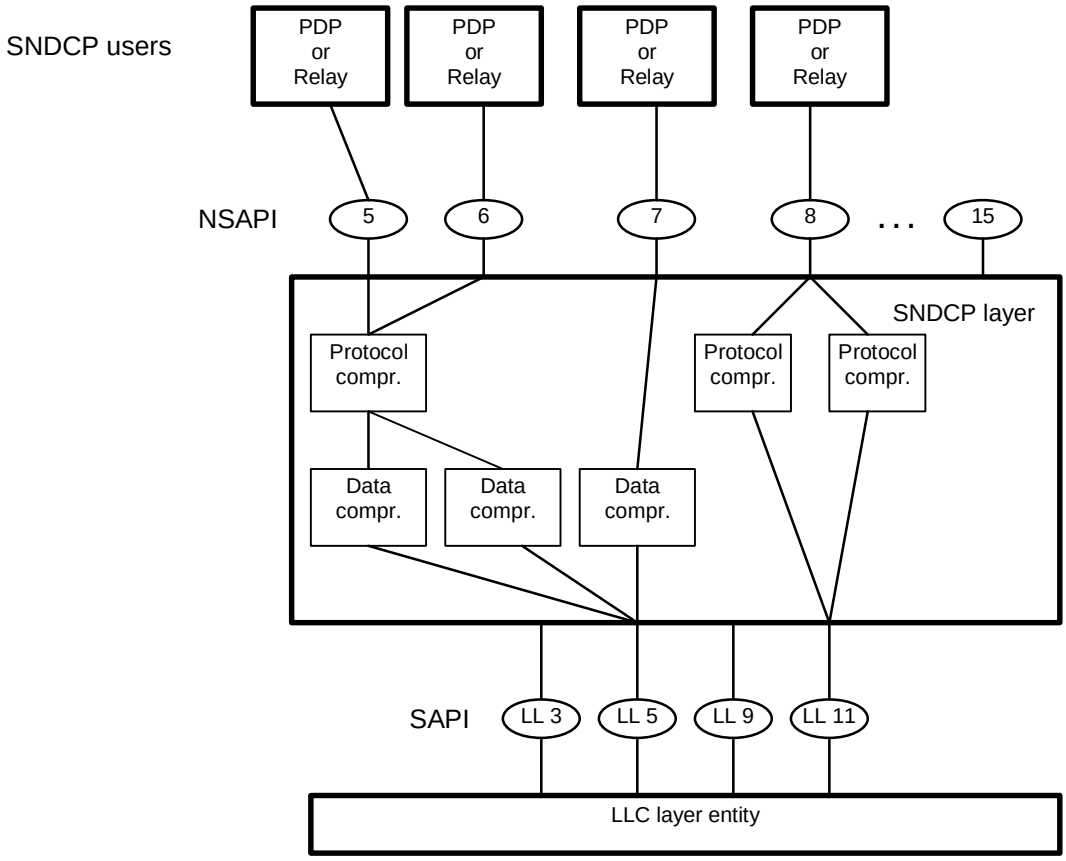

Figure 8: An example for the usage of NSAPIs, SNDCP functions, and SAPIs

6.6.1 Negotiation of multiple data compression types

Each SNDCP entity that supports data compression shall be able to negotiate one or several data compression entities with the compression field format shown in figure 9. The negotiation shall be carried out using the XID parameter negotiation specified in subclause 6.8. The initiating entity defines a set of requested compression entities, together with the algorithm and parameters for each compression entity. The set of entities and their algorithms and parameters shall be transmitted to the peer entity. The peer entity responds with the set of negotiated entities and their algorithms and parameters. The peer entity shall select the proposed parameter values or other appropriate values for the negotiated entities. If more than one data compression algorithm for a specific NSAPI is proposed during the XID negotiation then the receiving peer entity shall only choose one algorithm for that NSAPI.

~~For each NSAPI one or more data compression are chosen. This choice is also indicated in the SNDCP XID. Only NSAPIs that are using the same SAPI may use the same data compression entity. If more than one compression entity is chosen for an NSAPI, these entities must use different data compression algorithms. However, only one data compression entity is used for one N-PDU; i.e. the used data compression entity may be changed from N-PDU to N-PDU.~~

6.6.1.1 Format of the data compression field

Bit	8	7	6	5	4	3	2	1
Octet 1	P	X	X	Entity number				
Octet 2	X	X	X	Algorithm type				
Octet 3	Length=n-3							
Octet 4	DCOMP1				DCOMP2			
…	…				…			
Octet x	High-order octet							
…	…							
Octet n	Low-order octet							

Figure 9: Data compression field format for SNDCP XID negotiation

6.6.1.1.1 Spare bit (X)

The X bit shall be set to 0 by the transmitting SNDCP entity and shall be ignored by the receiving SNDCP entity.

6.6.1.1.2 Propose bit (P)

The P bit shall be set to 1 if a new compression entity is being proposed, otherwise it shall be set to 0. If the P bit is set to 1, then all octets shall be included, otherwise octet 2 and octets 4 to x-1 shall not be included. If the P bit is set to 1, then only enough number of octets shall be included to contain the number of DCOMP values needed by the corresponding compression algorithm (e.g. DCOMP3 and DCOMP4 shall not be included if the number of DCOMP values needed by a compression algorithm is one or two). If an odd number of DCOMP values are used by a compression algorithm, then the last DCOMP value shall be set to 0 in the compression field by the transmitting SNDCP entity, and it shall be ignored by the receiving SNDCP entity.

6.6.1.1.3 Entity number

The entity number shall be used to identify a data compression entity on a SAPI. See subclause 6.5.1.1.3 for the rules for assigning entity numbers. The assignment of entity numbers for protocol control information compression entities and data compression entities shall be independent.

6.6.1.1.4 Algorithm type

Table 6a shows the list of data compression algorithms supported by the SNDCP layer. When new compression algorithms are needed for SNDCP, table 6a shall be updated.

Table 6a: List of data compression algorithms supported by SNDCP

Data compression algorithm	Algorithm type (Range 0-31)
V.42 bis	0
V.44	1
-	Other values Reserved

6.6.1.1.5 DCOMP

One or more DCOMP values shall be assigned dynamically to a compression algorithm, based on the negotiation of the XID parameters for data compression. Each of the assigned DCOMP values denotes one compressed frame type of that compression algorithm.

The assignment of the DCOMP values shall follow the rules for the assignment of PCOMP values in subclause 6.5.1.1.5.

While transferring data, the compressed frame type for an N-PDU is conveyed in the DCOMP field of the SNDCP header of the first SN-PDU belonging to the N-PDU. Any successfully negotiated algorithm may be used for compression of an N-PDU.

6.6.1.2 Resetting compression entities following SNDCP XID negotiation

The LL-Establish primitives shall be used for the negotiation of data compression if:

- one or more parameters, excluding the applicable NSAPIs, of existing compression entities used with acknowledged peer-to-peer LLC operation are changed by the originator of the negotiation; or

- one or more NSAPIs are removed, by the originator of the negotiation, from existing compression entities used with acknowledged peer-to-peer LLC operation, except when all NSAPIs using the compression entity are removed, or when LLC is already in ADM.

Otherwise, either the LL-Establish primitives or the LL-XID primitives may be used.

If the LL-XID primitives are used for XID negotiation, then in addition to restrictions specified elsewhere in the present document, the following parameters of the data compression entities are non-negotiable by the responding SNDCP entity:

- any parameter of existing compression entities used with acknowledged peer-to-peer LLC operation.

If one or more parameters, other than the applicable NSAPIs, of a compression entity used with unacknowledged peer-to-peer LLC operation are changed, the compression entity shall be reset locally upon completion of the SNDCP XID negotiation.

6.6.1.3 Parameters for compression entities

On negotiating a compression entity, not all the parameters of the entity have to be specified. If a parameter is to be included, all the preceding parameters shall also be specified, and the length field shall be set to the sum of the lengths of all the parameters specified. If any of the parameters is not specified, the rules in subclause 6.8.2 shall apply.

3GPP TSG-CN1 Meeting #29 ***Tdoc N1-030390***
Sophia-Antipolis, France, 31 March – 04 April 2003

CR-Form-v7

CHANGE REQUEST

⌘ **24.008** **CR** **750** ⌘ **rev** **-** ⌘ Current version: **6.0.0** ⌘

*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 [X] Radio Access Network [ ] Core Network [X]

Title:	⌘	MS RAC encoding
Source:	⌘	Nokia
Work item code:	⌘	TEI-6
Date:	⌘	24/03/2003
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:

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:	⌘	Currently the encoding of the IEs in 24.008 is inconsistent, since normally the CSN structures only define the value part of the IE but MS RAC is defined with IEI and length octets shown.
Summary of change:	⌘	Deletion of the extra octets to align with the other IEs in 24.008
Consequences if not approved:	⌘	Inconsistent IE definitions

Clauses affected:	⌘	10.5.5.12a

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

Other comments:	⌘	This CR is almost editorial and should have no impact on the impelementations. Therefore it was not considered justified to change the frozen releases.

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.

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 Radio Access capability IE > ::=~~
~~**<MS Radio Access capability IEI** : 00100100 >~~
~~**<Length of MS RA capability**: <octet>> *length in octets of MS RA capability value part and spare bits*~~
<**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) > }
-- Additions in release 5
{ 0 | 1 < **High Multislot Capability** : bit(2) > }
< **GERAN Iu Mode Capability** : bit >;
-- error: struct too short, assume features do not exist
-- error: struct too long, ignore data and jump to next Access technology

CR-Form-v7

CHANGE REQUEST

⌘ **24.008** **CR** **768** ⌘ **rev** **-** ⌘ Current version: **6.0.0** ⌘

*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 [X] Radio Access Network [X] Core Network [X]

Title:	⌘	Wrong references in SETUP and redirected number/subaddress IEs
Source:	⌘	Siemens AG
Work item code:	⌘	TEI-6
Date:	⌘	07.05.2003
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:

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 section 9.3.23.1 Setup (mobile terminated call establishment) the reference to the Redirecting party BCD number and Redirecting party sub-address are wrong. In section 10.5.4.21b Redirecting party BCD number references to "Table 10.81" and "Table 10.83" are made but these tables do not exist. In section 10.5.4.21c Redirecting party subaddress references a reference to "Table 10.84" is made, but this table does not exist. The numbering scheme used for the figures of the Redirecting party BCD number and Redirecting party subaddress is not aligned with the rest of the specification. In K4 the reference to the Redirecting party BCD number and Redirecting party sub-address are wrong.
Summary of change:	⌘	The wrong references are corrected.
Consequences if not approved:	⌘	Inconsistent specification.

Clauses affected:	⌘	9.3.23.1; 10.5.4.21b; 10.5.4.21c ; K.4

Other specs affected: ⌘

Y	N	
	X	Other core specifications
	X	Test specifications
	X	O&M Specifications

⌘

Other comments: ⌘

9.3.23 Setup

9.3.23.1 Setup (mobile terminated call establishment)

This message is sent by the network to the mobile station to initiate a mobile terminated call establishment.

See table 9.70/3GPP TS 24.008.

Message type: SETUP

Significance: global

Direction: network to mobile station

Table 9.70/3GPP TS 24.008: SETUP message content (network to mobile station direction)

IEI	Information element	Type/Reference	Presence	Format	Length
	Call control Protocol discriminator	Protocol discriminator 10.2	M	V	1/2
	Transaction identifier	Transaction identifier 10.3.2	M	V	1/2
	Setup Message type	Message type 10.4	M	V	1
D-	BC repeat indicator	Repeat indicator 10.5.4.22	C	TV	1
04	Bearer capability 1	Bearer capability 10.5.4.5	O	TLV	3-16
04	Bearer capability 2	Bearer capability 10.5.4.5	O	TLV	3-16
1C	Facility	Facility 10.5.4.15	O	TLV	2-?
1E	Progress indicator	Progress indicator 10.5.4.21	O	TLV	4
34	Signal	Signal 10.5.4.23	O	TV	2
5C	Calling party BCD Number	Calling party BCD num. 10.5.4.9	O	TLV	3-14
5D	Calling party sub-Address	Calling party subaddr. 10.5.4.10	O	TLV	2-23
5E	Called party BCD Number	Called party BCD num. 10.5.4.7	O	TLV	3-19
6D	Called party sub-Address	Called party subaddr. 10.5.4.8	O	TLV	2-23
74	Redirecting party BCD number	Redirecting party BCD num. 10.5.4.~~21a~~21b	O	TLV	3-19
75	Redirecting party sub-address	Redirecting party subaddress. 10.5.4.~~21b~~21c	O	TLV	2-23
D-	LLC repeat indicator	Repeat indicator 10.5.4.22	O	TV	1
7C	Low layer Compatibility I	Low layer comp. 10.5.4.18	O	TLV	2-18
7C	Low layer Compatibility II	Low layer comp. 10.5.4.18	C	TLV	2-18
D-	HLC repeat indicator	Repeat indicator 10.5.4.22	O	TV	1
7D	High layer Compatibility i	High layer comp. 10.5.4.16	O	TLV	2-5
7D	High layer Compatibility ii	High layer comp. 10.5.4.16	C	TLV	2-5
7E	User-user	User-user 10.5.4.25	O	TLV	3-35
8-	Priority	Priority Level 10.5.1.11	O	TV	1
19	Alert	Alerting Pattern 10.5.4.26	O	TLV	3
2F	Network Call Control Capabilities	Network Call Control cap. 10.5.4.29	O	TLV	3
3A	Cause of No CLI	Cause of No CLI 10.5.4.30	O	TLV	3
41	Backup bearer capability	Backup bearer capability 10.5.4.4a	O	TLV	3-15

9.3.23.1.1 BC repeat indicator

The *BC repeat indicator* information element is included if and only if *bearer capability* 1 information element and *bearer capability 2* IE are both present in the message.

9.3.23.1.2 Bearer capability 1 and bearer capability 2

The *bearer capability 1* information element may be omitted in the case where the mobile subscriber is allocated only one directory number for all services (ref.: 3GPP TS 29.007 [38]). The *bearer capability 2* IE is missing at least if the *bearer capability 1* IE is missing.

If the MSC wishes to indicate capability for an altenative call mode, which can be entered through fallback, this is indicated by adding a *bearer capability information ele*ment (bearer capability) 2 element (see subclause 5.3.6).

9.3.23.1.3 Facility

This information element may be included for functional operation of supplementary services.

9.3.23.1.4 Progress indicator

This information element is included by the network

- in order to pass information about the call in progress e.g. in the event of interworking and/or
- to make the MS attach the user connection for speech.

9.3.23.1.4a Called party BCD number

For all bands except for PCS1900, the maximum length of this IE sent by the network shall be 13 octets

9.3.23.1.5 Called party subaddress

Included in the Network-to-mobile station direction if the calling user includes a *called party subaddress* information element in the SETUP message.

9.3.23.1.6 LLC repeat indicator

The *LLC repeat indicator* information element is included if and only if both following conditions hold:

- The *BC repeat indicator* IE is contained in the message.
- The *low layer compatibility I* IE is contained in the message.

If included, the *LLC repeat indicator* shall specify the same repeat indication as the *BC repeat indicator* IE.

9.3.23.1.7 Low layer compatibility I

Included in the network-to-mobile station direction if the calling user specified a low layer compatibility.

9.3.23.1.8 Low layer compatibility II

Included if and only if the *LLC repeat indicator* information element is contained in the message.

9.3.23.1.9 HLC repeat indicator

The *HLC repeat indicator* information element is included if and only both following conditions hold:

- The *BC repeat indicator* IE is contained in the message.
- The *high layer compatibility i* IE is contained in the message.

If included, the *HLC repeat indicator* shall specify the same repeat indication as the *BC repeat indicator* IE.

9.3.23.1.10 High layer compatibility i

Included in the network-to-mobile station direction if the calling user specified a high layer compatibility.

9.3.23.1.11 High layer compatibility ii

Included if and only if the *HLC repeat indicator* information element is contained in the message.

9.3.23.1.12 User-user

May be included in the network to called mobile station direction when the calling remote user included a user-user information element in the SETUP message.

9.3.23.1.13 Redirecting party BCD number

May be included in the network to called mobile station direction when the call has been redirected.

9.3.23.1.14 Redirecting party subaddress

May be included in the network to called mobile station direction when the calling remote user included a called party subaddress in the SETUP message and the call has been redirected

9.3.23.1.15 Priority

May be included by the network to indicate the priority of the incoming call if eMLPP is used.

9.3.23.1.16 Alert $(Network Indication of Alerting in the MS)$

May be included by the network to give some indication about alerting (category or level). If supported in the MS, this optional indication is to be used by the MS as specified in 3GPP TS 22.101 [8].

9.3.23.1.17 Network Call Control Capabilities

This information shall be included by the network to indicate its call control capabilities if the network supports multicall.and there are no other ongoing calls to the MS.

9.3.23.1.18 Cause of No CLI

This IE may be included by the network as defined by 3GPP TS 24.081 [25].

When both Calling Party BCD number IE and Cause of No CLI IE are included in SETUP message then the Cause of No CLI IE provides additional information on why the number digits are not present.

9.3.23.1.19 Backup bearer capability

The *backup bearer capability* IE may be included by the network only if there are no *bearer capability* IEs contained in the message.

NOTE: The MSC may use the *backup bearer capability* IE if it is not able to provide a complete *bearer capability* IE.

10.5.4.21b Redirecting party BCD number

The purpose of the redirecting party BCD number information element is to identify the redirecting party.

The redirecting party BCD number information element is coded as shown in figure 10.5.108a/3GPP TS 24.008~~88a~~.

The redirecting party BCD number is a type 4 information element. In the network to mobile station direction it has a minimum length of 3 octets and a maximum length of 19 octets.

8	7	6	5	4	3	2	1	
	Redirecting party BCD number IEI							octet 1
Length of redirecting party BCD number contents								octet 2
0/1 ext	type of number			Numbering plan identification				octet 3 (note 1)
1 ext	presentat. indicator		0	0 spare		0	Screening indicator	octet 3a* (note 1)
Number digit 2				Number digit 1				octet 4* (note 1)
Number digit 4				Number digit 3				octet 5* (note 1)
								:
Note 2)								:

Figure 10.5.108a~~88a~~/3GPP TS 24.008
***Redirecting party BCD number* information element**

NOTE 1: The contents of octets 3, 4, etc. are coded as shown in table 10.5.118/3GPP TS 24.008~~Table 10.81~~. The coding of octet 3a is defined in table 10.5.120/3GPP TS 24.008~~Table 10.83~~.

NOTE 2: If the redirecting party BCD number contains an odd number of digits, bits 5 to 8 of the last octet shall be filled with an end mark coded as "1111".

10.5.4.21c Redirecting party subaddress

The purpose of the Redirecting party subaddress is to identify a subaddress associated with the redirecting party. For the definition of a subaddress see Rec. ITU-T I.330.

The Redirecting party subaddress information element is coded as shown in figure 10.5.108b/3GPP TS 24.008~~88b~~ and table 10.5.121/3GPP TS 24.008~~table 10.84~~.

The Redirecting party subaddress is a type 4 information element with a minimum length of 2 octets and a maximum length of 23 octets.

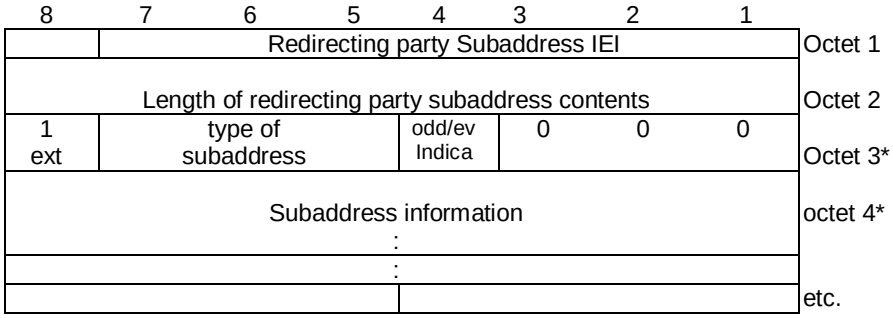

Figure 10.5.108b~~88b~~/3GPP TS 24.008
***Redirecting party subaddress* information element**

K.4 Call control information elements.

For the call control information elements listed below, the default coding of the information element identifiers is defined in table K.4/3GPP TS 24.008.

Table K.4/3GPP TS 24.008: Default information element identifier coding for call control information elements

									Reference clause
8	**7**	**6**	**5**	**4**	**3**	**2**	**1**		
1	:	:	:	-	-	-	-	Type 1 info elements	
	0	0	1	-	-	-	-	Shift	10.5.4.2 and .3
	0	1	1	-	-	-	-	Note	
	1	0	1	-	-	-	-	Repeat indicator	10.5.4.22
1	0	1	0	:	:	:	:	Type 2 information elements	
				0	0	0	0	More data	10.5.4.19
				0	0	0	1	CLIR Suppression	10.5.4.11a
				0	0	1	0	CLIR Invocation	10.5.4.11b
				0	0	1	1	Reverse call setup direction	10.5.4.22a
0	:	:	:	:	:	:	:	Type 3 & 4 info elements	
	0	0	0	0	1	0	0	Bearer capability	10.5.4.5
	0	0	0	1	0	0	0	Cause	10.5.4.11
	0	0	1	0	1	0	0	Note	
	0	0	1	0	1	0	1	Call Control Capabilities	10.5.4.5a
	0	0	1	1	1	0	0	Facility	10.5.4.15
	0	0	1	1	1	1	0	Progress indicator	10.5.4.21
	0	1	0	0	1	0	0	Auxiliary states	10.5.4.4
	0	1	0	0	1	1	1	Note	
	0	1	0	1	1	0	0	Keypad facility	10.5.4.17
	0	1	1	0	1	0	0	Signal	10.5.4.23
	1	0	0	1	1	0	0	Connected number	10.5.4.13
	1	0	0	1	1	0	1	Connected subaddress	10.5.4.14
	1	0	1	1	1	0	0	Calling party BCD number	10.5.4.9
	1	0	1	1	1	0	1	Calling party subaddress	10.5.4.10
	1	0	1	1	1	1	0	Called party BCD number	10.5.4.7
	1	1	0	1	1	0	1	Called party subaddress	10.5.4.8
	1	1	1	0	1	0	0	Redirecting Party BCD	10.5.4.21b~~a~~
	1	1	1	1	1	0	1	Redirecting Party subaddress	10.5.4.21c~~b~~
	1	1	1	1	1	0	0	Low layer compatib.	10.5.4.18
	1	1	1	1	1	0	1	High layer compatib.	10.5.4.16
	1	1	1	1	1	1	0	User-user	10.5.4.25
	1	1	1	1	1	1	1	SS version indicator	10.5.4.24

NOTE: These values were allocated but never used in earlier phases of the protocol.

***** next sections for information only *****

10.5.4.7 Called party BCD number

The purpose of the called party BCD number information element is to identify the called party.

The called party BCD number information element is coded as shown in figure 10.5.91/3GPP TS 24.008 and table 10.5.118/3GPP TS 24.008.

The called party BCD number is a type 4 information element with a minimum length of 3 octets and a maximum length of 43 octets. For PCS 1900 the maximum length is 19 octets.

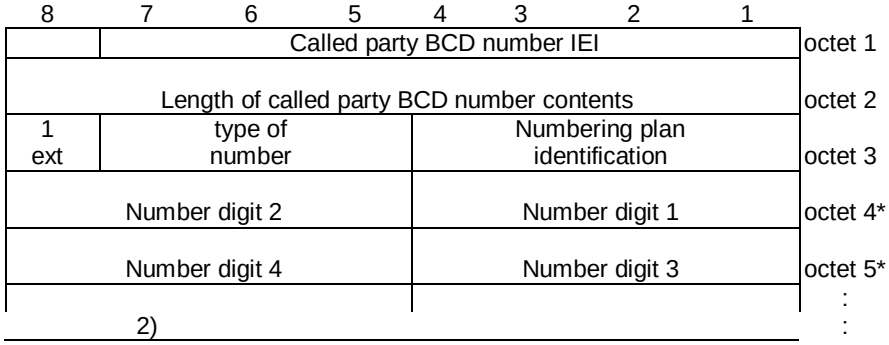

Figure 10.5.91/3GPP TS 24.008 Called party BCD number information element

NOTE 1: The number digit(s) in octet 4 precedes the digit(s) in octet 5 etc. The number digit which would be entered first is located in octet 4, bits 1 to 4.

NOTE 2: If the called party BCD number contains an odd number of digits, bits 5 to 8 of the last octet shall be filled with an end mark coded as "1111".

Since the information element must contain the complete called party BCD number there is no need for an additional complete indication.

Table 10.5.118/3GPP TS 24.008: Called party BCD number

Type of number (octet 3) (Note 1)			
Bits			
7	**6**	**5**	
0	0	0	unknown (Note 2)
0	0	1	international number (Note 3, Note 5)
0	1	0	national number (Note 3)
0	1	1	network specific number (Note 4)
1	0	0	dedicated access, short code
1	0	1	Reserved
1	1	0	Reserved
1	1	1	reserved for extension

NOTE 1: For the definition of "number" see ITU-T Recommendation I.330 and 3GPP TS 23.003 [10].

NOTE 2: The type of number "unknown" is used when the user or the network has no knowledge of the type of number, e.g. international number, national number, etc. In this case the number digits field is organized according to the network dialling plan, e.g. prefix or escape digits might be present.

NOTE 3: Prefix or escape digits shall not be included.

NOTE 4: The type of number "network specific number" is used to indicate administration/service number specific to the serving network, e.g. used to access an operator.

NOTE 5: The international format shall be accepted by the MSC when the call is destined to a destination in the same country as the MSC.

Table 10.5.118/3GPP TS 24.008: Called party BCD number (continued)

Numbering plan identification (octet 3)

Number plan (applies for type of number = 000, 001, 010 and 100)

Bits 4	3	2	1	
0	0	0	0	Unknown
0	0	0	1	ISDN/telephony numbering plan (Rec. E.164/E.163)
0	0	1	1	data numbering plan (Recommendation X.121)
0	1	0	0	telex numbering plan (Recommendation F.69)
1	0	0	0	national numbering plan
1	0	0	1	private numbering plan
1	0	1	1	reserved for CTS (see 3GPP TS 44.056 [91])
1	1	1	1	reserved for extension

All other values are reserved.

- When an MS is the recipient of number information from the network, any incompatibility between the number digits and the number plan identification shall be ignored and a STATUS message shall not be sent to the network.

- In the case of numbering plan "unknown", the number digits field is organized according to the network dialling plan; e.g. prefix or escape digits might be present.

Table 10.5.118/3GPP TS 24.008: Called party BCD number (continued)

Number digits (octets 4, etc.)

Bits 4	3	2	1	or 8	7	6	5	Number digit value
0	0	0	0					0
0	0	0	1					1
0	0	1	0					2
0	0	1	1					3
0	1	0	0					4
0	1	0	1					5
0	1	1	0					6
0	1	1	1					7
1	0	0	0					8
1	0	0	1					9
1	0	1	0					*
1	0	1	1					#
1	1	0	0					A
1	1	0	1					B
1	1	1	0					C
1	1	1	1					used as an endmark in the case of an odd number of number digits

10.5.4.8 Called party subaddress

The purpose of the Called party subaddress is to identify the subaddress of the called party of a call. For the definition of a subaddress see Rec. ITU-T I.330.

The Called party subaddress information element is coded as shown in figure 10.5.92/3GPP TS 24.008 and Table 10.5.119/3GPP TS 24.008.

The called party subaddress is a type 4 information element with a minimum length of 2 octets and a maximum length of 23 octets.

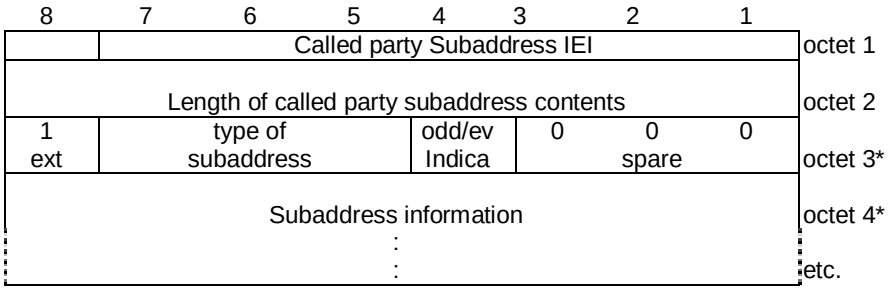

Figure 10.5.92/3GPP TS 24.008 Called party subaddress

Table 10.5.119/3GPP TS 24.008: Called party subaddress

Type of subaddress (octet 3)

Bits

7	**6**	**5**	
0	0	0	NSAP (X.213/ISO 8348 AD2)
0	1	0	User specified

All other values are reserved

Odd/even indicator (octet 3)

Bit

4	
0	even number of address signals
1	odd number of address signals

NOTE 1: The odd/even indicator is used when the type of subaddress is "user specified" and the coding is BCD.

Subaddress information (octet 4, etc...)

The NSAP X.213/ISO8348AD2 address shall be formatted as specified by octet 4 which contains the Authority and Format Identifier (AFI). The encoding is made according to the "preferred binary encoding" as defined in X.213/ISO8348AD2. For the definition of this type of subaddress, see Rec. ITU-T I.334.

A coding example is given in ANNEX A.

For User-specific subaddress, this field is encoded according to the user specification, subject to a maximum length of 20 octets.

NOTE 2: It is recommended that users apply NSAP subaddress type since this subaddress type allows the use of decimal, binary and IA5 characters in a standardised manner.

10.5.4.9 Calling party BCD number

The purpose of the calling party BCD number information element is to identify the origin of a call.

The calling party BCD number information element is coded as shown in figure 10.5.93/3GPP TS 24.008 and table 10.5.120/3GPP TS 24.008.

The calling party BCD number is a type 4 information element. In the network to mobile station direction it has a minimum length of 3 octets and a maximum length of 14 octets. (This information element is not used in the mobile station to network direction.).

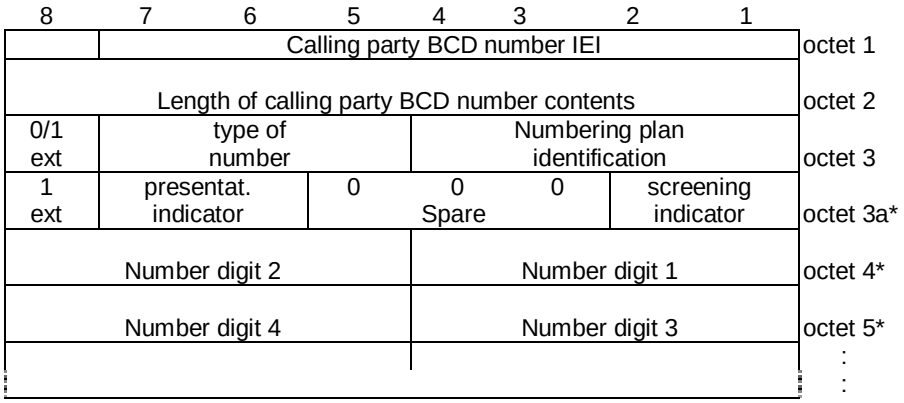

Figure 10.5.93/3GPP TS 24.008 Calling party BCD number information element

The contents of octets 3, 4, etc. are coded as shown in table 10.5.118. The coding of octet 3a is defined in table 10.5.120 below.

If the calling party BCD number contains an odd number of digits, bits 5 to 8 of the last octet shall be filled with an end mark coded as "1111".

Table 10.5.120/3GPP TS 24.008: Calling party BCD number

Presentation indicator (octet 3a)
Bits

7	**6**	
0	0	Presentation allowed
0	1	Presentation restricted
1	0	Number not available due to interworking
1	1	Reserved

If octet 3a is omitted the value "00 - Presentation allowed" is assumed.

Screening indicator (octet 3a)

Bits

2	**1**	
0	0	User-provided, not screened
0	1	User-provided, verified and passed
1	0	User-provided, verified and failed
1	1	Network provided

If octet 3a is omitted the value "0 0 - User provided, not screened" is assumed.

10.5.4.10 Calling party subaddress

The purpose of the Calling party subaddress is to identify a subaddress associated with the origin of a call. For the definition of a subaddress see Rec. ITU-T I.330.

The Calling party subaddress information element is coded as shown in figure 10.5.94/3GPP TS 24.008 and table 10.5.121/3GPP TS 24.008.

The calling party subaddress is a type 4 information element with a minimum length of 2 octets and a maximum length of 23 octets.

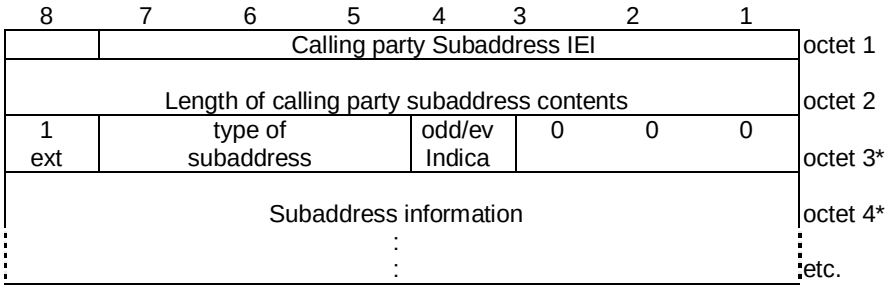

Figure 10.5.94/3GPP TS 24.008 Calling party subaddress

Table 10.5.121/3GPP TS 24.008: Calling party subaddress

Type of subaddress (octet 3)

Bits

7	**6**	**5**	
0	0	0	NSAP (X.213/ISO 8348 AD2)
0	1	0	User specified

All other values are reserved

Odd/even indicator (octet 3)

Bit

4	
0	even number of address signals
1	odd number of address signals

The odd/even indicator is used when the type of subaddress is "user specified" and the coding is BCD

Subaddress information (octet 4, etc...)

The NSAP X.213/ISO8348AD2 address shall be formatted as specified by octet 4 which contains the Authority and Format Identifier (AFI). The encoding is made according to the "preferred binary encoding" as defined in X.213/ISO8348AD2. For the definition of this type of this type of subaddress, see Rec. ITU-T I.332.

A coding example is given in annex A.

For User-specific subaddress, this field is encoded according to the user specification, subject to a maximum length of 20 octets.

NOTE: It is recommended that users apply NSAP subad dress type since this subaddress type allows the use of decimal, binary and IA5 characters in a standardised manner.