3GPP TSG CN Plenary Meeting #27 **NP-050135**
9th – 11th March 2005 Tokyo, JAPAN.

Source: TSG CN WG4

Title: Corrections on GPRS

Agenda item: 9.21

Document for: APPROVAL

Doc-2nd-Level	Spec	CR	Rev	Phase	Subject	Cat	Ver_C
N4-050429	29.060	528	1	Rel-6	Clarification to error handling of IEs of type TV	F	6.7.0

3GPP TSG-CN WG4 Meeting #26 **N4-050429**
Sydney, AUSTRALIA. 14th to 18th February 2005.

CR-Form-v7.1

CHANGE REQUEST

⌘ **29.060** **CR** **528** ⌘ **rev** **2** ⌘ Current version: **6.7.0** ⌘

*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:	⌘	Clarification to error handling of IEs of type TV
Source:	⌘	Vodafone
Work item code:	⌘	TEI6
Date:	⌘	17/02/2005
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:	⌘	To prevent a similar problem to the one discussed in N4-050039 from re-occurring. Currently, there are two types of error handling that can both apply; both of which conflict with one another and it is not clear which should prevail.
Summary of change:	⌘	Clarification is added to the handling of received IEs of type TV that are known but just not expected in the received message.
Consequences if not approved:	⌘	In the worse case, another future Denial of Service to the subscriber, similar to that discussed in N4-040039.

Clauses affected:	⌘	11.1.9, 11.1.11

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

Other comments: ⌘

How to create CRs using this form:
Comprehensive information and tips about how to create CRs can be found at http://www.3gpp.org/specs/CR.htm.
Below is a brief summary:

1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.

2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be

downloaded from the 3GPP server under ftp://ftp.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.

3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause containing the first piece of changed text. Delete those parts of the specification which are not relevant to the change request.

11 Error Handling

. . .

11.1 Protocol Errors

A protocol error is defined as a message with unknown, unforeseen or erroneous content. The term silently discarded used in the following subclauses means that the implementation shall discard the message without further processing and should log the event including the erroneous message and should include the error in a statistical counter.

An information element with 'Mandatory' in the 'Presence requirement' column of a message definition shall always be present in that message.

The conditions for a conditional information element define whether the information element is semantically:

- mandatorily present;
- optionally present;
- mandatorily absent.

An information element, which is semantically mandatorily present but is omitted from the message, is treated as missing data.

An information element, which is semantically mandatorily absent but is present in the message, is treated as unexpected data.

The Error Indication, Version Not Supported, RAN Information Relay, Supported Extension Headers Notification and the SGSN Context Acknowledge messages shall be considered as Responses for the purpose of this subclause.

The subclauses 11.1.1 to 11.1.13 shall be applied in decreasing priorities.

11.1.1 Different GTP Versions

If a receiving node receives a GTP message of an unsupported version, that node shall return a GTP Version Not Supported message indicating in the Version field of the GTP header the latest GTP version that that node supports. The received GTP-PDU shall then be discarded.

A GTP version '0' only GSN may not be listening on port 2123 and as such it will not be able to send back a Version Not Supported message to a peer trying to establish a dialogue with it using GTP-C. As such, a GSN supporting both version '1' and version '0' shall fall back to version '0' if the attempt to contact a peer using version '1' fails.

It is an implementation option keeping a shortlist of recently contacted version '0' only GSNs, as well of the version supported by those nodes sending back a Version Not Supported message.

11.1.2 GTP Message Too Short

When a GTP message is received, and is too short to contain the GTP header for the GTP version that the sender claims to use, the GTP-PDU message shall be silently discarded.

11.1.3 Unknown GTP Signalling Message

When a message using a Message Type value defining an Unknown GTP signalling message is received, it shall be silently discarded.

11.1.4 Unexpected GTP Signalling Message

When an unexpected GTP control plane message is received, e.g. a Response message for which there is no corresponding outstanding Request, or a GTP control plane message a GSN is not expected to handle (such as a PDU Notification Request received by a GGSN),, it shall be silently discarded.

11.1.5 Missing Mandatorily Present Information Element

The receiver of a GTP signalling Request message with a missing mandatorily present information element shall discard the request, should log the error, and shall send a Response with Cause set to 'Mandatory IE missing'. The receiver of a Response with a missing mandatory information element shall notify the upper layer and should log the error.

11.1.6 Invalid Length

In a received GTP signalling message Request, a mandatory TLV format information element may have a Length different from the Length defined in the version that this message claims to use. In this case, this information element shall be discarded, the error should be logged, and a Response shall be sent with Cause set to 'Mandatory IE incorrect'.

In a received GTP signalling message Response, if a mandatory TLV format information element has a Length different from the Length defined in the version that this message claims to use, then the requesting entity shall treat the GTP signalling procedure as having failed.

11.1.7 Invalid Mandatory Information Element

The receiver of a GTP signalling message Request including a mandatory information element with a Value that is not in the range defined for this information element value shall discard the request, should log the error, and shall send a response with Cause set to 'Mandatory IE incorrect'.

The receiver of a GTP signalling message Response including a mandatory information element with a Value that is not in the range defined for this information element shall notify the upper layer that a message with this sequence number has been received and should log the error.

If a GSN receives an information element with a value which is shown as reserved, it shall treat that information element as not being in the range defined for the information element.

NOTE: The receiver does not check the content of an information element field that is defined as 'spare'.

11.1.8 Invalid Optional Information Element

The receiver of a GTP signalling message including an optional information element with a Value that is not in the range defined for this information element value shall discard this IE, should log the error, and shall treat the rest of the message as if this IE was absent.

If a GSN receives an information element with a value which is shown as reserved, it shall treat that information element as not being in the range defined for the information element.

NOTE: The receiver does not check the content of an information element field that is defined as 'spare'.

11.1.9 Unknown Information Element

An information element with an unknown Type value shall be ignored by the receiver of the message. If this is a TLV element, this information element shall be skipped using its Length value. If this is an unknown TV element, the receiver shall discard the rest of the message. However, if the TV element is known but not expected, then the handling defined in section 11.1.11 shall apply.

If the receiving node cannot interpret the rest of the message because of the ignored information element, the receiving node shall discard the message and should log the error. If the message was a Request, it shall, in addition, return a response with Cause set to 'Invalid message format'.

11.1.10 Out of Sequence Information Elements

If two or more information elements are out of sequence in a message, the receiving node shall discard the message and should log the error. In addition, if the message was a Request, the receiving node shall return a Response with Cause set to 'Invalid message format'.

11.1.11 Unexpected Information Element

An information element with a Type value which is defined in ~~GTP~~ section 7.7 of the present specification but is not expected in the received GTP signalling message shall be ignored (skipped) and the rest of the message processed as if this information element was not present. For all information elements of type TV, a receiving entity shall be able to determine how long each IE is, even if that IE should never be received in any message by that particular network entity.