3GPP TSG_CN#7 **NP-000050**

ETSI SMG3 Plenary Meeting #7,

Madrid, Spain

13th – 15th March 2000

Agenda item: **5.3.3**

Source: **TSG_N WG3**

Title: **CRs to 3G Work Item UMTS**

Introduction:

This document contains **"2"** CRs on **Work Item UMTS,** that have been agreed by **TSG_N WG3,** and are forwarded to **TSG_N Plenary** meeting #7 for approval.

WG Tdoc	Spec	CR	Rev	Cat	Phase	Current V.	New V.	Subject
N3-000096	27.060	010		F	R99	3.3.0	3.4.0	Correction of the support for IPv6 for the MS.
N3-000067	29.061	011		F	R99	3.2.0	3.3.0	Correction for IPv6 support to the Gi reference point, CR to 29.061

3GPP TSG-N3/SMG3 WPD Meeting #8
Sophia Antipolis, France, 28 Feb- 03 Mar 2000

***Document* N3-000096**
e.g. for 3GPP use the format TP-99xxx
or for SMG, use the format P-99-xxx

CHANGE REQUEST

Please see embedded help file at the bottom of this page for instructions on how to fill in this form correctly.

27.060	CR	010	Current Version:	V 3.3.0

GSM (AA.BB) or 3G (AA.BBB) specification number ↑ *↑ CR number as allocated by MCC support team*

For submission to: CN#7	for approval	X	strategic		(for SMG use only)
list expected approval meeting # here ↑	for information		non-strategic		

Form: CR cover sheet, version 2 for 3GPP and SMG *The latest version of this form is available from: ftp://ftp.3gpp.org/Information/CR-Form-v2.doc*

Proposed change affects: (U)SIM [ ] ME [ ] UTRAN / Radio [ ] Core Network [X]
(at least one should be marked with an X)

Source: TSG_CN WG3 **Date:** 05.2.2000

Subject: Correction of the support for IPv6 for the MS.

Work item: UMTS

Category: *(only one category shall be marked with an X)*

F	Correction	X	**Release:**	Phase 2
A	Corresponds to a correction in an earlier release			Release 96
B	Addition of feature			Release 97
C	Functional modification of feature			Release 98
D	Editorial modification			Release 99 X
				Release 00

Reason for change: This CR aligns the 27.060 with the changes made to 23.060 to allow the IPv6 support work correctly with GPRS/UMTS.

Clauses affected: 2, 9

Other specs affected:

Other 3G core specifications	[ ]	→ List of CRs:
Other GSM core specifications	[ ]	→ List of CRs:
MS test specifications	[ ]	→ List of CRs:
BSS test specifications	[ ]	→ List of CRs:
O&M specifications	[ ]	→ List of CRs:

Other comments:

**************************************Next Change**************************************

2 References

[All references need to be checked once release 99 stabilizes.]

[34] IETF RFC 1661 (1994): “The Point-to-Point Protocol (PPP)” (STD 51).

[35] IETF RFC 1662 (1994): “PPP in HDLC-like framing” (STD 51).

[36] IETF RFC 1700 (1994): “Assigned Numbers” (STD 2).

[3]7 IETF RFC 1570 (1994):”PPP LCP Extensions“.

[38] IETF RFC 1989 (1996):”PPP Link Quality Monitoring“.

[39] IETF RFC 1332 (1992):”The PPP Internet Protocol Control Protocol (IPCP)“.

[40] IETF RFC 1877 (1995):”PPP IPCP Extensions for Name Server Addresses “.

[41] IETF RFC 2153 (1997):”PPP Vendor Extensions“.

[42] IETF RFC 1334 (1992):”PPP Authentication Protocols“.

[43] IETF RFC 1994 (1996):”PPP Challenge Handshake Authentication Protocol“.

[44] IETF RFC 2686 (1999):”The Multi-Class Extension to Multi-Link PPP”

[45] IETF RFC 1990 (1996):”The PPP Multilink Protocol (MP)“.

[46] IETF RFC 2472 (1998): ”IP Version 6 over PPP"

**************************************Next Change**************************************

9 IP Based Services

All protocols that are supported by the underlying IP protocol are applicable in the Packet Domain environment. However there may be some limitations due to the RF environment.

The IP protocol can be run over various underlying protocols as shown in the following figure.

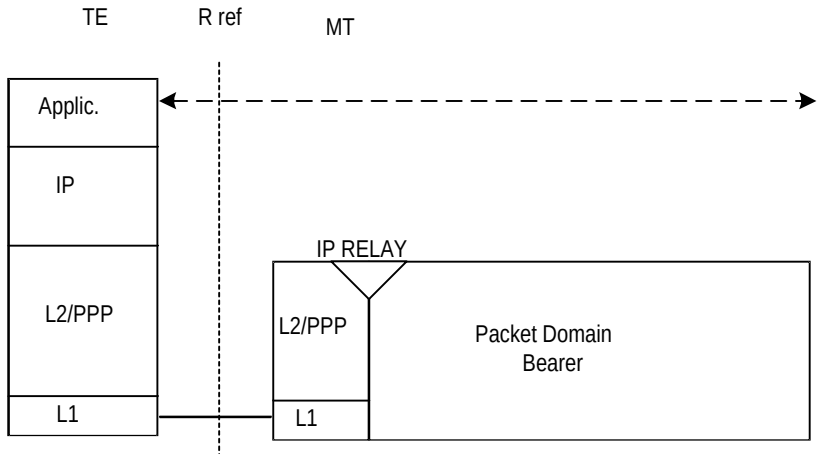

Figure 6: IP Based Services

PPP is a widely supported protocol in numerous operating systems and this alleviates the need for any Packet Domain specific protocol at the TE. PPP at the MT shall comply with the following specifications IETF STD 51 (RFC 1661, RFC 1662), RFC 1570, RFC 1989, ~~and~~ RFC 1332, and optionally RFC 2472 for IPv6. The Domain Name Server information shall be delivered as defined in RFC 1877. The delivery of vendor-specific packets and options shall conform to RFC 2153.

As an alternative to PPP, an L2 protocol can be used which is defined as a manufacturer's operating system dependent protocol capable of carrying IP frames over the R reference point. An example for such an L2 protocol is the Multi-Class Multi-Link (MCML) PPP. The MCML is defined in RFC 2686 and is based on Multi-Link (MP) PPP which is defined in RFC 1990.

9.1 Example mapping of functions between the R reference point and the Packet Domain bearer for IP over PPP

The following example illustrates the case when the IP over PPP functionality is used in the MT. The example does not include all the details of PPP, but only describes the logical operation of PPP connection establishment, host authentication and IP configuration.

Each interface at the R reference point can support only one PPP connection and each PPP connection can support only one IP session. Therefore, in PPP mode only one IP PDP context can be activated per interface at the R reference point. However, it is possible for a PCMCIA card (or other multiplexed interface) to support multiple virtual interfaces (communications ports) at the R reference point. Multiple PPP connections and IP contexts are possible in this case.

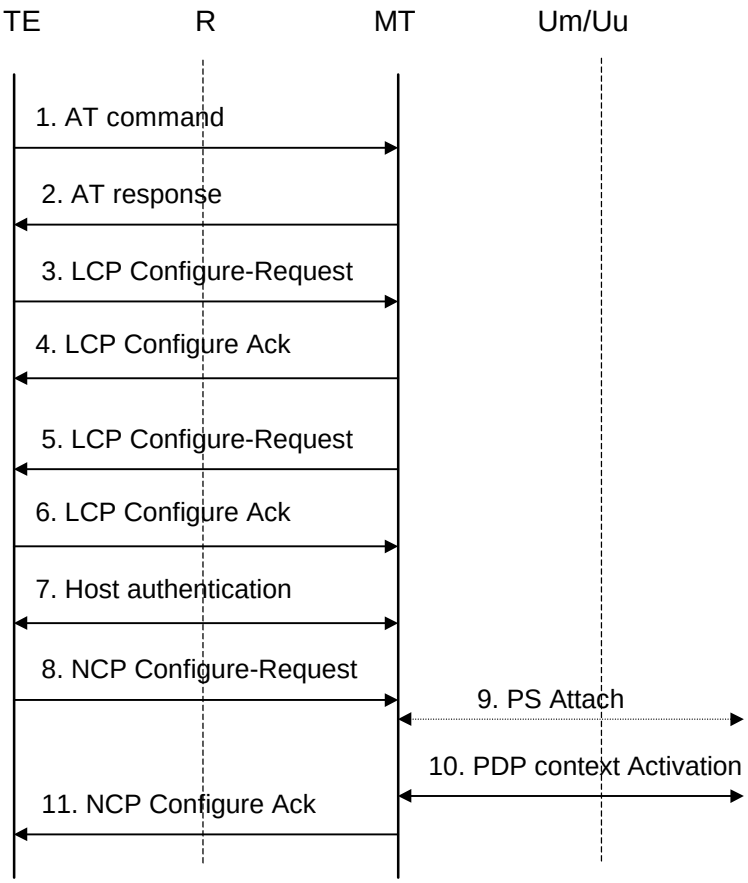

Figure 7: IP Over PPP Based Service

1) The TE issues AT commands to set up parameters and enter PPP mode (refer to subclause on AT commands for further details).

2) The MT sends AT responses to the TE.

3) The PPP protocol in the TE sends a LCP Configure-Request. This command is to establish a PPP link between the TE and the MT.

4) The MT returns LCP Configure-Ack to the TE to confirm that the PPP link has been established. The MT might previously have sent a LCP Configure-Nak in order to reject some options proposed by the TE. This in turn might have triggered a retransmission of the LCP Configure-Request with different options.

5) The PPP protocol in the MT sends a LCP Configure-Request in order to negotiate for the authentication protocol used for authentication of the host TE towards the MT. The MT shall initially negotiate for CHAP, and if this is unsuccessful, for PAP.

6) The TE returns a LCP Configure-Ack to the MT to confirm the use of the specified authentication protocol. The MT might previously have sent a LCP Configure-Nak in order to reject the protocol proposed by the TE. This in turn might have triggered a retransmission of the LCP Configure-Request with different options.

7) If the negotiated authentication protocol is either of CHAP or PAP, the TE authenticates itself towards the MT by means of that protocol. The MT stores the necessary authentication data and sends a locally generated positive acknowledgement of the authentication to the TE. If none of the protocols is supported by the host TE no authentication shall be performed. Refer to 3G TS 29.061 for further details on the authentication.

8) The PPP protocol in the TE sends to the MT a NCP Configure-Request. This command activates the IP protocol.

9) If the MS is not yet PS attached, the MT performs the PS Attach procedure as described in 3G TS 23.060.

10) The MT performs a PDP Context Activation as described in GSM 03.60. IP configuration parameters may be carried between the MT and the network in the Protocol Configuration Options IE in PDP Context Activation messages. The Protocol Configuration Options IE sent to the network may contain zero or one NCP Configure-Request packet (in addition to any LCP and authentication packets). The Protocol Configuration Options IE

received from the network may contain zero or one NCP Configure-Ack, zero or one Configure-Nak and/or zero or one Configure-Reject packets (in addition to any LCP and authentication packets).

11) Based on the information received in the Protocol Configuration Options IE, the MT acknowledges to the PPP protocol in the TE that the IP protocol is now activated by sending a NCP Configure-Ack command. Before sending a NCP Configure-Ack, the MT might previously have sent a NCP Configure-Nak and/or Configure-Reject in order to reject some IP parameters proposed by the TE. This in turn might have triggered a retransmission of the NCP Configure-Request with different parameter values. The decision to reject a specific parameter or parameter value may be based on the information received from the network in the Protocol Configuration Options IE. NCP Configure-Ack may also carry IP protocol related parameters such as dynamic IP address to the TE. The MT shall also pass name server information to the TE if the TE has requested for it and if this information is provided by the GGSN. Other packet types and options may optionally be delivered. The MT may choose to immediately deactivate the PDP context due to the information received from the network in the Protocol Configurations Options IE.

9.2 Example mapping of functions between the R reference point and the Packet Domain bearer for IP over MCML PPP

When MCML is used instead of standard PPP at the R-reference point, it is possible to support multiple IP sessions on one MCML connection. This is achieved by using an additional MP header after the standard PPP header. MCML provides two different MP headers, a 2-byte header to have four IP sessions and a 4-byte header to have sixteen IP sessions multiplexed over the MCML connection.

Since both MP and MCML closely follow the PPP connection establishment and negotiation model described in section 9.1, it is not replicated in this section. The major difference is the additional negotiation capabilities used during the LCP configuration negotiation.

3GPP TSG-N3/SMG3 WPD Meeting #8
Sophia Antipolis, France, 28 Feb- 03 Mar 2000

Document N3-000067
e.g. for 3GPP use the format TP-99xxx
or for SMG, use the format P-99-xxx

CHANGE REQUEST

Please see embedded help file at the bottom of this page for instructions on how to fill in this form correctly.

29.061	CR	011	Current Version:	3.2.0

GSM (AA.BB) or 3G (AA.BBB) specification number ↑ *↑ CR number as allocated by MCC support team*

For submission to:	CN#7	for approval	X	strategic		(for SMG use only)
list expected approval meeting # here ↑		for information		non-strategic		

Form: CR cover sheet, version 2 for 3GPP and SMG *The latest version of this form is available from: ftp://ftp.3gpp.org/Information/CR-Form-v2.doc*

Proposed change affects: (U)SIM [ ] ME [ ] UTRAN / Radio [ ] Core Network [X]
(at least one should be marked with an X)

Source: TSG_CN WG3 **Date:** 23.11.1999

Subject: Correction for IPv6 support to the Gi reference point

Work item: UMTS

Category: *(only one category shall be marked with an X)*

F	Correction	X	**Release:**	Phase 2	
A	Corresponds to a correction in an earlier release			Release 96	
B	Addition of feature			Release 97	
C	Functional modification of feature			Release 98	
D	Editorial modification			Release 99	X
				Release 00	

Reason for change: The reason is to correct the support for IPv6 and to align 29.061 with the modifications done to 23.060.

Clauses affected: 2, 11.2.1.1

Other specs affected:

Other 3G core specifications	[ ]	→ List of CRs:
Other GSM core specifications	[ ]	→ List of CRs:
MS test specifications	[ ]	→ List of CRs:
BSS test specifications	[ ]	→ List of CRs:
O&M specifications	[ ]	→ List of CRs:

Other comments:

2 References

(References to be cleaned up when release 99 is stable).

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.
- A non-specific reference to an ETS shall also be taken to refer to later versions published as an EN with the same number.

[26] IETF RFC 2131 (1997): “Dynamic Host Configuration Protocol”.

[27] IETF RFC 1542 (1993): “Clarification and Extensions for the Bootstrap Protocol”.

[X] IETF RFC2373 (1998): "IP version 6 Addressing Architecture"

[Y] IETF RFC 2462 (1998): "IPv6 Stateless Address Autoconfiguration"

******************************Next Change******************************

11.2.1 Access to Internet, Intranet or ISP through Packet Domain

The access to Internet, Intranet or ISP may involve specific functions such as : user authentication, user's authorization, end to end encryption between MS and Intranet/ISP, allocation of a dynamic address belonging to the PLMN/Intranet/ISP addressing space, etc.

For this purpose the Packet Domain may offer:

- either direct transparent access to the Internet.
- or a non transparent access to the Intranet/ISP. In this case the Packet Domain, i.e. the GGSN, takes part in the functions listed above.

11.2.1.1 Transparent access to the Internet

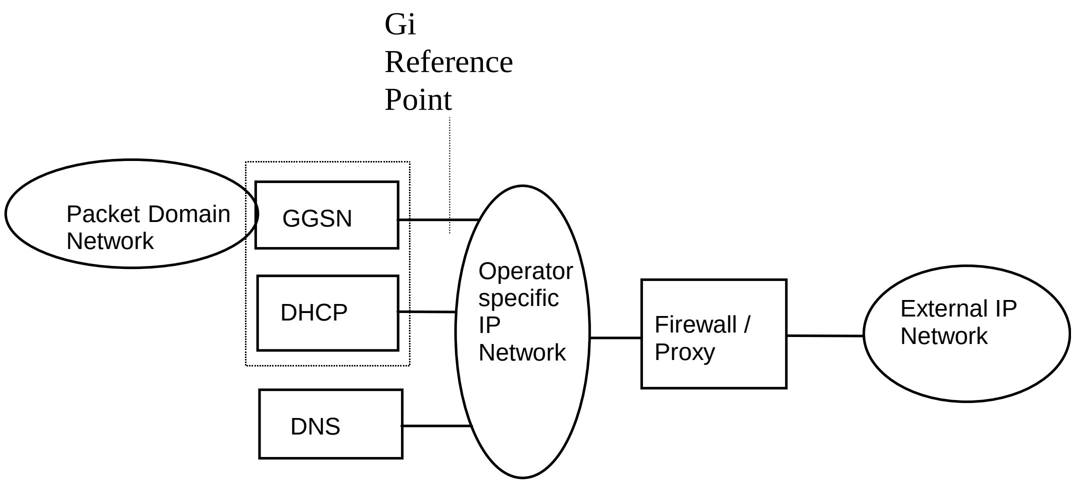

Figure 9: Example of the PDN Interworking Model, transparent case

In this case (see Figure 9),

- The MS is given an address belonging to the operator addressing space. The address is given either at subscription in which case it is a static address or at PDP context activation in which case it is a dynamic address. This address is used for packet forwarding between the Internet and the GGSN and within the GGSN. In IPv6, the address given is the link-local address. Thus, for the IPv6 it is not necessary to use a DHCP implementation for the address allocation, but any unique identifier for the MS in the GGSN is sufficient.
- The MS need not send any authentication request at PDP context activation and the GGSN need not take any part in the user authentication/authorization process.

The transparent case provides at least a basic ISP service. As a consequence of this it may therefore provide a bearer service for a tunnel to a private Intranet.

NB The remainder of this section deals with this specific case.

- The user level configuration may be carried out between the TE and the intranet, the Packet Domain network is transparent to this procedure.

The used protocol stack is depicted in Figure 10.

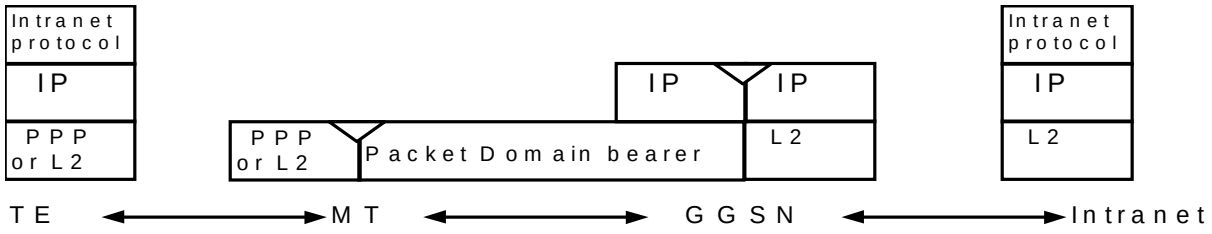

Figure 10: Transparent access to an Intranet

The communication between the PLMN and the Intranet may be performed over any network, even an insecure network e.g. the Internet. There is no specific security protocol between GGSN and the Intranet because security is ensured on an end to end basis between MS and the intranet by the «Intranet protocol».

User authentication and encryption of user data are done within the «Intranet protocol» if either of them is needed. This «Intranet protocol» may also carry private (IP) addresses belonging to the address space of the Intranet.

An example of an «Intranet protocol» is IPsec (see RFC 1825). If IPsec is used for this purpose then IPsec authentication header or security header may be used for user (data) authentication and for the confidentiality of user data (see RFC 1826 and RFC 1827). In this case private IP tunnelling within public IP takes place.