**3GPP TSG-CT WG3 Meeting #116e C3-213210**

**E-Meeting, 19th – 28th May 2021 (Revision of C3-212488)**

|  |
| --- |
| *CR-Form-v12.1* |
| **CHANGE REQUEST** |
|  |
|  | **29.061** | **CR** | **0536** | **rev** | **2** | **Current version:** | **17.2.0** |  |
|  |
| *For* [***HE******LP***](http://www.3gpp.org/3G_Specs/CRs.htm#_blank)*on using this form: comprehensive instructions can be found at* [*http://www.3gpp.org/Change-Requests*](http://www.3gpp.org/Change-Requests)*.* |
|  |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| ***Proposed change affects:*** | UICC apps |  | ME |  | Radio Access Network |  | Core Network | **X** |

|  |
| --- |
|  |
| ***Title:***  | Updates to support L2TP for CUPS |
|  |  |
| ***Source to WG:*** | Ericsson |
| ***Source to TSG:*** | CT3 |
|  |  |
| ***Work item code:*** | BEPoP |  | ***Date:*** | 2021-05-12 |
|  |  |  |  |  |
| ***Category:*** | **B** |  | ***Release:*** |  Rel-17 |
|  | *Use one of the following categories:****F*** *(correction)****A*** *(mirror corresponding to a change in an earlier release)****B*** *(addition of feature),* ***C*** *(functional modification of feature)****D*** *(editorial modification)*Detailed explanations of the above categories canbe found in 3GPP [TR 21.900](http://www.3gpp.org/ftp/Specs/html-info/21900.htm). | *Use one of the following releases:Rel-8 (Release 8)Rel-9 (Release 9)Rel-10 (Release 10)Rel-11 (Release 11)…Rel-15 (Release 15)Rel-16 (Release 16)Rel-17 (Release 17)Rel-18 (Release 18)* |
|  |  |
| ***Reason for change:*** | SA2 LS reply C3-212528/S2-2103232 supports the introduction of PFCP protocol extensions in Rel-17 to support L2TP tunnelling over N6/SGi for 5GS and EPS and assumes that the impact to interactions between PGW and the RADIUS/Diameter Server SGi will be fully developed by CT3, in line with the functionality provided for 5GS, attached with the approved TS 23.501, 23.502 and 23.214 CRs.TR 29.820 Solution#8 cluase 6.8.4 End to End Signalling Flow can also be referred and to be further detailed in this specificiation to support L2TP for CUPS across SGi interface.So before preparing the detail attributes/AVPs for RADIUS/Diameter messages, the general support L2TP tunneling for CUPS across SGi interface is needed in this CR. |
|  |  |
| ***Summary of change:*** | Adding L2TP RFC 2661 and general description including procedures supporting L2TP for CUPS across SGi interface. |
|  |  |
| ***Consequences if not approved:*** | Missing the general description on L2TP support for CUPS, cannot further implement the RADIU/Diameter message supporting L2TP in this specification, and cannot be referred by TS 29.561. |
|  |  |
| ***Clauses affected:*** | 2, 3.2, 11.2.1.y(new) |
|  |  |
|  | **Y** | **N** |  |  |
| ***Other specs*** | **X** |  |  Other core specifications  | TS 23.501 CR 2691TS 23.502 CR 2602TS 23.214 CR 0076 |
| ***affected:*** |  | **X** |  Test specifications |  |
| ***(show related CRs)*** |  | **X** |  O&M Specifications |  |
|  |  |
| ***Other comments:*** |  |
|  |  |
| ***This CR's revision history:*** |  |

**Additional discussion(if needed):**

**Proposed changes:**

\*\*\* 1st 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] Void.

[2] 3GPP TS 22.060: "General Packet Radio Service (GPRS); Service Description; Stage 1".

[3] 3GPP TS 23.060: "General Packet Radio Service (GPRS); Service Description; Stage 2".

[4] Void.

[5] Void.

[6] Void.

[7] Void.

[8] Void.

[9] Void.

[10] 3GPP TS 27.060: "Packet Domain; Mobile Station (MS) supporting Packet Switched services".

[11] ITU-T Recommendation E.164: "The international public telecommunication numbering plan".

[12] Void.

[13] Void.

[14] Void.

[15] IETF RFC 768 (1980): "User Datagram Protocol" (STD 6).

[16] IETF RFC 791 (1981): "Internet Protocol" (STD 5).

[17] IETF RFC 792 (1981): "Internet Control Message Protocol" (STD 5).

[18] IETF RFC 793 (1981): "Transmission Control Protocol" (STD 7).

[19] IETF RFC 1034 (1987): "Domain names – concepts and facilities" (STD 7).

[20] Void.

[21a] IETF RFC 1661 (1994): "The Point-to-Point Protocol (PPP)" (STD 51).

[21b] IETF RFC 1662 (1994): "PPP in HDLC-like Framing".

[22] IETF RFC 1700 (1994): "Assigned Numbers" (STD 2).

[23] 3GPP TS 44.008: "Mobile radio interface layer 3 specification; Core Network protocols; Stage 3".

[24] 3GPP TS 29.060: "General Packet Radio Service (GPRS); GPRS Tunnelling Protocol (GTP) across the Gn and Gp interface".

[25] IETF RFC 2794 (2000): "Mobile IP Network Address Identifier Extension for IPv4", P. Calhoun, C. Perkins.

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

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

[28] Void

[29] Void.

[30] IETF RFC 3344 (2002): "IP Mobility Support", C. Perkins.

[31] IETF RFC 2486 (1999): "The Network Access Identifier", B. Aboba and M. Beadles.

[32] Void.

[33] Void.

[34] Void.

[35] Void.

[36] Void.

[37] IETF RFC 2290 (1998): "Mobile-IPv4 Configuration Option for PPP IPCP", J. Solomon, S. Glass.

[38] IETF RFC 2865 (2000): "Remote Authentication Dial In User Service (RADIUS)", C. Rigney, S. Willens, A. Rubens, W. Simpson.

[39] IETF RFC 2866 (2000): "RADIUS Accounting", C. Rigney, Livingston.

[40] 3GPP TS 23.003: "Numbering, addressing and identification".

[41] IETF RFC 3576 (2003): "Dynamic Authorization Extensions to Remote Authentication Dial In User Service (RADIUS)", M.Chiba, M.Eklund, D.Mitton, B.Aboba.

[42] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

[43] Void.

[44] Void.

[45] IETF RFC 3118 (2001): "Authentication for DHCP Messages", R. Droms, W. Arbaugh.

[46] IETF RFC 3315 (2003) "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)", R. Droms, J. Bound, B. Volz, T. Lemon, C. Perkins, M. Carney.

[47] 3GPP TS 24.229: "IP Multimedia Call Control Protocol based on SIP and SDP".

[48] IETF RFC 2710 (1999): "Multicast Listener Discovery (MLD) for IPv6", S. Deering, W. Fenner, B. Haberman.

[49] IETF RFC 2460 (1998): "Internet Protocol, Version 6 (IPv6) Specification", S.Deering, R.Hinden.

[50] IETF RFC 3162 (2001): "RADIUS and IPv6", B. Adoba, G. Zorn, D. Mitton.

[51] IETF RFC 2548 (1999): "Microsoft Vendor-specific RADIUS Attributes", G.Zorn.

[52] 3GPP TS 23.228: "IP Multimedia Subsystem (IMS); Stage 2".

[53] Void

[54] 3GPP TS 24.008: "Mobile radio interface layer 3 specification; Core Network protocols; Stage 3".

[55] Void.

[56] Void

[57] Void.

[58] IETF RFC 1035 (1987): "Domain names – implementation and specification" (STD 13).

[59] Void.

[60] IETF RFC 1771 (1995): "A Border Gateway Protocol 4 (BGP-4)".

[61] IETF RFC 1825 (1995): "Security Architecture for the Internet Protocol".

[62] IETF RFC 1826 (1995): "IP Authentication Header".

[63] IETF RFC 1827 (1995): "IP Encapsulating Security Payload (ESP)".

[64] Void.

[65] 3GPP TS 23.246: "Multimedia Broadcast/Multicast Service (MBMS) Architecture and Functional Description".

[66] Void.

[67] IETF RFC 4005 (2005): "Diameter Network Access Server Application".

[68] 3GPP TS 23.141: "Presence Service; Architecture and functional description".

[69] 3GPP TS 32.422: "Subscriber and equipment trace: Trace Control and Configuration Management".

[70] 3GPP TS 48.018: "Base Station System (BSS) – Serving GPRS Support Node (SGSN); BSS GPRS Protocol (BSSGP)".

[71] 3GPP TS 23.107: "Quality of Service (QoS) Concept and Architecture".

[72] 3GPP TS 25.346: "Introduction of the Multimedia Broadcast Multicast Service (MBMS) in the Radio Access Network (RAN)".

[73] IETF RFC 4604 (2006): "Using Internet Group Management Protocol Version 3 (IGMPv3) and Multicast Listener Discovery Protocol Version 2 (MLDv2) for Source-Specific Multicast".

[74] IETF RFC 4607 (2006): "Source-Specific Multicast for IP".

[75] 3GPP TS 29.212: "Policy and Charging Control (PCC); Reference points".

[76] 3GPP TS 29.213: "Policy and charging control signalling flows and Quality of Service (QoS) parameter mapping".

[77] 3GPP TS 23.401: "General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access".

[78] 3GPP TS 23.402: "Architecture enhancements for non-3GPP accesses".

[79] IETF RFC 4039 (2005): "Rapid Commit Option for the Dynamic Host Configuration Protocol version 4 (DHCPv4)".

[80] IETF RFC 3736 (2004): "Stateless Dynamic Host Configuration Protocol (DHCP) Service for IPv6".

[81] 3GPP TS 29.274: "Evolved GPRS Tunnelling Protocol for EPS (GTPv2)".

[82] IETF RFC 4291 (2006): "IP Version 6 Addressing Architecture".

[83] IETF RFC 4862 (2007): "IPv6 Stateless Address Autoconfiguration".

[84] 3GPP TS 24.301: "Non-Access-Stratum (NAS) protocol for Evolved Packet System (EPS)".

[85] IETF RFC 2132 (1997): "DHCP Options and BOOTP Vendor Extensions".

[86] IETF RFC 3361 (2002): "Dynamic Host Configuration Protocol (DHCP-for-IPv4) Option for Session Initiation Protocol (SIP) Servers".

[87] IETF RFC 3646 (2003): "DNS Configuration options for Dynamic Host Configuration Protocol for IPv6 (DHCPv6)".

[88] IETF RFC 3319 (2003): "Dynamic Host Configuration Protocol (DHCPv6) Options for Session Initiation Protocol (SIP) Servers".

[89] IETF RFC 4861 (2007): "Neighbor Discovery for IP Version 6 (IPv6)".

[90] 3GPP TS 23.203: "Policy and charging control architecture".

[91] IETF RFC 4739 (2006): "Multiple Authentication Exchanges in the Internet Key Exchange (IKEv2) Protocol".

[92] 3GPP TS 25.413: "UTRAN Iu Interface RANAP Signalling".

[93] IETF RFC 5176 (2008): "Dynamic Authorization Extentions to Remote Authentication Dial In User Service (RADIUS)".

[94] 3GPP TS 36.331: "Evolved Universal Terrestrial Radio Access (E-UTRA); Radio Resource Control (RRC); Protocol specification".

[95] 3GPP TS 23.380: "IMS Restoration Procedures".

[96] 3GPP TS 29.303: "Domain Name System Procedures; Stage 3".

[97] IETF RFC 4818 (2007): "RADIUS Delegated-IPv6-Prefix Attribute".

[98] 3GPP TS 36.300: "Evolved Universal Terrestrial Radio Access (E-UTRA) and Evolved Universal Terrestrial Radio Access Network (E-UTRAN); Overall description"

[99] 3GPP TS 23.221: "Architectural requirements".

[100] 3GPP TS 23.682: "Architecture Enhancements to facilitate communications with Packet Data Networks and Applications".

[101] 3GPP TS 29.336: "Home Subscriber Server (HSS) Diameter interfaces for interworking with packet data networks and applications".

[102] IETF RFC 4282 (2005): "The Network Access Identifier".

[103] 3GPP TS 29.275: "Proxy Mobile IPv6 (PMIPv6) based Mobility and Tunnelling protocols; Stage 3".

[104] 3GPP TS 23.007: "Restoration procedures".

[105] 3GPP TS 29.229: "Cx and Dx interfaces based on Diameter protocol; Protocol details".

[106] 3GPP TS 25.446: "MBMS synchronisation protocol (SYNC)".

[107] 3GPP TS 25.323: "Packet Data Convergence Protocol (PDCP) specification".

[108] Void.

[109] IETF RFC 4960 (2007): "Stream Control Transmission Protocol".

[110] 3GPP TS 29.128: "Mobility Management Entity (MME) and Serving GPRS Support Node (SGSN) interfaces for interworking with packet data networks and applications ".

[111] IETF RFC 6733: "Diameter Base Protocol".

[112] 3GPP TS 23.285: "Architecture Enhancements for V2X services".

[113] 3GPP TS 29.468: "Group Communication System Enablers for LTE (GCSE\_LTE); MB2 Reference point; Stage 3".

[114] 3GPP TS 29.244: "Interface between the Control Plane and the User Plane of EPC Nodes; Stage 3".

[115] 3GPP TS 38.413: "NG Radio Access Network (NG-RAN); NG Application Protocol (NGAP)".

[116] IETF RFC 2869: "RADIUS Extensions".

[m2] IETF RFC 2661: " Layer Two Tunneling Protocol "L2TP".

\*\*\* 2nd Change \*\*\*

## 3.2 Abbreviations

Abbreviations used in the present document are listed in 3GPP TR 21.905 [42]. For the purposes of the present document, the following additional abbreviations apply:

5QI 5G QoS Identifier

AMBR Aggregate Maximum Bit Rate

APN Access Point Name

ARP Allocation and Retention Priority

ATM Asynchronous Transfer Mode

APCO Additional Protocol Configuration Options

BG Border Gateway

BM-SC Broadcast/Multicast Service Centre

CHAP Challenge Handshake Authentication Protocol

CIoT Cellular Internet of Things

DHCP Dynamic Host Configuration Protocol

DHCPv6 Dynamic Host Configuration Protocol version 6

DNS Domain Name System

DSMIPv6 Dual-Stack MIPv6

DVMRP Distance Vector Multicast Routing Protocol

EPC Evolved Packet Core

ePDG Evolved Packet Data Gateway

EPS Evolved Packet System

FQDN Fully Qualified Domain Name

GBR Guaranteed Bit Rate

GFBR Guaranteed Flow Bit Rate

GGSN Gateway GPRS Support Node

GTP-U GPRS Tunnelling Protocol for user plane

ICMP Internet Control Message Protocol

IETF Internet Engineering Task Force

IGMP Internet Group Management Protocol

IMS IP Multimedia Subsystem

IP Internet Protocol

IPCP IP Control Protocol (PPP NCP for IPv4)

IPv4 Internet Protocol version 4

IPv6 Internet Protocol version 6

IPV6CP IPv6 Control Protocol (PPP NCP for IPv6)

ISDN Integrated Services Digital Network

ISP Internet Service Provider

L2TP Layer Two Tunneling Protocol

LAC L2TP Access Concentrator

LAN Local Area Network

LNS L2TP Network Server

MBMS Multimedia Broadcast/Multicast Service

MBR Maximum Bit Rate

MFBR Maximum Flow Bit Rate

MIP Mobile IP

MLD Multicast Listener Discovery

MME Mobility Management Entity

MOSPF Multicast Open Shortest Path First

MS Mobile Station

MT Mobile Terminal

MTC Machine Type Communication

MTU Maximum Transfer Unit

NAI Network Access Identifier

NCGI NR Cell Global Identity

PAP Password Authentication Protocol

PCC Policy and Charging Control

PCO Protocol Configuration Options

PCRF Policy and Charging Rules Function

P-CSCF Proxy Call Session Control Function

PDCP Packet Data Convergence Protocol

PDN Packet Data Network

PDU Protocol Data Unit

P-GW PDN Gateway

PIM-SM Protocol Independent Multicast – Sparse Mode

PPP Point-to-Point Protocol

PS Packet Switched

QCI QoS Class Identifier

RADIUS Remote Authentication Dial In User Service

SCEF Service Capability Exposure Function

SGSN Serving GPRS Support Node

S-GW Serving Gateway

SMDS Switched Multimegabit Data Service

SMF Session Management Function

TCP Transmission Control Protocol

TE Terminal Equipment

TEID Tunnel End-point Identifier

TMGI Temporary Mobile Group Identity

TWAN Trusted WLAN Access Network

UDP User Datagram Protocol

\*\*\* 3rd Change \*\*\*

#### 11.2.1.y(new) Support L2TP for CUPS across SGi

L2TP (described in RFC 2661[m2]) is a standard method for tunneling encapsulated Point-to-Point Protocol (PPP) frames over an IP network. L2TP operates between two L2TP endpoints (LAC and LNS), and tunnels PPP-encapsulated IP traffic between these endpoints. L2TP runs over UDP/IP and was originally defined for systems where PPP is used by an end-device to connect to a network (e.g. via DSL connections, or 2G/3G PPP PDP context). In these cases, a LAC could be deployed in the network (e.g. in a BNG or GGSN/PGW) to tunnel the PPP traffic to a server (LNS) over an IP network.

For CUPS with the UE using IP PDN connection, the PPP functionality that is required to use L2TP is instead supported by the PGW-U, as illustrated in below figure. Upon receiving a PDN connection session establishment request from the UE via MME and SGW-C, PGW-C may depend on local L2TP configuration per APN or the received L2TP information from a DN AAA server in Access-Accept message, request the PGW-U to setup L2TP tunnel towards an L2TP network server (LNS) in the external DN and tunnel the PDN Connection user plane traffic in this L2TP tunnel. In this case the PGW-U acts as a L2TP access concentrator (LAC).

To enable this, the PGW-C may provide L2TP tunnel information to the PGW-U as LAC, such as LNS IP address as described in 3GPP TS 29.244 [114]. This L2TP tunnel information may be configured on the PGW-C as part of the APN configuration or received from the DN-AAA server. Alternatively, the L2TP tunnel parameters may be configured in the PGW-U. The L2TP tunnel parameters include necessary parameters for setting up L2TP tunnel towards the LNS (e.g. LNS address, tunnel password).

In addition, the PGW-C may provide PAP/CHAP authentication information to the PGW-U, for use in L2TP session establishment, in case it was received from the UE in the PCO or ePCO IE of the PDN Connection establishment request message.

When L2TP is to be used for a PDN Connection, the PGW-C may select a PGW-U and requests the UE IP address to be allocated by LNS according to 3GPP TS 29.244 [114], the PGW-U (LAC) may retrieve this IP address from the LNS.



Figure 11f: L2TP Tunnel between CUPS and external DN

Below figure describes the L2TP connection procedures between CUPS and external DN, upon the UE is accessed in EPS and the PGW-C and PGW-U has been negotiated supporting L2TP feature.



Figure 11g: L2TP connection procedures between CUPS and external DN

0. The PGW-C and the PGW-U negotiated supporting L2TP feature as specified in 3GPP TS 29.244 [114].

1. The PGW-C receives a PDN Connection session establishment request from the UE via MME and SGW-C.

 The UE may include the authentication information for PAP and/or CHAP in PCO or ePCO IE. The PGW-C may locally configure the UE authentication information for a given APN.

 The PGW-C may determine that an L2TP session is required for the PDN Connection session based on local configured L2TP parameters per APN.

2. The PGW-C may receive the L2TP Tunnel parameters (e.g. LNS IP address or FQDN, tunnel password) from the DN-AAA server in Access-Accept message or Diameter EAP Answer (DEA) message, or local configured.

3. If L2TP protocol is determined to support the PDN connection, the PGW-C selects a PGW-U supporting L2TP and be configured with the LAC name/addresses and then requests the PGW-U to setup an L2TP tunnel if needed and/or L2TP session towards the L2TP network server (LNS). For a given APN requiring L2TP function, multiple LACs may be configured to be connected with multiple LNSs in the Data Network. A PGW-U may be configured with the multiple LAC names and addresses for a given APN.

 The PGW-C sends PFCP Session Establishment Request to the PGW-U, which may include L2TP Tunnel Information for setting up a L2TP tunnel and L2TP session information to setup a L2TP session, together with the information for authentication used during L2TP Tunnel setup, as well as for L2TP session.

 The L2TP Tunnel Information includes LNS IPv4 address or IPv6 address of LNS, Tunnel Password.

 The L2TP Session Information includes specific information related to the PDN Connection, e.g. a Calling Number which may be set to UE's MSISDN, an indication to instruct that the PGW-U shall request the LNS to allocate an IP address for the PDN session, indications to instruct that the PGW-U shall request the LNS to provide DNS server addresses or NBNS server addresses etc. as specified in 3GPP TS 29.244 [114].

4. The PGW-U checks if any existing L2TP tunnel can be used to serve the PDN Connection according to the information provided in the L2TP Tunnel Information.

If the PGW-U decides to setup a new L2TP tunnel, it initiates L2TP Tunnel establishment by sending an SCCRQ (Start-Control-Connection-Request) message towards the LNS, the PGW-U will allocate a Tunnel ID, and it may include a CHAP Challenge to authenticate the LNS. The Challenge and Challenge Response (to be included in SCCCN) is produced by the PGW-U using the Tunnel Password received from the PGW-C.

 The LNS responds with an SCCRP (Start-Control-Connection-Reply) message, containing its allocated Tunnel ID and a CHAP Challenge Response to the Challenge in SCCRQ.

 The PGW-U then responds with a Challenge response for tunnel authentication in the SCCCN (Start-Control-Connection-Connected) message. An L2TP tunnel is established after the tunnel authentication is successful, with the reception of the SCCCN message sent by the PGW-U to the LNS.

 If the PGW-U decides to use an already existing L2TP tunnel for the requested PDN Connection from the PGW-C, it proceeds with step 5 below directly without current step.

5. Once the L2TP Tunnel is established (or already present) between the PGW-U and the LNS for the PDN Connection requested by the UE, the PGW-U proceeds with L2TP session setup towards the LNS.

 The PGW-U sends an ICRQ (Incoming-Call-Request) message towards the LNS, which contains the Tunnel ID assigned by the LNS, its assigned Session ID, and optionally, the Calling Number and Called Number. The LNS responds with an ICRP (Incoming-Call-Reply) message and provides the Session ID assigned by it to the LAC.

 The PGW-U then sends an ICCN (Incoming-Call-Connected) message. The PGW-U includes the UE authentication information from the PGW-C received via PCO or ePCO IE in step 1. In addition, the PGW-U (LAC) will act as a PPP endpoint to use LCP to communicate some link control parameters, e.g. MRU; to use PAP/CHAP to perform an authentication procedure; to use IPCP to request PDU Session IP Address, DNS server address and/or NBNS server address(es).

 Otherwise, after the reception of the ICCN message, the LNS responds with a ZLB Ack message. After the reception of ZLB Ack message, the LAC and LNS will use PPP LCP to communicate link specific control parameter, and indicate authentication type, then either PPP PAP/CHAP takes place. The PPP IPCP transactions takes places to retrieve UE IP Address, DNS server address and/or NBNS server address.

6. The status of the L2TP session setup is sent by the PGW-C to the PGW-U in a PFCP Session Establishment Response.

7. The PGW-C sends a PDU Session Establishment Response to the UE and the user data session is initiated, which may contain the DNS and NBNS Server information.

\*\*\* End of Changes \*\*\*