**3GPP TSG-CT WG3 Meeting #116e C3-213431**

**E-Meeting, 19th – 28th May 2021 (Revision of C3-213212)**

|  |
| --- |
| *CR-Form-v12.1* |
| **CHANGE REQUEST** |
|  |
|  | **29.061** | **CR** | **0538** | **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 in Diameter message flow |
|  |  |
| ***Source to WG:*** | Ericsson |
| ***Source to TSG:*** | CT3 |
|  |  |
| ***Work item code:*** | BEPoP |  | ***Date:*** | 2021-05-06 |
|  |  |  |  |  |
| ***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:*** | CT4 has been studied and agreed L2TP supporting for CUPS in WI BEPoP,TR 29.820 has also concluded to support L2TP tunneling over N6/SGi for 5GC/EPS is to be standardized based on the solution#8 as described in 6.8 in Rel-17, and CT3 scope has been added in WI BEPoP.Meanwhile, SA2 LS Reply on the support of L2TP with CUPS in rel-17 to support L2TP tunnelling over N6/SGi for 5GS and EPS, with TS 23.214 CR 0076 approved.Hence the related L2TP support and attributes for Diameter messages need to be added. |
|  |  |
| ***Summary of change:*** | Adding Diameter attributes within the grouped "Tunneling" AVP and the basic attributes in Diameter AAA message to support DN AAA server providing L2TP information. |
|  |  |
| ***Consequences if not approved:*** | Missing the Diameter attributes in the related Diameter message to support L2TP in this specification, and cannot be referred by TS 29.561. |
|  |  |
| ***Clauses affected:*** | 16a.4.2 |
|  |  |
|  | **Y** | **N** |  |  |
| ***Other specs*** | **X** |  |  Other core specifications  | TS 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 \*\*\*

### 16a.4.2 AAA Command

The AAA command, defined in Diameter NASREQ (IETF RFC 4005 [67]), is indicated by the Command-Code field set to 265 and the ‘R’ bit cleared in the Command Flags field., It is sent by the Diameter server to the GGSN/P-GW in response to the AAR command.

The relevant AVPs that are of use for the Gi/Sgi interface are detailed in the ABNF description below. Other valid AVPs for this command are not used for Gi/Sgi purposes and should be ignored by the receiver or processed according to the relevant specifications.

The "Tunneling" AVP may include the "Tunnel-Type" with value 3 to represent L2TP tunnel type, "Tunnel-Medium-Type" and "Tunnel-Server-Endpoint" AVPs. If more than one set of these "Tunneling" AVPs are provided, the optional "Tunnel-Preference" AVP may be provided in each set to identify the relative preference. The Tunnel-Password AVP may be used to authenticate to a remote server.

NOTE: The other optional AVPs within the "Tunneling" AVPs can be referred to the IETF RFC 4005 [67] with implementation specific.

Editor’s Note: Whether the Tunnel-Password can be included will be confirmed by SA3.

The bold marked AVPs in the message format indicate optional AVPs for Gi/Sgi, or modified existing AVPs.

Message Format:

<AA-Answer> ::= < Diameter Header: 265, PXY >

 < Session-Id >

 { Auth-Application-Id }

 { Auth-Request-Type }

 { Result-Code }

 { Origin-Host }

 { Origin-Realm }

 [ User-Name ]

 [ Service-Type ]

 \* [ Class ]

 [ Acct-Interim-Interval ]

 [ Error-Message ]

 [ Error-Reporting-Host ]

 [ Failed-AVP ]

 [ Idle-Timeout ]

 [ Authorization-Lifetime ]

 [ Auth-Grace-Period ]

 [ Auth-Session-State ]

 [ Re-Auth-Request-Type ]

 [ Multi-Round-Time-Out ]

 [ Session-Timeout ]

 \* [ Reply-Message ]

 [ Origin-State-Id ]

 \* [ Filter-Id ]

 [ Port-Limit ]

 [ Prompt ]

 [ Callback-Id ]

 [ Callback-Number ]

 \* [ Framed-Compression ]

 [ Framed-Interface-Id ]

 [ Framed-IP-Address ]

 \* [ Framed-IPv6-Prefix ]

 [ Framed-IPv6-Pool ]

 \* [ Framed-IPv6-Route ]

 \* [ Delegated-IPv6-Prefix ]

 [ Framed-IP-Netmask ]

 \* [ Framed-Route ]

 [ Framed-Pool ]

 [ Framed-IPX-Network ]

 [ Framed-MTU ]

 [ Framed-Protocol ]

 [ Framed-Routing ]

 \* [ Login-IP-Host ]

 \* [ Login-IPv6-Host ]

 [ Login-LAT-Group ]

 [ Login-LAT-Node ]

 [ Login-LAT-Port ]

 [ Login-LAT-Service ]

 [ Login-Service ]

 [ Login-TCP-Port ]

 \* [ NAS-Filter-Rule ]

 \* [ QoS-Filter-Rule ]

 \* [ Tunneling ]

 \* [ Redirect-Host ]

 [ Redirect-Host-Usage ]

 [ Redirect-Max-Cache-Time ]

 \* [ Proxy-Info ]

  **[ 3GPP-IPv6-DNS-Servers ]**

 \* **[ External-Identifier]**

 \* [ AVP ]

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