**3GPP TSG-CT WG3 Meeting #112eC3-205339**

**E-Meeting, 04th – 13th November 2020**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.0* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  | **29.561** | **CR** | **0037** | **rev** | **2** | **Current version:** | **16.5.0** |  |
|  | | | | | | | | |
| *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:*** | Clarification on using PAP/CHAP for 5GS interoperability | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | Qualcomm Incorporated, Vodafone | | | | | | | | | |
| ***Source to TSG:*** | CT3 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | TEI15 | | | | |  | ***Date:*** | | | 2020-10-20 |
|  |  | | | |  | |  | | |  |
| ***Category:*** | **A** |  | | | | | ***Release:*** | | | Rel-16 |
|  | *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 can be 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-12 (Release 12)* *Rel-13 (Release 13) Rel-14 (Release 14) Rel-15 (Release 15) Rel-16 (Release 16)* | |
|  |  | | | | | | | | | |
| ***Reason for change:*** | | For PAP/CHAP point to point authentication protocols in PCO, the SMF in release 15 and 16 doesn’t support using RADIUS/Diameter protocol for the corresponding PAP/CHAP information elements directly for interaction with external DN-AAA server. To this end, in Reply LS "PAP/CHAP and other point-to-point protocols usage in 5GS" (S2-2004481/C3-203599), SA2 has asked CT3 to consider the necessary enhancement so that usage by R15 UEs is permitted.  In contrast to SMF, a combined PGW-C/SMF node can support Radius/Diameter interface through its PGW component. Hence to be able to allow the UE to use PAP/CHAP in PCO, the operator can configure the network so that the UE provisioned to use PAP/CHAP to use a specific slice, which will cause the AMF to select a combined PGW-C/SMF that supports PAP/CHAP in PCO. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | Specification text is added that to support UEs provisioned to use PAP/CHAP in PCO, the network should be configured to select a combined PGW-C/SMF that supports this mechanism. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | It would remain ambiguous how release 16 UEs can use PAP/CHAP AAA in PCO. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 11.1.1 | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **Y** | **N** |  | | | |  | | |
| ***Other specs*** | |  | **X** | Other core specifications | | | | TS/TR ... CR ... | | |
| ***affected:*** | |  | **X** | Test specifications | | | | TS/TR ... CR ... | | |
| ***(show related CRs)*** | |  | **X** | O&M Specifications | | | | TS/TR ... CR ... | | |
|  | |  | | | | | | | | |
| ***Other comments:*** | |  | | | | | | | | |
|  | |  | | | | | | | | |
| ***This CR's revision history:*** | | Instead of note, changed added text to FASMO specification text.  Corrected WI code. | | | | | | | | |

# \*\*\* First change \*\*\*

11.1.1 RADIUS Authentication and Authorization

The SMF also represents the H-SMF in the home routed scenario in this subclause unless specified otherwise.

RADIUS Authentication and Authorization shall be used according to IETF RFC 2865 [8], IETF RFC 3162 [9] and IETF RFC 4818 [10]. In 5G, multiple authentication methods using Extensible Authentication Protocol (EAP) may be used such as EAP-TLS (see IETF RFC 5216 [11]), EAP-TTLS (see IETF RFC 5281 [37]). The SMF shall implement the RADIUS extension to support EAP as specified in IETF RFC 3579 [7].

If a UE uses PAP/CHAP, an appropriate configuration of S-NSSAI/DNN combination can be included in the UE's subscription to a select combined PGW-C/SMF that supports PAP/CHAP.

The RADIUS client function may reside in an SMF. When the SMF receives an initial access request (i.e. the SMF receives the Nsmf\_PDUSession\_CreateSMContext request with type "Initial request" for non-roaming case or local breakout case, or the H-SMF receives the Nsmf\_PDUSession\_Create Request with type "Initial request" for home routed case), the RADIUS client function may send the authentication information to a DN-AAA server, which is identified during the DNN provisioning.

The DN-AAA server performs authentication and authorization. The response (when positive) may contain network information, such as an IPv4 address and/or IPv6 prefix for the user when the SMF is interworking with the DN-AAA server.

The information delivered during the RADIUS authentication can be used to automatically correlate the user identity (e.g. SUPI) to the IPv4 address and/or IPv6 prefix, if applicable, assigned/confirmed by the SMF or the DN-AAA server respectively. The same procedure applies, in case of sending the authentication to a 'proxy' DN-AAA server.

For 5G, RADIUS Authentication is applicable to the initial access request. When the SMF receives an Access-Accept message from the DN-AAA server it shall complete the initial access procedure. If Access-Reject or no response is received, the SMF shall reject the initial access procedure with a suitable cause code.

When DN-AAA server authorizes the PDU Session Establishment, it may send DN authorization data for the established PDU Session to the SMF. The DN authorization data for the established PDU Session may include one or more of the following:

- a reference to authorization data for policy and charging control locally configured in the SMF or PCF;

- a list of allowed MAC addresses (maximum 16) for the Ethernet PDU Session;

- a list of allowed VLAN Ids (maximum 16) for the Ethernet PDU Session; and

- Session-AMBR for the PDU Session.

SMF policies may require DN authorization without DN authentication. In that case, when contacting the DN-AAA server for authorization, the SMF shall provide the GPSI of the UE if available.

The SMF may also use the RADIUS re-authorization procedure for the purpose of IPv4 address and/or IPv6 prefix allocation to the UE. The use cases that may lead this procedure are:

- IPv4 address and/or IPv6 prefix allocation after UPF selection during PDU session establishment procedure.

- IPv6 prefix allocation during adding additional PDU Session Anchor procedure for IPv6 multi-homing.

- IPv4 address allocation via DHCPv4 procedure after successful PDU session establishment procedure.

The SMF may also trigger request for DN authentication/authorization and/or IP address/prefix allocation based on UE subscription data retrieve from the UDM as defined in subclause 5.2.2.2.5 of 3GPP TS 29.503.

When an IPv4 address and/or IPv6 prefix (including any additional IPv6 prefix of IPv6 multi-homing) is (re-)allocated or de-allocated (not causing the PDU session to be released) by using a method not via the DN-AAA server and if the SMF was required by the DN-AAA server to report such change during authentication procedure or by local configuration, the SMF shall, if applicable, use the authentication session that was established before to inform the DN-AAA server by sending RADIUS Access-Request with the latest list of IPv4 address and/or IPv6 prefix(es).

When the SMF is notified by the UPF regarding the UE MAC address change (a new one is detected or a used one is inactive), if the SMF was required by the DN-AAA server to report such change during authentication procedure or by local configuration, the SMF shall, if applicable, use the authentication session that was established before to inform the DN-AAA server by sending RADIUS Access-Request with the latest list of UE MAC addresses in use.

DN-AAA may initiate QoS flow termination and re-authorization, see details in clause 11.2.3 and clause 11.2.4. In the present release, the DN-AAA initiated re-authentication is not supported.

# \*\*\* End of changes \*\*\*