**3GPP TSG-CT3 Meeting #116e C3-213xxx**

**E-Meeting, 19th – 28th May 2021 *(revision of C3-213160)***

|  |
| --- |
| *CR-Form-v12.1* |
| **CHANGE REQUEST** |
|  |
|  | **29.561** | **CR** | **0110** | **rev** |  | **Current version:** | **17.1.0** |  |
|  |
| *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:***  | Alignment of the DN authorizaiton data for the established PDU Session between the specificaitons of stage 2 and stage 3  |
|  |  |
| ***Source to WG:*** | China Telecom |
| ***Source to TSG:*** | CT3 |
|  |  |
| ***Work item code:*** | TEI17  |  | ***Date:*** | 2021-05-11 |
|  |  |  |  |  |
| ***Category:*** | **F** |  | ***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:*** | In sub 5.6.6 of TS 23.501, it states:- *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 DN Authorization Profile Index which is a reference to authorization data for policy and charging control locally configured in the SMF or PCF.**- a list of allowed MAC addresses for the PDU Session; this shall apply only for PDU Session of Ethernet PDU type and is further described in clause 5.6.10.2.**- a list of allowed VLAN tags for the PDU Session; this shall apply only for PDU Session of Ethernet PDU type and is further described in clause 5.6.10.2.**- DN authorized Session AMBR for the PDU Session. The DN Authorized Session AMBR for the PDU Session takes precedence over the subscribed Session-AMBR received from the UDM.**- Framed Route information (see clause 5.6.14) for the PDU Session.*However, in the according text in sub 11.1.1 and sub 12.1.1 of TS 29.561, they state:*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.*The DN authorization data for the established PDU Session is not complete in TS 29.561 and the data “Framed Route information for the PDU Session.” is missing, which is inconsistent with the text in sub 5.6.6 of TS 23.501.Hence the missing data should be added in TS 29.561 to keep the specs consistent. |
|  |  |
| ***Summary of change:*** | It proposes to add some DN authorization data for the established PDU Session when DN-AAA server authorizes the PDU Session Establishment. |
|  |  |
| ***Consequences if not approved:*** | The DN authorization data for the established PDU Session when DN-AAA server authorizes the PDU Session Establishment is inconsistent between the different specs. |
|  |  |
| ***Clauses affected:*** | 11.1.1, 12.1.1 |
|  |  |
|  | **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:*** |  |

\* \* \* 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].

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.

When the legacy applications require PAP/CHAP authentication with the UE accessing to the 5GS or to the 5GC and EPC interworking scenario and the legacy DN-AAA server does not support EAP, PAP/CHAP may be used as the authentication protocol, with the external network performing the risk assessment.

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.

- Framed Route information 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.

For the 5GS interworking with EPS scenario, EAP based secondary authentication and re-authentication is not applicable to the PDN connection when the UE is in EPS in this release.

In case EAP based authentication and authorization has been performed for the PDU Session while the UE was in 5GS, and if SMF+PGW-C determines that the UE has moved to the EPS (i.e. the SMF+PGW-C receives the modify bearer request or create session request from the S-GW), the following applies:

- the SMF+PGW-C may initiate RADIUS re-authorization procedure without re-authentication with the DN-AAA server based on local policy.

- DN-AAA re-authorization without re-authentication may be performed.

- when the SMF+PGW-C receives a re-authentication request from the DN-AAA server, the SMF+PGW-C shall inform the DN-AAA server that the re-authentication is not supported with proper error code. The SMF+PGW-C should not initiate PDN connection release.

NOTE: The DN-AAA server decides the actions to take (e.g. to request another re-authorization without the association with EAP based re-authentication or release the session) is out of 3GPP scope.

\* \* \* Second Change \* \* \* \*

### 12.1.1 Diameter Authentication and Authorization

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

Diameter Authentication and Authorization shall be used according to IETF RFC 7155 [23]. 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 support Diameter EAP application as specified in IETF RFC 4072 [25].

The SMF and the DN-AAA shall advertise the support of the Diameter NASREQ and EAP applications by including the value (1 and 5) of the application identifier in the Auth-Application-Id AVP (as specified in IETF RFC 4072 [25]) and the value of the 3GPP (10415) in the Vendor-Id AVP of the Capabilities-Exchange-Request and Capabilities-Exchange-Answer commands as specified in IETF RFC 6733 [24], i.e. as part of the Vendor-Specific-Application-Id AVP.

The Diameter 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 Diameter client function may send the authentication information to a DN-AAA server, which is identified during the DNN provisioning.

When the legacy applications require PAP/CHAP authentication with the UE accessing to the 5GS or to the 5GC and EPC interworking scenario and the legacy DN-AAA server does not support EAP, PAP/CHAP may be used as the authentication protocol, with the external network performing the risk assessment.

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 Diameter 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, Diameter Authentication is applicable to the initial access request. When the SMF receives a positive response 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;

- 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.

- Framed Route information 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 Diameter 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 Diameter DER or AAR 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 Diameter DER or AAR with the latest list of UE MAC addresses in use.

DN-AAA may initiate QoS flow termination, see details in clause 12.2.3. DN-AAA may initiate re-authorization and optional re-authentication, see details in clause 12.2.4 and 12.2.5.

For the 5GS interworking with EPS scenario, EAP based secondary authentication and re-authentication is not applicable to the PDN connection when the UE is in EPS in this release.

In case EAP based authentication and authorization has been performed for the PDU Session while the UE was in 5GS, and if SMF+PGW-C determines that the UE has moved to the EPS (i.e. the SMF+PGW-C receives the modify bearer request or create session request from the S-GW), the following applies:

- the SMF+PGW-C may initiate RADIUS re-authorization procedure without re-authentication with the DN-AAA server based on local policy.

- DN-AAA re-authorization without re-authentication may be performed.

- when the SMF+PGW-C receives a re-authentication request from the DN-AAA server, the SMF+PGW-C shall inform the DN-AAA server that the re-authentication is not supported with proper error code. The SMF+PGW-C should not initiate PDN connection release.

NOTE: The DN-AAA server decides the actions to take (e.g. to request another re-authorization without the association with EAP based re-authentication or release the session) is out of 3GPP scope.

\* \* \* End of Change \* \* \* \*