**3GPP TSG-CT WG3 Meeting #115e C3-212271**

**E-Meeting, 14th – 23rd April 2021 (Revision of C3-21xxxx)**

|  |
| --- |
| *CR-Form-v12.1* |
| **CHANGE REQUEST** |
|  |
|  | **29.561** | **CR** | **0099** | **rev** | **-** | **Current version:** | **16.7.0** |  |
|  |
| *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:***  | Clarify 5GS interworking with EPS for EAP based secondary AUTH in RADIUS message flow |
|  |  |
| ***Source to WG:*** | Ericsson |
| ***Source to TSG:*** | CT3 |
|  |  |
| ***Work item code:*** | 5GS\_Ph1-CT |  | ***Date:*** | 2021-03-26 |
|  |  |  |  |  |
| ***Category:*** | **F** |  | ***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 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 reply LS on Secondary AUTH for 5GS interworking with EPS ([C3-211611](https://www.3gpp.org/ftp/tsg_ct/WG3_interworking_ex-CN3/TSGC3_114e/Docs/C3-211611.zip)) states EAP based secondary authorization/ authentication has only been defined for 5GS and is thus not applicable to EPS in existing releases Rel-16 TS 23.502 clause 4.11.0a adding a new subclause specify that secondary authentication with a DN-AAA server is not supported when the UE is in EPS. Secondary authorization (without authentication of the UE) with a DN-AAA server is supported when the UE is in EPS. Secondary authorization (without authentication of the UE) with a DN-AAA server, as specified in clause 4.3.2.3, is supported when the UE is in EPS.Rel-17 has been updated with EAP based secondary authentication and re-authentication not supporting in EPS, and how does SMF handle the follow procedure is described in clause 11.1.1 in this specification.Rel-16 also need to be updated with EPS not supporting EAP based secondary authentication and re-authentication, Secondary authorization (without authentication of the UE) with a DN-AAA server is supported when the UE is in EPS, while how does SMF handle the related procedure is implementation specific in clause 11.1 1 in this specification. |
|  |  |
| ***Summary of change:*** | Updates in clause 11.1.1 that EPS does not support EAP based secondary authentication and re-authentication, Secondary authorization (without authentication of the UE) with a DN-AAA server is supported when the UE is in EPS, while how does SMF handle the follow procedure is implementation specific with Note description |
|  |  |
| ***Consequences if not approved:*** | For 5GS interworking with 5GS scenario, it is not clear whether EAP based secondary authentication and re-authentication is supported by EPS or not, will arouse the related implementation and deployment problems. |
|  |  |
| ***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:*** |  |

**Additional discussion(if needed):**

**Proposed changes:**

\*\*\* 1st 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.

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.

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. Secondary authorization (without authentication of the UE) with a DN-AAA server is supported when the UE is in EPS.

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), how to handle the following procedure is implementation specific.

NOTE: The SMF+PGW-C can initiate RADIUS re-authorization procedure without re-authentication with the DN-AAA server based on local policy. 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 Changes \*\*\*