**3GPP TSG-CT3 Meeting #112e C3-205xxx**

**E-Meeting, 04th – 13th November 2020 (Revision of C3-205191)**

|  |
| --- |
| *CR-Form-v12.1* |
| **CHANGE REQUEST** |
|  |
|  | **29.561** | **CR** | **0062** | **rev** | **1** | **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 | **X** | Radio Access Network |  | Core Network | **X** |

|  |
| --- |
|  |
| ***Title:***  | Adding PAP/CHAP in Diameter message flow(successful case) |
|  |  |
| ***Source to WG:*** | China Telecom, Huawei, Ericsson |
| ***Source to TSG:*** | CT3 |
|  |  |
| ***Work item code:*** | PAP\_CHAP |  | ***Date:*** | 2020-10-26 |
|  |  |  |  |  |
| ***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:*** | It was agreed that CT WGs to lead the required work on support PAP/CHAP to cater for the migration from EPS to 5GS and potential requirements related with legacy deployments for access to corporate networks, e.g. support of PAP/CHAP in AAA server owned by 3rd parties.Similar as done in 4G, in TS 29.561, the Diameter message flow of Authentication, Authorization and Accounting procedures support the authentication/authorization mechanism including PAP/CHAP as well. |
|  |  |
| ***Summary of change:*** | Adding some description for using PAP/CHAP in Diameter message flow (successful case) when the legacy applications requiring it. |
|  |  |
| ***Consequences if not approved:*** | Missing the description of using PAP/CHAP in 5GS when the legacy applications requiring it, and the legacy DN-AAA server not supporting EAP, can not working with 5GS. |
|  |  |
| ***Clauses affected:*** | 12.1.1, 12.2.1 |
|  |  |
|  | **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:*** |  |

\*\*\* 1st 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 in 5GS 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 or PCF;

- a list of allowed MAC addresses (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 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.

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.

\*\*\* Next Change \*\*\*

### 12.2.1 Authentication, Authorization and Accounting procedures

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

When an 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) message for a given DNN, the SMF may (depending on the configuration for this DNN) send a Diameter DER message to a DN-AAA server. Upon receipt of the DER message, the DN-AAA server shall respond with an DEA message. Multi-round authentication using the DEA and DER messages may be used. The DN-AAA server finally authenticates and authorizes the user by replying with the DEA message. If the DN-AAA server is also responsible for IPv4 address and/or IPv6 prefix allocation, the DN-AAA server shall return the allocated IPv4 address and/or IPv6 prefix in the DEA message.

For re-authentication and re-authorization, the SMF shall send a DER message to the DN-AAA server and the DN-AAA server shall respond with a DEA message. Multi-round authentication using the DEA and DER messages may be used. The DN-AAA server finally authenticates and authorizes the user by replying with the DEA message.

The SMF may initiate Diameter re-authorization procedures for the purpose of IPv4 address and/or IPv6 prefix allocation (or renew the lease). In this case, the SMF shall set the Session-Id to the value used in the initial request, the Auth-Request-Type AVP to "AUTHORIZE\_ONLY" and the 3GPP-Allocate-IP-Type AVP to the type of IP address to be allocated in the AA-Request message sent to the AAA server. If the SMF is using DHCP signalling towards the UE and the DN-AAA server includes the Session-Timeout attribute in the Access-Accept, the SMF may use the Session-Timeout value as the DHCP lease time. The SMF shall not set the DHCPv4 lease time value higher than the Session-Timeout value. The SMF may renew the DHCP lease to the UE without re-authorization towards the DN-AAA server providing that the new lease expiry is no later than the Session-Timeout timer expiry. If the SMF wishes to extend the lease time beyond the current Session-Timeout expiry, it shall initiate a new AAA re-authorization.

Even if the SMF was not involved in user authentication, it may send a Diameter Accounting-Request (START) message to a DN-AAA server. If no Diameter session is already open for the same PDU session a Diameter session needs to be activated, otherwise the existing Diameter session is used to send the Accounting-Request (START). If accounting is used per QoS flow, the QFI will identify the particular bearer this accounting message refers to. This message contains parameters, e.g. the tuple which includes the user ID and IPv4 address and/or IPv6 prefix, to be used by application servers (e.g. WAP gateway) in order to identify the user. This message also indicates to the DN-AAA server that the user session has started.

If some external applications require Diameter Accounting-Request (START) information before they can process user packets, then the selected DNN (SMF) may be configured in such a way that the SMF drops user data until an Accounting-Answer (START) indicating success is received from the DN-AAA server. The SMF may wait for the Accounting-Answer (START) before sending the final authentication response message in Namf\_Communication\_N1N2MessageTransfer service operation. The SMF may reject the initial access request if the Accounting-Answer (START) is not received. The authentication and accounting servers may be separately configured for each DNN.

For IPv4 PDU type, if IPv4 address is allocated via DHCPv4 signalling between the UE and the DN-AAA after PDU session establishment, the SMF may wait to send the Accounting-Request START message until the UE receives its IPv4 address in a DHCPACK.

When the SMF receives a message indicating a QoS flow or PDU session release request and providing a Diameter Accounting-Request START message was sent previously, the SMF shall send a Diameter Accounting-Request (STOP) message to the DN-AAA server, which indicates the termination of this particular QoS flow or PDU session. The SMF shall immediately send the corresponding response (e.g. Nsmf\_PDUSession\_UpdateSMContext response) to the AMF, without waiting for an Accounting-Answer (STOP) message from the DN-AAA server.

If the last QoS flow of a PDU session is deactivated, the SMF shall additionally send an STR message to the DN-AAA server. The DN-AAA server shall reply with an STA message and shall deallocate the IPv4 address and/or IPv6 prefix initially allocated to the subscriber.

The following figure 12.2.1-1 is an example message flow to show the procedure of Diameter Authentication and Accounting between an SMF and a DN-AAA server:

1. UE initiates the PDU Session Establishment procedure, including authentication/authorization information.

2. The AMF sends Nsmf\_PDUSession\_CreateSMContext Request including the authentication/authorization information to the SMF and the SMF responds to the service operation.

 According to the configuration in the SMF, step 6 to step 9 are executed before step 3 if the SMF needs to send an EAP-Request message to the UE.

 In the case of home routed, the AMF sends Nsmf\_PDUSession\_CreateSMContext Request including the authentication/authorization information to the V-SMF and the V-SMF sends Nsmf\_PDUSession\_Create Request including the authentication/authorization information to the H-SMF.

3. If the N4 session has not been established before, the SMF triggers the N4 Session Establishment procedure to the UPF.

In the case of home routed, the V-SMF triggers the N4 Session Establishment procedure to the V-UPF and the H-SMF triggers the N4 Session Establishment procedure to the H-UPF.

4. The SMF sends the DER message to the DN-AAA via the UPF, the message is forwarded from the SMF to the DN-AAA by the UPF in N4 user plane message.

In the case of home routed, the H-SMF sends the Access-Request message to the DN-AAA via the H-UPF, the message is forwarded from the H-SMF to the DN-AAA by the H-UPF in N4 user plane message.

5-10. The DN-AAA responds with the DEA message to the SMF via the UPF, the message is forwarded from the DN-AAA to the SMF by the UPF in N4 user plane message. The authentication/authorization information is further transferred to UE via Namf\_Communication\_N1N2MessageTransfer service and NAS SM Transport message. UE responds to the received authentication/authorization data and such information is transferred in NAS SM Transport message and Nsmf\_PDUSession\_UpdateSMContext service, then finally sent to the DN-AAA by the SMF, via the UPF, in the DER message.

In the case of home routed, the DN-AAA responds with the Access-Challenge message to the H-SMF via the H-UPF, the message is forwarded from the DN-AAA to the H-SMF by the H-UPF in N4 user plane message. The authentication/authorization information is transferred to V-SMF via Nsmf\_PDUSession\_Update service and is further transferred to UE via Namf\_Communication\_N1N2MessageTransfer service and NAS SM Transport message. UE responds to the received authentication/authorization data and such information is transferred in NAS SM Transport message, Nsmf\_PDUSession\_UpdateSMContext service and Nsmf\_PDUSession\_Update servic, then finally sent to the DN-AAA by the H-SMF, via the H-UPF, in the Access-Request message.

NOTE: Step 5 to step 10 can be repeated depending on the authentication/authorization mechanism used (e.g.EAP-TLS).

11. The SMF receives final result of authentication/authorization from the DN-AAA in the DEA message, via the UPF.

12. The SMF requests to start accounting by sending the Accounting-Request (START) message to the DN-AAA via the UPF.

13. The SMF proceeds with the PDU session establishment procedure and includes the authentication/authorization information in Namf\_Communication\_N1N2MessageTransfer service.

In the case of home routed, the H-SMF proceeds with the PDU session establishment procedure and includes the authentication/authorization information is transferred to V-SMF via Nsmf\_PDUSession\_Update service and is further transferred to the AMF via Namf\_Communication\_N1N2MessageTransfer service.

14. The DN-AAA responds with the Accounting-Response (START) message. The SMF may wait for the Accounting-Response (START) before sending the Namf\_Communication\_N1N2MessageTransfer request in step 13.

 In the case of home routed, the H-SMF may wait for the Accounting-Response (START) before sending the Nsmf\_PDUSession\_Update service in step 13.

15. The AMF sends the NAS PDU Session Establishment Request with the authentication/authorization information to the UE.

16. The UE sends a NAS message Deregistration Request to the AMF.

17. The AMF sends Nsmf\_PDUSession\_ReleaseSMContext Request to the SMF and the SMF responds to the service operation.

 In the case of home routed, the AMF sends Nsmf\_PDUSession\_ReleaseSMContext Request to the V-SMF and the V-SMF sends the Nsmf\_PDUSession\_Release Request to the H-SMF.

18-19. The SMF requests to stop accounting by sending the Accounting-Request (STOP) message to the DN-AAA via the UPF and the DN-AAA responds with the Accounting-Response (STOP) message.



Figure 12.2.1-1: Diameter Authentication and Accounting example (successful case)

When PAP/CHAP is used as the authentication protocol with the external DN-AAA server which does not support EAP, the Diameter Authentication procedures refer to the non transparent access procedures in clause 11.2.1 and related descriptions in clasue 16a in 3GPP TS 29.061 [5].

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