**3GPP TSG-CT WG4 Meeting #105-eC4-21xxxx**

**E-Meeting, 17th – 27th August 2021was C4-214259**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.1* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  | **29.273** | **CR** | **0528** | **rev** | **-** | **Current version:** | **17.0.0** |  |
|  | | | | | | | | |
| *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 |  |

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | | | | | | | | | |
| ***Title:*** |  | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | ZTE | | | | | | | | | |
| ***Source to TSG:*** | CT4 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | TEI17 | | | | |  | ***Date:*** | | | 2021-08-24 |
|  |  | | | |  | |  | | |  |
| ***Category:*** | D |  | | | | | ***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 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-15 (Release 15) Rel-16 (Release 16) Rel-17 (Release 17) Rel-18 (Release 18)* | |
|  |  | | | | | | | | | |
| ***Reason for change:*** | | The AVP of WLAN Location Information is specified with "Access-Network-Information"by mistake. It should be "Access-Network-Info". | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | Correct the AVP name: "Access-Network-Information" to "Access-Network-Info". | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | Incorrect AVP name. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 4.1.2.1.1, 7.1.2.1.1, 7.1.2.2.1 | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **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:*** | |  | | | | | | | | |

\* \* \* First Change \* \* \* \*

##### 4.1.2.1.1 General

This procedure follows the STa Authentication and Authorization procedure, with the following differences:

- Information elements that would reflect information about the user's service request and about the access network are not included or are optional in the authentication and authorization request.

- The information elements that describe the user's subscription profile are not downloaded to the non-3GPP access network.

NOTE: The information elements related to the IP Mobility Mode Selection function are not supported over this interface.

Table 4.1.2.1/1: SWa Authentication and Authorization Request

|  |  |  |  |
| --- | --- | --- | --- |
| Information element name | Mapping to Diameter AVP | Cat. | Description |
| User Identity | User-Name | M | This information element shall contain the identity of the user. The identity shall be represented in NAI form as specified in the IETF RFC 4282 [15] and shall be formatted as defined in clause 19 of 3GPP TS 23.003 [14]. This IE shall include the leading digit used to differentiate between authentication schemes. |
| EAP payload | EAP-payload | M | This IE shall contain the Encapsulated EAP payload used for the UE – 3GPP AAA Server mutual authentication |
| Authentication Request Type | Auth-Request-Type | M | This IE shall define whether the user is to be authenticated only, authorized only or both. AUTHORIZE\_AUTHENTICATE shall be used in this case. |
| UE Layer-2 address | Calling-Station-ID | M | This IE shall carry the Layer-2 address of the UE. |
| Access Type | RAT-Type | C | If present, this IE shall contain the untrusted non-3GPP access network technology type that is serving the UE. |
| Access Network Identity | ANID | O | If present, this IE shall contain the access network identifier used for key derivation at the HSS. (See 3GPP TS 24.302 [26] for all possible values)  It shall be included if the non-3GPP access network selects the EAP-AKA' authentication method. |
| Full Name for Network | Full-Network-Name | O | If present, this IE shall contain the full name for network as specified in 3GPP TS 24.302 [26]. This AVP may be inserted by the non-3GPP access network depending on its local policy and only when it is not connected to the UE's Home Network |
| Short Name for Network | Short-Network-Name | O | If present, this IE shall contain the short name for network as specified in 3GPP TS 24.302 [26]. This AVP may be inserted by the non-3GPP access network depending on its local policy and only when it is not connected to the UE's Home Network |
| Transport Access Type | Transport-Access-Type | C | For interworking with Fixed Broadband access networks (see 3GPP TS 23.139 [39]), if the access network needs to receive the IMSI of the UE in the authentication response, then this information element shall be present, and it shall contain the value "BBF" (see clause 5.2.3.19). |
| Supported Features  (See 3GPP TS 29.229 [24]) | Supported-Features | O | If present, this information element shall contain the list of features supported by the origin host for the lifetime of the Diameter session. |
| AAA Failure Indication | AAA-Failure-Indication | O | If present, this information element shall indicate that the request is sent after the non-3GPP access network has determined that a previously assigned 3GPP AAA Server is unavailable. |
| WLAN Location Information | Access-Network-Info | O | If present, this IE shall contain the location information of the WLAN Access Network where the UE is attached. |
| WLAN Location Timestamp | User-Location-Info-Time | O | This IE may be present if the WLAN Location Information IE is present.  When present, this IE shall contain the NTP time at which the UE was last known to be in the location reported in the WLAN Location Information. |

Table 4.1.2.1/2: SWa Authentication and Authorization Answer

|  |  |  |  |
| --- | --- | --- | --- |
| Information element name | Mapping to Diameter AVP | Cat. | Description |
| User Identity | User-Name | M | This information element shall contain the identity of the user. The identity shall be represented in NAI form as specified in IETF RFC 4282 [15] and shall be formatted as defined in clause 19 of 3GPP TS 23.003 [14]. This IE shall include the leading digit used to differentiate between authentication schemes. |
| EAP payload | EAP payload | M | This IE shall contain the Encapsulated EAP payload used for UE- 3GPP AAA Server mutual authentication. |
| Authentication Request Type | Auth-Request-Type | M | It shall contain the value AUTHORIZE\_AUTHENTICATE. See IETF RFC 4072 [5]. |
| Result code | Result-Code /  Experimental- Result | M | This IE shall contain the result of the operation. Result codes are as in Diameter base protocol (see IETF RFC 6733 [58]). Experimental-Result AVP shall be used for SWa errors. This is a grouped AVP which shall contain the 3GPP Vendor ID in the Vendor-Id AVP, and the error code in the Experimental-Result-Code AVP. |
| Session Alive Time | Session-Timeout | O | This AVP may be present if the Result-Code AVP is set to DIAMETER \_SUCCESS. If present, it shall contain the maximum number of seconds the user session is allowed to remain active. |
| Accounting Interim Interval | Accounting Interim-Interval | O | If present, this IE shall contain the Charging duration |
| Pairwise Master Key | EAP-Master-Session-Key | C | This IE shall be present if the Result-Code AVP is set to DIAMETER\_SUCCESS. |
| 3GPP AAA Server URI | Redirect-Host | C | This information element shall be present if the Result-Code value is set to DIAMETER\_REDIRECT\_INDICATION. When the user has previously been authenticated by another 3GPP AAA Server, it shall contain the Diameter URI of the 3GPP AAA Server currently serving the user. The node receiving this IE shall behave as defined in the Diameter base protocol (see IETF RFC 6733 [58]). The command shall contain zero or more occurrences of this information element. When choosing a destination for the redirected message from multiple Redirect-Host AVPs, the receiver shall send the Diameter request to the first 3GPP AAA Server in the ordered list received in the Diameter response. If no successful response to the Diameter request is received, the receiver shall send the Diameter request to the next 3GPP AAA Server in the ordered list. This procedure shall be repeated until a successful response is received from a 3GPP AAA Server. |
| Trust Relationship Indicator | AN-Trusted | M | This AVP shall contain the 3GPP AAA Server's decision on handling the non-3GPP access network, i.e. trusted or untrusted. For the SWa case, the value "UNTRUSTED" shall be used. |
| Supported Features  (See 3GPP TS 29.229 [24]) | Supported-Features | O | If present, this information element shall contain the list of features supported by the origin host for the lifetime of the Diameter session. |
| Permanent User Identity | Mobile-Node-Identifier | C | This information element shall only be sent if the Result-Code AVP is set to DIAMETER\_SUCCESS and if the Transport Access Type in the request command indicated that the UE is accessing the EPC from a Fixed Broadband access network (i.e., the Transport-Access-Type AVP takes the value "BBF"); it shall contain an AAA/HSS assigned permanent user identity (i.e. an IMSI in root NAI format as defined in clause 19 of 3GPP TS 23.003 [14]) to be used by the non-3GPP access network in subsequent PCC procedure for identifying the user in the EPS network. This IE shall not include the leading digit prepended in front of the IMSI used to differentiate between authentication schemes. |

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

##### 7.1.2.1.1 General

The authentication and authorization procedure shall be used between the ePDG and 3GPP AAA Server/Proxy. When a PDN connection is activated by the UE an IKEv2 exchange shall be initiated. It shall be invoked by the ePDG, on receipt from the UE of a "tunnel establishment request" message. This shall take the form of forwarding an IKEv2 exchange with the purpose of authenticating in order to set up an IKE Security Association (SA) between the UE and the ePDG.

During the Access Authentication and Authorization procedure the ePDG may provide information on its PMIPv6 or GTPv2 capabilities to the 3GPP AAA Server. The 3GPP AAA Server may perform IP mobility mode selection between NBM or HBM as specified in clause 4.1.3.2 of 3GPP TS 23.402 [3]. The 3GPP AAA Server may provide to the ePDG an indication if either NBM or local IP address assignment shall be used. If NBM shall be used, the ePDG then decides the S2b protocol variant to use.

The User-Name AVP may contain a decorated NAI (as defined in clause 19.3.3 of 3GPP TS 23.003 [14]). In this case the 3GPP AAA Proxy shall process the decorated NAI and support routing of the Diameter request messages based on the decorated NAI as described in IETF RFC 5729 [37].

Upon a successful authorization, when NBM is used, the 3GPP AAA server shall return NBM related information back to the ePDG. This information may include the assigned PDN GW, UE IPv6 HNP and/or UE IPv4-HoA.

Upon a successful authorization, when DSMIPv6 is used, to enable HA address discovery based on IKEv2 (see TS 24.303 [13]), the 3GPP AAA server may also download PDN GW identity to the ePDG.

The PDN GW identity is a FQDN and/or IP address of the PDN GW. If a FQDN is provided, the ePDG shall derive it to IP address according to the selected mobility management protocol.

If DSMIPv6 is used, a single IKE SA is used for all PDN connections of the user. If PMIPv6 or GTPv2 is used, a separate IKE SA is created for each PDN connection of the user (refer to 3GPP TS 24.302 [26]).

Each new additional IKE SA shall be handled in a different Diameter session. In such cases, the IP mobility mode selected during the first authentication and authorization procedure is valid for all PDN connections of the user, therefore, dynamic IP mobility mode selection is not executed during the further procedures. The ePDG may select the same or different S2b protocol variant(s) towards different PDN GWs when NBM has been selected.

Based on local policies, EPC access for emergency services over an untrusted WLAN access is supported as specified in clause 4.5.7.2.1 of 3GPP TS 23.402 [3] for:

- UEs with a valid EPC subscription that are authenticated and authorized for EPC services;

- UEs that are authenticated only;

- UEs with an unauthenticated IMSI; and/or

- UICC-less UEs.

The SWm reference point shall perform authentication and authorization based on the reuse of the DER/DEA command set defined in Diameter EAP application, IETF RFC 4072 [5].

Table 7.1.2.1.1/1: Authentication and Authorization Request

|  |  |  |  |
| --- | --- | --- | --- |
| Information element name | Mapping to Diameter AVP | Cat. | Description |
| User Identity | User-Name | M | This information element shall contain the identity of the user. The identity shall be represented in NAI form as specified in IETF RFC 4282 [15] and shall be formatted as defined in clause 19 of 3GPP TS 23.003 [14]. This IE shall include the leading digit used to differentiate between authentication schemes, if it contains a NAI other than an Emergency NAI for Limited Service State. |
| EAP payload | EAP-Payload | M | This information element shall contain the encapsulated EAP payload used for the UE - 3GPP AAA Server mutual authentication |
| Authentication Request Type | Auth-Request- Type | M | This information element shall indicate whether the user is to be authenticated only, authorized only or both. It shall have the value of AUTHORIZE\_AUTHENTICATE. |
| APN | Service-Selection | C | This information element shall contain the Network Identifier part of the APN for which the UE is requesting authorization. This AVP shall be present if the ePDG has received an APN from the UE and the UE did not indicate the establishment of an emergency session in the IKEv2 signalling. This AVP shall be absent if the UE indicated the establishment of an emergency session during the IKEv2 tunnel establishment (see clause 7.2.5 of 3GPP TS 24.302 [26]). |
| Visited Network Identifier (See 9.2.3.1.2) | Visited-Network-Identifier | C | This information element shall contain the identifier that allows the home network to identify the Visited Network.  This AVP shall be present if the ePDG is not in the UE's home network i.e. the UE is roaming. |
| Access Type | RAT-Type | C | This information element shall be present if the access type is known by the ePDG. If present, it shall contain the non-3GPP access network access technology type that is serving the UE. When not known by the ePDG, this information element should be present and, in that case, it shall take the value VIRTUAL (1). |
| Mobility features | MIP6-Feature-Vector | O | This AVP shall be present, if the handling of any of the flags listed here requires dynamic (i.e. per user) handling for the VPLMN-HPLMN relation of the ePDG and 3GPP AAA Server. If present, the AVP shall contain the mobility features supported by the ePDG. Flags that are not relevant in the actual relation shall be set to zero.  If dynamic IP mobility mode selection is used, the PMIP6\_SUPPORTED flag and/or the GTPv2\_SUPPORTED flag shall be set by the ePDG if PMIPv6 and/or GTPv2 are supported. PMIP6\_SUPPORTED flag is defined in IETF RFC 5779 [2].  The MIP6\_INTEGRATED flag shall be used to indicate to the 3GPP AAA server that the ePDG supports IKEv2 based Home Agent address discovery. |
| AAA Failure Indication | AAA-Failure-Indication | O | If present, this information element shall indicate that the request is sent after the ePDG has determined that a previously assigned 3GPP AAA Server is unavailable. |
| Supported Features  (See 3GPP TS 29.229 [24]) | Supported-Features | O | If present, this information element shall contain the list of features supported by the origin host for the lifetime of the Diameter session. |
| UE local IP address | UE-Local-IP-Address | O | The ePDG shall include this IE based on local policy for Fixed Broadband access network interworking as specified in 3GPP TS 23.139 [39].  The ePDG may also include this IE, regardless of Fixed Broadband access network interworking.  If present, it shall contain the source IPv4 or IPv6 address of the IKE\_SA\_AUTH message from the UE. |
| Terminal Information | Terminal-Information | C | The ePDG shall include this IE and set it to the user's Mobile Equipment Identity, if this information is available.  For an untrusted WLAN access, this grouped AVP shall contain the IMEI AVP and, if available, the Software-Version AVP.  When the RAT type is not known by the ePDG, but the UE has provided the IMEI(SV), this grouped AVP shall contain the IMEI AVP and, if available, the Software-Version AVP. |
| Emergency Services | Emergency-Services | C | An ePDG which supports emergency services shall include this information element, with the Emergency-Indication bit set, if the UE indicated the establishment of an emergency session during the IKEv2 tunnel establishment (see clause 7.2.5 of 3GPP TS 24.302 [26]). |

Table 7.1.2.1.1/2: Authentication and Authorization Answer

|  |  |  |  |
| --- | --- | --- | --- |
| Information element name | Mapping to Diameter AVP | Cat. | Description |
| User Identity | User-Name | O | This information element, if present, shall contain the identity of the user. The identity shall be represented in NAI form as specified in IETF RFC 4282 [15] and shall be formatted as defined in clause 19 of 3GPP TS 23.003 [14]. This IE shall include the leading digit used to differentiate between authentication schemes, if it contains a NAI other than an Emergency NAI for Limited Service State. |
| EAP payload | EAP-Payload | O | If present, this information element shall contain the encapsulated EAP payload used for UE - 3GPP AAA Server mutual authentication |
| Master-Session-Key | EAP-Master-Session-Key | C | This IE shall contain keying material for protecting the communication between the user and the ePDG. It shall be present when Result Code is set to DIAMETER\_SUCCESS. |
| Authentication Request Type | Auth-Request-Type | M | It shall contain the value AUTHORIZE\_AUTHENTICATE. See IETF RFC 4072 [5]. |
| Result code | Result-Code / Experimental-Result-Code | M | This IE shall contain the result of the operation.  The Result-Code AVP shall be used for errors defined in the Diameter base protocol (see IETF RFC 6733 [58]) or as per in NASREQ (see IETF RFC 4005 [4]. |
| 3GPP AAA Server URI | Redirect-Host | C | This information element shall be sent if the Result-Code value is set to DIAMETER\_REDIRECT\_INDICATION. When the user has previously been authenticated by another 3GPP AAA Server, it shall contain the Diameter URI of the 3GPP AAA Server currently serving the user. The node receiving this IE shall behave as defined in the Diameter base protocol (see IETF RFC 6733 [58]). The command shall contain zero or more occurrences of this information element. When choosing a destination for the redirected message from multiple Redirect-Host AVPs, the receiver shall send the Diameter request to the first 3GPP AAA Server in the ordered list received in the Diameter response. If no successful response to the Diameter request is received, the receiver shall send the Diameter request to the next 3GPP AAA Server in the ordered list. This procedure shall be repeated until a successful response is received from a 3GPP AAA Server. |
| Mobility Capabilities | MIP6-Feature-Vector | O | This AVP shall be present if it was received in the authentication and authorization request and the authentication and authorization succeeded. It shall contain the authorized mobility features. Flags that are not relevant in the actual relation shall be set to zero.  The PMIP6\_SUPPORTED flag and/or the GTPv2\_SUPPORTED flag shall be set to indicate that NBM (PMIPv6 or GTPv2) is to be used. The ASSIGN\_LOCAL\_IP flag shall be set to indicate that a local IP address is to be assigned.  The MIP6\_INTEGRATED flag shall be set if a Home Agent address is provided for IKEv2 based Home Agent address discovery. In the latter case HA information for IKEv2 discovery is provided via the APN-Configuration AVP. |
| APN-OI replacement | APN-OI-Replacement | C | This AVP shall indicate the domain name to replace the APN-OI in the non-roaming case or in the home routed roaming case when constructing the PDN GW FQDN upon which it needs to perform a DNS resolution. See 3GPP TS 23.003 [3]. It shall only be included if NBM is used, the Emergency-Indication bit of the Emergency-Services AVP is not set in the Authentication and Authorization Request and the Result-Code AVP is set to DIAMETER\_SUCCESS. |
| APN and PGW Data | APN-Configuration | C | This information element shall only be sent if the Result-Code AVP is set to DIAMETER\_SUCCESS and the Emergency-Indication bit of the Emergency-Services AVP is not set in the Authentication and Authorization Request.  The APN-Configuration is a grouped AVP, defined in 3GPP TS 29.272 [29]. When NBM is used, the following information elements per APN may be included:  - APN  - APN-AMBR  - Authorized 3GPP QoS Profile  - User home IP Address (if static IPv4 and/or IPv6 is allocated to the UE's subscribed APN)  - Allowed PDN types  - PDN GW identity (if the PDN connection was active in case of HO, or if there is a static PDN GW allocated to the UE's subscribed APN)  - PDN GW allocation type  - VPLMN Dynamic Address Allowed  - Visited Network Identifier  - Interworking-5GS-Indicator  When local IP address assignment is used, this AVP shall only be present if IKEv2 based Home Agent discovery is used and  - if the PDN connection was active in case of HO, or  - if there is static PDN GW allocated to the UE's subscribed APN, or  - if the 3GPP AAA Server/Proxy selects the PDN GW based on the identity of the ePDG  In these cases, the following information elements shall be included:  - HA-APN (Home Agent APN as defined in 3GPP TS 23.003 [14])  - PDN GW identity  NOTE 1. |
| Trace information | Trace-Info | C | This AVP shall be included if the subscriber and equipment trace has been activated for the user in the HSS and signalling based activation is used to download the trace activation from the HSS to the ePDG.  Only the Trace-Data AVP shall be included to the Trace-Info AVP and  shall contain the following AVPs:  - Trace-Reference  - Trace-Depth  - Trace-Event-List, for PGW  - Trace-Collection-Entity  The following AVPs may also be included in the Trace-Data AVP:  - Trace-Interface-List, for PGW, if this AVP is not present, trace report generation is requested for all interfaces for PGW listed in 3GPP TS 32.422 [32]  - Trace-NE-Type-List, with the only allowed value being "PDN GW". If this AVP is not included, trace activation in PDN GW is required. |
| MSISDN | Subscription-ID | C | This AVP shall contain the MSISDN of the UE and shall be sent only if it is available. |
| Session time | Session-Timeout | C | If the authorization succeeded, then this IE shall contain the time this authorization is valid for. |
| Permanent User Identity | Mobile-Node-Identifier | C | This information element shall be present if NBM is used.  If the user is authenticated, it shall contain an AAA/HSS assigned permanent user identity (i.e. IMSI in root NAI format as defined in clause 19 of 3GPP TS 23.003 [14]) to be used by:  - the MAG in subsequent PBUs as the MN-ID identifying the user in the EPS network for PMIP based S2b,  - by the ePDG to derive the IMSI to send in subsequent Create Session Request for GTP based S2b.  For an emergency PDN connection, if the UE is UICC-less (i.e. the User Identity IE in the request contains an IMEI) or if the IMSI is not authenticated, the Permanent User Identity shall contain the IMEI in Emergency NAI for Limited Service State format as defined in clause 19 of 3GPP TS 23.003 [14].  If this IE contains an identity based on IMSI, this IE shall not include the leading digit prepended in front of the IMSI used to differentiate between authentication schemes. |
| Serving GW Address | MIP6-Agent-Info | O | This AVP shall be used only in chained S2b-S8 cases and it shall be sent only if the Result-Code AVP is set to DIAMETER\_SUCCESS. |
| UE Charging Data | 3GPP-Charging-Characteristics | O | This information element contains the type of charging method to be applied to the user (see 3GPP TS 29.061 [31]). |
| Supported Features  (See 3GPP TS 29.229 [24]) | Supported-Features | O | If present, this information element shall contain the list of features supported by the origin host for the lifetime of the Diameter session. |
| WLAN Location Information | Access-Network-Info | O | If present, this IE shall contain the location information of the WLAN Access Network where the UE is attached. |
| WLAN Location Timestamp | User-Location-Info-Time | C | This IE should be present if the WLAN Location Information IE is present.  When present, this IE shall contain the NTP time at which the UE was last known to be in the location reported in the WLAN Location Information. |
| Emergency Info | Emergency-Info | C | This IE shall only be present if the Result-Code AVP is set to DIAMETER\_SUCCESS. When present, it shall contain the identity of the dynamically allocated PDN-GW used for the establishment of emergency PDN connections. It shall be present for a non-roaming authenticated user, if this information was received from the HSS and if the Emergency-Services AVP is present, with the Emergency-Indication bit set, in the Authentication and Authorization Request. |
| UE Usage Type | UE-Usage-Type | C | This IE shall be present if this information is available in the user subscription. When present, this IE shall contain the UE Usage Type of the subscriber. |
| Core Network Restrictions | Core-Network-Restrictions | C | This IE shall be present if this information is available in the user subscription. When present, this IE shall contain the Core Network Restrictions of the subscriber. |
| NOTE 1: If a static PDN GW allocated to the UE's subscribed APN has been received from the HSS, the 3GPP AAA Server/Proxy shall only provide the static PDN GW identity in the Authentication and Authorization Answer. | | | |

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

##### 7.1.2.2.1 General

This procedure shall be used between the ePDG and 3GPP AAA Server and Proxy. It shall be invoked by the ePDG, upon receipt of a valid Re-Authorization Request message from the 3GPP AAA Server (see clause 7.1.2.5). It may also be initiated by the ePDG, when the ePDG detects a change of the outer IP address of the UE, to:

- update the 3GPP AAA Server with the new UE local IP address; and

- retrieve the most up to date WLAN Location Information stored at the 3GPP AAA Server, when the 3GPP AAA server has sent WLAN Location Information during the initial Authentication and Authorization procedure (see clause 4.5.7.2.8 of 3GPP TS 23.402 [3]).

This procedure shall be used by the ePDG to update the previously provided authorization parameters. This may happen due to a modification of the subscriber profile in the HSS (for example, removal of a specific APN associated with the subscriber, or change of the identity of a dynamically allocated PDN GW, see clause 8.1.2.3).

This procedure is mapped to the Diameter command codes AA-Request (AAR) and AA-Answer (AAA) specified in RFC 4005 [4]. Information element contents for these messages are shown in tables 7.1.2.2.1/1 and 7.1.2.2.1/2.

Table 7.1.2.2.1/1: SWm Authorization Request

|  |  |  |  |
| --- | --- | --- | --- |
| Information element name | Mapping to Diameter AVP | Cat. | Description |
| Permanent User Identity | User-Name | M | This information element shall contain the permanent identity of the user. The identity shall be represented in NAI form as specified in IETF RFC 4282 [15] and shall be formatted as defined in clause 19 of 3GPP TS 23.003 [14]. If this IE contains an identity based on IMSI, this IE shall not include the leading digit prepended in front of the IMSI used to differentiate between authentication schemes. |
| Request Type | Auth-Request -Type | M | This information element shall contain the type of request. It shall have the value AUTHORIZE\_ONLY. |
| AAR Flags | AAR-Flags | O | This IE contains a bit mask. See 7.2.3.5 for the meaning of the bits.  This IE may be present and indicate that the ePDG requests to retrieve the most up to date WLAN Location Information of the UE, if the ePDG received the WLAN Location Information during the initial Authentication and Authorization procedure. |
| UE local IP address | UE-Local-IP-Address | C | This IE shall be present if the ePDG provided the UE Local IP address in the initial Authentication and Authorization Request and the UE Local IP address has changed. |

Table 7.1.2.2.1/2: SWm Authorization Answer

|  |  |  |  |
| --- | --- | --- | --- |
| Information element name | Mapping to Diameter AVP | Cat. | Description |
| Permanent User Identity | User-Name | M | This information element shall contain the permanent identity of the user. The identity shall be represented in NAI form as specified in IETF RFC 4282 [15], and shall be formatted as defined in clause 19 of 3GPP TS 23.003 [14]. If this IE contains an identity based on IMSI, this IE shall not include the leading digit prepended in front of the IMSI used to differentiate between authentication schemes. |
| Request Type | Auth-Request -Type | M | It shall contain the value AUTHORIZE\_ONLY. See IETF RFC 4072 [5]. |
| Registration Result | Result-Code/ Experimental Result Code | M | This IE shall contain the result of the operation.  The Result-Code AVP shall be used for errors defined in the Diameter base protocol (see IETF RFC 6733 [58]) or as per in NASREQ (see IETF RFC 4005 [4]). |
| UE IPv4 Home Address | PMIP6-IPv4-Home-Address | O | If the authorization succeeded, and the user has an IPv4-HoA statically defined as part of his profile data, then this IE may be present. It shall contain the IPv4-HoA allocated and assigned to the UE. |
| APN-OI replacement | APN-OI-Replacement | C | This AVP shall indicate the domain name to replace the APN-OI in the non-roaming case or in the home routed roaming case when constructing the PDN GW FQDN upon which it needs to perform a DNS resolution. See 3GPP TS 23.003 [3]. It shall only be included if NBM is used, the Emergency-Indication bit of the Emergency-Services AVP was not set in the initial Authentication and Authorization Request, and the Result-Code AVP is set to DIAMETER\_SUCCESS. |
| APN and PGW Data | APN-Configuration | C | This information element shall only be sent if the Result-Code AVP is set to DIAMETER\_SUCCESS and the Emergency-Indication bit of the Emergency-Services AVP was not set in the initial Authentication and Authorization Request.  APN-Configuration is a grouped AVP, defined in 3GPP TS 29.272 [29]. When NBM is used, the following information elements per APN may be included:  - APN  - APN-AMBR  - Authorized 3GPP QoS profile  - Statically allocated User IP Address (IPv4 and/or IPv6)  - Allowed PDN types  - PDN GW identity  - PDN GW allocation type  - VPLMN Dynamic Address Allowed  - Visited Network Identifier  When local IP address assignment is used, this AVP shall only be present if IKEv2 based Home Agent discovery is used and  - if the PDN connection was active in case of HO, or  - if there is static PDN GW allocated to the UE's subscribed APN.  In these cases, the following information elements shall be included:  - HA-APN (Home Agent APN as defined in 3GPP TS 23.003 [14])  - PDN GW identity |
| Trace information | Trace-Info | C | This AVP shall be included if the subscriber and equipment trace has been activated for the user in the HSS and signalling based activation is used to download the trace activation from the HSS to the ePDG.  Only the Trace-Data AVP shall be included if trace activation is requested. Only the Trace-Reference AVP shall be included if trace deactivation is requested.  If the Trace-Data AVP is included, it shall contain the following AVPs:  - Trace-Reference  - Trace-Depth  - Trace-Event-List, for PGW  - Trace-Collection-Entity  The following AVPs may also be included in the Trace-Data AVP:  - Trace-Interface-List, for PGW, if this AVP is not present, trace report generation is requested for all interfaces for PGW listed in 3GPP TS 32.422 [32]  - Trace-NE-Type-List, with the only allowed value being "PDN GW". If this AVP is not included, trace activation in PDN GW is required. |
| MSISDN | Subscription-ID | C | This AVP shall contain the MSISDN of the UE and shall be sent only if it is available. |
| UE Charging Data | 3GPP-Charging-Characteristics | O | If present, this information element shall contain the type of charging method to be applied to the user (see 3GPP TS 29.061 [31]). |
| Session time | Session-Timeout | C | If the authorization succeeded, then this IE shall contain the time this authorization is valid for. |
| WLAN Location Information | Access-Network-Info | O | If present, this IE shall contain the location information of the WLAN Access Network where the UE is attached. |
| WLAN Location Timestamp | User-Location-Info-Time | C | This IE should be present if the WLAN Location Information IE is present.  When present, this IE shall contain the NTP time at which the UE was last known to be in the location reported in the WLAN Location Information. |

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