**3GPP TSG-CT WG1 Meeting #124-eC1-** **203535**

**Electronic meeting, 2-10 June 2020**

|  |
| --- |
| *CR-Form-v12.0* |
| **CHANGE REQUEST** |
|  |
|  | **24.301** | **CR** | **3404** | **rev** | **-** | **Current version:** | **16.4.0** |  |
|  |
| *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:***  | Provisioning of DNS server security information to the UE |
|  |  |
| ***Source to WG:*** | Samsung |
| ***Source to TSG:*** | C1 |
|  |  |
| ***Work item code:*** | 5GProtoc616 |  | ***Date:*** | 2020-05-24 |
|  |  |  |  |  |
| ***Category:*** | **B** |  | ***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-12 (Release 12)**Rel-13 (Release 13)Rel-14 (Release 14)Rel-15 (Release 15)Rel-16 (Release 16)* |
|  |  |
| ***Reason for change:*** | This CR implements the highlighted requirement captured in SA3 CR .*X.2 Security aspects of DNS**It is recommended that the UE and DNS server(s) support DNS over (D)TLS as specified in RFC 7858 [xx] and RFC 8310 [yy]. The DNS server(s) that are deployed within the 3GPP network can enforce the use of DNS over (D)TLS. The UE can be pre-configured with the DNS server security information (out-of-band configurations specified in the IETF RFCs like, credentials to authenticate the DNS server, supported security mechanisms, port number, etc.), or the core network can configure the DNS server security information to the UE.* |
|  |  |
| ***Summary of change:*** | Define a protocol container in ePCO to transfer the DNS server security information. |
|  |  |
| ***Consequences if not approved:*** | SA3 requirement will not be fullfiled. |
|  |  |
| ***Clauses affected:*** | 6.4.1.3 and 6.5.1.2 |
|  |  |
|  | **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:*** |  |

#### 6.4.1.3 Default EPS bearer context activation accepted by the UE

Upon receipt of the ACTIVATE DEFAULT EPS BEARER CONTEXT REQUEST message, if the UE provided an APN for the establishment of the PDN connection, the UE shall stop timer T3396 if it is running for the APN provided by the UE. If the UE did not provide an APN for the establishment of the PDN connection and the request type was different from "emergency" and from "handover of emergency bearer services", the UE shall stop the timer T3396 associated with no APN if it is running. If the ACTIVATE DEFAULT EPS BEARER CONTEXT REQUEST message was received in response to a request for an emergency PDN connection, the UE shall not stop the timer T3396 associated with no APN if it is running. For any case, the UE shall then send an ACTIVATE DEFAULT EPS BEARER CONTEXT ACCEPT message and enter the state BEARER CONTEXT ACTIVE. When the default bearer is activated as part of the attach procedure, the UE shall send the ACTIVATE DEFAULT EPS BEARER CONTEXT ACCEPT message together with ATTACH COMPLETE message. When the default bearer is activated as the response to the stand-alone PDN CONNECTIVITY REQUEST message, the UE shall send the ACTIVATE DEFAULT EPS BEARER CONTEXT ACCEPT message alone.

If a WLAN offload indication information element is included in the ACTIVATE DEFAULT EPS BEARER CONTEXT REQUEST message, the UE shall store the WLAN offload acceptability values for this PDN connection and use the E-UTRAN offload acceptability value to determine whether this PDN connection is offloadable to WLAN or not.

The UE checks the PTI in the ACTIVATE DEFAULT EPS BEARER CONTEXT REQUEST message to identify the UE requested PDN connectivity procedure to which the default bearer context activation is related (see subclause 6.5.1).

If the UE receives a serving PLMN rate control IE in the ACTIVATE DEFAULT EPS BEARER CONTEXT REQUEST message, the UE shall store the serving PLMN rate control IE value and use the stored serving PLMN rate control value as the maximum allowed limit of uplink User data container IEs included in ESM DATA TRANSPORT messages for the corresponding PDN connection in accordance with 3GPP TS 23.401 [10].

If the UE receives an APN rate control parameters container in the protocol configuration options IE or extended protocol configuration options IE in the ACTIVATE DEFAULT EPS BEARER CONTEXT REQUEST message, the UE shall store the APN rate control parameters value and use the stored APN rate control parameters value as the maximum allowed limit of uplink user data related to the APN indicated in the ACTIVATE DEFAULT EPS BEARER CONTEXT REQUEST message in accordance with 3GPP TS 23.401 [10]. If the UE has a previously stored APN rate control parameters value for this APN, the UE shall replace the stored APN rate control parameters value for this APN with the received APN rate control parameters value.

If the UE receives an additional APN rate control parameters for exception data container in the protocol configuration options IE or extended protocol configuration options IE in the ACTIVATE DEFAULT EPS BEARER CONTEXT REQUEST message, the UE shall store the additional APN rate control parameters for exception data value and use the stored additional APN rate control parameters for exception data value as the maximum allowed limit of uplink exception data related to the APN indicated in the ACTIVATE DEFAULT EPS BEARER CONTEXT REQUEST message in accordance with 3GPP TS 23.401 [10]. If the UE has a previously stored additional APN rate control parameters for exception data value for this APN, the UE shall replace the stored additional APN rate control parameters for exception data value for this APN with the received additional APN rate control parameters for exception data value.

If the UE receives a small data rate control parameters container in the protocol configuration options IE or the extended protocol configuration options IE in the ACTIVATE DEFAULT EPS BEARER CONTEXT REQUEST message, the UE shall store the small data rate control parameters value and use the stored small data rate control parameters value as the maximum allowed limit of uplink user data for the corresponding PDU session that becomes transferred after inter-system change from S1 mode to N1 mode in accordance with 3GPP TS 23.501 [8].

If the UE receives an additional small data rate control parameters for exception data container in the protocol configuration options IE or the extended protocol configuration options IE in the ACTIVATE DEFAULT EPS BEARER CONTEXT REQUEST message, the UE shall store the additional small data rate control parameters for exception data value and use the stored additional small data rate control parameters for exception data value as the maximum allowed limit of uplink exception data for the corresponding PDU session that becomes transferred after inter-system change from S1 mode to N1 mode in accordance with 3GPP TS 23.501 [8].

If the UE receives non-IP Link MTU parameter, Ethernet Frame Payload MTU parameter, or IPv4 Link MTU parameter of the protocol configuration options IE or of the extended protocol configuration options IE in the ACTIVATE DEFAULT EPS BEARER CONTEXT REQUEST message, the UE shall pass the received Non-IP Link MTU, Ethernet Frame Payload MTU size, or IPv4 Link MTU to the upper layer.

NOTE 1: The Non-IP Link MTU and the IPv4 Link MTU size correspond to the maximum length of user data that can be sent either in the user data container in the ESM DATA TRANSPORT message or via S1-U interface.

NOTE 2: The Ethernet frame payload MTU size corresponds to the maximum length of a payload of an Ethernet frame that can be sent either in the user data container in the ESM DATA TRANSPORT message or via S1-U interface.

If the network wants to enforce the use of DNS over (D)TLS, the network shall include the extended protocol configuration options IE in the ACTIVATE DEFAULT EPS BEARER CONTEXT REQUEST message and include the DNS server security information. Upon receiving the DNS server security information, the UE shall pass it to the upper layer. The UE shall use this information to send the DNS over (D)TLS (See 3GPP TS 33.401 [19] ).

NOTE 3: Support of DNS over (D) TLS is based on the informative requirements as specified in 3GPP TS 33.401 [19] and hence it has no normative enforcement to be implemented.

Upon receipt of the ACTIVATE DEFAULT EPS BEARER CONTEXT ACCEPT message, the MME shall enter the state BEARER CONTEXT ACTIVE and stop the timer T3485, if the timer is running. If the PDN CONNECTIVITY REQUEST message included a low priority indicator set to "MS is configured for NAS signalling low priority", the MME shall store the NAS signalling low priority indication within the default EPS bearer context.

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

#### 6.5.1.2 UE requested PDN connectivity procedure initiation

In order to request connectivity to a PDN, the UE shall send a PDN CONNECTIVITY REQUEST message to the MME, start timer T3482 and enter the state PROCEDURE TRANSACTION PENDING (see example in figure 6.5.1.2.1).

When the PDN CONNECTIVITY REQUEST message is sent together with an ATTACH REQUEST message, the UE shall not start timer T3482 and shall not include the APN.

NOTE 1: If the UE needs to provide protocol configuration options which require ciphering or provide an APN, or both, during the attach procedure, the ESM information transfer flag is included in the PDN CONNECTIVITY REQUEST. The MME then at a later stage in the PDN connectivity procedure initiates the ESM information request procedure in which the UE can provide the MME with protocol configuration options or APN or both.

In order to request a PDN connection for emergency bearer services or for access to RLOS, the UE shall not include an APN in the PDN CONNECTIVITY REQUEST message or, when applicable, in the ESM INFORMATION RESPONSE message.

In order to request connectivity to a PDN using the default APN, the UE includes the access point name IE in the PDN CONNECTIVITY REQUEST message or, when applicable, in the ESM INFORMATION RESPONSE message, according to the following conditions:

- if use of a PDN using the default APN requires PAP/CHAP, then the UE should include the Access point name IE; and

- in all other conditions, the UE need not include the Access point name IE.

In order to request connectivity to an additional PDN using a specific APN, the UE shall include the requested APN in the PDN CONNECTIVITY REQUEST message.

In the PDN type IE the UE shall either indicate the IP version capability of the IP stack associated with the UE or non IP or Ethernet as specified in subclause 6.2.2.

If the PDN type value of the PDN type IE is set to IPv4 or IPv6 or IPv4v6 and the UE indicates "Control plane CIoT EPS optimization supported" in the UE network capability IE of the ATTACH REQUEST message, the UE may include the Header compression configuration IE in the PDN CONNECTIVITY REQUEST message.

The UE shall set the request type to "initial request" when the UE is establishing a new PDN connectivity to a PDN in an attach procedure or in a stand-alone PDN connectivity procedure or when the UE is a 5G-RG and requests establishment of a PDN connection as a user-plane resource of an MA PDU session to be established. The UE shall set the request type to "emergency" when the UE is requesting a new PDN connectivity for emergency bearer services. The UE shall set the request type to "handover" when the connectivity to a PDN is to be transferred from a non-3GPP access network to the 3GPP access network, when the UE initiates the procedure to add 3GPP access to the PDN connection which is already established over WLAN, when the UE supporting N1 mode requests transfer of an existing non-emergency PDU session in 5GS or when the UE is a 5G-RG and requests establishment of a PDN connection as a user-plane resource of an already established MA PDU session. The UE shall set the request type to "handover of emergency bearer services" when a PDN connection for emergency bearer services is to be transferred from a WLAN to the 3GPP access network or when the UE supporting N1 mode requests transfer of an existing emergency PDU session in 5GS. The UE shall set the request type to "RLOS" when the UE is requesting a new PDN connection for RLOS.

If the UE supports DSMIPv6, the UE may include a request for obtaining the IPv6 address and optionally the IPv4 address of the home agent in the Protocol configuration options IE in the PDN CONNECTIVITY REQUEST message. The UE may also include a request for obtaining the IPv6 Home Network Prefix. The UE shall request the IPv6 Home Network Prefix only if the UE has requested the home agent IPv6 address. The requested home agent address(es) and the Home Network Prefix are related to the APN the UE requested connectivity for.

The UE may set the ESM information transfer flag in the PDN CONNECTIVITY REQUEST message to indicate that it has ESM information, i.e. protocol configuration options, APN, or both, that needs to be sent after the NAS signalling security has been activated between the UE and the MME.

If the UE supports A/Gb mode or Iu mode or both, the UE shall indicate the support of the network requested bearer control procedures (see 3GPP TS 24.008 [13]) in A/Gb mode or Iu mode in the protocol configuration options IE.

If the UE supports N1 mode and the request type is:

a) "initial request" or "emergency", the UE shall generate a PDU session ID, associate the PDU session ID with the PDN connection that is being established, and include the PDU session ID in the protocol configuration options IE or the extended protocol configuration options IE;

b) "handover" or "handover of emergency bearer services", and the UE requests:

1) transfer of an existing PDU session in 5GS or establishment of a PDN connection as a user-plane resource of an already established MA PDU session, the UE shall associate the PDU session ID of the PDU session with the PDN connection that is being established for the existing PDU session and include the PDU session ID in the protocol configuration options IE or the extended protocol configuration options IE; or

2) transfer of an existing PDN connection in a non-3GPP access connected to the EPC and a PDU session ID is associated with the existing PDN connection, the UE shall include the PDU session ID in the protocol configuration options IE or the extended protocol configuration options IE.

NOTE 2: The UE can also have an S-NSSAI associated with the PDN connection, if the S-NSSAI was provided by the network during the PDN connection establishment via non-3GPP access to EPC (see 3GPP TS 24.302 [48]). The UE stores this S-NSSAI for later use during inter-system change from S1 mode to N1 mode.

If the UE supporting N1 mode supports receiving QoS rules with the length of two octets or QoS flow descriptions with the length of two octets via the extended protocol configuration options IE, the UE shall include the QoS rules with the length of two octets support indicator or the QoS flow descriptions with the length of two octets support indicator, respectively, in the protocol configuration options IE or the extended protocol configuration options IE.

Protocol configuration options provided in the ESM INFORMATION RESPONSE message replace any protocol configuration options provided in the PDN CONNECTIVITY REQUEST message.

When the UE initiates the procedure to add 3GPP access to the PDN connection that is already established over WLAN, the UE shall provide the same APN as that of the PDN connection established over WLAN in the PDN connectivity procedure as specified in the subclause 6.2.2 of 3GPP TS 23.161 [34].

If the UE supports APN rate control, the UE shall include an APN rate control support indicator and an additional APN rate control for exception data support indicator in the protocol configuration options IE or extended protocol configuration options IE.

If the UE supports DNS over (D) TLS (see 3GPP TS 33.501 [24]), the UE shall include the extended protocol configuration options IE in the PDN CONNECTIVITY REQUEST message and include DNS server security information Indicator.

NOTE 3: Support of DNS over (D) TLS is based on the informative requirements as specified in 3GPP TS 33.401 [19] and hence it has no normative enforcement to be implemented.



Figure 6.5.1.2.1: UE requested PDN connectivity procedure