**3GPP TSG-CT WG1 Meeting #133-eC1-21XXXX**

**E-meeting, 11-19 November 2021 *was C1-216791***

|  |
| --- |
| *CR-Form-v12.1* |
| **CHANGE REQUEST** |
|  |
|  | **24.502** | **CR** | **0196** | **rev** | **1** | **Current version:** | **17.4.0** |  |
|  |
| *For* [***HELP***](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 |  |

|  |
| --- |
|  |
| ***Title:***  | Protocol type field of GRE |
|  |  |
| ***Source to WG:*** | Huawei, HiSilicon  |
| ***Source to TSG:*** | C1 |
|  |  |
| ***Work item code:*** | 5GProtoc17-non3GPP |  | ***Date:*** | 2021-11-XX |
|  |  |  |  |  |
| ***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:*** | According to the following text quoted from RFC2784, GRE’s protocol type filed shall be set to the protocol type of the payload packet.*The Protocol Type field contains the protocol type of the payload packet. These Protocol Types are defined in [RFC1700] as "ETHER TYPES" and in [ETYPES]. An implementation receiving a packet containing a Protocol Type which is not listed in [RFC1700] or [ETYPES] SHOULD discard the packet.*However in current 3GPP’s specification, the GRE’s protocol type filed is blindly set to 0.*If a user data packet message is transmitted over non-3GPP access between the UE and the N3IWF for untrusted non-3GPP access and the TNGF for the trusted non-3GPP access, the user data packet message shall be encapsulated as a GRE user data packet with a GRE header as specified in clause 9.3.3. In the GRE encapsulated user data packet:**a0) the protocol type field is set to zero;*The implementation of GRE in 3GPP contradicts the origanl design in IETF.  |
| ***Summary of change:*** | Clarify that the GRE’s protocol type filed shall be set as RFC2784 required |
|  |  |
| ***Consequences if not approved:*** | Implementation is inconsistent with RFC2784 |
|  |  |
| ***Clauses affected:*** | 8.3.2, 9.3.3 |
|  |  |
|  | **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:*** |  |

\*\*\*\*\* start of 1st change \*\*\*\*\*

### 8.3.2 Generic routing encapsulation (GRE)

If a user data packet message is transmitted over non-3GPP access between the UE and the N3IWF for untrusted non-3GPP access and the TNGF for the trusted non-3GPP access, the user data packet message shall be encapsulated as a GRE user data packet with a GRE header as specified in clause 9.3.3. In the GRE encapsulated user data packet:

a0) the protocol type field is set per IETF RFC 2784 [14] based on the protocol type of user data packet;

a) the payload packet field is set to the user data packet;

b) the QFI field of the key field of the GRE header field is set to the QFI associated with the user data packet;

c) if the N3IWF for untrusted non-3GPP access and the TNGF for trusted non-3GPP access:

1) needs to send RQI for a downlink user data packet, the RQI field of the key field of the GRE header is set to "RQI is indicated" as defined in table 9.3.3-3; or

2) does not need to send RQI for a downlink user data packet, the RQI field of the key field of the GRE header is set to "RQI is not indicated" as defined in table 9.3.3-3; and

d) if the UE sends an uplink user data packet, the RQI field of the key field of the GRE header is set to "RQI is not indicated" as defined in table 9.3.3-3.

If the IKE\_AUTH response message contains:

a) the INTERNAL\_IP4\_ADDRESS attribute and the CREATE\_CHILD\_SA request message creating the user plane IPsec SA contains the UP\_IP4\_ADDRESS notify payload in clause 7.5.4, an inner IPv4 datagram shall be constructed where:

1) the GRE user data packet shall be encapsulated as the payload of the inner IPv4 datagram with IPv4 header where:

A) if the UE constructs the inner IPv4 datagram, the source address field shall be set to the IPv4 address in the INTERNAL\_IP4\_ADDRESS attribute and the destination address field shall be set to the IPv4 address in the UP\_IP4\_ADDRESS notify payload;

B) if the N3IWF for untrusted non-3GPP access and the TNGF for trusted non-3GPP access constructs the inner IPv4 datagram, the source address field shall be set to the IPv4 address in the UP\_IP4\_ADDRESS notify payload and the destination address field shall be set to the IPv4 address in the INTERNAL\_IP4\_ADDRESS attribute; and

C) the protocol field shall be set to 2FH;

2) the inner IPv4 datagram shall be protected employing the ESP protocol in tunnel mode as specified in IETF RFC 4303 [11] where:

A) the SPI field in the ESP packet shall be set to the SPI of the user plane IPsec SA; and

B) the next header field in the ESP packet shall be set to 04H,

 and the inner IPv4 datagram encapsulating the GRE encapsulated user data can be fragmented as described in IETF RFC 791 [24] before being protected by ESP protocol;

3) if the DSCP field is associated with the user plane IPsec SA, the DSCP field as specified in IETF RFC 2474 [26] of the IP packet encapsulating the ESP protected inner IPv4 datagram shall be set to the value of the DSCP field included in the 5G\_QOS\_INFO Notify payload; and

4) the IP packet encapsulating the ESP protected inner IPv4 datagram shall be sent to the peer for the SPI of the user plane IPsec SA; or

b) the INTERNAL\_IP6\_ADDRESS attribute and the CREATE\_CHILD\_SA request message creating the user plane IPsec SA contains the UP\_IP6\_ADDRESS notify payload in clause 7.5.4, an inner IPv6 datagram shall be constructed where:

1) the GRE user data packet shall be encapsulated as the payload of the inner IPv6 datagram with IPv6 header where:

A) if the UE constructs the inner IPv6 datagram, the source address field shall be set to the IPv6 address in the INTERNAL\_IP6\_ADDRESS attribute and the destination address field shall be set to the IPv6 address in the UP\_IP6\_ADDRESS notify payload;

B) if the N3IWF for untrusted non-3GPP access and the TNGF for trusted non-3GPP access constructs the inner IPv6 datagram, the source address field shall be set to the IPv6 address in the UP\_IP6\_ADDRESS notify payload and the destination address field shall be set to the IPv6 address in the INTERNAL\_IP6\_ADDRESS attribute; and

C) the next header field shall be set to 2FH;

2) the inner IPv6 datagram shall be protected employing the ESP protocol in tunnel mode as specified in IETF RFC 4303 [11] where:

A) the SPI field in the ESP packet shall be set to the SPI of the user plane IPsec SA; and

B) the next header field in the ESP packet shall be set to 29H;

 and the inner IPv6 datagram encapsulating the GRE encapsulated user data can be fragmented as described in IETF RFC 8200 [25] before being protected by ESP protocol; and

3) if the DSCP field is associated with the user plane IPsec SA, the DSCP field as specified in IETF RFC 2474 [26] of the IP packet encapsulating the ESP protected inner IPv6 datagram shall be set to the value of the DSCP field included in the 5G\_QOS\_INFO Notify payload; and

4) theIP packet encapsulating the ESP protected inner IPv6 datagram shall be sent to the peer for the SPI of the user plane IPsec SA.

If a user data packet message is transmitted over non-3GPP access between the UE and the N3IWF for untrusted non-3GPP access and the TNGF for trusted non-3GPP access, the user data packet message shall be encapsulated in the payload of an inner IP datagram which is further encapsulated by ESP protocol in tunnel mode as specified in IETF RFC 4303 [11]. In order to avoid any IP fragmentation by the sending entity over the non-3GPP access network, the maximum inner IP datagram length shall be set by the sending entity such that the length of the resulting outer IP datagram does not exceed the MTU of the non-3GPP access network. If the length of the user data packet message exceeds the payload size corresponding to the maximum inner IP datagram length and IP fragmentation is needed:

a) the inner IP IPv4 datagram or inner IP IPv6 datagram shall be fragmented; and

b) the IP packet encapsulating the ESP protected inner IPv4 datagram and the IP packet encapsulating the ESP protected inner IPv6 datagram shall not be fragmented.

\*\*\*\*\* end of 1st change \*\*\*\*\*

\*\*\*\*\* start of 2nd change \*\*\*\*\*

### 9.3.3 GRE encapsulated user data packet

GRE encapsulated user data packet is coded according to figure 9.3.3-1 and table 9.3.3-1.

|  |  |
| --- | --- |
| Bits |  |
| 7 | 6 | 5 | 4 | 3 | 2 | 1 | 0 | Octets |
| GRE header | 1 - 8 |
| Payload packet | 9 - x |

Figure 9.3.3-1: GRE encapsulated user data packet

Table 9.3.3-1: GRE encapsulated user data packet

|  |
| --- |
| Octet 1 to octet 8 are the GRE header field defined in IETF RFC 2784 [14] and IETF RFC 2890 [15]. The GRE header field is coded according to figure 9.3.3-2 and table 9.3.3-2. |
| Octet 9 to octet x are the Payload packet field. The Payload packet field contains one user data packet. |

|  |  |
| --- | --- |
| Bits |  |
| 7 | 6 | 5 | 4 | 3 | 2 | 1 | 0 | Octets |
| C | Reserved0 | K | S | Reserved0 | 1 |
| Reserved0 | Ver | 2 |
| Protocol type | 3 - 4 |
| Key | 5 - 8 |

Figure 9.3.3-2: GRE header field

Table 9.3.3-2: GRE header field

|  |
| --- |
| Bit 7 of octet 1 is the C bit defined in IETF RFC 2784 [14]. The C bit is set to zero. |
| Bits 6, 3, 2, 1 and 0 of octet 1 and bits 7, 6, 5, 4, and 3 of octet 2 are the Reserved0 field defined in IETF RFC 2784 [14] and IETF RFC 2890 [15]. |
| Bit 5 of octet 1 is the K bit defined in IETF RFC 2890 [15]. The K bit is set to one. |
| Bit 4 of octet 1 is the S bit defined in IETF RFC 2890 [15]. The S bit is set to zero. |
| Bits 2, 1 and 0 of octet 2 is the Ver field defined in IETF RFC 2784 [14]. |
| Octet 3 and octet 4 are the Protocol Type field defined in IETF RFC 2784 [14]. |
| Octet 5 to octet 8 are the Key field defined in IETF RFC 2890 [15]. The Key field is coded according to figure 9.3.3-3 and table 9.3.3-3. |
|  |

|  |  |
| --- | --- |
| Bits |  |
| 7 | 6 | 5 | 4 | 3 | 2 | 1 | 0 | Octets |
| 0Spare | 0Spare | QFI | 5 |
| 0Spare | 0Spare | 0Spare | 0Spare | 0Spare | 0Spare | 0Spare | 0Spare | 6 |
| 0Spare | 0Spare | 0Spare | 0Spare | 0Spare | 0Spare | 0Spare | 0Spare | 7 |
| RQI | 0Spare | 0Spare | 0Spare | 0Spare | 0Spare | 0Spare | 0Spare | 8 |

Figure 9.3.3-3: Key field of GRE header

Table 9.3.3-3: Key field of GRE header

|  |
| --- |
| RQI (octet 8, bit 7) |
| Bit |
| 7 |
| 0 |  | RQI is not indicated |
| 1 |  | RQI is indicated |
|  |
| QFI (octet 5, bits 5 to 0) |
| Bits |
| 5 | 4 | 3 | 2 | 1 | 0 |  |  |
| 0 | 0 | 0 | 0 | 0 | 0 |  | QFI 0 |
|  to |
| 1 | 1 | 1 | 1 | 1 | 1 |  | QFI 63 |
|  |

\*\*\*\*\* end of 2nd change \*\*\*\*\*