**3GPP TSG-CT WG1 Meeting #123-eC1-202580**

**Electronic meeting, 16-24 April 2020**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.0* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  | **24.502** | **CR** | **0131** | **rev** | **1** | **Current version:** | **16.3.0** |  |
|  | | | | | | | | |
| *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:*** | Enable N3IWF to initiate TCP connection establishment upon failure | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | Nokia, Nokia Shanghai Bell | | | | | | | | | |
| ***Source to TSG:*** | C1 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | 5GProtoc16-non3GPP | | | | |  | ***Date:*** | | | 2020-03-20 |
|  |  | | | |  | |  | | |  |
| ***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 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-12 (Release 12)* *Rel-13 (Release 13) Rel-14 (Release 14) Rel-15 (Release 15) Rel-16 (Release 16)* | |
|  |  | | | | | | | | | |
| ***Reason for change:*** | | TS 24.502 specifies in clause 8.2.3 that " *For transport of NAS messages, the UE shall initiate establishment of a TCP connection as defined in IETF RFC793 [27].*" However, in certain cases the N3IWF may fail and upon recovery we may end up with a half-open connection. The issue is described in the following excerpt from RFC 793, and in our case TCP A is N3IWF/TNGF and TCP B is the UE.  "*Assume that two user processes A and B are communicating with one another when a crash occurs causing loss of memory to A's TCP. Depending on the operating system supporting A's TCP, it is likely that some error recovery mechanism exists. When the TCP is up again, A is likely to start again from the beginning or from a recovery point. As a result, A will probably try to OPEN the connection again or try to SEND on the connection it believes open. In the latter case, it receives the error message "connection not open" from the local (A's) TCP. In an attempt to establish the connection, A's TCP will send a segment containing SYN. This scenario leads to the example shown in figure 10. After TCP A crashes, the user attempts to re-open the connection. TCP B, in the meantime, thinks the connection is open.*  *TCP A (N3IWF) TCP B (UE)*  *1. (CRASH) (send 300,receive 100)*  *2. CLOSED ESTABLISHED*  *3. SYN-SENT --> <SEQ=400><CTL=SYN> --> (??)*  *4. (!!) <-- <SEQ=300><ACK=100><CTL=ACK> <-- ESTABLISHED*  *5. SYN-SENT --> <SEQ=100><CTL=RST> --> (Abort!!)*  *6. SYN-SENT CLOSED*  *7. SYN-SENT --> <SEQ=400><CTL=SYN> -->*  *Half-Open Connection Discovery*  *Figure 10.*  When the SYN arrives at line 3, TCP B, being in a synchronized state, and the incoming segment outside the window, responds with an acknowledgment indicating what sequence it next expects to hear (ACK 100).  TCP A sees that this segment does not acknowledge anything it sent and, being unsynchronized, sends a reset (RST) because it has detected a half-open connection.  TCP B aborts at line 5.  TCP A will continue to try to establish the connection; the problem is now reduced to the basic 3-way handshake of figure 7."  *"*  In this case the N3IWF/TNGF cannot perform steps 3 and 7, i.e.cannot establish the connection as suggested by RFC 793. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | Add that the N3IWF/TNGF can also initiate the establishment of TCP connection. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | In case of N3IWF failure NAS messages cannot be exchanged until the UE detects the issue and reinitiates the connection establishment. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 8.2.1, 8.2.2, 8.2.3A(new) | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **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:*** | |  | | | | | | | | |

\*\*\*\*\* Next change \*\*\*\*\*

### 8.2.1 General

In trusted and untrusted non-3GPP access, after the completion of IKE SA and establishment of signalling IPsec SA as specified in subclause 7.3 for untrusted non-3GPP access and subclause 7.3A for trusted non-3GPP access, the UE establishes with the N3IWF for untrusted non-3GPP access or the TNGF for trusted non-3GPP access a TCP connection for transport of NAS messages over the inner IP layer and the signalling IPsec SA as specified in subclause 8.2.3. Once the TCP connection for transport of NAS messages is established, the UE performs NAS procedures over the TCP connection for transport of NAS messages. All uplink and downlink NAS mobility management messages and NAS session management messages are relayed between the UE and the AMF via N3IWF for untrusted non-3GPP access and the TNGF for trusted non-3GPP access using the TCP connection for transport of NAS messages as specified in subclause 8.2.4. Upon detection of a TCP connection failure, the UE and the N3IWF for untrusted non-3GPP access or the UE and the TNGF for trusted non-3GPP access re-establish the TCP connection as specified in subclause 8.2.3A

If the TCP connection for transport of NAS messages is established, if a is detected the UE, the N3IWF for untrusted non-3GPP access or the TNGF for trusted non-3GPP access re-establishes the TCP connection as specified in subclause 8.2.3A.When the TCP connection for transport of NAS messages is no longer needed, the UE, the N3IWF for untrusted non-3GPP access or the TNGF for trusted non-3GPP access release the TCP connection as specified in subclause 8.2.5.

In wireline access, after completion of EAP-5G authentication as specified in clause 7A, all uplink and downlink NAS mobility management messages and NAS session management messages are relayed between the 5G-RG and the AMF via W-AGF serving the 5G-RG using the W-CP connection without EAP-5G encapsulation. Transport using the W-CP connection is out of scope of the present document.

\*\*\*\*\* Next change \*\*\*\*\*

### 8.2.2 TCP packet encapsulation

NOTE 1: This subclause is used for encapsulating of TCP packets when establishing TCP connection as described in subclause 8.2.3, when re-establishing TCP connection as described in subclause 8.2.3A, when transporting NAS messages over TCP connection as described in subclause 8.2.4, and when releasing TCP connection as described in subclause 8.2.5.

If a TCP packet is transported between the UE and the N3IWFfor untrusted non-3GPP access or the TNGF for trusted non-3GPP access, and:

a) if the IKE\_AUTH response message contained the INTERNAL\_IP4\_ADDRESS attribute and the NAS\_IP4\_ADDRESS notify payload, an inner IPv4 datagram shall be constructed where:

1) the TCP packet shall be encapsulated in 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;

- the destination address field shall be set to the IPv4 address in the NAS\_IP4\_ADDRESS notify payload; and

- the destination port number shall be set to the NAS\_TCP\_PORT notify payload;

B) if the N3IWF for untrusted non-3GPP access or the TNGF for trusted non-3GPP accessconstructs the inner IPv4 datagram:

- the source address field shall be set to the IPv4 address in the NAS\_IP4\_ADDRESS notify payload;

- the source port number shall be set to the NAS\_TCP\_PORT notify payload;

- the destination address field shall be set to the IPv4 address in the INTERNAL\_IP4\_ADDRESS attribute; and

- the destination port number shall be set to the UE's TCP port number; and

NOTE 2: Since the UE always initiates the NAS message exchange with the N3IWF for untrusted non-3GPP access and the TNGF for trusted non-3GPP access, the N3IWF for untrusted non-3GPP access and the TNGF for trusted non-3GPP access receive the UE's TCP port number in the TCP SYN packet exchange and use it when sending NAS messages towards the UE or when re-establishing the TCP connection upon failure.

C) the protocol field shall be set to 06H;

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 signalling IPsec SA; and

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

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

b) if the IKE\_AUTH response message contained the INTERNAL\_IP6\_ADDRESS attribute and the NAS\_IP6\_ADDRESS notify payload, an inner IPv6 datagram shall be constructed where:

1) the TCP packet shall be encapsulated in 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;

- the source port number shall be set to the UE's TCP port number;

- the destination address field shall be set to the IPv6 address in the NAS\_IP6\_ADDRESS notify payload; and

- the destination port number shall be set to the NAS\_TCP\_PORT notify payload;

B) if the N3IWF for untrusted non-3GPP access or 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 NAS\_IP6\_ADDRESS notify payload;

- the source port number shall be set to the NAS\_TCP\_PORT notify payload;

- the destination address field shall be set to the IPv6 address in the INTERNAL\_IP6\_ADDRESS attribute; and

- the destination port number shall be set to the UE's TCP port number; and

NOTE 3: Since the UE always initiates the NAS message exchange with the N3IWF for untrusted non-3GPP access and the TNGF for trusted non-3GPP access, the N3IWF for untrusted non-3GPP access and the TNGF for trusted non-3GPP access receive the UE's TCP port number in the TCP SYN packet exchange and use it when sending NAS messages towards the UE or when re-establishing the TCP connection upon failure.

C) the next header field shall be set to 06H;

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 signalling IPsec SA; and

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

3) the IP packet encapsulating the ESP protected inner IPv6 datagram shall be sent to the peer for the SPI of the signalling IPsec SA.

If the UE receives an IKE\_AUTH response message containing both NAS\_IP4\_ADDRESS and NAS\_IP6\_ADDRESS notify payload, the UE:

a) shall select and use either NAS\_IP4\_ADDRESS or NAS\_IP6\_ADDRESS;

b) shall not switch between NAS\_IP4\_ADDRESS and NAS\_IP6\_ADDRESS for TCP packet transport during the lifetime of the IKE SA; and

c) shall not switch between NAS\_IP4\_ADDRESS and NAS\_IP6\_ADDRESS when rekeying any child SA or IKE SA.

The ESP packet format is shown in figure 8.2.2-1 and figure 8.2.2-2:

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Bits | | | | | | | |  |
| 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 | Octets |
| Security Parameters Index (SPI) | | | | | | | | 1-4 |
| Sequence Number | | | | | | | | 5-8 |
| Payload data (inner IP packet containing TCP packet) | | | | | | | | 9-m |
| Padding | | | | | | | | (m+1) - n |
| Padding length | | | | | | | | n+1 |
| Next header | | | | | | | | n+2 |
| Integrity Check Value (ICV) | | | | | | | | (n+2) - x |

Figure 8.2.2-1: ESP packet format for TCP packet (re-)establishing or releasing TCP connection

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Bits | | | | | | | |  |
| 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 | Octets |
| Security Parameters Index (SPI) | | | | | | | | 1-4 |
| Sequence Number | | | | | | | | 5-8 |
| Payload data (inner IP packet containing TCP packet encapsulating NAS message or partial NAS message) | | | | | | | | 9-m |
| Padding | | | | | | | | (m+1) - n |
| Padding length | | | | | | | | n+1 |
| Next header | | | | | | | | n+2 |
| Integrity Check Value (ICV) | | | | | | | | (n+2) - x |

Figure 8.2.2-2: ESP packet format for TCP packet encapsulating NAS message or partial NAS message

\*\*\*\* Next change \*\*\*\*\*

### 8.2.3A Re-establishment of TCP connection for transport of NAS messages

Upon detection that the transport of a NAS message over the TCP connection is unsuccessful due to TCP connection failure ,e.g. as indicated by the reception of a TCP error message, the UE and the N3IWF for untrusted non-3GPP access or the UE and the TNGF for trusted non-3GPP access shall re-establish the TCP connection as defined in IETF RFC793 [27]. The UE and the N3IWF for untrusted non-3GPP access or the UE and the TNGF for trusted non-3GPP access shall construct and transport TCP packets according to subclause 8.2.2.