**3GPP TSG-CT WG1 Meeting #136-eC1-22xxxx**

**E-Meeting, 12th – 20th May 2022**

|  |
| --- |
| *CR-Form-v12.1* |
| **CHANGE REQUEST** |
|  |
|  | **24.554** | **CR** | **0068** | **rev** | **3** | **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 | **X** | Radio Access Network |  | Core Network |  |

|  |
| --- |
|  |
| ***Title:***  | Handling of synchronization failure for 5G ProSe UE-to-network relay security |
|  |  |
| ***Source to WG:*** | Nokia, Nokia Shanghai Bell, Ericsson |
| ***Source to TSG:*** | C1 |
|  |  |
| ***Work item code:*** | 5G\_ProSe |  | ***Date:*** | 2022-04-29 |
|  |  |  |  |  |
| ***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:*** | As stated in TS 33.503 clause 6.3.3.2.2, in the user plane solution for 5G ProSe UE-to-network relay security:*Handling of synchronization failure (for details of synchronization failures – see TS 33.102[11]) when UE processes the authentication challenge in the GPI is performed similarly to clause 6.7.3.2.1.2 in TS 33.303 [4]. The 5G ProSe UE-to-Network Relay shall send the key request message to the 5G PKMF of the 5G ProSe Remote UE via the 5G PKMF of the 5G ProSe UE-to-Network Relay upon receiving the Direct Security Mode Failure message from the 5G ProSe Remote UE. The key request message shall include the RAND and AUTS received from the 5G ProSe Remote UE. The 5G PKMF of the 5G ProSe Remote UE shall request GPI as described in step 4c.*Hence the corresponding requirements for that synchronization failure situation needs to be reflected in stage-3 spec.It is worth to note that, the *Direct Security Mode Failure* mentioned in the text above has another name in stage 3 spec TS 24.554, which is *Direct link security mode reject.* |
|  |  |
| ***Summary of change:*** | 1- Including RAND and AUTS in the Direct link security mode reject from the Remote UE to the Relay UE, in order to enable the Relay UE sending them to the PKMF.2- Implementing the corresponding changes in the Direct security mode control procedure. |
|  |  |
| ***Consequences if not approved:*** | The synchronization failure situation is not handled in stage-3 specs. |
|  |  |
| ***Clauses affected:*** | 7.2.10.5, 10.3.15.1, 10.3.15.cc (new), 10.3.15.dd (new), 11.3.8, 11.3.aa (new), 11.3.bb (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:*** | **Changes in Rev 2:**This CR was already agreed in CT1#135-e, but it was found that there are some wrong bullets numbering that needs correction, which is done in this CR as following:11.3.15.cc --> 10.3.15.cc11.3.15.dd --> 10.3.15.dd |

\*\*\*\*\* First change \*\*\*\*\*

#### 7.2.10.5 5G ProSe direct link security mode control procedure not accepted by the target UE

If the PROSE DIRECT LINK SECURITY MODE COMMAND message cannot be accepted, the target UE shall send a PROSE DIRECT LINK SECURITY MODE REJECT message, and the target UE shall abort the ongoing procedure that triggered the initiation of the 5G ProSe direct link security mode control procedure unless the ongoing procedure is a 5G ProSe direct link establishment procedure and the Target user info is not included in the PROSE DIRECT LINK ESTABLISHMENT REQUEST message. The PROSE DIRECT LINK SECURITY MODE REJECT message contains a PC5 signalling protocol cause IE indicating one of the following cause values:

#5: lack of resources for 5G ProSe direct link;

#7: integrity failure;

#8: UE security capabilities mismatch;

#9: LSB of KNRP-sess ID conflict;

#10: UE PC5 unicast signalling security policy mismatch;

#14: Authentication synchronisation error; or

#111: protocol error, unspecified.

If this 5G ProSe direct link security mode control procedure is triggered during the 5G ProSe direct link establishment procedure and the implementation-specific maximum number of established NR 5G ProSe direct links has been reached, then the target UE shall send a PROSE DIRECT LINK SECURITY MODE REJECT message containing PC5 signalling protocol cause value #5 "lack of resources for 5G ProSe direct link".

If the PROSE DIRECT LINK SECURITY MODE COMMAND message cannot be accepted because the 5G ProSe direct link security mode control procedure was triggered during a 5G ProSe direct link establishment procedure, that the selected security algorithms in the PROSE DIRECT LINK SECURITY MODE COMMAND message included the null integrity protection algorithm and the target UE's 5G ProSe direct signalling integrity protection policy is set to "Signalling integrity protection required", the target UE shall include PC5 signalling protocol cause #10 "UE PC5 unicast signalling security policy mismatch" in the PROSE DIRECT LINK SECURITY MODE REJECT message.

If the PROSE DIRECT LINK SECURITY MODE COMMAND message cannot be accepted because the 5G ProSe direct link security mode control procedure was triggered during a 5G ProSe direct link re-keying procedure, the integrity protection algorithm currently in use for the 5G ProSe direct link is different from the null integrity protection algorithm and the selected security algorithms in the PROSE DIRECT LINK SECURITY MODE COMMAND message include the null integrity protection algorithm, the target UE, the target UE shall include PC5 signalling protocol cause #10 "UE PC5 unicast signalling security policy mismatch" in the PROSE DIRECT LINK SECURITY MODE REJECT message.

If the target UE detects that the received UE security capabilities IE in the PROSE DIRECT LINK SECURITY MODE COMMAND message has been altered compared to the latest values that the target UE sent to the initiating UE in the PROSE DIRECT LINK ESTABLISHMENT REQUEST message or PROSE DIRECT LINK REKEYING REQUEST message, the target UE shall include PC5 signalling protocol cause #8 "UE security capabilities mismatch" in the PROSE DIRECT LINK SECURITY MODE REJECT message.

If the target UE detects that the LSB of KNRP-sess ID included in the PROSE DIRECT LINK SECURITY MODE COMMAND message are set to the same value as those received from another UE in response to the target UE's PROSE DIRECT LINK ESTABLISHMENT REQUEST message, the target UE shall include PC5 signalling protocol cause #9 "LSB of KNRP-sess ID conflict" in the PROSE DIRECT LINK SECURITY MODE REJECT message.

If the 5G ProSe direct link security mode control procedure is for direct communication between the 5G ProSe remote UE and the 5G ProSe UE-to-network relay UE, and the PROSE DIRECT LINK SECURITY MODE COMMAND message cannot be accepted due to a synchronisation error when processing the authentication vector contained in the GPI sent by the 5G ProSe UE-to-network relay UE to the 5G ProSe remote UE, if any, the target UE shall include PC5 signalling protocol cause #14 "Authentication synchronisation error" in the PROSE DIRECT LINK SECURITY MODE REJECT message and shall include the RAND and AUTS parameters in the PROSE DIRECT LINK SECURITY MODE REJECT message.

After the PROSE DIRECT LINK SECURITY MODE REJECT message is generated, the target UE shall pass this message to the lower layers for transmission along with the initiating UE's layer-2 ID for 5G ProSe direct communication and the target UE's layer-2 ID for 5G ProSe direct communication.

Upon receipt of the PROSE DIRECT LINK SECURITY MODE REJECT message, the initiating UE shall stop timer T5089, provide an indication to the lower layer of deactivation of the 5G ProSe direct security protection and deletion of security context for the 5G ProSe direct link, if applicable and:

a) if the PC5 signalling protocol cause IE in the PROSE DIRECT LINK SECURITY MODE REJECT message is set to #9 "LSB of KNRP-sess ID conflict", retransmit the PROSE DIRECT LINK SECURITY MODE COMMAND message with a different value for the LSB of KNRP-sess ID and restart timer T5089;

b) if the PC5 signalling protocol cause IE in the PROSE DIRECT LINK SECURITY MODE REJECT message is set to #14 "Authentication synchronisation error", the message contained a RAND and an AUTS, and the 5G ProSe direct link security mode control procedure is for direct communication between the 5G ProSe remote UE and the 5G ProSe UE-to-network relay UE, may fetch a fresh GPI from the PKMF by sending a Key Request message including RAND and AUTS as specified in 3GPP TS 33.503 [34]; or

c) if the PC5 signalling protocol cause IE is set to the value other than #9 "LSB of KNRP-sess ID conflict" and other than #14 "Authentication synchronisation error", abort the ongoing procedure that triggered the initiation of the 5G ProSe direct link security mode control procedure.

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

#### 10.3.15.1 Message definition

This message is sent by a UE to another peer UE to reject a PROSE DIRECT LINK SECURITY MODE COMMAND message. See table 10.3.15.1.1.

Message type: PROSE DIRECT LINK SECURITY MODE REJECT

Significance: dual

Direction: UE to peer UE

Table 10.3.15.1.1: PROSE DIRECT LINK SECURITY MODE REJECT message content

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| IEI | Information Element | Type/Reference | Presence | Format | Length |
|  | PROSE DIRECT LINK SECURITY MODE REJECT message identity | ProSe PC5 signalling message type11.3.1. | M | V | 1 |
|  | Sequence number | Sequence number11.3.2 | M | V | 1 |
|  | PC5 signalling protocol cause | PC5 signalling protocol cause11.3.8 | M | V | 1 |
| YY | RAND | RAND11.3.aa | O | TV | 17 |
| ZZ | AUTS | AUTS11.3.bb | O | TV | 15 |

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

#### 10.3.15.cc RAND

The UE shall include this IE if there is a synchronisation error and the 5G ProSe direct link security mode control procedure is for direct communication between the 5G ProSe remote UE and the 5G ProSe UE-to-network relay UE.

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

#### 10.3.15.dd AUTS

The UE shall include this IE if there is a synchronisation error and the 5G ProSe direct link security mode control procedure is for direct communication between the 5G ProSe remote UE and the 5G ProSe UE-to-network relay UE.

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

### 11.3.8 PC5 signalling protocol cause

The purpose of the PC5 signalling protocol cause information element is to indicate the cause used in the PC5 signalling protocol procedures.

The PC5 signalling protocol cause is a type 3 information element with a length of 2 octets.

The PC5 signalling protocol cause information element is coded as shown in figure 11.3.8.1 and table 11.3.8.1.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  |
| PC5 signalling protocol cause IEI | octet 1 |
| PC5 signalling cause value | octet 2 |

Figure 11.3.8.1: PC5 signalling protocol cause information element

Table 11.3.8.1: PC5 signalling protocol cause information element

|  |
| --- |
| PC5 signalling cause value (octet 2) |
|  |
| Bits |
| 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  |  |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 |  | Direct communication to the target UE not allowed |
| 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 |  | Direct communication to the target UE no longer needed |
| 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1 |  | Conflict of layer-2 ID for unicast communication is detected |
| 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 |  | Direct connection is not available anymore |
| 0 | 0 | 0 | 0 | 0 | 1 | 0 | 1 |  | Lack of resources for 5G ProSe direct link |
| 0 | 0 | 0 | 0 | 0 | 1 | 1 | 0 |  | Authentication failure |
| 0 | 0 | 0 | 0 | 0 | 1 | 1 | 1 |  | Integrity failure |
| 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 |  | UE security capabilities mismatch |
| 0 | 0 | 0 | 0 | 1 | 0 | 0 | 1 |  | LSB of KNRP-sess ID conflict |
| 0 | 0 | 0 | 0 | 1 | 0 | 1 | 0 |  | UE PC5 unicast signalling security policy mismatch |
| 0 | 0 | 0 | 0 | 1 | 0 | 1 | 1 |  | Required service not allowed |
| 0 | 0 | 0 | 0 | 1 | 1 | 0 | 0 |  | Security policy not aligned |
| 0 | 0 | 0 | 0 | 1 | 1 | 0 | 1 |  | Congestion situation |
|  |  |  |  |  |  |  |  |  |  |
| 0 | 0 | 0 | 0 | 1 | 1 | 1 | 0 |  | Authentication synchronisation error |
|  |  |  |  |  |  |  |  |  |  |
| 0 | 1 | 1 | 0 | 1 | 1 | 1 | 1 |  | Protocol error, unspecified |
|  |  |  |  |  |  |  |  |  |  |
| Any other value received by the UE shall be treated as 0110 1111, "protocol error, unspecified". |

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

### 11.3.aa RAND

The purpose of the RAND information element is to provide the UE with a non-predictable challenge (see 3GPP TS 33.503 [34]).

The RAND information element is coded as shown in figure 11.3.aa.1 and table 11.3.aa.1.

The RAND is a type 3 information element with a length of 17 octets.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  |
| RAND IEI | octet 1 |
| RAND value | octet 2 |
|  | octet 17 |

**Figure 11.3.aa.1: RAND information element**

**Table 11.3.aa.1: RAND information element**

|  |
| --- |
| RAND value (octet 2 to 17)The RAND value consists of 128 bits (see 3GPP TS 33.503 [34]). |

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

### 11.3.bb AUTS

The purpose of theAUTS information element is to provide the network with the necessary information to begin a re-synchronisation (see 3GPP TS 33.503 [34]).

The AUTS information element is coded as shown in figure 11.3.bb.1 and table 11.3.bb.1.

The AUTS is a type 3 information element with a length of 15 octets.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  |
| AUTS IEI | octet 1 |
| AUTS value | octet 2 |
|  | octet 15 |

**Figure 11.3.bb.1: AUTS information element**

**Table 11.3.bb.1: AUTS information element**

|  |
| --- |
| AUTS value (octet 2 to 15)This contains AUTS (see 3GPP TS 33.503 [34]) |

\*\*\*\*\* End of changes \*\*\*\*\*