**3GPP TSG-CT WG1 Meeting #135-eC1-222638**

**E-Meeting, 6th – 12th April 2022**

|  |
| --- |
| *CR-Form-v12.1* |
| **CHANGE REQUEST** |
|  |
|  | **554** | **CR** | **0022** | **rev** | **-** | **Current version:** | **.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 | **X** |

|  |
| --- |
|  |
| ***Title:***  |  |
|  |  |
| ***Source to WG:*** | CATT |
| ***Source to TSG:*** | C1 |
|  |  |
| ***Work item code:*** | 5G\_ProSe |  | ***Date:*** | 2022-03-28 |
|  |  |  |  |  |
| ***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:*** | Based on clause 6.3.2.2 of TS 33.503 security procedure over User Plane, the corresponding security aspect for 5G ProSe communication via 5G ProSe layer-3 UE-to-network relay can be added to Stage 3 specification. |
|  |  |
| ***Summary of change:*** | 1. Add description that the UE includes the PRUK ID and PLMN ID IEs in the PROSE DIRECT LINK ESTABLISHMENT REQUEST message in the procedure;
2. Add PRUK ID and PLMN ID IEs to the definition of PROSE DIRECT LINK ESTABLISHMENT REQUEST message, and definitions of these IEs.
 |
|  |  |
| ***Consequences if not approved:*** | Security procedure for 5G ProSe communication via 5G ProSe layer-3 UE-to-network relay is incomplete in stage 3. |
|  |  |
| ***Clauses affected:*** | 2, 3.2, 7.2.2.2, 10.3.1.1, 10.3.1.X (new), 10.3.1.Y (new), 11.3.yy (new), 11.3.zz (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:*** |  |

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

# 2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non‑specific.

- For a specific reference, subsequent revisions do not apply.

- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document in the same Release as the present document.

[1] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

[2] 3GPP TS 23.304: "Proximity based Services (ProSe) in the 5G System (5GS); Stage 2".

[3] IETF RFC 7230: "Hypertext Transfer Protocol (HTTP/1.1): Message Syntax and Routing".

[4] IETF RFC 7231: "Hypertext Transfer Protocol (HTTP/1.1): Semantics and Content".

[5] 3GPP TS 24.526: "UE policies for 5G System (5GS); Stage 3".

[6] OMA-WAP-TS-PushOTA-V2\_1-20110405-A: "Push Over the Air".

[7] OMA-AD-Push-V2\_2-20110809-A: "Push Architecture".

[8] WAP-168-ServiceLoad-20010731-a: "Service Loading".

[9] 3GPP TS 29.555: "Inter-5G Direct Discovery Name Management Function (DDNMF) signalling aspects; Stage 3".

[10] 3GPP TS 29.503: "5G System; Unified Data Management Services; Stage 3".

[11] 3GPP TS 24.501: "Non-Access-Stratum (NAS) protocol for 5G System (5GS); Stage 3".

[12] 3GPP TS 23.003: "Numbering, addressing and identification".

[13] 3GPP TS 38.331: "NR; Radio Resource Control (RRC); Protocol Specification".

[14] 3GPP TS 23.122: "Non-Access-Stratum (NAS) functions related to Mobile Station (MS) in idle mode".

[15] 3GPP TS 38.304: "User Equipment (UE) procedures in Idle mode and RRC Inactive state".

[16] 3GPP TS 38.323: "NR; Packet Data Convergence Protocol (PDCP) specification".

[17] 3GPP TS 24.555: "Proximity-services (ProSe) in 5G System (5GS); User Equipment (UE) policies; Stage 3".

[18] 3GPP TS 24.587: "Vehicle-to-Everything (V2X) services in 5G System (5GS); Protocol aspects; Stage 3".

[19] 3GPP TS 29.557: "5G System; Application Function ProSe Service; Stage 3".

[20] 3GPP TS 24.007: "Mobile radio interface signalling layer-3; General aspects".

[21] 3GPP TS 38.300: "NR; NR and NG-RAN Overall Description; Stage 2".

[22] 3GPP TS 23.501: "System Architecture for the 5G System; Stage 2".

[23] IETF RFC 2131: "Dynamic Host Configuration Protocol".

[24] IETF RFC 4039: "Rapid Commit Option for the Dynamic Host Configuration Protocol version 4 (DHCPv4)".

[25] IETF RFC 4862: "IPv6 Stateless Address Autoconfiguration".

[26] 3GPP TS 24.502: "Access to the 5G System (5GS) via non-3GPP access networks; Stage 3".

[27] ITU-T Recommendation E.212: "The international identification plan for mobile terminals and mobile users".

[28] ISO/IEC 10118-3:2018: "IT Security techniques – Hash-functions – Part 3: Dedicated hash-functions".

[29] W3C REC-xmlschema-2-20041028: "XML Schema Part 2: Datatypes".

[30] IETF RFC 4122: "A Universally Unique IDentifier (UUID) URN Namespace".

[31] 3GPP TS 24.008: "Mobile Radio Interface Layer 3 specification; Core Network Protocols; Stage 3".

[32] IETF RFC 826: "An Ethernet Address Resolution Protocol".

[33] 3GPP TS 23.503: "Policy and Charging Control Framework for the 5G System; Stage 2".

[34] 3GPP TS 33.503: "Security Aspects of Proximity based Services (ProSe) in the 5G System (5GS)".

[35] 3GPP TS 23.303: "Proximity-based services (ProSe); Stage 2".

[36] 3GPP TS 33.303: "Proximity-based Services (ProSe); Security aspects".

[37] 3GPP TS 33.536: "Security aspects of 3GPP support for advanced Vehicle-to-Everything (V2X) services".

[38] IETF RFC 3927: "Dynamic Configuration of IPv4 Link-Local Addresses".

[xx] IETF RFC 7542: "The Network Access Identifier".

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

## 3.2 Abbreviations

For the purposes of the present document, the abbreviations given in 3GPP TR 21.905 [1] and the following apply. An abbreviation defined in the present document takes precedence over the definition of the same abbreviation, if any, in 3GPP TR 21.905 [1].

5G DDNMF 5G Direct Discovery Name Management Function

5G ProSe 5G Proximity-based Services

DN Data Network

DUCK Discovery User Confidentility Key

DUIK Discovery User Integrity Key

DUSK Discovery User Scrambling Key

GFBR Guaranteed Flow Bit Rate

LSB Least Significant 8 Bits

MSB Most Significant 8 Bits

MFBR Maximum Flow Bit Rate

MIC Message Integrity Check

NCGI NG-RAN Cell Global ID

PC5 LINK-AMBR PC5 Link Aggregated Bit Rate

PDUID ProSe Discovery UE ID

PKMF ProSe Key Management Function

PQI PC5 5QI

ProSeP 5G ProSe Policy

PRUK Prose Remote User Key

PSDK Public Safety Discovery Key

RQI Reflective QoS Indication

RPAUID Restricted ProSe Application User ID

RSC Relay Service Code

TTL Time-To-Live

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

#### 7.2.2.2 5G ProSe direct link establishment procedure initiation by initiating UE

The initiating UE shall meet the following pre-conditions before initiating this procedure:

a) a request from upper layers to transmit the packet for ProSe application over PC5;

b) the communication mode is unicast mode (e.g., pre-configured as specified in clause 5.2.4 or indicated by upper layers);

c) the link layer identifier for the initiating UE (i.e., layer-2 ID used for unicast communication) is available (e.g., pre-configured or self-assigned) and is not being used by other existing 5G ProSe direct links within the initiating UE;

d) the link layer identifier for the destination UE (i.e., the unicast layer-2 ID of the target UE or the broadcast layer-2 ID) is available to the initiating UE (e.g., pre-configured, obtained as specified in clause 5.2 or known via prior ProSe direct communication);

NOTE 1: In the case where different ProSe applications are mapped to distinct default destination layer-2 IDs, when the initiating UE intends to establish a single unicast link that can be used for more than one ProSe identifiers, the UE can select any of the default destination layer-2 ID for unicast initial signalling.

e) the initiating UE is either authorised for 5G ProSe direct communication over PC5 in NR-PC5 in the serving PLMN, has a valid authorization for 5G ProSe direct communication over PC5 in NR-PC5 when not served by NG-RAN, or is authorized to use a 5G ProSe UE-to-network relay UE. The UE considers that it is not served by NG-RAN if the following conditions are met:

1) not served by NG-RAN for ProSe direct communication over PC5;

2) in limited service state as specified in 3GPP TS 23.122 [14], if the reason for the UE being in limited service state is one of the following;

i) the UE is unable to find a suitable cell in the selected PLMN as specified in 3GPP TS 38.304 [15];

ii) the UE received a REGISTRATION REJECT message or a SERVICE REJECT message with the 5GMM cause #11 "PLMN not allowed" as specified in 3GPP TS 24.501 [11]; or

iii) the UE received a REGISTRATION REJECT message or a SERVICE REJECT message with the 5GMM cause #7 "5GS services not allowed" as specified in 3GPP TS 24.501 [11]; or

3) in limited service state as specified in 3GPP TS 23.122 [14] for reasons other than i), ii) or iii) above, and located in a geographical area for which the UE is provisioned with "non-operator managed" radio parameters as specified in clause 5.2;

f) there is no existing 5G ProSe direct link for the pair of peer application layer IDs, or there is an existing 5G ProSe direct link for the pair of peer application layer IDs and:

1) the network layer protocol of the existing 5G ProSe direct link is not identical to the network layer protocol required by the upper layer in the initiating UE for this ProSe application;

2) the security policy (either signalling security policy or user plane security policy) corresponding to the ProSe identifier is not compatible with the security policy of the existing 5G ProSe direct link; or

3) in case of the 5G ProSe direct link establishment procedure is for direct communication between the remote UE and the UE-to-network relay UE, the existing 5G ProSe direct link for the peer UE is established with a different RSC or without an RSC;

g) the number of established 5G ProSe direct links is less than the implementation-specific maximum number of established 5G ProSe direct links allowed in the UE at a time; and

h) timer T5088 is not associated with the link layer identifier for the destination UE or timer T5088 associated with the link layer identifier for the destination UE has already expired or stopped.

After receiving the service data or request from the upper layers, the initiating UE shall derive the PC5 QoS parameters and assign the PQFI(s) for the PC5 QoS flows(s) to be established as specified in clause 7.2.7.

In order to initiate the 5G ProSe direct link establishment procedure, the initiating UE shall create a PROSE DIRECT LINK ESTABLISHMENT REQUEST message. The initiating UE:

a) shall include the source user info set to the initiating UE's application layer ID received from upper layers;

b) shall include the ProSe identifier(s) received from upper layer if the 5G ProSe direct link establishment procedure is not for 5G ProSe direct communication between the remote UE and the UE-to-network relay UE;

c) shall include the target user info set to the target UE's application layer ID if received from upper layers, or to the identity of the 5G ProSe UE-to-network relay UE obtained during the 5G ProSe UE-to-network relay discovery procedure, or if the destination layer-2 ID is the unicast layer-2 ID of target UE;

d) shall include the key establishment information container if the UE PC5 unicast signalling integrity protection policy is set to "Signalling integrity protection required" or "Signalling integrity protection preferred", and may include the key establishment information container if the UE PC5 unicast signalling integrity protection policy is set to "Signalling integrity protection not needed";

NOTE 2: The key establishment information container is provided by upper layers.

e) shall include a Nonce\_1 set to the 128-bit nonce value generated by the initiating UE for the purpose of session key establishment over this 5G ProSe direct link if the UE PC5 unicast signalling integrity protection policy is set to "Signalling integrity protection required" or "Signalling integrity protection preferred";

f) shall include its UE security capabilities indicating the list of algorithms that the initiating UE supports for the security establishment of this 5G ProSe direct link;

g) shall include the most significant 8 bits (MSB) of KNRP-sess ID chosen by the initiating UE as specified in 3GPP TS 33.503 [34] if the UE PC5 unicast signalling integrity protection policy is set to "Signalling integrity protection required" or "Signalling integrity protection preferred";

h) may include a KNRP ID if the initiating UE has an existing KNRP for the target UE;

i) shall include its UE PC5 unicast signalling security policy. In the case where the different ProSe applications are mapped to the different PC5 unicast signalling security policies, when the initiating UE intends to establish a single unicast link that can be used for more than one ProSe application, each of the signalling security polices of those ProSe applications shall be compatible, e.g., "Signalling integrity protection not needed" and "Signalling integrity protection required" are not compatible. In case the 5G ProSe direct link establishment procedure is for direct communication between 5G ProSe layer-3 remote UE and 5G ProSe layer-3 UE-to-network relay UE, the Signalling integrity protection policy shall be set to "Signalling integrity protection required";

j) shall include the Relay service code IE set to the relay service code of the target relay UE if the 5G ProSe direct link establishment procedure is for direct communication between the 5G ProSe remote UE and the 5G ProSe UE-to-network relay UE;

k) shall include the UE identity IE set to the SUCI of the initiating UE if:

1) the 5G ProSe direct link establishment procedure is for direct communication between the 5G ProSe remote UE and the 5G ProSe UE-to-network relay UE; and

2) the security for 5G ProSe UE-to-network relay uses the security procedure over control plane as specified in 3GPP TS 33.503 [34], or, the security for 5G ProSe UE-to-network relay uses the security procedure over user plane and the initiating UE does not have a valid PRUK as specified in 3GPP TS 33.503 [34];

l) shall include the PRUK ID of the initiating UE if:

1) the 5G ProSe direct link establishment procedure is for direct communication between the 5G ProSe remote UE and the 5G ProSe UE-to-network relay UE;

2) the initiating UE have a valid PRUK; and

3) the security for 5G ProSe UE-to-network relay uses the security procedure over user plane as specified in 3GPP TS 33.503 [34]; and

m) shall include the HPLMN ID of the initiating UE, if the PRUK ID of the initiating UE does not contain the HPLMN ID of the initiating UE or the routing information to the 5G PKMF of the initiating UE.

Editor's note: It is FFS how the UE determines whether the security for 5G ProSe layer-3 relay uses the security procedure over control plane or the security procedure over user plane as specified in 3GPP TS 33.503 [34].

After the PROSE DIRECT LINK ESTABLISHMENT REQUEST message is generated, the initiating UE shall pass this message to the lower layers for transmission along with the initiating UE's layer-2 ID for unicast communication and:

a) the destination layer-2 ID used for unicast initial signalling; or

b) the destination layer-2 ID set to the source layer-2 ID of the selected 5G ProSe UE-to-network relay UE during the 5G ProSe UE-to-network relay discovery procedure as defined in clause 8.2.1;

and start timer T5080.

The UE shall not send a new PROSE DIRECT LINK ESTABLISHMENT REQUEST message to the same target UE identified by the same application layer ID while timer T5080 is running. If the target user info IE is not included in the PROSE DIRECT LINK ESTABLISHMENT REQUEST message (i.e., ProSe application oriented 5G ProSe direct link establishment procedure), the initiating UE shall handle multiple PROSE DIRECT LINK ESTABLISHMENT ACCEPT messages, if any, received from different target UEs for the establishment of multiple 5G ProSe direct links before the expiry of timer T5080.

NOTE 3: In order to ensure successful 5G ProSe direct link establishment, T5080 should be set to a value larger than the sum of T5089 and T5092.



Figure 7.2.2.2.1: UE oriented 5G ProSe direct link establishment procedure



Figure 7.2.2.2.2: ProSe service oriented 5G ProSe direct link establishment procedure

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

### 10.3.1 ProSe direct link establishment request

#### 10.3.1.1 Message definition

This message is sent by a UE to another peer UE to establish a direct link. See table 10.3.1.1.1.

Message type: PROSE DIRECT LINK ESTABLISHMENT REQUEST

Significance: dual

Direction: UE to peer UE

Table 10.3.1.1.1: PROSE DIRECT LINK ESTABLISHMENT REQUEST message content

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| IEI | Information Element | Type/Reference | Presence | Format | Length |
|  | PROSE DIRECT LINK ESTABLISHMENT REQUEST message identity | ProSe PC5 signalling message type11.3.1 | M | V | 1 |
|  | Sequence number | Sequence number11.3.2 | M | V | 1 |
|  | Source user info | Application layer ID11.3.4 | M | LV | 2-256 |
|  | UE security capabilities | UE security capabilities11.3.11 | M | LV | 3-9 |
|  | UE PC5 unicast signalling security policy | UE PC5 unicast signalling security policy11.3.12 | M | V | 1 |
| 7B | ProSe identifiers | ProSe identifier11.3.3 | O | TLV-E | 21-65538 |
| 74 | Key establishment information container | Key establishment information container11.3.9 | O | TLV-E | 4-65538 |
| 56 | Nonce\_1 | Nonce11.3.10 | O | TV | 17 |
| 5C | MSB of KNRP-sess ID | MSB of KNRP-sess ID11.3.13 | O | TV | 2 |
| 28 | Target user info | Application layer ID11.3.4 | O | TLV | 3-257 |
| 58 | KNRP ID | KNRP ID11.3.14 | O | TV | 5 |
| 54 | Relay service code | Relay service code11.3.26 | O | TV | 4 |
| 7D | UE identity | 5GS mobile identity11.3.30 | O | TLV-E | 4-n |
| 2X | PRUK ID | PRUK ID11.3.yy | O | TLV | 3-n |
| 5Y | HPLMN ID | PLMN ID11.3.zz | O | TV | 2 |

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

#### 10.3.1.X PRUK ID

The UE shall include this IE if the 5G ProSe direct link establishment procedure is for direct communication between the 5G ProSe remote UE and the 5G ProSe UE-to-network relay UE, the security procedure over user plane for 5G ProSe UE-to-network relay is used and the UE have a valid PRUK.

#### 10.3.1.Y HPLMN ID

The UE shall include this IE if the the PRUK ID of the UE does not contain the HPLMN ID of the UE or the routing information to the 5G PKMF of the UE.

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

### 11.3.yy PRUK ID

The purpose of the PRUK ID information element is to carry the identity of the PRUK.

The PRUK ID is a type 4 information element with a minimal length of 3 octets and a maximum length of 255 octets.

The PRUK ID information element is coded as shown in figure 11.3.Z.1 and table 11.3.Z.1.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  |
| PRUK ID IEI | octet 1 |
| Length of PRUK ID contents | octet 2 |
| 0Spare | 0Spare | 0Spare | 0Spare | 0Spare | 0Spare | 0Spare | PRUK ID format | octet 3 |
| PRUK ID | octet 4\*-n\* |

Figure 11.3.Z.1: PRUK ID information element

Table 11.3.Z.1: PRUK ID information element

|  |
| --- |
| PRUK ID format (bit 1 of octet 3) |
| Bit |
| 1 |  |
| 0 | network access identifier (NAI) |
| 1 | 64-bit string |
| Bits 2 to 8 of octet 3 are spare and shall be coded as zero. |
| PRUK ID (octet 4 to octet n)Identifier of ProSe Relay User Key (PRUK). |

### 11.3.zz PLMN ID

The PLMN ID information element is coded as specified in 3GPP TS 23.003 [12].

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