**3GPP TSG-CT WG1 Meeting #135-eC1-222567**

**E-Meeting, 6th – 12th April 2022**

|  |
| --- |
| *CR-Form-v12.1* |
| **CHANGE REQUEST** |
|  |
|  | **24.554** | **CR** |  | **rev** | **1** | **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 | **X** |

|  |
| --- |
|  |
| ***Title:***  | ProSe remote user key procedure |
|  |  |
| ***Source to WG:*** | OPPO, Ericsson, Qualcomm |
| ***Source to TSG:*** | C1 |
|  |  |
| ***Work item code:*** | 5G\_ProSe |  | ***Date:*** | 2022-4-8 |
|  |  |  |  |  |
| ***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:*** | In clause 6.3.3.2.2 of TS 33.503, for UP authentication, remote UE shall obtain the PRUK and PRUK ID from its PKMF, to prepare for the later authentication between relay UE and network.Based on below requirement in TS 33.503,*The 5G ProSe Remote UE shall establish a secure connection with the 5G PKMF via PC8 reference point. Security for PC8 interface relies on Ua security if GBA specified in TS 33.220 [8] is used (see clause 5.2.3.4) or Ua\* security if AKMA specified in TS 33.535 [5] is used (see clause 5.2.5.4).*The PC8 interface protocol is similar with PC3a interface protocol and UP connection is used for interaction between UE and PKMF for GBA method. Therefore, the control plane protocal over PC8 should be defined in 24.554. |
|  |  |
| ***Summary of change:*** | Add ProSe remote user key request and response over PC8. |
|  |  |
| ***Consequences if not approved:*** | Missing stage 2 requirements. |
|  |  |
| ***Clauses affected:*** | 2, 3.2, 8.2.x.2.3(new), 8.2.x.2.3.1(new), 8.2.x.2.3.2(new), 8.2.x.2.3.3(new), 8.2.x.2.3.4(new), 8.2.x.2.3.5(new), 8.2.x.2.3.6(new), 8.2.x.2.3.7(new), 10.y(new), 10.y.1(new), 10.y.2(new), 10.y.3(new), 10.y.4(new), 10.y.4.1(new), 10.y.4.2(new), 11.z(new), 11.z.1(new), 11.z.2(new), 11.z.2.1(new), 11.z.2.2(new), 11.z.2.3(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".

[rfc20] IETF RFC 20: "ASCII format for Network Interchange".

\* \* \* 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 Function5G ProSe 5G Proximity-based Services

AKMA Authentication and Key Management for Applications

DN Data Network

DUCK Discovery User Confidentility Key

DUIK Discovery User Integrity Key

DUSK Discovery User Scrambling Key

GBA Generic Bootstrapping Architecture

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

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 \* \* \* \*

##### 8.2.x.2.3 5G ProSe remote user key request procedure

###### 8.2.x.2.3.1 General

The purpose of the 5G ProSe remote user key request procedure is for the UE authorized to act as a 5G ProSe remote UE to obtain a PRUK and a PRUK ID.

Before initiating this procedure, the 5G ProSe remote UE needs to be authorized to use a 5G ProSe layer-3 UE-to-network relay UE or a 5G ProSe layer-2 UE-to-network relay UE in the registered PLMN or local PLMN based on the configuration parameters as specified in clause 5.2.5.

###### 8.2.x.2.3.2 5G ProSe remote user key request procedure initiation

If the UE is authorized to use a 5G ProSe layer-3 UE-to-network relay UE or a 5G ProSe layer-2 UE-to-network relay UE in the registered PLMN or local PLMN, it shall initiate this procedure when it has discovered the 5G ProSe UE-to-network relay UE which provides the wanted connectivity service.

The UE shall initiate the 5G ProSe remote user key request procedure by sending a PROSE\_PRUK\_REQUEST message with the <PRUK-request> element. In the <PRUK-request> element, the UE:

a) shall include a new transaction ID not used in any other direct discovery procedures in PC8 interface; and

b) shall include the PRUK ID set to the PRUK ID associated with the UE stored PRUK, if the UE stores PRUK;

Figure 8.2.x.2.3.2.1 illustrates the interaction of the UE and the 5G PKMF in the 5G ProSe remote user key request procedure.



Figure 8.2.x.2.3.2.1: 5G ProSe remote user key request procedure

###### 8.2.x.2.3.3 5G ProSe remote user key request procedure accepted by the 5G PKMF

Upon receiving a PROSE\_PRUK\_REQUEST message, the 5G PKMF shall check whether the UE is authorized to act as a 5G ProSe remote UE. If authorized, the 5G PKMF shall then send a PROSE\_PRUK\_RESPONSE message with the <PRUK-response>element. In the <PRUK-response>element, the 5G PKMF shall include:

a) the transaction ID set to the value of the transaction ID received in the PROSE\_PRUK\_REQUEST message from the UE;

b) the PRUK ID set to the value of the PRUK ID associated with the PRUK; and

c) the PRUK set to the value of the allocated PRUK to the UE.

###### 8.2.x.2.3.4 5G ProSe remote user key request procedure completion by the UE

Upon receipt of the PROSE\_PRUK\_RESPONSE message, if the transaction ID matches the value sent by the UE in a PROSE\_PRUK\_REQUEST message, the UE shall delete any previously stored PRUK and PRUK ID and store the received PRUK and the associated PRUK ID.

###### 8.2.x.2.3.5 5G ProSe remote user key request procedure not accepted by the 5G PKMF

If the PROSE\_PRUK\_REQUEST message cannot be accepted by the 5G PKMF, the 5G PKMF sends a PROSE\_PRUK\_RESPONSE message containing a <response-reject> element to the UE including an appropriate PC8 control protocol cause value and including the transaction ID set to the value of the transaction ID received in the PC8\_PRUK\_REQUEST message.

Upon receipt of the PROSE\_PRUK\_RESPONSE message, if the transaction ID matches the value sent by the UE in a PROSE\_PRUK\_REQUEST message, the UE shall consider the 5G ProSe remote user key request procedure as rejected.

If the UE is not authorized for acting as a 5G ProSe remote UE, the 5G PKMF shall send the PROSE\_PRUK\_RESPONSE message containing a <response-reject> element with PC8 control protocol cause value #1 "UE authorization failure".

###### 8.2.X.2.3.6 Abnormal cases in the UE

The following abnormal cases can be identified:

a) Indication from the transport layer of transmission failure of PROSE\_PRUK\_REQUEST message (e.g., after TCP retransmission timeout)

 The UE shall close the existing secure connection to the 5G PKMF, establish a new secure connection and then restart the PRUK request procedure.

b) No response from the 5G PKMF after the PROSE\_PRUK\_REQUEST message has been successfully delivered (e.g., TCP ACK has been received for the PROSE\_PRUK\_REQUEST message)

 The UE shall retransmit the PROSE\_PRUK\_REQUEST message.

NOTE: The timer to trigger retransmission and the maximum number of allowed retransmissions are UE implementation specific.

###### 8.2.X.2.3.7 Abnormal cases in the 5G PKMF

The following abnormal cases can be identified:

a) Indication from the lower layer of transmission failure of PROSE\_PRUK\_RESPONSE message

 After receiving an indication from lower layer that the PROSE\_PRUK\_RESPONSE message has not been successfully acknowledged (e.g., TCP ACK is not received), the 5G PKMF shall abort the procedure.

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

## 10.y 5G ProSe security messages over PC8

### 10.y.1 General

This clause defines the XML schema and MIME type related to 5G ProSe security messages.

### 10.y.2 application/3gpp-5gprose+xml

The MIME type is used to carry information related to the 5G ProSe security operation. It shall be coded as an XML document containing one of the following 5G ProSe security messages:

a) PROSE\_PRUK\_REQUEST; or

b) PROSE\_PRUK\_RESPONSE.

Each of those messages is presented in the XML document as an XML element named after the corresponding message.

### 10.y.3 XML schema

Implementations in compliance with the present document shall implement the XML schema defined below for messages used in 5G ProSe security procedures over PC8 interface.

<?xml version="1.0" encoding="UTF-8"?>

<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema"

 xmlns="urn:3GPP:ns:5GProSe:Security:2022"

 elementFormDefault="qualified"

 targetNamespace="urn:3GPP:ns:5GProSe: Security:2022">

 <xs:annotation>

 <xs:documentation>

 Info for 5G ProSe Security Control Messages Syntax

 </xs:documentation>

 </xs:annotation>

<!-- Complex types defined for transaction-level -->

 <xs:complexType name="PRUKReq-info">

 <xs:sequence>

 <xs:element name="transaction-ID" type="xs:integer"/>

 <xs:element name="PRUK-ID" type="xs:string" minOccurs="0" />

 <xs:element name="anyExt" type="anyExtType" minOccurs="0"/>

 <xs:any namespace="##other" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>

 </xs:sequence>

 <xs:anyAttribute namespace="##any" processContents="lax"/>

 </xs:complexType>

 <xs:complexType name="PRUKRsq-info">

 <xs:sequence>

 <xs:element name="transaction-ID" type="xs:integer"/>

 <xs:element name="PRUK-ID" type="xs:string"/>

 <xs:element name="PRUK" type="xs:hexBinary"/>

 <xs:element name="anyExt" type="anyExtType" minOccurs="0"/>

 <xs:any namespace="##other" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>

 </xs:sequence>

 <xs:anyAttribute namespace="##any" processContents="lax"/>

 </xs:complexType>

 <!-- Complex types defined for Message-level -->

 <xs:complexType name="prose-pruk-request">

 <xs:sequence>

 <xs:element name="PRUK-request" type="PRUKReq-info" minOccurs="0" maxOccurs="unbounded"/>

 <xs:element name="anyExt" type="anyExtType" minOccurs="0"/>

 <xs:any namespace="##other" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>

 </xs:sequence>

 <xs:anyAttribute namespace="##any" processContents="lax"/>

 </xs:complexType>

 <xs:complexType name="prose-pruk-response">

 <xs:sequence>

 <xs:element name="PRUK-response" type="PRUKRsq-info" minOccurs="0" maxOccurs="unbounded"/>

 <xs:element name="anyExt" type="anyExtType" minOccurs="0"/>

 <xs:any namespace="##other" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>

 </xs:sequence>

 <xs:anyAttribute namespace="##any" processContents="lax"/>

 </xs:complexType>

 <!-- extension allowed -->

 <xs:complexType name="DiscMsgExtType">

 <xs:sequence>

 <xs:any namespace="##any" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>

 </xs:sequence>

 <xs:anyAttribute namespace="##any" processContents="lax"/>

 </xs:complexType>

 <!-- XML attribute for any future extensions -->

 <xs:complexType name="anyExtType">

 <xs:sequence>

 <xs:any namespace="##any" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>

 </xs:sequence>

 </xs:complexType>

<!-- Top level Security Message definition -->

 <xs:element name="prose-security-message">

 <xs:complexType>

 <xs:choice>

 <xs:element name="PROSE\_PRUK\_REQUEST" type="prose-pruk-request"/>

 <xs:element name="PROSE\_PRUK\_RESPONSE" type="prose-pruk-response"/>

 <xs:element name="message-ext" type="DiscMsgExtType"/>

 <xs:any namespace="##other" processContents="lax"/>

 </xs:choice>

 </xs:complexType>

 </xs:element>

</xs:schema>

An entity receiving the XML body ignores any unknown XML element and any unknown XML attribute.

### 10.y.4 Semantics

#### 10.y.4.1 General

The <prose-security-message> element is the root element of this XML document and it can be one of the following elements:

a) <PROSE\_PRUK\_REQUEST>;

b) <PROSE\_PRUK\_RESPONSE>;

c) <message-ext> element containing other discovery message defined in future releases; or

d) an element from other namespaces defined in future releases.

#### 10.y.4.2 Semantics of <PROSE\_PRUK\_REQUEST>

The <PROSE\_PRUK\_REQUEST> element contains one or more of the following elements:

a) zero, one or more <PRUK-request> element which contains transactions sent from the UE to the 5G PKMF. Each <PRUK-request> consists of:

1) a <transaction-ID> element containing the parameter defined in clause 11.z.2.1;

2) an optional <PRUK-ID> element containing the parameter defined in clause 11.z.2.3;

3) zero or one <anyExt> element containing elements defined in future releases;

4) zero, one or more elements from other namespaces defined in future releases; and

5) zero, one or more attributes defined in future releases;

b) zero, one or more <PRUK-response> element which contains transactions sent from the 5G PKMF to the UE. Each <PRUK-response> consists of:

1) a <transaction-ID> element containing the parameter defined in clause 11.z.2.1;

2) a <PRUK-ID> element containing the parameter defined in clause 11.z.2.3;

3) a <PRUK> element containing the parameter defined in clause 11.z.2.2;

4) zero or one <anyExt> element containing elements defined in future releases;

5) zero, one or more elements from other namespaces defined in future releases; and

6) zero, one or more attributes defined in future releases.\* \* \* Next Change \* \* \* \*

## 11.z 5G ProSe security message over PC8 formats

### 11.z.1 Data types format in XML schema

To exchange structured information over the transport protocol, XML text format/notation is introduced.

The corresponding XML data types for the data types used in ProSe messages are provided in table 11.z.1.1.

Table 11.z.1.1: Primitive or derived types for ProSe parameter type

|  |  |
| --- | --- |
| ProSe parameter type | Type in XML schema |
| Integer | xs:integer |
| String | xs:string |
| Boolean | xs:boolean |
| Binary | xs:hexBinary |
| Bit string | xs:hexBinary |
| Time | xs:dateTime |

For complex data types described in clause 11.z.2, an XML "complexType" can be used.

Message construction shall be compliant with W3C REC-xmlschema-2-20041028: "XML Schema Part 2: Datatypes" [29]

### 11.z.2 Parameters in 5G ProSe security messages over PC8

#### 11.z.2.1 Transaction ID

This parameter is used to uniquely identify a PC8 control protocol for 5G ProSe security transaction when it is combined with other PC8 control protocol for 5G ProSe security transactions in the same transport message. The UE shall set this parameter to a new number for each outgoing new key request. The transaction ID is an integer in the 0-255 range.

#### 11.z.2.2 PRUK

This parameter is used to indicate the PRUK allocated by the 5G PKMF. The calculation of the PRUK is defined in 3GPP TS 33.503 [34].

#### 11.z.2.3 PRUK ID

This parameter is used to indicate the identifier of the UE stored PRUK. The format of the PRUK ID consists of two parts:

a) Type which is the 1st character of the PRUK-ID value: an ASCII character, as defined in IETF RFC 20 [rfc20], coded in table 11.z.2.5.1; and

Table 11.z.2.3.1: Type

|  |
| --- |
| ASCII character "0" Reserved |
| ASCII character "1" NAI |
| ASCII character "2" 64-bit string |
| other ASCII characters unused |

b) Value of PRUK ID which is 2nd and later characters of the PRUK-ID value:

1) if the type indicates NAI, the coding of PRUK ID is the NAI format as defined in clause 28.7.3 of 3GPP TS 23.003 [12]; or

2) if the type indicates 64-bit string, the coding of PRUK ID is a 64-bit string, encoded using 16 hexadecimal digits, each digit indicated by an ASCII character "0" - "9" or "A" - "F", as defined in IETF RFC 20 [rfc20].

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