**3GPP TSG-CT WG1 Meeting #137-eC1-224967**

**E-Meeting, 18th – 26th August 2022**

|  |
| --- |
| *CR-Form-v12.1* |
| **CHANGE REQUEST** |
|  |
|  | **24.501** | **CR** | **4616** | **rev** | **-** | **Current version:** | **17.7.1** |  |
|  |
| *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:***  | Introducing the 5GPRUK ID in the Relay key Request procedure |
|  |  |
| ***Source to WG:*** | Nokia, Nokia Shanghai Bell, ZTE |
| ***Source to TSG:*** | C1 |
|  |  |
| ***Work item code:*** | 5G\_ProSe |  | ***Date:*** | 2022-07-04 |
|  |  |  |  |  |
| ***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 specified in TS 33.503, clause 6.3.3.3.2 for the control plane security solution for the UE-to-network relay:*3. Upon receiving the DCR message, the 5G ProSe UE-to-Network Relay shall send the Relay Key Request to the AMF of the 5G ProSe UE-to-Network Relay, including SUCI or 5GPRUK ID, RSC and Nonce\_1 received in the DCR message. The 5G ProSe UE-to-Network Relay shall also include in the message a transaction identifier that identifies the 5G ProSe Remote UE for the subsequent messages over 5G ProSe UE‑to‑Network Relay's NAS messages.**….**12. The AUSF of the 5G ProSe Remote UE shall send the KNR\_ProSe, Nonce\_2 in Nausf\_UEAuthentication\_ProseAuthenticate Response message to the 5G ProSe UE-to-Network Relay via the AMF of the 5G ProSe UE-to-Network Relay. EAP Success message shall be included* ***if*** *step 7 is performed successfully. The AUSF of the 5G ProSe Remote UE shall also include the 5GPRUK ID in the message if generated in step 8.**13. When receiving a KNR\_ProSe from the AUSF of the 5G ProSe Remote UE via the AMF of the 5G ProSe UE-to-Network Relay, the 5G ProSe UE-to-Network Relay derives PC5 session key Krelay-sess and confidentiality key Krelay-enc (if applicable) and integrity key Krelay-int from KNR****\_****ProSe, as defined in clause 6.3.3.3.3 of the present document. KNR\_ProSe ID and Krelay-sess ID are established in the same way as KNRP ID and KNRP-sess ID in TS 33.536 [6]. The EAP Success message and 5GPRUK ID are also sent from the AMF of the 5G ProSe UE‑to-Network Relay to UE-to-Network Relay if received from AUSF.*The above indicates the following requirements:1- The RELAY KEY REQUEST message can contain the 5GPRUK ID instead of the SUCI, where in that case the AUSF can decide not to trigger an authentication procedure for the Remote UE.2- The "EAP-success" in the RELAY KEY ACCEPT message is an optional container, where the AUSF/AMF may not send it to the Remote UE (in case the authentication for the Remote UE is not triggered, i.e. when 5GPRUK ID is available).3- The AUSF/AMF may return the 5GPRUK ID -if newly generated- to the Relay UE. |
|  |  |
| ***Summary of change:*** | As explained above, implementing the following requirements:1- Introducing the possibility to include the 5GPRUK ID (instead of the SUCI) in the Relay Key Request procedure, and doing the related changes in the procedure description, the message definition, and related IEs.2- Changing the EAP-success to be an optional IE in the RELAY KEY ACCEPT message, and doing the related changes in the procedure description, the message definition, and related IEs.3- Introducing the possibility to include the 5GPRUK ID in the RELAY KEY ACCEPT message and doing the related changes in the procedure description, the message definition, and related IEs.4- The corresponding ENs are removed since they are now resolved. |
|  |  |
| ***Consequences if not approved:*** | Incomplete specification, where the control plane security solution for UE-to-network relay will not work correctly, and misalignment with TS 33.503 |
|  |  |
| ***Clauses affected:*** | 3.2, 5.5.4.1, 5.5.4.3, 5.5.4.4, 8.2.35.1, 9.11.3.89, 9.11.3.90 |
|  |  |
|  | **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 \*\*\*\*\*

## 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].

4G-GUTI 4G-Globally Unique Temporary Identifier

5GCN 5G Core Network

5G-GUTI 5G-Globally Unique Temporary Identifier

5GMM 5GS Mobility Management

5G-RG 5G Residential Gateway

5G-BRG 5G Broadband Residential Gateway

5G-CRG 5G Cable Residential Gateway

5GS 5G System

5GSM 5GS Session Management

5G-S-TMSI 5G S-Temporary Mobile Subscription Identifier

5G-TMSI 5G Temporary Mobile Subscription Identifier

5GPRUK 5G ProSe Remote User Key

5QI 5G QoS Identifier

ACS Auto-Configuration Server

AKA Authentication and Key Agreement

AKMA Authentication and Key Management for Applications

A-KID AKMA Key Identifier

A-TID AKMA Temporary Identifier

AMBR Aggregate Maximum Bit Rate

AMF Access and Mobility Management Function

APN Access Point Name

AS Access stratum

ATSSS Access Traffic Steering, Switching and Splitting

AUSF Authentication Server Function

CAG Closed access group

CGI Cell Global Identity

CHAP Challenge Handshake Authentication Protocol

DDX Downlink Data Expected

DL Downlink

DN Data Network

DNN Data Network Name

DNS Domain Name System

eDRX Extended DRX cycle

DS-TT Device-Side TSN Translator

EUI Extended Unique Identifier

E-UTRAN Evolved Universal Terrestrial Radio Access Network

EAC Early Admission Control

EAP-AKA' Improved Extensible Authentication Protocol method for 3rd generation Authentication and Key Agreement

EAS Edge Application Server

EASDF Edge Application Server Discovery Function

ECIES Elliptic Curve Integrated Encryption Scheme

ECS Edge Configuration Server

ECSP Edge Computing Service Provider

EDC Edge DNS Client

EEC Edge Enabler Client

EPD Extended Protocol Discriminator

EMM EPS Mobility Management

EPC Evolved Packet Core Network

EPS Evolved Packet System

EPS-UPIP User-plane integrity protection in EPS

ESM EPS Session Management

FN-RG Fixed Network RG

FN-BRG Fixed Network Broadband RG

FN-CRG Fixed Network Cable RG

Gbps Gigabits per second

GFBR Guaranteed Flow Bit Rate

GUAMI Globally Unique AMF Identifier

IAB Integrated access and backhaul

IMEI International Mobile station Equipment Identity

IMEISV International Mobile station Equipment Identity and Software Version number

IMSI International Mobile Subscriber Identity

IP-CAN IP-Connectivity Access Network

KSI Key Set Identifier

LADN Local Area Data Network

LCS LoCation Services

LMF Location Management Function

LPP LTE Positioning Protocol

MAC Message Authentication Code

MA PDU Multi-Access PDU

MBS Multicast/Broadcast Services

Mbps Megabits per second

MCS Mission Critical Service

MFBR Maximum Flow Bit Rate

MICO Mobile Initiated Connection Only

MINT Minimization of Service Interruption

MPS Multimedia Priority Service

MSK MBS Service Key

MTK MBS Traffic Key

MUSIM Multi-USIM

N3IWF Non-3GPP Inter-Working Function

N5CW Non-5G-Capable over WLAN

N5GC Non-5G Capable

NAI Network Access Identifier

NITZ Network Identity and Time Zone

ngKSI Key Set Identifier for Next Generation Radio Access Network

NPN Non-public network

NR New Radio

NSAC Network Slice Admission Control

NSACF Network Slice Admission Control Function

NSAG Network slice AS group

NSSAA Network slice-specific authentication and authorization

NSSAAF Network Slice-Specific and SNPN authentication and authorization Function

NSSAI Network Slice Selection Assistance Information

NSSRG Network Slice Simultaneous Registration Group

NSWO Non-Seamless WLAN Offload

ON-SNPN Onboarding Standalone Non-Public Network

OS Operating System

OS Id OS Identity

PAP Password Authentication Protocol

PCO Protocol Configuration Option

PEI Permanent Equipment Identifier

PEIPS Paging Early Indication with Paging Subgrouping

PNI-NPN Public Network Integrated Non-Public Network

PRUK ProSe Remote User Key

ProSe Proximity based Services

ProSeP 5G ProSe policy

PTI Procedure Transaction Identity

PVS Provisioning Server

QFI QoS Flow Identifier

QoS Quality of Service

QRI QoS Rule Identifier

RACS Radio Capability Signalling Optimisation

(R)AN (Radio) Access Network

RFSP RAT Frequency Selection Priority

RG Residential Gateway

RPLMN Registered PLMN

RQA Reflective QoS Attribute

RQI Reflective QoS Indication

RSC Relay Service Code

RSN Redundancy Sequence Number

RSNPN Registered SNPN

S-NSSAI Single NSSAI

SA Security Association

SDF Service Data Flow

SDT Small Data Transmission

SMF Session Management Function

SGC Service Gap Control

SNN Serving Network Name

SNPN Stand-alone Non-Public Network

SOR Steering of Roaming

SOR-CMCI Steering of Roaming Connected Mode Control Information

SUCI Subscription Concealed Identifier

SUPI Subscription Permanent Identifier

TA Tracking Area

TAC Tracking Area Code

TAI Tracking Area Identity

Tbps Terabits per second

TMGI Temporary Mobile Group Identity

TNGF Trusted Non-3GPP Gateway Function

TSC Time Sensitive Communication

TSCTSF Time Sensitive Communication and Time Synchronization Function

TWIF Trusted WLAN Interworking Function

TSN Time-Sensitive Networking

UAS Uncrewed Aerial System

UAV Uncrewed Aerial Vehicle

UDM Unified Data Management

UL Uplink

UPDS UE policy delivery service

UPF User Plane Function

UPSC UE Policy Section Code

UPSI UE Policy Section Identifier

URN Uniform Resource Name

URSP UE Route Selection Policy

USS UAS Service Supplier

UUAA USS UAV Authorization/Authentication

V2X Vehicle-to-Everything

V2XP V2X policy

W-AGF Wireline Access Gateway Function

WLAN Wireless Local Area Network

WUS Wake-up signal

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

#### 5.5.4.1 General

The purpose of the authentication and key agreement procedure for 5G ProSe UE-to-network relay is to perform the authentication for 5G ProSe remote UE initiated by the 5G ProSe UE-to-network relay and to agree on the KAUSF\_P and KNR\_ProSe when the security for 5G ProSe communication via 5G ProSe UE-to-network relay is performed over control plane as specified in 3GPP TS 33.503 [56].

The procedure as shown in figure 5.5.4.1.1 is initiated by the UE when the UE receives the ProSe direct link establishment request including the SUCI or the 5GPRUK ID of the 5G ProSe remote UE from the 5G ProSe remote UE, for establishing secure PC5 unicast link as specified in 3GPP TS 24.554 [19E].

If the network decides to process the relay key request message, the EAP based authentication and key agreement procedure is initiated and controlled by the network. The exchanges of EAP messages between the 5G ProSe remote UE and the network are relayed by the UE.



Figure 5.5.4.1.1: Authentication and key agreement procedure for 5G ProSe UE-to-network relay

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

#### 5.5.4.3 UE-initiated authentication and key agreement procedure initiation

Upon receiving a ProSe direct link establishment request from the 5G ProSe remote UE including the SUCI or the 5GPRUK ID of the 5G ProSe remote UE, for establishing a secure PC5 unicast link as specified in 3GPP TS 24.554 [19E] when the security for 5G ProSe communication via 5G ProSe UE-to-network relay is performed over control plane as specified in 3GPP TS 33.503 [56], the UE shall:

a) allocate a PRTI value as specified in clause 5.5.4.2;

b) create a RELAY KEY REQUEST message;

c) set the PRTI IE of the RELAY KEY REQUEST message to the allocated PRTI value;

d) set the relay key request parameters IE of the RELAY KEY REQUEST message with SUCI or 5GPRUK ID, relay service code, and nonce\_1 received from the of the 5G ProSe remote UE;

e) send the RELAY KEY REQUEST message; and

f) start the timer T35xx upon sending the RELAY KEY REQUEST message.

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

#### 5.5.4.4 UE-initiated authentication and key agreement procedure accepted by the network

Upon receiving the RELAY KEY REQUEST message, the AMF processes the message and interacts with the AUSF as specified in 3GPP TS 33.503 [56]. If EAP-AKA' authentication for the 5G ProSe UE-to-network relay is initiated by the network, the AMF shall:

a) create a RELAY AUTHENTICATION REQUEST message;

b) set the PRTI IE of the RELAY AUTHENTICATION REQUEST message to the PRTI value of the received RELAY KEY REQUEST message;

c) set the EAP message IE of the RELAY AUTHENTICATION REQUEST message to EAP request message received from the AUSF; and

d) send the RELAY AUTHENTICATION REQUEST message to the UE.

Upon receiving the RELAY AUTHENTICATION REQUEST message, the UE stops the timer T35xx and forwards the EAP message to the 5G ProSe remote UE as specified in 3GPP TS 24.554 [19E].

Upon receiving the EAP response message from the 5G ProSe remote UE as specified in 3GPP TS 24.554 [19E], the UE shall:

a) create a RELAY AUTHENTICATION RESPONSE message;

b) set the PRTI IE of the RELAY AUTHENTICATION RESPONSE message to the PRTI value of the received RELAY AUTHENTICATION REQUEST message;

c) set the EAP message IE of the RELAY AUTHENTICATION RESPONSE message to EAP request message received from the 5G ProSe remote UE; and

d) start a timer T35xx upon sending the RELAY AUTHENTICATION RESPONSE message to the AMF.

After receiving the RELAY AUTHENTICATION RESPONSE message, the AMF may send a new RELAY AUTHENTICATION REQUEST message carrying EAP request message according to further handling of EAP-AKA' authentication from the AUSF as specified in 3GPP TS 33.503 [56]. The UE repeats the handling of the RELAY AUTHENTICATION REQUEST message as described above.

Upon receiving the message from the AUSF that the authentication is successful, the AMF shall:

a) create a RELAY KEY ACCEPT message;

b) set the PRTI IE of the RELAY KEY ACCEPT message to the PRTI value of the RELAY KEY REQUEST message;

c) include the EAP message IE of the RELAY KEY ACCEPT message set to EAP-success message received from the AUSF, if any;

d) include the relay key response parameters IE of the RELAY KEY ACCEPT message set to Key KNR\_ProSe and nonce\_2 received from AUSF; and

e) include the 5GPRUK ID, if provided by AUSF, in the relay key response parameters IE of the RELAY KEY ACCEPT message.

Upon receiving the RELAY KEY ACCEPT message, the UE shall forward the EAP-success message, if any, and nonce\_2 to the 5G ProSe remote UE as specified in 3GPP TS 24.554 [19E], and considers the authentication is completed successfully.

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

#### 8.2.35.1 Message definition

The RELAY KEY ACCEPT message is sent by the AMF to the UE as specified in 3GPP TS 33.503 [56]. See table 8.2.35.1.

Message type: RELAY KEY ACCEPT

Significance: dual

Direction: network to UE

Table 8.2.35.1: RELAY KEY ACCEPT message content

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| IEI | Information Element | Type/Reference | Presence | Format | Length |
|  | Extended protocol discriminator | Extended protocol discriminator9.2 | M | V | 1 |
|  | Security header type | Security header type9.3 | M | V | 1/2 |
|  | Spare half octet | Spare half octet9.5 | M | V | 1/2 |
|  | Relay key accept message identity | Message type9.7 | M | V | 1 |
|  | PRTI | ProSe relay transaction identity9.11.3.aa | M | V | 1 |
|  |  |  |  |  |  |
|  | Relay key response parameters | Relay key response parameters9.11.3.cc | M | TLV-E | TBD |
| 78 | EAP message | EAP message9.11.2.2 | O | TLV-E | 7-1503 |

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

#### 9.11.3.89 Relay key request parameters

The purpose of the relay key request parameters information element is to transport the parameters of the key request for 5G ProSe UE-to-network relay as specified in 3GPP TS 33.503 [56].

The relay key request parameters information element is coded as shown in figure 9.11.3.89.1, figure 9.11.3.89.2 and table 9.11.3.89.1.

The relay key request parameters is a type 6 information element.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  |
| Relay key request parameters IEI | octet 1 |
| Length of Relay key request parameters | octet 2octet 3 |
| Relay service code | octet 4octet 6 |
| Nonce\_1 | octet 7octet 22 |
| Remote UE identity | octet 23octet n |

Figure 9.11.3.89.1: Relay key request parameters information element

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  |
| 0spare | 0spare | 0spare | 0spare | 0spare | 0spare | 0spare | RUIT | octet 23 |
| Remote UE ID | octet 23+1octet n |

Figure 9.11.3.89.2: Remote UE identity

Table 9.11.3.89.1: Relay key request parameters information element

|  |
| --- |
| Relay service code (octet 4 to 6)The relay service code contains 24-bit relay service code as defined in 3GPP TS 24.554 [19E].Nonce\_1 (octet 7 to 22)Nonce\_1 is the 128-bit nonce value as defined in 3GPP TS 24.554 [19E].Remote UE ID type (RUIT) (octet 23, bit 1)Bit**1**0 SUCI1 5GPRUK IDRemote UE ID (octet 23+1 to n)Remote UE ID indicates the value of the 5G ProSe remote UE identity.If the Remote UE ID type is set to SUCI, the Remote UE ID is coded as 5GS mobile identity IE starting from octet 2 with the Type of identity set to "SUCI" (see subclause 9.11.3.4).If the Remote UE ID type is set to 5GPRUK ID, the Remote UE ID is coded as the 5GPRUK ID as defined in 3GPP TS 33.503 [56]. |

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

#### 9.11.3.90 Relay key response parameters

The purpose of the relay key response parameters information element is to transport the parameters of the key response for 5G ProSe UE-to-network relay as specified in 3GPP TS 33.503 [56].

The relay key response parameters information element is coded as shown in figure 9.11.3.90.1 and table 9.11.3.90.1.

The relay key response parameters is a type 6 information element.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  |
| Relay key response parameters IEI | octet 1 |
| Length of Relay key response parameters | octet 2octet 3 |
| 0spare | 0spare | 0spare | 0spare | 0spare | 0spare | 0spare | 5GPII | octet 4 |
| Key KNR\_ProSe | octet 5octet 36 |
| Nonce\_2 | octet 37octet 52 |
| 5GPRUK ID | octet 53\*octet m\* |

Figure 9.11.3.90.1: Relay key response parameters information element

Table 9.11.3.90.1: Relay key response parameters information element

|  |
| --- |
| 5GPRUK ID indication (5GPII) (octet 4, bit 1)Bit**1**0 5GPRUK ID not included1 5GPRUK ID includedKey KNR\_ProSe (octet 5 to 36)Key KNR\_ProSe contains a 256-bit root key that is established between the two entities that communicating using NR PC5 unicast link as defined in 3GPP TS 33.503 [56].Nonce\_2 (octet 37 to 52)Nonce\_2 is the 128-bit nonce value as defined in 3GPP TS 24.554 [19E].5GPRUK ID (octet 53 to m)The 5GPRUK ID is defined in 3GPP TS 33.503 [56]. |

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