

DESCRIPTION

Title of Invention: NETWORK RELAY SECURITY

TECHNICAL FIELD

[0001] This disclosure is directed generally to digital wireless communications.

BACKGROUND

[0002] Mobile telecommunication technologies are moving the world toward an increasingly connected and networked society. In comparison with the existing wireless networks, next generation systems and wireless communication techniques will need to support a much wider range of use-case characteristics and provide a more complex and sophisticated range of access requirements and flexibilities.

[0003] Long-Term Evolution (LTE) is a standard for wireless communication for mobile devices and data terminals developed by 3rd Generation Partnership Project (3GPP). LTE Advanced (LTE-A) is a wireless communication standard that enhances the LTE standard. The 5th generation of wireless system, known as 5G, advances the LTE and LTE-A wireless standards and is committed to supporting higher data-rates, large number of connections, ultra-low latency, high reliability and other emerging business needs.

SUMMARY

[0004] Techniques are disclosed for performing network relay security.

[0005] A first wireless communication method includes receiving, by a network device, a request message that includes an identifier associated with a first communication device; determining, by the network device in response to the receiving, that the first communication device is authenticated based on a local policy of the network device; and sending, by the network device in response to the determining, a message to a second communication device to relay to the first communication device, where the message indicates that the identifier is rejected by the network device for communication with the first communication device, or where the message indicates that the first communication device is triggered to send another identifier.

[0006] In some embodiments, the message is a reject message that includes a cause of a rejection and a transaction identifier, the reject message indicates that the identifier is rejected by the network device for communication with the first communication device, and the method further comprises: receiving, from the first communication device and in response to the sending, a second message that includes a subscription concealed identifier (SUCI). In some embodiments, the message is an identity request message that includes a transaction identifier, and the method further comprises: receiving, from the first communication device and in response to the sending, a second message that includes a subscription concealed identifier (SUCI). In some embodiments, the second communication device is authorized to act as a relay between the first communication device and a communication network that includes the network device. In some embodiments, the identifier includes a 5G ProSe Relay User Key (PRUK) identifier (ID). In some embodiments, the network device includes a remote access and mobility management function (AMF) device.

[0007] A second wireless communication method includes receiving, by a first network device from a second network device, a first request message that includes an identifier associated with a first communication device; transmitting, by the first network device to a third network device, a second request message that includes the identifier; and receiving, by the first network device and in response to the second request message, a response message from the third network device, wherein the response message indicates whether the third network device identifies a relay key using the identifier.

[0008] In some embodiment, the third network device is determined by the first network device based on the identifier. In some embodiment, after the receiving and prior to the transmitting, the method further comprises: transmitting, by the first network device, a third request to the third network device, wherein the third request includes the identifier; and receiving, from the third network device, another identifier that identifies the third network device. In some embodiment, the identifier includes a 5G ProSe Relay User Key (PRUK) identifier (ID) that includes a routing identifier or a routing indicator (RID), and wherein the relay key includes 5G PRUK. In some embodiment, the 5G PRUK ID includes a first part that includes the RID and a prose temporary user equipment identifier (P-TID), and a second part that includes a home network identifier, and the first part precedes the second part.

[0009] In some embodiment, a second communication device is authorized to act as a relay between the first communication device and a communication network that includes any one or more of first network device, the second network device, and the third network device. In some embodiment, the first network device includes an authentication server function (AUSF) device, the second network device includes a remote access and mobility management function (AMF) device, and the third network device includes a prose anchor function (PAnF).

[0010] A third wireless communication method includes transmitting, by a second network device to a third network device, a request message that includes an identifier associated with a first communication device; and receiving, by the second network device and in response to the request message, a response message from the third network device, wherein the response message indicates whether the third network device identifies a relay key using the identifier.

[0011] In some embodiments, the third network device is determined by the second network device based on the identifier. In some embodiments, prior to the transmitting, the method further comprises: transmitting, by the second network device, a second request to the third network device, wherein the third request includes the identifier; and receiving, from a first network device, another identifier that identifies the third network device, wherein the first network device includes an authentication server function (AUSF) device. In some embodiments, the identifier includes a 5G ProSe Relay User Key (PRUK) identifier (ID) that includes a routing identifier or a routing indicator (RID), and wherein the relay key includes 5G PRUK. In some embodiments, the 5G PRUK ID includes a first part that includes the RID and a prose temporary user equipment identifier (P-TID), and a second part that includes a home network identifier, and the first part precedes the second part.

[0012] In some embodiments, a second communication device is authorized to act as a relay between the first communication device and a communication network that includes any one or more of the second network device, and the third network device. In some embodiments, the second network device includes a remote access and mobility management function (AMF) device, and the third network device includes a prose anchor function (PAnF).

[0013] A fourth wireless communication method includes receiving, by a first network device from a second network device, a first request message that includes first identifier associated with a first communication device and a second identifier; transmitting, by the first network device to a third network device, a second request message that includes the first

identifier; and receiving, by the first network device and in response to the second request message, a response message from the third network device, wherein the response message indicates whether the third network device authenticated the first communication device.

[0014] In some embodiments, the first identifier includes a 5G ProSe Relay User Key (PRUK) identifier (ID), and the second identifier includes a subscription concealed identifier (SUCI). In some embodiments, a second communication device is authorized to act as a relay between the first communication device and a communication network that includes any one or more of the first network device, the second network device, and the third network device. In some embodiments, the first network device includes an authentication server function (AUSF) device, the second network device includes a remote access and mobility management function (AMF) device, and the third network device includes a unified data management (UDM).

[0015] In yet another exemplary aspect, the above-described methods are embodied in the form of processor-executable code and stored in a non-transitory computer-readable storage medium. The code included in the computer readable storage medium when executed by a processor, causes the processor to implement the methods described in this patent document.

[0016] In yet another exemplary embodiment, a device that is configured or operable to perform the above-described methods is disclosed.

[0017] The above and other aspects and their implementations are described in greater detail in the drawings, the descriptions, and the claims.

BRIEF DESCRIPTION OF THE DRAWING

[0018] FIG. 1 shows an architecture for 5G Core Network.

[0019] FIGS. 2A-2B show a security procedure over control plane.

[0020] FIGS. 3A-3B show an example flowchart of a security procedure where the Remote user equipment (UE) uses either subscription concealed identifier (SUCI) or 5G ProSe Relay User Key (PRUK) identifier (ID) without prose anchor function (PAnF) and authentication server function (AUSF) store the 5G PRUK.

[0021] FIGS. 4A-4B shows an example flowchart of a security procedure where the Remote UE uses either SUCI or 5G PRUK ID and AUSF generates K_{NR_Prose} and unified data management (UDM) stores 5G RPUK.

[0022] FIGS. 5A-5B show an example flowchart of a security procedure where the Remote UE uses either SUCI or 5G PRUK ID and AUSF generates K_{NR_Prose} , and UDM generates and stores 5G PRUK.

[0023] FIGS. 6A-6B show an example flowchart of a security procedure where the Remote UE uses either SUCI or 5G PRUK ID and UDM generates 5G PRUK and K_{NR_Prose} and stores 5G PRUK.

[0024] FIGS. 7A-7B show an example flowchart of a security procedure where the Remote UE uses both SUCI and 5G PRUK ID and AUSF generates K_{NR_Prose} , and UDM stores 5G PRUK.

[0025] FIGS. 8A-8B show an example flowchart of a security procedure where the Remote UE uses both SUCI and 5G PRUK ID and AUSF generates K_{NR_Prose} and stores 5G PRUK.

[0026] FIGS. 9A-9B show an example flowchart of a security procedure where the Remote UE uses both SUCI and 5G PRUK ID and AUSF generates K_{NR_Prose} , and UDM generates and stores 5G PRUK.

[0027] FIGS. 10A-10B show an example flowchart of a security procedure where the Remote UE uses both SUCI and 5G PRUK ID and UDM generates K_{NR_Prose} and stores 5G PRUK.

[0028] FIGS. 11A-11B show an example flowchart of a security procedure where the Remote UE uses either SUCI or 5G PRUK ID and AUSF finds PAnF, and AUSF generates K_{NR_Prose} .

[0029] FIGS. 12A-12B show an example flowchart of a security procedure where the Remote UE uses either SUCI or 5G PRUK ID and AMF finds PAnF, and PAnF generates K_{NR_Prose} .

[0030] FIGS. 13A-13B show an example flowchart of a security procedure where the Remote UE uses either SUCI or 5G PRUK ID and AUSF finds PAnF, and PAnF generate K_{NR_Prose} .

[0031] FIGS. 14A-14B show an example flowchart of a security procedure where the Remote UE uses both SUCI and 5G PRUK ID and AUSF finds PAnF, and AUSF generate K_{NR_Prose} .

[0032] FIGS. 15A-15B show an example flowchart of a security procedure where the Remote UE uses both SUCI and 5G PRUK ID and AMF finds PAnF, and PAnF generate K_{NR_Prose} .

[0033] FIGS. 16A-16B show an example flowchart of a security procedure where the Remote UE uses both SUCI and 5G PRUK ID and AUSF finds PAnF, and PAnF generate K_{NR_Prose} .

[0034] FIG. 17 shows an example flowchart for an authentication technique.

[0035] FIG. 18 shows an exemplary block diagram of a hardware platform that may be a part of a network device or a communication device.

[0036] FIG. 19 shows an example of wireless communication including a base station (BS) and user equipment (UE) based on some implementations of the disclosed technology.

[0037] FIG. 20 shows an example flowchart for facilitating network security between a network device and a remote communication device.

[0038] FIGS. 21 to 22 show example flowcharts for receiving by a network device a message that indicates whether another network device identifies a relay key using an identifier.

[0039] FIG. 23 shows a flowchart for receiving a message by a network node that indicates whether another network node authenticates a communication device.

DETAILED DESCRIPTION

[0040] 3GPP system is designed to authorize a UE to access 5GC via a 5G UE-to-Network Relay and to authorize a UE to perform as a UE-to-Network Relay. Without a proper authorization, unauthorized entities will be able to access 5GC via UE-to-Network Relay or act as UE-to-Network Relays creating a vulnerability and causing possible (D)DOS attacks or leading to unauthorized service usage on both 5GS and UE-to-Network Relay.

[0041] Security procedure over control plane is specified in TR 33.503 clause 6.3.3.3. UE will generate 5G ProSe Relay User Key (PRUK) identifier (ID) after authentication of UE. However, the PRUK ID also can be used to access the network. How to use the PRUK ID to access the network is not specified.

[0042] The example headings for the various sections below are used to facilitate the understanding of the disclosed subject matter and do not limit the scope of the claimed subject matter in any way. Accordingly, one or more features of one example section can be combined

with one or more features of another example section. Furthermore, 5G terminology is used for the sake of clarity of explanation, but the techniques disclosed in the present document are not limited to 5G technology only, and may be used in wireless systems that implemented other protocols.

[0043] I. Introduction

[0044] FIG. 1 shows an architecture for 5G Core Network. In the architecture, 5G DDNMF is introduced into 5GC as a new network function. 5G DDNMF has similar functions from architecture point of view to the DDNMF part of ProSe Function.

[0045] Security procedure over control plane is shown in FIGS. 2A-2B and as further described with step numbers below. FIG. 2B is a continuation of the process in FIG. 2A.

[0046] 0. The 5G ProSe Remote UE and the 5G ProSe UE-to-Network Relay can be registered with the network. The 5G ProSe UE-to-Network Relay can be authenticated and authorized by the network to provide UE-to-Network relay service. The 5G ProSe Remote UE can be authenticated and authorized by the network to receive UE-to-Network relay service. PC5 security policies are provisioned to the 5G ProSe Remote UE and the 5G ProSe UE-to-Network Relay respectively during this authorization and information provisioning procedure.

[0047] 1. The 5G ProSe Remote UE can initiate discovery procedure using any of Model A or Model B method.

[0048] 2-5. After the discovery of the 5G ProSe UE-to-Network Relay, the 5G ProSe Remote UE can send a Direct Communication Request to the 5G ProSe UE-to-Network Relay for establishing secure PC5 unicast link. The 5G ProSe Remote UE can include its security capabilities and PC5 security signalling policy in the DCR message. The message can also include subscription concealed identifier (SUCI), Relay Service Code, Nonce_1. Upon receiving the DCR message, the 5G ProSe UE-to-Network Relay can send the Relay Key Request to the AMF of the 5G ProSe UE-to-Network Relay, including partial parameters received in the DCR message. The 5G ProSe UE-to-Network Relay can 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 and PC5 messages. The AMF of the 5G ProSe UE-to-Network Relay can verify whether the 5G ProSe UE-to-Network Relay is authorized to provide the UE-to-Network relay service. The AMF of the 5G ProSe UE-to-Network Relay can select an authentication server function (AUSF) based on SUCI and forward the parameters received in

Relay Key Request to the AUSF in Nausf_UEAuthentication_ProseAuthenticate Request message. The Nausf_UEAuthentication_ProseAuthenticate Request message can contain the 5G ProSe Remote UE's SUCI, Relay Service Code, Nonce_1. The AUSF can initiate a 5G ProSe Remote UE specific authentication using the ProSe specific parameters received (e.g., RSC, etc.).

[0049] 6. The AUSF of the 5G ProSe Remote UE can retrieve the Authentication Vectors from the UDM via Nudm_UEAuthentication_GetProseAv Request message and trigger authentication of the 5G ProSe Remote UE. This authentication is performed between the AUSF of the 5G ProSe Remote UE and the 5G ProSe Remote UE via the AMF of the 5G ProSe UE-to-Network Relay and the 5G ProSe UE-to-Network Relay. Based on SUPI, the UDM can choose the authentication method.

[0050] 7a. If EAP-AKA' is selected by UDM, the AUSF of the 5G ProSe Remote UE can trigger authentication of the 5G ProSe Remote UE based on EAP-AKA'. The AUSF of the 5G ProSe Remote UE generates the EAP-Request/AKA'-Challenge message and send EAP-Request/AKA'-Challenge message to the AMF of the 5G ProSe UE-to-Network Relay in a Nausf_UEAuthentication_ProseAuthenticate Response message.

[0051] 7b. The AMF of the 5G ProSe UE-to-Network Relay can forward the Relay Authentication Request (including the EAP-Request/AKA'-Challenge) to the 5G ProSe UE-to-Network Relay over NAS message, including transaction identifier of the 5G ProSe Remote UE in the message. The NAS message is protected using the NAS security context created for the 5G ProSe UE-to-Network Relay.

[0052] 7c. Based on the transaction identifier, the 5G ProSe UE-to-Network Relay can forwards the EAP-Request/AKA'-Challenge to the 5G ProSe Remote UE over PC5 messages.

[0053] The USIM in the 5G ProSe Remote UE verifies the freshness of the received values by checking whether AUTN can be accepted.

[0054] For EAP-AKA', the USIM computes a response RES. The USIM can return RES, CK, IK to the ME. The ME can derive CK' and IK'.

[0055] 7d. The 5G ProSe Remote UE can return EAP-Response/AKA'-Challenge to the 5G ProSe UE-to-Network Relay over PC5 messages.

- [0056] 7e. The 5G ProSe UE-to-Network Relay forwards the EAP-Response/AKA'-Challenge together with the transaction identifier of the 5G ProSe Remote UE to the AMF of the 5G ProSe UE-to-Network Relay in a NAS message Relay Authentication Response.
- [0057] 7f. The AMF of the 5G ProSe UE-to-Network Relay forwards EAP-Response/AKA'-Challenge to the AUSF of the 5G ProSe Remote UE via Nausf_UEAuthentication_ProSeAuthenticate Request.
- [0058] The AUSF of the 5G ProSe Remote UE performs the UE authentication by verifying the received information.
- [0059] For EAP-AKA', the AUSF of the 5G ProSe Remote UE and the 5G ProSe Remote UE may exchange EAP-Request/AKA'-Notification and EAP-Response /AKA'-Notification messages via the AMF of the 5G ProSe UE-to-Network Relay. After the exchanges, the AUSF of the 5G ProSe Remote UE derives K_{AUSF} without calculating the K_{SEAF} .
- [0060] The AUSF of the 5G ProSe Remote UE and the 5G ProSe Remote UE can derive a new K_{AUSF_P} (different from K_{AUSF}). NAS SMC procedure is not performed between 5G ProSe Remote UE and AMF of the 5G ProSe UE-to-Network Relay.
- [0061] 8. As shown in FIG. 2B, which continues the process from FIG. 2A, on successful authentication, the AUSF of the 5G ProSe Remote UE and the 5G ProSe Remote UE can generate 5GPRUK as specified in Annex A.2 and 5GPRUK ID using the newly derived K_{AUSF_P} .
- [0062] 9. The AUSF of the 5G ProSe Remote UE can generate the K_{NR_ProSe} key.
- [0063] 10-11. The AUSF of the 5G ProSe Remote UE can send the K_{NR_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. When receiving a K_{NR_ProSe} from the AUSF of the 5G ProSe Remote UE, the AMF of the 5G ProSe UE-to-Network Relay can not attempt to trigger NAS SMC procedure with the 5G ProSe Remote UE. The 5G ProSe UE-to-Network Relay derives PC5 session key $K_{relay-sess}$ and confidentiality and integrity keys from K_{NR_ProSe} .
- [0064] 12. The 5G ProSe UE-to-Network Relay can send the received Nonce_2 to the 5G ProSe Remote UE in Direct Security mode command message, which is protected using $K_{relay-int}$ or/and $K_{relay-enc}$ derived from $K_{relay-sess}$ according to the negotiated PC5 signalling policies between the 5G ProSe Remote UE and the 5G ProSe UE-to-Network Relay.

[0065] 13-15b. The 5G ProSe Remote UE can use the 5GPRUK ID to locate the KAUSF_P/5GPRUK to be used for the PC5 link security. The 5G ProSe Remote UE can generate the KNR_ProSe key to be used for Remote access via the 5G ProSe UE-to-Network Relay in the same way as defined in step 9. The 5G ProSe Remote UE can derive PC5 session key Krelay-sess and confidentiality and integrity keys from KNR_ProSe the same way as defined in step 11. The 5G ProSe Remote UE can send the Direct Security Mode Complete message containing its PC5 user plane security policies to the 5G ProSe UE-to-Network relay, which is protected by Krelay-int or/and Krelay-enc derived from Krelay-sess according to the negotiated PC5 signalling policies between the 5G ProSe Remote UE and the 5G ProSe UE-to-Network Relay. After the successful verification of the Direct Security Mode complete message, the 5G ProSe UE-to-Network Relay responds a Direct Communication Accept message to the 5G ProSe Remote UE to finish the PC5 connection establishment procedures.

[0066] Further communication between the 5G ProSe Remote UE and the Network takes place securely via the 5G ProSe UE-to-Network Relay.

[0067] **II. Case 1: The Remote UE use SUCI or 5G PRUK ID. No PAnF.**

[0068] **II.(a) Case 1.1: AUSF generate K_{NR_Prose} and store 5G PRUK.**

[0069] FIGS. 3A-3B show an example flowchart of a security procedure where the Remote UE uses either SUCI or 5G PRUK ID without PAnF. FIG. 3B is a continuation of the process in FIG. 3A.

[0070] 0. The Remote UE and relay UE can be registered with the network. The UE-to-Network relay can be authenticated and authorized by the network to support as a relay UE. Remote UE can be authenticated and authorized by the network to act as a Remote UE.

[0071] 1. The remote UE can initiate discovery procedure using any of Model A or Model B method .

[0072] 2. After the discovery of the UE-to-Network relay, the Remote UE can send a Direct Communication Request to the relay UE for establishing secure PC5 unicast link. The Remote UE can include its security capabilities and security policy in the DCR message. The message can also include 5GPRUK ID if available, Relay Service Code, Nonce_1. If UE has no available 5G PRUK ID or the 5G PRUK ID has been reject before, the UE can use SUCI instead of 5G PRUK ID.

[0073] 3. Upon receiving the DCR message, the Relay UE can send the relay key request to the relay AMF, including the parameters received in the DCR message.

[0074] 4. The Relay AMF can verify whether the relay UE is authorized to act as U2N relay. The Relay AMF decides to whether to authenticate the Remote UE. If so, AMF use Option 1 or Option 2. Otherwise go to step 5a.

[0075] Option 1

[0076] 4a. If the Relay AMF decide to authenticate the Remote UE based on its (the Relay AMF's) local policy, then the Relay AMF sends Reject message include the cause and the transaction identifier. The local policy may indicate that, for example, the AMF may store a mapping between 5G PRUK ID and network function (NF) instance ID), but if the mapping information is not available, e.g., the NF instance ID is invalid, then the AMF cannot find the NF related to the 5G PRUK ID. In some embodiments, if AMF may not know how to use the 5G PRUK ID, the AMF may trigger the remote UE to use SUCI, so that the remote UE can be authenticated whenever the remote UE try to use the relay UE service. In such embodiments, the 5G PRUK can be refreshed. In some embodiments, if the AMF receives a reject message or no key response from the other NF, the AMF can send a message to the relay UE to send to the remote UE to trigger the remote UE to send SUCI.

[0077] 4b. The Relay UE forward the Reject message to the Remote UE. The cause in the Reject message indicates that Remote UE should send another message so that the Reject message triggers the Remote UE to send a new DCR message as mentioned in 4c.

[0078] 4c. The Remote UE sends a new DCR message, the message can include the Remote UE's SUCI, Relay service code and Nonce_1. The Nonce_1 can be the same or different with the Nonce_1 in step 2.

[0079] 4d. The Relay UE can send the relay key request to the relay AMF, including the parameters received in the DCR message. Then go to Step 5.

[0080] Option 2

[0081] 4e. If the Relay AMF decide to authenticate the Remote UE based on its (the Relay AMF's) local policy, then the Relay AMF sends Identity Request message include the transaction identifier.

[0082] 4f. The Relay UE forward the Identity Request message to the Remote UE. The Identity request message indicates to the Remote UE that the Relay AMF is requesting SUCI from the Remote UE.

[0083] 4g. The Remote UE sends its SUCI in the Identity Response message

[0084] 4h. The Relay UE forward the Identity Response message to the Relay AMF. Then go to Step 5.

[0085] 5a. The relay AMF can select AUSF based on 5GPRUK ID and sends a Nausf_UEAuthentication_ProseAuthenticate Request to AUSF. The request message include 5GPRUK ID, RSC, Nonce1, SN name.

[0086] If AMF can use 5G PRUK ID to find a AUSF instance ID which is stored in the Relay AMF, then the AMF select the AUSF.

[0087] If RID is included in the 5G PRUK ID, the AUSF selection should consider the RID.

[0088] The 5GPRUK ID may be generated as follows:

[0089] 5GPRUK ID is in NAI format as specified in clause 2.2 of IETF RFC 7542, e.g. username@realm. The username part can include the RID and the P-TID (Prose Temporary UE Identifier), and the realm part can include Home Network Identifier.

[0090] The P-TID is derived from K_{AUSF} or K_{ausf_p} .

[0091] 5b. If the AUSF can not find the 5G PRUK which is related to the 5G PRUK ID. The AUSF sends a reject response to the AMF with a cause.

[0092] 5c. AMF use Option 1 or Option 2.

[0093] 5. As shown in FIG. 3B, which is a continuation of the process in FIG. 3A, the relay AMF sends a Nausf_UEAuthentication_ProseAuthenticate Request to AUSF. The request message include 5GPRUK ID, RSC, Nonce1, SN name.

[0094] 6a~6b. The AUSF can retrieve the Authentication Vectors from the UDM via Nudm_UEAuthentication_GetProseAv Request message and trigger authentication of the remote UE.

[0095] 7a. If EAP-AKA' is selected by UDM, the AUSF of the 5G ProSe Remote UE can trigger authentication of the 5G ProSe Remote UE based on EAP-AKA'. The AUSF of the 5G ProSe Remote UE generates the EAP-Request/AKA'-Challenge message and send EAP-Request/AKA'-Challenge message to the AMF of the 5G ProSe UE-to-Network Relay in a Nausf_UEAuthentication_ProSeAuthenticate Response message.

- [0096]** 7b. The AMF of the 5G ProSe UE-to-Network Relay can forward the Relay Authentication Request (including the EAP-Request/AKA'-Challenge) to the 5G ProSe UE-to-Network Relay over NAS message, including transaction identifier of the 5G ProSe Remote UE in the message. The NAS message is protected using the NAS security context created for the 5G ProSe UE-to-Network Relay.
- [0097]** 7c. Based on the transaction identifier, the 5G ProSe UE-to-Network Relay can forwards the EAP-Request/AKA'-Challenge to the 5G ProSe Remote UE over PC5 messages.
- [0098]** The USIM in the 5G ProSe Remote UE verifies the freshness of the received values by checking whether AUTN can be accepted.
- [0099]** For EAP-AKA', the USIM computes a response RES. The USIM can return RES, CK, IK to the ME. The ME can derive CK' and IK'.
- [0100]** 7d. The 5G ProSe Remote UE can return EAP-Response/AKA'-Challenge to the 5G ProSe UE-to-Network Relay over PC5 messages.
- [0101]** 7e. The 5G ProSe UE-to-Network Relay forwards the EAP-Response/AKA'-Challenge together with the transaction identifier of the 5G ProSe Remote UE to the AMF of the 5G ProSe UE-to-Network Relay in a NAS message Relay Authentication Response.
- [0102]** 7f. The AMF of the 5G ProSe UE-to-Network Relay forwards EAP-Response/AKA'-Challenge to the AUSF of the 5G ProSe Remote UE via Nausf_UEAuthentication_ProSeAuthenticate Request.
- [0103]** The AUSF of the 5G ProSe Remote UE performs the UE authentication by verifying the received information .
- [0104]** For EAP-AKA', the AUSF of the 5G ProSe Remote UE and the 5G ProSe Remote UE may exchange EAP-Request/AKA'-Notification and EAP-Response /AKA'-Notification messages via the AMF of the 5G ProSe UE-to-Network Relay. After the exchanges, the AUSF of the 5G ProSe Remote UE derives KAUSF without calculating the KSEAF.
- [0105]** The AUSF of the 5G ProSe Remote UE and the 5G ProSe Remote UE can derive a new K_{AUSF_P} (different from K_{AUSF}). NAS SMC procedure is not performed between 5G ProSe Remote UE and AMF of the 5G ProSe UE-to-Network Relay.
- [0106]** 8. On successful authentication, the AUSF of the 5G ProSe Remote UE and the 5G ProSe Remote UE can generate 5GPRUK and 5GPRUK ID using the newly derived K_{AUSF_P} .
- [0107]** 9. AUSF sends a Nudm_UEAuthentication_ProseResultConfirmation to the UDM.

[0108] 10. The AUSF of the 5G ProSe Remote UE can generate the K_{NR_ProSe} key.

[0109] 11. The AUSF of the 5G ProSe Remote UE can send the K_{NR_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. When receiving a K_{NR_ProSe} from the AUSF of the 5G ProSe Remote UE, the AMF of the 5G ProSe UE-to-Network Relay can not attempt to trigger NAS SMC procedure with the 5G ProSe Remote UE. The 5G ProSe UE-to-Network Relay derives PC5 session key Krelay-sess and confidentiality and integrity keys from K_{NR_ProSe} .

[0110] 12. The 5G ProSe UE-to-Network Relay can send the received Nonce_2 to the 5G ProSe Remote UE in Direct Security mode command message, which is protected using Krelay-int or/and Krelay-enc derived from Krelay-sess according to the negotiated PC5 signalling policies between the 5G ProSe Remote UE and the 5G ProSe UE-to-Network Relay.

[0111] 13-15b. The 5G ProSe Remote UE can use the 5GPRUK ID to locate the KAUSF_P/5GPRUK to be used for the PC5 link security. The 5G ProSe Remote UE can generate the K_{NR_ProSe} key to be used for Remote access via the 5G ProSe UE-to-Network Relay. The 5G ProSe Remote UE can derive PC5 session key Krelay-sess and confidentiality and integrity keys from K_{NR_ProSe} . The 5G ProSe Remote UE can send the Direct Security Mode Complete message containing its PC5 user plane security policies to the 5G ProSe UE-to-Network relay, which is protected by Krelay-int or/and Krelay-enc derived from Krelay-sess according to the negotiated PC5 signalling policies between the 5G ProSe Remote UE and the 5G ProSe UE-to-Network Relay. After the successful verification of the Direct Security Mode complete message, the 5G ProSe UE-to-Network Relay responds a Direct Communication Accept message to the 5G ProSe Remote UE to finish the PC5 connection establishment procedures.

[0112] FIG. 20 shows an example flowchart for facilitating network security between a network device and a remote communication device. Operation 2002 includes receiving, by a network device, a request message that includes an identifier associated with a first communication device. Operation 2004 includes determining, by the network device in response to the receiving, that the first communication device is authenticated based on a local policy of the network device. Operation 2006 includes sending, by the network device in response to the determining, a message to a second communication device to relay to the first communication

device, where the message indicates that the identifier is rejected by the network device for communication with the first communication device, or where the message indicates that the first communication device is triggered to send another identifier.

[0113] In some embodiments, the message is a reject message that includes a cause of a rejection and a transaction identifier, the reject message indicates that the identifier is rejected by the network device for communication with the first communication device, and the method further comprises: receiving, from the first communication device and in response to the sending, a second message that includes a subscription concealed identifier (SUCI). In some embodiments, the message is an identity request message that includes a transaction identifier, and the method further comprises: receiving, from the first communication device and in response to the sending, a second message that includes a subscription concealed identifier (SUCI). In some embodiments, the second communication device is authorized to act as a relay between the first communication device and a communication network that includes the network device. In some embodiments, the identifier includes a 5G ProSe Relay User Key (PRUK) identifier (ID). In some embodiments, the network device includes a remote access and mobility management function (AMF) device.

[0114] II.(b) Case 1.2: AUSF generate K_{NR_Prose} and UDM store 5G PRUK.

[0115] UDM stores 5G PRUK

[0116] FIGS. 4A-4B show an example flowchart of a security procedure where AUSF generates K_{NR_Prose} and UDM stores 5G RPUK. FIG. 4B is a continuation of the process in FIG. 4A.

[0117] 0. The Remote UE and relay UE can be registered with the network. The UE-to-Network relay can be authenticated and authorized by the network to support as a relay UE. Remote UE can be authenticated and authorized by the network to act as a Remote UE.

[0118] 1. The remote UE can initiate discovery procedure using any of Model A or Model B method .

[0119] 2. After the discovery of the UE-to-Network relay, the Remote UE can send a Direct Communication Request to the relay UE for establishing secure PC5 unicast link. The Remote UE can include its security capabilities and security policy in the DCR message. The message can also include 5GPRUK ID if available, Relay Service Code, Nonce_1. If UE has no available

5G PRUK ID or the 5G PRUK ID has been reject before, the UE can use SUCI instead of 5G PRUK ID.

[0120] 3. Upon receiving the DCR message, the Relay UE can send the relay key request to the relay AMF, including the parameters received in the DCR message.

[0121] 4. The Relay AMF can verify whether the relay UE is authorized to act as U2N relay. The Relay AMF decides to whether to authenticate the Remote UE. If so, AMF use Option 1 or Option 2. Otherwise go to step 5a.

[0122] Option 1

[0123] 4a. If the Relay AMF decide to authenticate the Remote UE based on its (the Relay AMF's) local policy, then the Relay AMF sends Reject message include the cause and the transaction identifier.

[0124] 4b. The Relay UE forward the Reject message to the Remote UE.

[0125] 4c. The Remote UE sends a new DCR message, the message can include the Remote UE's SUCI, Relay service code and Nonce_1. The Nonce_1 can be the same or different with the Nonce_1 in step 2.

[0126] 4d. The Relay UE can send the relay key request to the relay AMF, including the parameters received in the DCR message. Then go to Step 5.

[0127] Option 2

[0128] 4e. If the Relay AMF decide to authenticate the Remote UE based on its (the Relay AMF's) local policy, then the Relay AMF sends Identity Request message include the transaction identifier.

[0129] 4f. The Relay UE forward the Identity Request message to the Remote UE.

[0130] 4g. The Remote UE sends its SUCI in the Identity Response message

[0131] 4h. The Relay UE forward the Identity Response message to the Relay AMF. Then go to Step 5.

[0132] 5a. The relay AMF can select AUSF based on 5GPRUK ID and sends a Nausf_UEAuthentication_ProseAuthenticate Request to AUSF. The request message include 5GPRUK ID, RSC, Nonce1, SN name.

[0133] 5b. The AUSF sends the Nudm_Prosekey_Get Request to UDM

[0134] 5c. The UDM may decide to authenticate the UE based on its local policy and sends a reject message with a cause to AUSF. Then AUSF forwards the Reject message to Relay AMF, Relay AMF uses Option 1 or Option 2.

[0135] 5d. If UDM decides not to authenticate the UE, then UDM sends a response to the AUSF with the 5G PRUK. The UDM may also send a Nonce_2 to AUSF. Then go to step 10.

[0136]

[0137] 5. As shown in FIG. 4B, which is a continuation of the process in FIG. 4A, the relay AMF sends a Nausf_UEAuthentication_ProseAuthenticate Request to AUSF. The request message includes 5GPRUK ID, RSC, Nonce1, SN name.

[0138] 6a~6b. The AUSF can retrieve the Authentication Vectors from the UDM via Nudm_UEAuthentication_GetProseAv Request message and trigger authentication of the remote UE.

[0139] 7a. If EAP-AKA' is selected by UDM, the AUSF of the 5G ProSe Remote UE can trigger authentication of the 5G ProSe Remote UE based on EAP-AKA'. The AUSF of the 5G ProSe Remote UE generates the EAP-Request/AKA'-Challenge message and sends EAP-Request/AKA'-Challenge message to the AMF of the 5G ProSe UE-to-Network Relay in a Nausf_UEAuthentication_ProSeAuthenticate Response message.

[0140] 7b. The AMF of the 5G ProSe UE-to-Network Relay can forward the Relay Authentication Request (including the EAP-Request/AKA'-Challenge) to the 5G ProSe UE-to-Network Relay over NAS message, including transaction identifier of the 5G ProSe Remote UE in the message. The NAS message is protected using the NAS security context created for the 5G ProSe UE-to-Network Relay.

[0141] 7c. Based on the transaction identifier, the 5G ProSe UE-to-Network Relay can forward the EAP-Request/AKA'-Challenge to the 5G ProSe Remote UE over PC5 messages.

[0142] The USIM in the 5G ProSe Remote UE verifies the freshness of the received values by checking whether AUTN can be accepted.

[0143] For EAP-AKA', the USIM computes a response RES. The USIM can return RES, CK, IK to the ME. The ME can derive CK' and IK'.

[0144] 7d. The 5G ProSe Remote UE can return EAP-Response/AKA'-Challenge to the 5G ProSe UE-to-Network Relay over PC5 messages.

- [0145] 7e. The 5G ProSe UE-to-Network Relay forwards the EAP-Response/AKA'-Challenge together with the transaction identifier of the 5G ProSe Remote UE to the AMF of the 5G ProSe UE-to-Network Relay in a NAS message Relay Authentication Response.
- [0146] 7f. The AMF of the 5G ProSe UE-to-Network Relay forwards EAP-Response/AKA'-Challenge to the AUSF of the 5G ProSe Remote UE via Nausf_UEAuthentication_ProSeAuthenticate Request.
- [0147] The AUSF of the 5G ProSe Remote UE performs the UE authentication by verifying the received information.
- [0148] For EAP-AKA', the AUSF of the 5G ProSe Remote UE and the 5G ProSe Remote UE may exchange EAP-Request/AKA'-Notification and EAP-Response /AKA'-Notification messages via the AMF of the 5G ProSe UE-to-Network Relay. After the exchanges, the AUSF of the 5G ProSe Remote UE derives K_{AUSF} without calculating the K_{SEAF} .
- [0149] The AUSF of the 5G ProSe Remote UE and the 5G ProSe Remote UE can derive a new K_{AUSF_P} (different from K_{AUSF}). NAS SMC procedure is not performed between 5G ProSe Remote UE and AMF of the 5G ProSe UE-to-Network Relay.
- [0150] 8. On successful authentication, the AUSF of the 5G ProSe Remote UE and the 5G ProSe Remote UE can generate 5GPRUK and 5GPRUK ID using the newly derived K_{AUSF_P} .
- [0151] 9. AUSF sends a Nudm_UEAuthentication_ProseResultConfirmation to the UDM. The message includes SUPI, RSC, 5GPRUK and 5GPRUK ID.
- [0152] 10. The AUSF of the 5G ProSe Remote UE can generate the K_{NR_ProSe} key. If UDM sends a Nonce_2 to AUSF, then the AUSF uses the Nonce_2 to generate the K_{NR_ProSe} key. Otherwise, AUSF generates the Nonce_2 itself.
- [0153] 11. The AUSF of the 5G ProSe Remote UE can send the K_{NR_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. When receiving a K_{NR_ProSe} from the AUSF of the 5G ProSe Remote UE, the AMF of the 5G ProSe UE-to-Network Relay can not attempt to trigger NAS SMC procedure with the 5G ProSe Remote UE. The 5G ProSe UE-to-Network Relay derives PC5 session key K_{relay_sess} and confidentiality and integrity keys from K_{NR_ProSe} .
- [0154] 12. The 5G ProSe UE-to-Network Relay can send the received Nonce_2 to the 5G ProSe Remote UE in Direct Security mode command message, which is protected using K_{relay} .

int or/and Krelay-enc derived from Krelay-sess according to the negotiated PC5 signalling policies between the 5G ProSe Remote UE and the 5G ProSe UE-to-Network Relay.

[0155] 13-15b. The 5G ProSe Remote UE can use the 5GPRUK ID to locate the $K_{AUSF_P/5GPRUK}$ to be used for the PC5 link security. The 5G ProSe Remote UE can generate the K_{NR_ProSe} key to be used for Remote access via the 5G ProSe UE-to-Network Relay. The 5G ProSe Remote UE can derive PC5 session key Krelay-sess and confidentiality and integrity keys from K_{NR_ProSe} . The 5G ProSe Remote UE can send the Direct Security Mode Complete message containing its PC5 user plane security policies to the 5G ProSe UE-to-Network relay, which is protected by Krelay-int or/and Krelay-enc derived from Krelay-sess according to the negotiated PC5 signalling policies between the 5G ProSe Remote UE and the 5G ProSe UE-to-Network Relay. After the successful verification of the Direct Security Mode complete message, the 5G ProSe UE-to-Network Relay responds a Direct Communication Accept message to the 5G ProSe Remote UE to finish the PC5 connection establishment procedures.

[0156] II.(c) Case 1.3: AUSF generate K_{NR_ProSe} . UDM generate and store 5G PRUK.

[0157] FIGS. 5A-5B show an example flowchart of a security procedure where AUSF generates K_{NR_ProSe} , and UDM generates and stores 5G PRUK. FIG. 5B is a continuation of the process in FIG. 5A.

[0158] 0. The Remote UE and relay UE can be registered with the network. The UE-to-Network relay can be authenticated and authorized by the network to support as a relay UE. Remote UE can be authenticated and authorized by the network to act as a Remote UE.

[0159] 1. The remote UE can initiate discovery procedure using any of Model A or Model B method.

[0160] 2. After the discovery of the UE-to-Network relay, the Remote UE can send a Direct Communication Request to the relay UE for establishing secure PC5 unicast link. The Remote UE can include its security capabilities and security policy in the DCR message. The message can also include 5GPRUK ID if available, Relay Service Code, Nonce_1. If UE has no available 5G PRUK ID or the 5G PRUK ID has been reject before, the UE can use SUCI instead of 5G PRUK ID.

[0161] 3. Upon receiving the DCR message, the Relay UE can send the relay key request to the relay AMF, including the parameters received in the DCR message.

[0162] 4. The Relay AMF can verify whether the relay UE is authorized to act as U2N relay. The Relay AMF decides to whether to authenticate the Remote UE. If so, AMF use Option 1 or Option 2. Otherwise go to step 5a.

[0163] Option 1

[0164] 4a. If the Relay AMF decide to authenticate the Remote UE based on its (the Relay AMF's) local policy, then the Relay AMF sends Reject message include the cause and the transaction identifier.

[0165] 4b. The Relay UE forward the Reject message to the Remote UE.

[0166] 4c. The Remote UE sends a new DCR message, the message can include the Remote UE's SUCI, Relay service code and Nonce_1. The Nonce_1 can be the same or different with the Nonce_1 in step 2.

[0167] 4d. The Relay UE can send the relay key request to the relay AMF, including the parameters received in the DCR message. Then go to Step 5.

[0168] Option 2

[0169] 4e. If the Relay AMF decide to authenticate the Remote UE based on its (the Relay AMF's) local policy, then the Relay AMF sends Identity Request message include the transaction identifier.

[0170] 4f. The Relay UE forward the Identity Request message to the Remote UE.

[0171] 4g. The Remote UE sends its SUCI in the Identity Response message

[0172] 4h. The Relay UE forward the Identity Response message to the Relay AMF. Then go to Step 5.

[0173] 5a. The relay AMF can select AUSF based on 5GPRUK ID and sends a Nausf_UEAuthentication_ProseAuthenticate Request to AUSF. The request message include 5GPRUK ID, RSC, Nonce1, SN name.

[0174] 5b. The AUSF sends the Nausf_UEAuthentication_ProseAuthenticate Request to UDM

[0175] 5c. The UDM may decide to authenticate the UE based on its local policy and sends a reject message with a cause to AUSF. Then AUSF forward the Reject message to Relay AMF, Relay AMF use Option 1 or Option 2. Then go to step 10a.

[0176] 5. As shown in FIG. 5B, which is a continuation of the process in FIG. 5A, the relay AMF sends a Nausf_UEAuthentication_ProseAuthenticate Request to AUSF. The request message include 5GPRUK ID, RSC, Nonce1, SN name.

[0177] 6a~6b. The AUSF can retrieve the Authentication Vectors from the UDM via Nudm_UEAuthentication_GetProseAv Request message and trigger authentication of the remote UE.

[0178] 7a. If EAP-AKA' is selected by UDM, the AUSF of the 5G ProSe Remote UE can trigger authentication of the 5G ProSe Remote UE based on EAP-AKA'. The AUSF of the 5G ProSe Remote UE generates the EAP-Request/AKA'-Challenge message and send EAP-Request/AKA'-Challenge message to the AMF of the 5G ProSe UE-to-Network Relay in a Nausf_UEAuthentication_ProSeAuthenticate Response message.

[0179] 7b. The AMF of the 5G ProSe UE-to-Network Relay can forward the Relay Authentication Request (including the EAP-Request/AKA'-Challenge) to the 5G ProSe UE-to-Network Relay over NAS message, including transaction identifier of the 5G ProSe Remote UE in the message. The NAS message is protected using the NAS security context created for the 5G ProSe UE-to-Network Relay.

[0180] 7c. Based on the transaction identifier, the 5G ProSe UE-to-Network Relay can forwards the EAP-Request/AKA'-Challenge to the 5G ProSe Remote UE over PC5 messages.

[0181] The USIM in the 5G ProSe Remote UE verifies the freshness of the received values by checking whether AUTN can be .

[0182] For EAP-AKA', the USIM computes a response RES. The USIM can return RES, CK, IK to the ME. The ME can derive CK' and IK'.

[0183] 7d. The 5G ProSe Remote UE can return EAP-Response/AKA'-Challenge to the 5G ProSe UE-to-Network Relay over PC5 messages.

[0184] 7e. The 5G ProSe UE-to-Network Relay forwards the EAP-Response/AKA'-Challenge together with the transaction identifier of the 5G ProSe Remote UE to the AMF of the 5G ProSe UE-to-Network Relay in a NAS message Relay Authentication Response.

[0185] 7f. The AMF of the 5G ProSe UE-to-Network Relay forwards EAP-Response/AKA'-Challenge to the AUSF of the 5G ProSe Remote UE via Nausf_UEAuthentication_ProSeAuthenticate Request.

[0186] The AUSF of the 5G ProSe Remote UE performs the UE authentication by verifying the received information.

[0187] For EAP-AKA', the AUSF of the 5G ProSe Remote UE and the 5G ProSe Remote UE may exchange EAP-Request/AKA'-Notification and EAP-Response /AKA'-Notification messages via the AMF of the 5G ProSe UE-to-Network Relay. After the exchanges, the AUSF of the 5G ProSe Remote UE derives K_{AUSF} without calculating the K_{SEAF} .

[0188] The AUSF of the 5G ProSe Remote UE and the 5G ProSe Remote UE can derive a new K_{AUSF_P} (different from K_{AUSF}). NAS SMC procedure is not performed between 5G ProSe Remote UE and AMF of the 5G ProSe UE-to-Network Relay.

[0189] 8. On successful authentication, the AUSF of the 5G ProSe Remote UE and the 5G ProSe Remote UE can generate 5GPRUK and 5GPRUK ID using the newly derived K_{AUSF_P} .

[0190] 9. AUSF sends a Nudm_UEAuthentication_ProseResultConfirmation to the UDM. The message includes SUPI, RSC.

[0191] 10a. UDM sends a Nudm_ProseKey_Get Response to the AUSF with the 5G PRUK. The UDM may also send a Nonce_2 to AUSF

[0192] 10. The AUSF of the 5G ProSe Remote UE can generate the K_{NR_ProSe} key. If UDM sends a Nonce_2 to AUSF, then the AUSF uses the Nonce_2 to generate the K_{NR_ProSe} key. Otherwise, AUSF generates the Nonce_2 itself.

[0193] 11. The AUSF of the 5G ProSe Remote UE can send the K_{NR_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. When receiving a K_{NR_ProSe} from the AUSF of the 5G ProSe Remote UE, the AMF of the 5G ProSe UE-to-Network Relay can not attempt to trigger NAS SMC procedure with the 5G ProSe Remote UE. The 5G ProSe UE-to-Network Relay derives PC5 session key K_{relay_sess} and confidentiality and integrity keys from K_{NR_ProSe} .

[0194] 12. The 5G ProSe UE-to-Network Relay can send the received Nonce_2 to the 5G ProSe Remote UE in Direct Security mode command message, which is protected using K_{relay_int} or/and K_{relay_enc} derived from K_{relay_sess} according to the negotiated PC5 signalling policies between the 5G ProSe Remote UE and the 5G ProSe UE-to-Network Relay.

[0195] 13-15b. The 5G ProSe Remote UE can use the 5GPRUK ID to locate the K_{AUSF_P} /5GPRUK to be used for the PC5 link security. The 5G ProSe Remote UE can generate

the K_{NR_ProSe} key to be used for Remote access via the 5G ProSe UE-to-Network Relay. The 5G ProSe Remote UE can derive PC5 session key $K_{relay-sess}$ and confidentiality and integrity keys from K_{NR_ProSe} . The 5G ProSe Remote UE can send the Direct Security Mode Complete message containing its PC5 user plane security policies to the 5G ProSe UE-to-Network relay, which is protected by $K_{relay-int}$ or/and $K_{relay-enc}$ derived from $K_{relay-sess}$ according to the negotiated PC5 signalling policies between the 5G ProSe Remote UE and the 5G ProSe UE-to-Network Relay. After the successful verification of the Direct Security Mode complete message, the 5G ProSe UE-to-Network Relay responds a Direct Communication Accept message to the 5G ProSe Remote UE to finish the PC5 connection establishment procedures.

[0196] II.(d) Case 1.4: UDM generate 5G PRUK and K_{NR_ProSe} and store 5G PRUK.

[0197] FIGS. 6A-6B show an example flowchart of a security procedure where UDM generates 5G PRUK and K_{NR_ProSe} and stores 5G PRUK. FIG. 6B is a continuation of the process in FIG. 6A.

[0198] 0. The Remote UE and relay UE can be registered with the network. The UE-to-Network relay can be authenticated and authorized by the network to support as a relay UE. Remote UE can be authenticated and authorized by the network to act as a Remote UE.

[0199] 1. The remote UE can initiate discovery procedure using any of Model A or Model B method.

[0200] 2. After the discovery of the UE-to-Network relay, the Remote UE can send a Direct Communication Request to the relay UE for establishing secure PC5 unicast link. The Remote UE can include its security capabilities and security policy in the DCR message. The message can also include 5GPRUK ID if available, Relay Service Code, Nonce_1. If UE has no available 5G PRUK ID or the 5G PRUK ID has been reject before, the UE can use SUCI instead of 5G PRUK ID.

[0201] 3. Upon receiving the DCR message, the Relay UE can send the relay key request to the relay AMF, including the parameters received in the DCR message.

[0202] 4. The Relay AMF can verify whether the relay UE is authorized to act as U2N relay. The Relay AMF decides to whether to authenticate the Remote UE. If so, AMF use Option 1 or Option 2. Otherwise go to step 5a.

[0203] Option 1

[0204] 4a. If the Relay AMF decide to authenticate the Remote UE based on its (the Relay AMF's) local policy, then the Relay AMF sends Reject message include the cause and the transaction identifier.

[0205] 4b. The Relay UE forward the Reject message to the Remote UE.

[0206] 4c. The Remote UE sends a new DCR message, the message can include the Remote UE's SUCI, Relay service code and Nonce_1. The Nonce_1 can be the same or different with the Nonce_1 in step 2.

[0207] 4d. The Relay UE can send the relay key request to the relay AMF, including the parameters received in the DCR message. Then go to Step 5.

[0208] Option 2

[0209] 4e. If the Relay AMF decide to authenticate the Remote UE based on its (the Relay AMF's) local policy, then the Relay AMF sends Identity Request message include the transaction identifier.

[0210] 4f. The Relay UE forward the Identity Request message to the Remote UE.

[0211] 4g. The Remote UE sends its SUCI in the Identity Response message

[0212] 4h. The Relay UE forward the Identity Response message to the Relay AMF. Then go to Step 5.

[0213] 5a. The relay AMF can select AUSF based on 5GPRUK ID and sends a Nausf_UEAuthentication_ProseAuthenticate Request to AUSF. The request message include 5GPRUK ID, RSC, Nonce1, SN name.

[0214] 5b. The AUSF sends the Nausf_UEAuthentication_ProseAuthenticate Request to UDM

[0215] 5c. The UDM may decide to authenticate the UE based on its local policy and sends a reject message with a cause to AUSF. Then AUSF forward the Reject message to Relay AMF, Relay AMF use Option 1 or Option 2. Then go to step 10.

[0216]

[0217] 5. As shown in FIG. 6B, which is a continuation of the process in FIG. 5A, the relay AMF sends a Nausf_UEAuthentication_ProseAuthenticate Request to AUSF. The request message include 5GPRUK ID, RSC, Nonce1, SN name.

[0218] 6a~6b. The AUSF can retrieve the Authentication Vectors from the UDM via Nudm_UEAuthentication_GetProseAv Request message and trigger authentication of the remote UE. The request message include 5GPRUK ID, RSC, Nonce1, SN name.

[0219] 7a. If EAP-AKA' is selected by UDM, the AUSF of the 5G ProSe Remote UE can trigger authentication of the 5G ProSe Remote UE based on EAP-AKA'. The AUSF of the 5G ProSe Remote UE generates the EAP-Request/AKA'-Challenge message and send EAP-Request/AKA'-Challenge message to the AMF of the 5G ProSe UE-to-Network Relay in a Nausf_UEAuthentication_ProSeAuthenticate Response message.

[0220] 7b. The AMF of the 5G ProSe UE-to-Network Relay can forward the Relay Authentication Request (including the EAP-Request/AKA'-Challenge) to the 5G ProSe UE-to-Network Relay over NAS message, including transaction identifier of the 5G ProSe Remote UE in the message. The NAS message is protected using the NAS security context created for the 5G ProSe UE-to-Network Relay.

[0221] 7c. Based on the transaction identifier, the 5G ProSe UE-to-Network Relay can forwards the EAP-Request/AKA'-Challenge to the 5G ProSe Remote UE over PC5 messages.

[0222] The USIM in the 5G ProSe Remote UE verifies the freshness of the received values by checking whether AUTN can be accepted.

[0223] For EAP-AKA', the USIM computes a response RES. The USIM can return RES, CK, IK to the ME. The ME can derive CK' and IK'.

[0224] 7d. The 5G ProSe Remote UE can return EAP-Response/AKA'-Challenge to the 5G ProSe UE-to-Network Relay over PC5 messages.

[0225] 7e. The 5G ProSe UE-to-Network Relay forwards the EAP-Response/AKA'-Challenge together with the transaction identifier of the 5G ProSe Remote UE to the AMF of the 5G ProSe UE-to-Network Relay in a NAS message Relay Authentication Response.

[0226] 7f. The AMF of the 5G ProSe UE-to-Network Relay forwards EAP-Response/AKA'-Challenge to the AUSF of the 5G ProSe Remote UE via Nausf_UEAuthentication_ProSeAuthenticate Request.

[0227] The AUSF of the 5G ProSe Remote UE performs the UE authentication by verifying the received information.

[0228] For EAP-AKA', the AUSF of the 5G ProSe Remote UE and the 5G ProSe Remote UE may exchange EAP-Request/AKA'-Notification and EAP-Response /AKA'-Notification

messages via the AMF of the 5G ProSe UE-to-Network Relay. After the exchanges, the AUSF of the 5G ProSe Remote UE derives K_{AUSF} without calculating the K_{SEAF} .

[0229] The AUSF of the 5G ProSe Remote UE and the 5G ProSe Remote UE can derive a new K_{AUSF_P} (different from K_{AUSF}). NAS SMC procedure is not performed between 5G ProSe Remote UE and AMF of the 5G ProSe UE-to-Network Relay.

[0230] 8. On successful authentication, AUSF sends a `Nudm_UEAuthentication_ProseResultConfirmation` to the UDM. The message includes SUPI, RSC.

[0231] 9a. The UDM and the 5G ProSe Remote UE can generate 5GPRUK and 5GPRUK ID using the newly derived K_{AUSF_P} .

[0232] 9b. The UDM can generate the K_{NR_ProSe} key.

[0233] 10. UDM sends a `Nudm_ProseKey_Get Response` to the AUSF with the K_{NR_ProSe} , `Nonce_2`.

[0234] 11. The AUSF of the 5G ProSe Remote UE can send the K_{NR_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. When receiving a K_{NR_ProSe} from the AUSF of the 5G ProSe Remote UE, the AMF of the 5G ProSe UE-to-Network Relay can not attempt to trigger NAS SMC procedure with the 5G ProSe Remote UE. The 5G ProSe UE-to-Network Relay derives PC5 session key K_{relay_sess} and confidentiality and integrity keys from K_{NR_ProSe} .

[0235] 12. The 5G ProSe UE-to-Network Relay can send the received `Nonce_2` to the 5G ProSe Remote UE in `Direct Security mode command` message, which is protected using K_{relay_int} or/and K_{relay_enc} derived from K_{relay_sess} according to the negotiated PC5 signalling policies between the 5G ProSe Remote UE and the 5G ProSe UE-to-Network Relay.

[0236] 13-15b. The 5G ProSe Remote UE can use the 5GPRUK ID to locate the $K_{AUSF_P}/5GPRUK$ to be used for the PC5 link security. The 5G ProSe Remote UE can generate the K_{NR_ProSe} key to be used for Remote access via the 5G ProSe UE-to-Network Relay. The 5G ProSe Remote UE can derive PC5 session key K_{relay_sess} and confidentiality and integrity keys from K_{NR_ProSe} . The 5G ProSe Remote UE can send the `Direct Security Mode Complete` message containing its PC5 user plane security policies to the 5G ProSe UE-to-Network relay, which is protected by K_{relay_int} or/and K_{relay_enc} derived from K_{relay_sess} according to the

negotiated PC5 signalling policies between the 5G ProSe Remote UE and the 5G ProSe UE-to-Network Relay. After the successful verification of the Direct Security Mode complete message, the 5G ProSe UE-to-Network Relay responds a Direct Communication Accept message to the 5G ProSe Remote UE to finish the PC5 connection establishment procedures.

[0237] III. Case 2: The Remote UE use SUCI and 5G PRUK ID. No PAnF.

[0238] III.(a) Case 2.1 AUSF generate K_{NR_Prose} and UDM store 5G PRUK

[0239] FIGS. 7A-7B show an example flowchart of a security procedure where AUSF generates K_{NR_Prose} , and UDM stores 5G PRUK. FIG. 7B is a continuation of the process in FIG. 7A.

[0240] 0. The Remote UE and relay UE can be registered with the network. The UE-to-Network relay can be authenticated and authorized by the network to support as a relay UE. Remote UE can be authenticated and authorized by the network to act as a Remote UE.

[0241] 1. The remote UE can initiate discovery procedure using any of Model A or Model B method .

[0242] 2. After the discovery of the UE-to-Network relay, the Remote UE can send a Direct Communication Request to the relay UE for establishing secure PC5 unicast link. The Remote UE can include its security capabilities and security policy in the DCR message. The message can also include SUCI and 5GPRUK ID if available, Relay Service Code, Nonce_1.

[0243] 3. Upon receiving the DCR message, the Relay UE can send the relay key request to the relay AMF, including the parameters received in the DCR message.

[0244] 4. The Relay AMF can verify whether the relay UE is authorized to act as U2N relay.

[0245] 5a. The relay AMF can select AUSF based on 5GPRUK ID and sends a Nausf_UEAuthentication_ProseAuthenticate Request to AUSF. The request message include SUCI, 5GPRUK ID, RSC, Nonce1 , SN name.

[0246] 5b. The AUSF sends a Nudm_ProseKey_Get Request to UDM.

[0247] 5c. If UDM decide not to authenticate the Remote UE, the UDM sends a response to AUSF with 5G PRUK to the AUSF, the UDM may also sends a Nonce_2 to AUSF. Then go to step 10.

[0248] 5d. If UDM decide to authenticate the Remote UE, the UDM sends a reject response to the AUSF with a cause.

[0249] 6a~6b. As shown in FIG. 7B, which is a continuation of the process in FIG. 7A, the AUSF can retrieve the Authentication Vectors from the UDM via Nudm_UEAuthentication_GetProseAv Request message and trigger authentication of the remote UE.

[0250] 7a. If EAP-AKA' is selected by UDM, the AUSF of the 5G ProSe Remote UE can trigger authentication of the 5G ProSe Remote UE based on EAP-AKA'. The AUSF of the 5G ProSe Remote UE generates the EAP-Request/AKA'-Challenge message defined in clause 6.1.3.1 of TS 33.501 and send EAP-Request/AKA'-Challenge message to the AMF of the 5G ProSe UE-to-Network Relay in a Nausf_UEAuthentication_ProSeAuthenticate Response message.

[0251] 7b. The AMF of the 5G ProSe UE-to-Network Relay can forward the Relay Authentication Request (including the EAP-Request/AKA'-Challenge) to the 5G ProSe UE-to-Network Relay over NAS message, including transaction identifier of the 5G ProSe Remote UE in the message. The NAS message is protected using the NAS security context created for the 5G ProSe UE-to-Network Relay.

[0252] 7c. Based on the transaction identifier, the 5G ProSe UE-to-Network Relay can forwards the EAP-Request/AKA'-Challenge to the 5G ProSe Remote UE over PC5 messages.

[0253] The USIM in the 5G ProSe Remote UE verifies the freshness of the received values by checking whether AUTN can be accepted.

[0254] For EAP-AKA', the USIM computes a response RES. The USIM can return RES, CK, IK to the ME. The ME can derive CK' and IK'.

[0255] 7d. The 5G ProSe Remote UE can return EAP-Response/AKA'-Challenge to the 5G ProSe UE-to-Network Relay over PC5 messages.

[0256] 7e. The 5G ProSe UE-to-Network Relay forwards the EAP-Response/AKA'-Challenge together with the transaction identifier of the 5G ProSe Remote UE to the AMF of the 5G ProSe UE-to-Network Relay in a NAS message Relay Authentication Response.

[0257] 7f. The AMF of the 5G ProSe UE-to-Network Relay forwards EAP-Response/AKA'-Challenge to the AUSF of the 5G ProSe Remote UE via Nausf_UEAuthentication_ProSeAuthenticate Request.

[0258] The AUSF of the 5G ProSe Remote UE performs the UE authentication by verifying the received information.

[0259] For EAP-AKA', the AUSF of the 5G ProSe Remote UE and the 5G ProSe Remote UE may exchange EAP-Request/AKA'-Notification and EAP-Response /AKA'-Notification messages via the AMF of the 5G ProSe UE-to-Network Relay. After the exchanges, the AUSF of the 5G ProSe Remote UE derives K_{AUSF} without calculating the K_{SEAF} .

[0260] The AUSF of the 5G ProSe Remote UE and the 5G ProSe Remote UE can derive a new K_{AUSF_P} (different from K_{AUSF}). NAS SMC procedure is not performed between 5G ProSe Remote UE and AMF of the 5G ProSe UE-to-Network Relay.

[0261] 8. On successful authentication, the AUSF of the 5G ProSe Remote UE and the 5G ProSe Remote UE can generate 5GPRUK and 5GPRUK ID using the newly derived K_{AUSF_P} .

[0262] 9. AUSF sends a Nudm_UEAuthentication_ProseResultConfirmation to the UDM.

[0263] 10. The AUSF of the 5G ProSe Remote UE can generate the K_{NR_ProSe} key.

[0264] 11. The AUSF of the 5G ProSe Remote UE can send the K_{NR_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. When receiving a K_{NR_ProSe} from the AUSF of the 5G ProSe Remote UE, the AMF of the 5G ProSe UE-to-Network Relay can not attempt to trigger NAS SMC procedure with the 5G ProSe Remote UE. The 5G ProSe UE-to-Network Relay derives PC5 session key K_{relay_sess} and confidentiality and integrity keys from K_{NR_ProSe} .

[0265] 12. The 5G ProSe UE-to-Network Relay can send the received Nonce_2 to the 5G ProSe Remote UE in Direct Security mode command message, which is protected using K_{relay_int} or/and K_{relay_enc} derived from K_{relay_sess} according to the negotiated PC5 signalling policies between the 5G ProSe Remote UE and the 5G ProSe UE-to-Network Relay.

[0266] 13-15b. The 5G ProSe Remote UE can use the 5GPRUK ID to locate the $K_{AUSF_P}/5GPRUK$ to be used for the PC5 link security. The 5G ProSe Remote UE can generate the K_{NR_ProSe} key to be used for Remote access via the 5G ProSe UE-to-Network Relay. The 5G ProSe Remote UE can derive PC5 session key K_{relay_sess} and confidentiality and integrity keys from K_{NR_ProSe} . The 5G ProSe Remote UE can send the Direct Security Mode Complete message containing its PC5 user plane security policies to the 5G ProSe UE-to-Network relay, which is protected by K_{relay_int} or/and K_{relay_enc} derived from K_{relay_sess} according to the negotiated PC5 signalling policies between the 5G ProSe Remote UE and the 5G ProSe UE-to-Network Relay. After the successful verification of the Direct Security Mode complete message, the 5G

ProSe UE-to-Network Relay responds a Direct Communication Accept message to the 5G ProSe Remote UE to finish the PC5 connection establishment procedures.

[0267] FIG. 23 shows a flowchart for receiving a message by a network node that indicates whether another network node authenticates a communication device. Operation 2302 includes receiving, by a first network device from a second network device, a first request message that includes first identifier associated with a first communication device and a second identifier. Operation 2304 includes transmitting, by the first network device to a third network device, a second request message that includes the first identifier. Operation 2306 includes receiving, by the first network device and in response to the second request message, a response message from the third network device, wherein the response message indicates whether the third network device authenticated the first communication device.

[0268] In some embodiments, the first identifier includes a 5G ProSe Relay User Key (PRUK) identifier (ID), and the second identifier includes a subscription concealed identifier (SUCI). In some embodiments, a second communication device is authorized to act as a relay between the first communication device and a communication network that includes any one or more of the first network device, the second network device, and the third network device. In some embodiments, the first network device includes an authentication server function (AUSF) device, the second network device includes a remote access and mobility management function (AMF) device, and the third network device includes a unified data management (UDM).

[0269] III.(b) Case 2.2 AUSF generate K_{NR_Prose} and store 5G PRUK

[0270] FIGS. 8A-8B show an example flowchart of a security procedure where AUSF generates K_{NR_Prose} and stores 5G PRUK. FIG. 8B is a continuation of the process in FIG. 8A.

[0271] 0. The Remote UE and relay UE can be registered with the network. The UE-to-Network relay can be authenticated and authorized by the network to support as a relay UE. Remote UE can be authenticated and authorized by the network to act as a Remote UE.

[0272] 1. The remote UE can initiate discovery procedure using any of Model A or Model B method as specified.

[0273] 2. After the discovery of the UE-to-Network relay, the Remote UE can send a Direct Communication Request to the relay UE for establishing secure PC5 unicast link. The Remote

UE can include its security capabilities and security policy in the DCR message. The message can also include SUCI and 5GPRUK ID if available, Relay Service Code, Nonce₁.

[0274] 3. Upon receiving the DCR message, the Relay UE can send the relay key request to the relay AMF, including the parameters received in the DCR message.

[0275] 4. The Relay AMF can verify whether the relay UE is authorized to act as U2N relay.

[0276] 5a. The relay AMF can select AUSF based on SUCI or 5GPRUK ID and sends a Nausf_UEAuthentication_ProseAuthenticate Request to AUSF. The request message include 5GPRUK ID, RSC, Nonce₁, SN name. If the AUSF can find the 5G PRUK, then go to step 10. Otherwise continue step 6a.

[0277] If AMF can use 5G PRUK ID to find a AUSF instance ID which is stored in the Relay AMF, then the AMF select the AUSF.

[0278] If RID is included in the 5G PRUK ID, the AUSF selection should consider the RID.

[0279] The 5GPRUK ID may be generated as follows:

[0280] 5GPRUK ID is in NAI format as specified in clause 2.2 of IETF RFC 7542, e.g. username@realm. The username part can include the RID and the P-TID (Prose Temporary UE Identifier), and the realm part can include Home Network Identifier.

[0281] The P-TID is derived from K_{AUSF} or K_{ausf_p} .

[0282] The AUSF selection may also consider the RID in SUCI.

[0283] 6a~6b. The AUSF can retrieve the Authentication Vectors from the UDM via Nudm_UEAuthentication_GetProseAv Request message and trigger authentication of the remote UE.

[0284] 7a. If EAP-AKA' is selected by UDM, the AUSF of the 5G ProSe Remote UE can trigger authentication of the 5G ProSe Remote UE based on EAP-AKA'. The AUSF of the 5G ProSe Remote UE generates the EAP-Request/AKA'-Challenge message¹ and send EAP-Request/AKA'-Challenge message to the AMF of the 5G ProSe UE-to-Network Relay in a Nausf_UEAuthentication_ProSeAuthenticate Response message.

[0285] 7b. The AMF of the 5G ProSe UE-to-Network Relay can forward the Relay Authentication Request (including the EAP-Request/AKA'-Challenge) to the 5G ProSe UE-to-Network Relay over NAS message, including transaction identifier of the 5G ProSe Remote UE in the message. The NAS message is protected using the NAS security context created for the 5G ProSe UE-to-Network Relay.

[0286] 7c. Based on the transaction identifier, the 5G ProSe UE-to-Network Relay can forwards the EAP-Request/AKA'-Challenge to the 5G ProSe Remote UE over PC5 messages.

[0287] The USIM in the 5G ProSe Remote UE verifies the freshness of the received values by checking whether AUTN can be accepted.

[0288] For EAP-AKA', the USIM computes a response RES. The USIM can return RES, CK, IK to the ME. The ME can derive CK' and IK'.

[0289] 7d. The 5G ProSe Remote UE can return EAP-Response/AKA'-Challenge to the 5G ProSe UE-to-Network Relay over PC5 messages.

[0290] 7e. The 5G ProSe UE-to-Network Relay forwards the EAP-Response/AKA'-Challenge together with the transaction identifier of the 5G ProSe Remote UE to the AMF of the 5G ProSe UE-to-Network Relay in a NAS message Relay Authentication Response.

[0291] 7f. The AMF of the 5G ProSe UE-to-Network Relay forwards EAP-Response/AKA'-Challenge to the AUSF of the 5G ProSe Remote UE via Nausf_UEAuthentication_ProSeAuthenticate Request.

[0292] The AUSF of the 5G ProSe Remote UE performs the UE authentication by verifying the received information.

[0293] For EAP-AKA', the AUSF of the 5G ProSe Remote UE and the 5G ProSe Remote UE may exchange EAP-Request/AKA'-Notification and EAP-Response /AKA'-Notification messages via the AMF of the 5G ProSe UE-to-Network Relay. After the exchanges, the AUSF of the 5G ProSe Remote UE derives K_{AUSF} without calculating the K_{SEAF} .

[0294] The AUSF of the 5G ProSe Remote UE and the 5G ProSe Remote UE can derive a new K_{AUSF_P} (different from K_{AUSF}). NAS SMC procedure is not performed between 5G ProSe Remote UE and AMF of the 5G ProSe UE-to-Network Relay.

[0295] 8. On successful authentication, the AUSF of the 5G ProSe Remote UE and the 5G ProSe Remote UE can generate 5GPRUK and 5GPRUK ID using the newly derived K_{AUSF_P} .

[0296] 9. AUSF sends a Nudm_UEAuthentication_ProseResultConfirmation to the UDM.

[0297] 10. As shown in FIG. 8B, which is a continuation of the process in FIG. 8A, the AUSF of the 5G ProSe Remote UE can generate the K_{NR_ProSe} key.

[0298] 11. The AUSF of the 5G ProSe Remote UE can send the K_{NR_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. The AUSF may also send the AUSF

instance ID in the Response message. When AMF receive the AUSF instance ID, AMF should store the mapping (5G PRUK ID, AUSF ID). When receiving a KNR_ProSe from the AUSF of the 5G ProSe Remote UE, the AMF of the 5G ProSe UE-to-Network Relay can not attempt to trigger NAS SMC procedure with the 5G ProSe Remote UE. The 5G ProSe UE-to-Network Relay derives PC5 session key Krelay-sess and confidentiality and integrity keys from K_{NR_ProSe}.

[0299] 12. The 5G ProSe UE-to-Network Relay can send the received Nonce_2 to the 5G ProSe Remote UE in Direct Security mode command message, which is protected using Krelay-int or/and Krelay-enc derived from Krelay-sess according to the negotiated PC5 signalling policies between the 5G ProSe Remote UE and the 5G ProSe UE-to-Network Relay.

[0300] 13-15b. The 5G ProSe Remote UE can use the 5GPRUK ID to locate the KAUSF_P/5GPRUK to be used for the PC5 link security. The 5G ProSe Remote UE can generate the KNR_ProSe key to be used for Remote access via the 5G ProSe UE-to-Network Relay. The 5G ProSe Remote UE can derive PC5 session key Krelay-sess and confidentiality and integrity keys from KNR_ProSe. The 5G ProSe Remote UE can send the Direct Security Mode Complete message containing its PC5 user plane security policies to the 5G ProSe UE-to-Network relay, which is protected by Krelay-int or/and Krelay-enc derived from Krelay-sess according to the negotiated PC5 signalling policies between the 5G ProSe Remote UE and the 5G ProSe UE-to-Network Relay. After the successful verification of the Direct Security Mode complete message, the 5G ProSe UE-to-Network Relay responds a Direct Communication Accept message to the 5G ProSe Remote UE to finish the PC5 connection establishment procedures.

[0301] III.(c) Case 2.3 AUSF generate K_{NR_ProSe}. UDM generate and store 5G PRUK

[0302] FIGS. 9A-9B show an example flowchart of a security procedure where AUSF generates K_{NR_ProSe}, and UDM generates and stores 5G PRUK. FIG. 9B is a continuation of the process in FIG. 9A.

[0303] 0. The Remote UE and relay UE can be registered with the network. The UE-to-Network relay can be authenticated and authorized by the network to support as a relay UE. Remote UE can be authenticated and authorized by the network to act as a Remote UE.

[0304] 1. The remote UE can initiate discovery procedure using any of Model A or Model B method.

[0305] 2. After the discovery of the UE-to-Network relay, the Remote UE can send a Direct Communication Request to the relay UE for establishing secure PC5 unicast link. The Remote UE can include its security capabilities and security policy in the DCR message. The message can also include SUCI and 5GPRUK ID if available, Relay Service Code, Nonce_1.

[0306] 3. Upon receiving the DCR message, the Relay UE can send the relay key request to the relay AMF, including the parameters received in the DCR message.

[0307] 4. The Relay AMF can verify whether the relay UE is authorized to act as U2N relay.

[0308] 5a. The relay AMF can select AUSF based on SUCI or 5GPRUK ID and sends a Nausf_UEAuthentication_ProseAuthenticate Request to AUSF. The request message include 5GPRUK ID, RSC, Nonce1, SN name.

[0309] 5b. The AUSF sends the Nudm_Prosekey_Get Request to UDM

[0310] 5c. The UDM may decide to authenticate the UE based on its local policy and sends a reject message with a cause to AUSF.

[0311] 6a~6b. As shown in FIG. 9B, which is a continuation of the process in FIG. 9A, the AUSF can retrieve the Authentication Vectors from the UDM via Nudm_UEAuthentication_GetProseAv Request message and trigger authentication of the remote UE.

[0312] 7a. If EAP-AKA' is selected by UDM, the AUSF of the 5G ProSe Remote UE can trigger authentication of the 5G ProSe Remote UE based on EAP-AKA'. The AUSF of the 5G ProSe Remote UE generates the EAP-Request/AKA'-Challenge message and send EAP-Request/AKA'-Challenge message to the AMF of the 5G ProSe UE-to-Network Relay in a Nausf_UEAuthentication_ProSeAuthenticate Response message.

[0313] 7b. The AMF of the 5G ProSe UE-to-Network Relay can forward the Relay Authentication Request (including the EAP-Request/AKA'-Challenge) to the 5G ProSe UE-to-Network Relay over NAS message, including transaction identifier of the 5G ProSe Remote UE in the message. The NAS message is protected using the NAS security context created for the 5G ProSe UE-to-Network Relay.

[0314] 7c. Based on the transaction identifier, the 5G ProSe UE-to-Network Relay can forwards the EAP-Request/AKA'-Challenge to the 5G ProSe Remote UE over PC5 messages.

[0315] The USIM in the 5G ProSe Remote UE verifies the freshness of the received values by checking whether AUTN can be accepted.

[0316] For EAP-AKA', the USIM computes a response RES. The USIM can return RES, CK, IK to the ME. The ME can derive CK' and IK'.

[0317] 7d. The 5G ProSe Remote UE can return EAP-Response/AKA'-Challenge to the 5G ProSe UE-to-Network Relay over PC5 messages.

[0318] 7e. The 5G ProSe UE-to-Network Relay forwards the EAP-Response/AKA'-Challenge together with the transaction identifier of the 5G ProSe Remote UE to the AMF of the 5G ProSe UE-to-Network Relay in a NAS message Relay Authentication Response.

[0319] 7f. The AMF of the 5G ProSe UE-to-Network Relay forwards EAP-Response/AKA'-Challenge to the AUSF of the 5G ProSe Remote UE via Nausf_UEAuthentication_ProSeAuthenticate Request.

[0320] The AUSF of the 5G ProSe Remote UE performs the UE authentication by verifying the received information.

[0321] For EAP-AKA', the AUSF of the 5G ProSe Remote UE and the 5G ProSe Remote UE may exchange EAP-Request/AKA'-Notification and EAP-Response /AKA'-Notification messages via the AMF of the 5G ProSe UE-to-Network Relay. After the exchanges, the AUSF of the 5G ProSe Remote UE derives KAUSF without calculating the KSEAF.

[0322] The AUSF of the 5G ProSe Remote UE and the 5G ProSe Remote UE can derive a new KAUSF_P (different from KAUSF). NAS SMC procedure is not performed between 5G ProSe Remote UE and AMF of the 5G ProSe UE-to-Network Relay.

[0323] 8.AUSF sends a Nudm_UEAuthentication_ProseResultConfirmation to the UDM

[0324] 9a. On successful authentication, the UDM and the 5G ProSe Remote UE can generate 5GPRUK and 5GPRUK ID using the newly derived KAUSF_P.

[0325] 9b. UDM sends a Nudm_ProseKey_Get Response to the AUSF with the 5G PRUK. The UDM may also sends a Nonce_2 to AUSF

[0326] 10.The AUSF of the 5G ProSe Remote UE can generate the K_{NR_ProSe} key. If UDM sends a Nonce_2 to AUSF, then the AUSF use the Nonce_2 to generate the K_{NR_ProSe} key. Otherwise, AUSF generate the Nonce_2 itself.

[0327] 11. The AUSF of the 5G ProSe Remote UE can send the K_{NR_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. When receiving a K_{NR_ProSe} from the AUSF of the 5G ProSe Remote UE, the AMF of the 5G ProSe UE-to-Network Relay can not

attempt to trigger NAS SMC procedure with the 5G ProSe Remote UE. The 5G ProSe UE-to-Network Relay derives PC5 session key Krelay-sess and confidentiality and integrity keys from K_{NR_ProSe} .

[0328] 12. The 5G ProSe UE-to-Network Relay can send the received Nonce_2 to the 5G ProSe Remote UE in Direct Security mode command message, which is protected using Krelay-int or/and Krelay-enc derived from Krelay-sess according to the negotiated PC5 signalling policies between the 5G ProSe Remote UE and the 5G ProSe UE-to-Network Relay.

[0329] 13-15b. The 5G ProSe Remote UE can use the 5GPRUK ID to locate the $K_{AUSF_P/5GPRUK}$ to be used for the PC5 link security. The 5G ProSe Remote UE can generate the K_{NR_ProSe} key to be used for Remote access via the 5G ProSe UE-to-Network Relay. The 5G ProSe Remote UE can derive PC5 session key Krelay-sess and confidentiality and integrity keys from K_{NR_ProSe} . The 5G ProSe Remote UE can send the Direct Security Mode Complete message containing its PC5 user plane security policies to the 5G ProSe UE-to-Network relay, which is protected by Krelay-int or/and Krelay-enc derived from Krelay-sess according to the negotiated PC5 signalling policies between the 5G ProSe Remote UE and the 5G ProSe UE-to-Network Relay. After the successful verification of the Direct Security Mode complete message, the 5G ProSe UE-to-Network Relay responds a Direct Communication Accept message to the 5G ProSe Remote UE to finish the PC5 connection establishment procedures.

[0330] III.(d) Case 2.4 UDM generate K_{NR_ProSe} and store 5G PRUK

[0331] FIGS. 10A-10B show an example flowchart of a security procedure where UDM generates K_{NR_ProSe} and stores 5G PRUK. FIG. 10B is a continuation of the process in FIG. 10A.

[0332] 0. The Remote UE and relay UE can be registered with the network. The UE-to-Network relay can be authenticated and authorized by the network to support as a relay UE. Remote UE can be authenticated and authorized by the network to act as a Remote UE.

[0333] 1. The remote UE can initiate discovery procedure using any of Model A or Model B method.

[0334] 2. After the discovery of the UE-to-Network relay, the Remote UE can send a Direct Communication Request to the relay UE for establishing secure PC5 unicast link. The Remote UE can include its security capabilities and security policy in the DCR message. The message can also include SUCI and 5GPRUK ID if available, Relay Service Code, Nonce_1.

[0335] 3. Upon receiving the DCR message, the Relay UE can send the relay key request to the relay AMF, including the parameters received in the DCR message.

[0336] 4. The Relay AMF can verify whether the relay UE is authorized to act as U2N relay.

[0337] 5a. The relay AMF can select AUSF based on SUCI or 5GPRUK ID and sends a Nausf_UEAuthentication_ProseAuthenticate Request to AUSF. The request message include 5GPRUK ID, RSC, Nonce1, SN name.

[0338] 5b. The AUSF sends the Nudm_Prosekey_Get Request to UDM

[0339] 5c. The UDM may decide to authenticate the UE based on its local policy and sends a reject message with a cause to AUSF and continue the step 6a. Otherwise go to step 9b.

[0340] 6a~6b. As shown in FIG. 10B, which is a continuation of the process in FIG. 10A, the AUSF can retrieve the Authentication Vectors from the UDM via Nudm_UEAuthentication_GetProseAv Request message and trigger authentication of the remote UE.

[0341] 7a. If EAP-AKA' is selected by UDM, the AUSF of the 5G ProSe Remote UE can trigger authentication of the 5G ProSe Remote UE based on EAP-AKA'. The AUSF of the 5G ProSe Remote UE generates the EAP-Request/AKA'-Challenge message defined in clause 6.1.3.1 of TS 33.501 and send EAP-Request/AKA'-Challenge message to the AMF of the 5G ProSe UE-to-Network Relay in a Nausf_UEAuthentication_ProSeAuthenticate Response message.

[0342] 7b. The AMF of the 5G ProSe UE-to-Network Relay can forward the Relay Authentication Request (including the EAP-Request/AKA'-Challenge) to the 5G ProSe UE-to-Network Relay over NAS message, including transaction identifier of the 5G ProSe Remote UE in the message. The NAS message is protected using the NAS security context created for the 5G ProSe UE-to-Network Relay.

[0343] 7c. Based on the transaction identifier, the 5G ProSe UE-to-Network Relay can forwards the EAP-Request/AKA'-Challenge to the 5G ProSe Remote UE over PC5 messages.

[0344] The USIM in the 5G ProSe Remote UE verifies the freshness of the received values by checking whether AUTN can be accepted.

[0345] For EAP-AKA', the USIM computes a response RES. The USIM can return RES, CK, IK to the ME. The ME can derive CK' and IK'.

[0346] 7d. The 5G ProSe Remote UE can return EAP-Response/AKA'-Challenge to the 5G ProSe UE-to-Network Relay over PC5 messages.

[0347] 7e. The 5G ProSe UE-to-Network Relay forwards the EAP-Response/AKA'-Challenge together with the transaction identifier of the 5G ProSe Remote UE to the AMF of the 5G ProSe UE-to-Network Relay in a NAS message Relay Authentication Response.

[0348] 7f. The AMF of the 5G ProSe UE-to-Network Relay forwards EAP-Response/AKA'-Challenge to the AUSF of the 5G ProSe Remote UE via Nausf_UEAuthentication_ProSeAuthenticate Request.

[0349] The AUSF of the 5G ProSe Remote UE performs the UE authentication by verifying the received information.

[0350] For EAP-AKA', the AUSF of the 5G ProSe Remote UE and the 5G ProSe Remote UE may exchange EAP-Request/AKA'-Notification and EAP-Response /AKA'-Notification messages via the AMF of the 5G ProSe UE-to-Network Relay. After the exchanges, the AUSF of the 5G ProSe Remote UE derives KAUSF without calculating the KSEAF.

[0351] The AUSF of the 5G ProSe Remote UE and the 5G ProSe Remote UE can derive a new K_{AUSF_P} (different from K_{AUSF}). NAS SMC procedure is not performed between 5G ProSe Remote UE and AMF of the 5G ProSe UE-to-Network Relay.

[0352] 8. AUSF sends a Nudm_UEAuthentication_ProseResultConfirmation to the UDM. The message may include SUPI, RSC, Nonce_1. The message may also include Nonce_2.

[0353] 9a. On successful authentication, the UDM and the 5G ProSe Remote UE can generate 5GPRUK and 5GPRUK ID using the newly derived K_{AUSF_P} .

[0354] 9b. UDM can generate the K_{NR_ProSe} key. If the UDM receive Nonce_2 from AUSF, the UDM use the Nonce_2 to generate the K_{NR_ProSe} key. Otherwise, UDM generate the Nonce_2 itself.

[0355] 10. UDM sends a Nudm_ProseKey_Get Response to the AUSF with the K_{NR_ProSe} key. If UDM generate the Nonce_2 itself, UDM also include the Nonce_2 in the response.

[0356] 11. The AUSF of the 5G ProSe Remote UE can send the K_{NR_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. When receiving a K_{NR_ProSe} from the AUSF of the 5G ProSe Remote UE, the AMF of the 5G ProSe UE-to-Network Relay can not attempt to trigger NAS SMC procedure with the 5G ProSe Remote UE. The 5G ProSe UE-to-

Network Relay derives PC5 session key $K_{\text{relay-sess}}$ and confidentiality and integrity keys from $K_{\text{NR_ProSe}}$.

[0357] 12. The 5G ProSe UE-to-Network Relay can send the received Nonce_2 to the 5G ProSe Remote UE in Direct Security mode command message, which is protected using $K_{\text{relay-int}}$ or/and $K_{\text{relay-enc}}$ derived from $K_{\text{relay-sess}}$ according to the negotiated PC5 signalling policies between the 5G ProSe Remote UE and the 5G ProSe UE-to-Network Relay.

[0358] 13-15b. The 5G ProSe Remote UE can use the 5GPRUK ID to locate the KAUSF_P/5GPRUK to be used for the PC5 link security. The 5G ProSe Remote UE can generate the $K_{\text{NR_ProSe}}$ key to be used for Remote access via the 5G ProSe UE-to-Network Relay. The 5G ProSe Remote UE can derive PC5 session key $K_{\text{relay-sess}}$ and confidentiality and integrity keys from $K_{\text{NR_ProSe}}$. The 5G ProSe Remote UE can send the Direct Security Mode Complete message containing its PC5 user plane security policies to the 5G ProSe UE-to-Network relay, which is protected by $K_{\text{relay-int}}$ or/and $K_{\text{relay-enc}}$ derived from $K_{\text{relay-sess}}$ according to the negotiated PC5 signalling policies between the 5G ProSe Remote UE and the 5G ProSe UE-to-Network Relay. After the successful verification of the Direct Security Mode complete message, the 5G ProSe UE-to-Network Relay responds a Direct Communication Accept message to the 5G ProSe Remote UE to finish the PC5 connection establishment procedures.

[0359] **IV. Case 3: The Remote UE use SUCI or 5G PRUK ID. PAnF involved to store the 5G PRUK.**

[0360] IV.(a) Case 3.1 AUSF finds (or determines) PAnF. AUSF generate $K_{\text{NR_ProSe}}$

[0361] FIGS. 11A-11B shows an example flowchart of a security procedure AUSF finds PAnF, and AUSF generates $K_{\text{NR_ProSe}}$. FIG. 11B is a continuation of the process in FIG. 11A.

[0362] 0. The Remote UE and relay UE can be registered with the network. The UE-to-Network relay can be authenticated and authorized by the network to support as a relay UE. Remote UE can be authenticated and authorized by the network to act as a Remote UE.

[0363] 1. The remote UE can initiate discovery procedure using any of Model A or Model B method.

[0364] 2. After the discovery of the UE-to-Network relay, the Remote UE can send a Direct Communication Request to the relay UE for establishing secure PC5 unicast link. The Remote UE can include its security capabilities and security policy in the DCR message. The message

can also include 5GPRUK ID if available, Relay Service Code, Nonce_1. If UE has no available 5G PRUK ID or the 5G PRUK ID has been reject before, the UE can use SUCI instead of 5G PRUK ID.

[0365] 3. Upon receiving the DCR message, the Relay UE can send the relay key request to the relay AMF, including the parameters received in the DCR message.

[0366] 4. The Relay AMF can verify whether the relay UE is authorized to act as U2N relay. The Relay AMF decides to whether to authenticate the Remote UE. If so, AMF use Option 1 or Option 2. Otherwise go to step 5a.

[0367] Option 1

[0368] 4a. If the Relay AMF decide to authenticate the Remote UE based on its (the Relay AMF's) local policy, then the Relay AMF sends Reject message include the cause and the transaction identifier.

[0369] 4b. The Relay UE forward the Reject message to the Remote UE.

[0370] 4c. The Remote UE sends a new DCR message, the message can include the Remote UE's SUCI, Relay service code and Nonce_1. The Nonce_1 can be the same or different with the Nonce_1 in step 2.

[0371] 4d. The Relay UE can send the relay key request to the relay AMF, including the parameters received in the DCR message. Then go to Step 5.

[0372] Option 2

[0373] 4e. If the Relay AMF decide to authenticate the Remote UE based on its (the Relay AMF's) local policy, then the Relay AMF sends Identity Request message include the transaction identifier.

[0374] 4f. The Relay UE forward the Identity Request message to the Remote UE.

[0375] 4g. The Remote UE sends its SUCI in the Identity Response message

[0376] 4h. The Relay UE forward the Identity Response message to the Relay AMF. Then go to Step 5.

[0377] 5a. The relay AMF sends a Nausf_UEAuthentication_ProseAuthenticate Request to AUSF. The request message include 5GPRUK ID, RSC, Nonce1, SN name.

[0378] 5b. The AUSF can select PAnF based on 5GPRUK ID and sends a Npanf_ProseKey_Get Request to PAnF. The request message include 5GPRUK ID, RSC.

- [0379] If AUSF can use 5G PRUK ID to find a PAnF instance ID which is stored in the AUSF, then the AUSF select the PAnF.
- [0380] If RID is included in the 5G PRUK ID, the PAnF selection should consider the RID.
- [0381] The 5GPRUK ID may be generated as follows:
- [0382] 5GPRUK ID is in NAI format as specified in clause 2.2 of IETF RFC 7542, e.g. username@realm. The username part can include the RID and the P-TID (Prose Temporary UE Identifier), and the realm part can include Home Network Identifier.
- [0383] The P-TID is derived from K_{AUSF} or K_{ausf_p} .
- [0384] 5c. If the PAnF can find the 5G PRUK, then sends a Npanf_ProseKey_Get Response with 5G PRUK to the AUSF. The response may also include the Nonce_2.
- [0385] 5d. If the PAnF can not find the 5G PRUK, then sends a Reject Response to the AUSF. Then AUSF forward the Reject response to Relay AMF.
- [0386] 5e. AMF use Option 1 or Option 2.
- [0387] 5. As shown in FIG. 11B, which is a continuation of the process in FIG. 11A, the relay AMF sends a Nausf_UEAuthentication_ProseAuthenticate Request to AUSF. The request message include 5GPRUK ID, RSC, Nonce1, SN name.
- [0388] 6a~6b. The AUSF can retrieve the Authentication Vectors from the UDM via Nudm_UEAuthentication_GetProseAv Request message and trigger authentication of the remote UE.
- [0389] 7a. If EAP-AKA' is selected by UDM, the AUSF of the 5G ProSe Remote UE can trigger authentication of the 5G ProSe Remote UE based on EAP-AKA'. The AUSF of the 5G ProSe Remote UE generates the EAP-Request/AKA'-Challenge message defined in clause 6.1.3.1 of TS 33.501 and send EAP-Request/AKA'-Challenge message to the AMF of the 5G ProSe UE-to-Network Relay in a Nausf_UEAuthentication_ProSeAuthenticate Response message.
- [0390] 7b. The AMF of the 5G ProSe UE-to-Network Relay can forward the Relay Authentication Request (including the EAP-Request/AKA'-Challenge) to the 5G ProSe UE-to-Network Relay over NAS message, including transaction identifier of the 5G ProSe Remote UE in the message. The NAS message is protected using the NAS security context created for the 5G ProSe UE-to-Network Relay.

- [0391] 7c. Based on the transaction identifier, the 5G ProSe UE-to-Network Relay can forwards the EAP-Request/AKA'-Challenge to the 5G ProSe Remote UE over PC5 messages.
- [0392] The USIM in the 5G ProSe Remote UE verifies the freshness of the received values by checking whether AUTN can be accepted.
- [0393] For EAP-AKA', the USIM computes a response RES. The USIM can return RES, CK, IK to the ME. The ME can derive CK' and IK'.
- [0394] 7d. The 5G ProSe Remote UE can return EAP-Response/AKA'-Challenge to the 5G ProSe UE-to-Network Relay over PC5 messages.
- [0395] 7e. The 5G ProSe UE-to-Network Relay forwards the EAP-Response/AKA'-Challenge together with the transaction identifier of the 5G ProSe Remote UE to the AMF of the 5G ProSe UE-to-Network Relay in a NAS message Relay Authentication Response.
- [0396] 7f. The AMF of the 5G ProSe UE-to-Network Relay forwards EAP-Response/AKA'-Challenge to the AUSF of the 5G ProSe Remote UE via Nausf_UEAuthentication_ProSeAuthenticate Request.
- [0397] The AUSF of the 5G ProSe Remote UE performs the UE authentication by verifying the received information.
- [0398] For EAP-AKA', the AUSF of the 5G ProSe Remote UE and the 5G ProSe Remote UE may exchange EAP-Request/AKA'-Notification and EAP-Response /AKA'-Notification messages via the AMF of the 5G ProSe UE-to-Network Relay. After the exchanges, the AUSF of the 5G ProSe Remote UE derives KAUSF without calculating the KSEAF.
- [0399] The AUSF of the 5G ProSe Remote UE and the 5G ProSe Remote UE can derive a new K_{AUSF_P} (different from K_{AUSF}). NAS SMC procedure is not performed between 5G ProSe Remote UE and AMF of the 5G ProSe UE-to-Network Relay.
- [0400] 8. On successful authentication, the AUSF of the 5G ProSe Remote UE and the 5G ProSe Remote UE can generate 5GPRUK and 5GPRUK ID using the newly derived K_{AUSF_P} .
- [0401] 9. AUSF sends a Nudm_UEAuthentication_ProseResultConfirmation to the UDM.
- [0402] 10a. The AUSF select a PAnF and sends a Npanf_ProseKey_Register Request to the PAnF. This message include 5GPRUK ID, 5GPRUK, RSC.
- [0403] 10b. The PAnF sends a Npanf_ProseKey_Register Response to AUSF. The Response may include the PAnF instance ID. The Response may also include Nonce_2.
- [0404] 10. The AUSF of the 5G ProSe Remote UE can generate the K_{NR_ProSe} key.

[0405] 11. The AUSF of the 5G ProSe Remote UE can send the K_{NR_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. When receiving a K_{NR_ProSe} from the AUSF of the 5G ProSe Remote UE, the AMF of the 5G ProSe UE-to-Network Relay can not attempt to trigger NAS SMC procedure with the 5G ProSe Remote UE. The 5G ProSe UE-to-Network Relay derives PC5 session key $K_{relay-sess}$ and confidentiality and integrity keys from K_{NR_ProSe} .

[0406] 12. The 5G ProSe UE-to-Network Relay can send the received Nonce_2 to the 5G ProSe Remote UE in Direct Security mode command message, which is protected using $K_{relay-int}$ or/and $K_{relay-enc}$ derived from $K_{relay-sess}$ according to the negotiated PC5 signalling policies between the 5G ProSe Remote UE and the 5G ProSe UE-to-Network Relay.

[0407] 13-15b. The 5G ProSe Remote UE can use the 5GPRUK ID to locate the $K_{AUSF_P/5GPRUK}$ to be used for the PC5 link security. The 5G ProSe Remote UE can generate the K_{NR_ProSe} key to be used for Remote access via the 5G ProSe UE-to-Network Relay. The 5G ProSe Remote UE can derive PC5 session key $K_{relay-sess}$ and confidentiality and integrity keys from K_{NR_ProSe} . The 5G ProSe Remote UE can send the Direct Security Mode Complete message containing its PC5 user plane security policies to the 5G ProSe UE-to-Network relay, which is protected by $K_{relay-int}$ or/and $K_{relay-enc}$ derived from $K_{relay-sess}$ according to the negotiated PC5 signalling policies between the 5G ProSe Remote UE and the 5G ProSe UE-to-Network Relay. After the successful verification of the Direct Security Mode complete message, the 5G ProSe UE-to-Network Relay responds a Direct Communication Accept message to the 5G ProSe Remote UE to finish the PC5 connection establishment procedures.

[0408] FIG. 21 shows an example flowchart for receiving by a network device a message that indicates whether another network device identifies a relay key using an identifier. Operation 2102 includes receiving, by a first network device from a second network device, a first request message that includes an identifier associated with a first communication device. Operation 2104 includes transmitting, by the first network device to a third network device, a second request message that includes the identifier. Operation 2106 includes receiving, by the first network device and in response to the second request message, a response message from the third network device, wherein the response message indicates whether the third network device identifies a relay key using the identifier.

[0409] In some embodiment, the third network device is determined by the first network device based on the identifier. In some embodiment, after the receiving and prior to the transmitting, the method further comprises: transmitting, by the first network device, a third request to the third network device, wherein the third request includes the identifier; and receiving, from the third network device, another identifier that identifies the third network device. In some embodiment, the identifier includes a 5G ProSe Relay User Key (PRUK) identifier (ID) that includes a routing identifier or a routing indicator (RID), and wherein the relay key includes 5G PRUK. In some embodiment, the 5G PRUK ID includes a first part that includes the RID and a prose temporary user equipment identifier (P-TID), and a second part that includes a home network identifier, and the first part precedes the second part.

[0410] In some embodiment, a second communication device is authorized to act as a relay between the first communication device and a communication network that includes any one or more of first network device, the second network device, and the third network device. In some embodiment, the first network device includes an authentication server function (AUSF) device, the second network device includes a remote access and mobility management function (AMF) device, and the third network device includes a prose anchor function (PAnF).

[0411] IV.(b) Case 3.2 AMF find PAnF. PAnF generate K_{NR_Prose}

[0412] FIGS. 12A-12B show an example flowchart of a security procedure where AMF finds PAnF, and PAnF generates K_{NR_Prose} . FIG. 12B is a continuation of the process in FIG. 12A.

[0413] 0. The Remote UE and relay UE can be registered with the network. The UE-to-Network relay can be authenticated and authorized by the network to support as a relay UE. Remote UE can be authenticated and authorized by the network to act as a Remote UE.

[0414] 1. The remote UE can initiate discovery procedure using any of Model A or Model B method.

[0415] 2. After the discovery of the UE-to-Network relay, the Remote UE can send a Direct Communication Request to the relay UE for establishing secure PC5 unicast link. The Remote UE can include its security capabilities and security policy in the DCR message. The message can also include 5GPRUK ID if available, Relay Service Code, Nonce_1. If UE has no available 5G PRUK ID or the 5G PRUK ID has been reject before, the UE can use SUCI instead of 5G PRUK ID.

[0416] 3. Upon receiving the DCR message, the Relay UE can send the relay key request to the relay AMF, including the parameters received in the DCR message.

[0417] 4. The Relay AMF can verify whether the relay UE is authorized to act as U2N relay. The Relay AMF decides to whether to authenticate the Remote UE. If so, AMF use Option 1 or Option 2. Otherwise go to step 5a.

[0418] Option 1

[0419] 4a. If the Relay AMF decide to authenticate the Remote UE based on its (the Relay AMF's) local policy, then the Relay AMF sends Reject message include the cause and the transaction identifier.

[0420] 4b. The Relay UE forward the Reject message to the Remote UE.

[0421] 4c. The Remote UE sends a new DCR message, the message can include the Remote UE's SUCI, Relay service code and Nonce_1. The Nonce_1 can be the same or different with the Nonce_1 in step 2.

[0422] 4d. The Relay UE can send the relay key request to the relay AMF, including the parameters received in the DCR message. Then go to Step 5.

[0423] Option 2

[0424] 4e. If the Relay AMF decide to authenticate the Remote UE based on its (the Relay AMF's) local policy, then the Relay AMF sends Identity Request message include the transaction identifier.

[0425] 4f. The Relay UE forward the Identity Request message to the Remote UE.

[0426] 4g. The Remote UE sends its SUCI in the Identity Response message

[0427] 4h. The Relay UE forward the Identity Response message to the Relay AMF. Then go to Step 5.

[0428] 5a. The relay AMF select PAnF based on 5GPRUK ID and sends a Npanf_ProseKey_Get Request to PAnF. The request message include 5GPRUK ID, RSC, Nonce1.

[0429] If AMF can use 5G PRUK ID to find a PAnF instance ID which is stored in the AMF, then the AMF select the PAnF.

[0430] If RID is included in the 5G PRUK ID, the PAnF selection should consider the RID.

[0431] The 5GPRUK ID may be generated as follows:

[0432] 5GPRUK ID is in NAI format as specified in clause 2.2 of IETF RFC 7542, e.g. username@realm. The username part can include the RID and the P-TID (Prose Temporary UE Identifier), and the realm part can include Home Network Identifier.

[0433] The P-TID is derived from K_{AUSF} or K_{ausf_p} .

[0434] 5b. If the PAnF can find the 5G PRUK, then go to Step 11a. If the PAnF can not find the 5G PRUK, then sends a Reject Response to the AMF.

[0435] 5c. AMF use Option 1 or Option 2.

[0436] 5. As shown in FIG. 12B, which is a continuation of the process in FIG. 12A, the relay AMF sends a Nausf_UEAuthentication_ProseAuthenticate Request to AUSF. The request message include 5GPRUK ID, RSC, Nonce1, SN name.

[0437] 6a~6b. The AUSF can retrieve the Authentication Vectors from the UDM via Nudm_UEAuthentication_GetProseAv Request message and trigger authentication of the remote UE.

[0438] 7a. If EAP-AKA' is selected by UDM, the AUSF of the 5G ProSe Remote UE can trigger authentication of the 5G ProSe Remote UE based on EAP-AKA'. The AUSF of the 5G ProSe Remote UE generates the EAP-Request/AKA'-Challenge message and send EAP-Request/AKA'-Challenge message to the AMF of the 5G ProSe UE-to-Network Relay in a Nausf_UEAuthentication_ProseAuthenticate Response message.

[0439] 7b. The AMF of the 5G ProSe UE-to-Network Relay can forward the Relay Authentication Request (including the EAP-Request/AKA'-Challenge) to the 5G ProSe UE-to-Network Relay over NAS message, including transaction identifier of the 5G ProSe Remote UE in the message. The NAS message is protected using the NAS security context created for the 5G ProSe UE-to-Network Relay.

[0440] 7c. Based on the transaction identifier, the 5G ProSe UE-to-Network Relay can forwards the EAP-Request/AKA'-Challenge to the 5G ProSe Remote UE over PC5 messages.

[0441] The USIM in the 5G ProSe Remote UE verifies the freshness of the received values by checking whether AUTN can be accepted.

[0442] For EAP-AKA', the USIM computes a response RES. The USIM can return RES, CK, IK to the ME. The ME can derive CK' and IK'.

[0443] 7d. The 5G ProSe Remote UE can return EAP-Response/AKA'-Challenge to the 5G ProSe UE-to-Network Relay over PC5 messages.

- [0444] 7e. The 5G ProSe UE-to-Network Relay forwards the EAP-Response/AKA'-Challenge together with the transaction identifier of the 5G ProSe Remote UE to the AMF of the 5G ProSe UE-to-Network Relay in a NAS message Relay Authentication Response.
- [0445] 7f. The AMF of the 5G ProSe UE-to-Network Relay forwards EAP-Response/AKA'-Challenge to the AUSF of the 5G ProSe Remote UE via Nausf_UEAuthentication_ProSeAuthenticate Request.
- [0446] The AUSF of the 5G ProSe Remote UE performs the UE authentication by verifying the received information.
- [0447] For EAP-AKA', the AUSF of the 5G ProSe Remote UE and the 5G ProSe Remote UE may exchange EAP-Request/AKA'-Notification and EAP-Response /AKA'-Notification messages via the AMF of the 5G ProSe UE-to-Network Relay. After the exchanges, the AUSF of the 5G ProSe Remote UE derives KAUSF without calculating the KSEAF.
- [0448] The AUSF of the 5G ProSe Remote UE and the 5G ProSe Remote UE can derive a new K_{AUSF_P} (different from K_{AUSF}). NAS SMC procedure is not performed between 5G ProSe Remote UE and AMF of the 5G ProSe UE-to-Network Relay.
- [0449] 8. On successful authentication, the AUSF of the 5G ProSe Remote UE and the 5G ProSe Remote UE can generate 5GPRUK and 5GPRUK ID using the newly derived K_{AUSF_P} .
- [0450] 9. AUSF sends a Nudm_UEAuthentication_ProseResultConfirmation to the UDM.
- [0451] 10a. The AUSF select a PAnF and sends a Npanf_ProseKey_Register Request to the PAnF. This message include 5GPRUK ID, 5GPRUK, RSC.
- [0452] 10b. The PAnF sends a Npanf_ProseKey_Register Response to AUSF. The Response may include the PAnF instance ID.
- [0453] 10c. The AUSF sends a Nausf_UEAuthentication_ProseAuthenticate Response to AMF. The message include 5G PRUK ID. The message may also include PAnF ID.
- [0454] 10d. The AMF select the PAnF based on the 5G PRUK ID. If AMF received PAnF ID from AUSF, the AMF select the PAnF. The AMF sends a Npanf_ProseKey_Get Request to PAnF, the message include 5GPRUK ID, RSC, Nonce_1.
- [0455] 11a. The PAnF can generate the K_{NR_ProSe} key.
- [0456] 11b. The PAnF sends a Npanf_ProseKey_Get Response to the AMF.
- [0457] 12. The 5G ProSe UE-to-Network Relay can send the received Nonce_2 to the 5G ProSe Remote UE in Direct Security mode command message, which is protected using Krelay-

int or/and Krelay-enc derived from Krelay-sess according to the negotiated PC5 signalling policies between the 5G ProSe Remote UE and the 5G ProSe UE-to-Network Relay.

[0458] 13-15b. The 5G ProSe Remote UE can use the 5GPRUK ID to locate the $K_{AUSF_P/5GPRUK}$ to be used for the PC5 link security. The 5G ProSe Remote UE can generate the K_{NR_ProSe} key to be used for Remote access via the 5G ProSe UE-to-Network Relay. The 5G ProSe Remote UE can derive PC5 session key Krelay-sess and confidentiality and integrity keys from K_{NR_ProSe} . The 5G ProSe Remote UE can send the Direct Security Mode Complete message containing its PC5 user plane security policies to the 5G ProSe UE-to-Network relay, which is protected by Krelay-int or/and Krelay-enc derived from Krelay-sess according to the negotiated PC5 signalling policies between the 5G ProSe Remote UE and the 5G ProSe UE-to-Network Relay. After the successful verification of the Direct Security Mode complete message, the 5G ProSe UE-to-Network Relay responds a Direct Communication Accept message to the 5G ProSe Remote UE to finish the PC5 connection establishment procedures.

[0459] FIG. 22 shows an example flowchart for receiving by a network device a message that indicates whether another network device identifies a relay key using an identifier. Operation 2202 includes transmitting, by a second network device to a third network device, a request message that includes an identifier associated with a first communication device. Operation 2204 includes receiving, by the second network device and in response to the request message, a response message from the third network device, wherein the response message indicates whether the third network device identifies a relay key using the identifier.

[0460] In some embodiments, the third network device is determined by the second network device based on the identifier. In some embodiments, prior to the transmitting, the method further comprises: transmitting, by the second network device, a second request to the third network device, wherein the third request includes the identifier; and receiving, from a first network device, another identifier that identifies the third network device, wherein the first network device includes an authentication server function (AUSF) device. In some embodiments, the identifier includes a 5G ProSe Relay User Key (PRUK) identifier (ID) that includes a routing identifier or a routing indicator (RID), and wherein the relay key includes 5G PRUK. In some embodiments, the 5G PRUK ID includes a first part that includes the RID and a prose temporary user equipment identifier (P-TID), and a second part that includes a home network identifier, and the first part precedes the second part.

[0461] In some embodiments, a second communication device is authorized to act as a relay between the first communication device and a communication network that includes any one or more of the second network device, and the third network device. In some embodiments, the second network device includes a remote access and mobility management function (AMF) device, and the third network device includes a prose anchor function (PAnF).

[0462] IV.(c) Case 3.3 AUSF find PAnF. PAnF generate K_{NR_Prose}

[0463] FIGS. 13A-13B show an example flowchart of a security procedure where AUSF finds PAnF, and PAnF generate K_{NR_Prose} . FIG. 13B is a continuation of the process in FIG. 13A.

[0464] 0. The Remote UE and relay UE can be registered with the network. The UE-to-Network relay can be authenticated and authorized by the network to support as a relay UE. Remote UE can be authenticated and authorized by the network to act as a Remote UE.

[0465] 1. The remote UE can initiate discovery procedure using any of Model A or Model B method.

[0466] 2. After the discovery of the UE-to-Network relay, the Remote UE can send a Direct Communication Request to the relay UE for establishing secure PC5 unicast link. The Remote UE can include its security capabilities and security policy in the DCR message. The message can also include 5GPRUK ID if available, Relay Service Code, Nonce_1. If UE has no available 5G PRUK ID or the 5G PRUK ID has been reject before, the UE can use SUCI instead of 5G PRUK ID.

[0467] 3. Upon receiving the DCR message, the Relay UE can send the relay key request to the relay AMF, including the parameters received in the DCR message.

[0468] 4. The Relay AMF can verify whether the relay UE is authorized to act as U2N relay. The Relay AMF decides to whether to authenticate the Remote UE. If so, AMF use Option 1 or Option 2. Otherwise go to step 5a.

[0469] Option 1

[0470] 4a. If the Relay AMF decide to authenticate the Remote UE based on its (the Relay AMF's) local policy, then the Relay AMF sends Reject message include the cause and the transaction identifier.

[0471] 4b. The Relay UE forward the Reject message to the Remote UE.

[0472] 4c. The Remote UE sends a new DCR message, the message can include the Remote UE's SUCI, Relay service code and Nonce_1. The Nonce_1 can be the same or different with the Nonce_1 in step 2.

[0473] 4d. The Relay UE can send the relay key request to the relay AMF, including the parameters received in the DCR message. Then go to Step 5.

[0474] Option 2

[0475] 4e. If the Relay AMF decide to authenticate the Remote UE based on its (the Relay AMF's) local policy, then the Relay AMF sends Identity Request message include the transaction identifier.

[0476] 4f. The Relay UE forward the Identity Request message to the Remote UE.

[0477] 4g. The Remote UE sends its SUCI in the Identity Response message

[0478] 4h. The Relay UE forward the Identity Response message to the Relay AMF. Then go to Step 5.

[0479] 5a. The relay AMF sends a Nausf_UEAuthentication_ProseAuthenticate Request to AUSF. The request message include 5GPRUK ID, RSC, Nonce1, SN name.

[0480] 5b. The AUSF can select PAnF based on 5GPRUK ID and sends a Npanf_ProseKey_Get Request to PAnF. The request message include 5GPRUK ID, RSC, Nonce_1. The request may also include the Nonce_2.

[0481] If AUSF can use 5G PRUK ID to find a PAnF instance ID which is stored in the AUSF, then the AUSF select the PAnF.

[0482] If RID is included in the 5G PRUK ID, the PAnF selection should consider the RID.

[0483] The 5GPRUK ID may be generated as follows:

[0484] 5GPRUK ID is in NAI format as specified in clause 2.2 of IETF RFC 7542, e.g. username@realm. The username part can include the RID and the P-TID (Prose Temporary UE Identifier), and the realm part can include Home Network Identifier.

[0485] The P-TID is derived from K_{AUSF} or K_{ausf_p} .

[0486] 5c. If the PAnF can find the 5G PRUK, then sends a Npanf_ProseKey_Get Response with K_{NR_Prose} to the AUSF. If the PAnF received Nonce_2 from AUSF, the PAnF use the Nonce_2 to generate K_{NR_Prose} . Otherwise, the PAnF generate the Nonce_2 itself and include the Nonce_2 in the response.

[0487] 5d. If the PAnF can not find the 5G PRUK, then sends a Reject Response to the AUSF. Then AUSF forward the Reject response to Relay AMF.

[0488] 5e. AMF use Option 1 or Option 2.

[0489] 5. As shown in FIG. 13B, which is a continuation of the process in FIG. 13A, the relay AMF sends a Nausf_UEAuthentication_ProseAuthenticate Request to AUSF. The request message include 5GPRUK ID, RSC, Nonce1, SN name.

[0490] 6a~6b. The AUSF can retrieve the Authentication Vectors from the UDM via Nudm_UEAuthentication_GetProseAv Request message and trigger authentication of the remote UE.

[0491] 7a. If EAP-AKA' is selected by UDM, the AUSF of the 5G ProSe Remote UE can trigger authentication of the 5G ProSe Remote UE based on EAP-AKA'. The AUSF of the 5G ProSe Remote UE generates the EAP-Request/AKA'-Challenge message defined in clause 6.1.3.1 of TS 33.501 and send EAP-Request/AKA'-Challenge message to the AMF of the 5G ProSe UE-to-Network Relay in a Nausf_UEAuthentication_ProseAuthenticate Response message.

[0492] 7b. The AMF of the 5G ProSe UE-to-Network Relay can forward the Relay Authentication Request (including the EAP-Request/AKA'-Challenge) to the 5G ProSe UE-to-Network Relay over NAS message, including transaction identifier of the 5G ProSe Remote UE in the message. The NAS message is protected using the NAS security context created for the 5G ProSe UE-to-Network Relay.

[0493] 7c. Based on the transaction identifier, the 5G ProSe UE-to-Network Relay can forwards the EAP-Request/AKA'-Challenge to the 5G ProSe Remote UE over PC5 messages.

[0494] The USIM in the 5G ProSe Remote UE verifies the freshness of the received values by checking whether AUTN can be accepted.

[0495] For EAP-AKA', the USIM computes a response RES. The USIM can return RES, CK, IK to the ME. The ME can derive CK' and IK'.

[0496] 7d. The 5G ProSe Remote UE can return EAP-Response/AKA'-Challenge to the 5G ProSe UE-to-Network Relay over PC5 messages.

[0497] 7e. The 5G ProSe UE-to-Network Relay forwards the EAP-Response/AKA'-Challenge together with the transaction identifier of the 5G ProSe Remote UE to the AMF of the 5G ProSe UE-to-Network Relay in a NAS message Relay Authentication Response.

[0498] 7f. The AMF of the 5G ProSe UE-to-Network Relay forwards EAP-Response/AKA'-Challenge to the AUSF of the 5G ProSe Remote UE via Nausf_UEAuthentication_ProSeAuthenticate Request.

[0499] The AUSF of the 5G ProSe Remote UE performs the UE authentication by verifying the received information.

[0500] For EAP-AKA', the AUSF of the 5G ProSe Remote UE and the 5G ProSe Remote UE may exchange EAP-Request/AKA'-Notification and EAP-Response /AKA'-Notification messages via the AMF of the 5G ProSe UE-to-Network Relay. After the exchanges, the AUSF of the 5G ProSe Remote UE derives K_{AUSF} without calculating the K_{SEAF} .

[0501] The AUSF of the 5G ProSe Remote UE and the 5G ProSe Remote UE can derive a new K_{AUSF_P} (different from K_{AUSF}). NAS SMC procedure is not performed between 5G ProSe Remote UE and AMF of the 5G ProSe UE-to-Network Relay.

[0502] 8. On successful authentication, the AUSF of the 5G ProSe Remote UE and the 5G ProSe Remote UE can generate 5GPRUK and 5GPRUK ID using the newly derived K_{AUSF_P} .

[0503] 9. AUSF sends a Nudm_UEAuthentication_ProseResultConfirmation to the UDM.

[0504] 10a. The AUSF select a PAnF and sends a Npanf_ProseKey_Register Request to the PAnF. This message include 5GPRUK ID, 5GPRUK, RSC, Nonce_1. The Request may also include Nonce_2.

[0505] 10b. The PAnF generate the K_{NR_Prose} Key.

[0506] 10c. The PAnF sends a Npanf_ProseKey_Register Response with K_{NR_Prose} to AUSF. The Response may include the PAnF instance ID. The Response may also include Nonce_2.

[0507] 11. The AUSF of the 5G ProSe Remote UE can send the K_{NR_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. When receiving a K_{NR_ProSe} from the AUSF of the 5G ProSe Remote UE, the AMF of the 5G ProSe UE-to-Network Relay can not attempt to trigger NAS SMC procedure with the 5G ProSe Remote UE. The 5G ProSe UE-to-Network Relay derives PC5 session key $K_{relay-sess}$ and confidentiality and integrity keys from K_{NR_ProSe} .

[0508] 12. The 5G ProSe UE-to-Network Relay can send the received Nonce_2 to the 5G ProSe Remote UE in Direct Security mode command message, which is protected using $K_{relay-sess}$.

int or/and Krelay-enc derived from Krelay-sess according to the negotiated PC5 signalling policies between the 5G ProSe Remote UE and the 5G ProSe UE-to-Network Relay.

[0509] 13-15b. The 5G ProSe Remote UE can use the 5GPRUK ID to locate the $K_{AUSF_P/5GPRUK}$ to be used for the PC5 link security. The 5G ProSe Remote UE can generate the K_{NR_ProSe} key to be used for Remote access via the 5G ProSe UE-to-Network Relay . The 5G ProSe Remote UE can derive PC5 session key Krelay-sess and confidentiality and integrity keys from K_{NR_ProSe} . The 5G ProSe Remote UE can send the Direct Security Mode Complete message containing its PC5 user plane security policies to the 5G ProSe UE-to-Network relay, which is protected by Krelay-int or/and Krelay-enc derived from Krelay-sess according to the negotiated PC5 signalling policies between the 5G ProSe Remote UE and the 5G ProSe UE-to-Network Relay. After the successful verification of the Direct Security Mode complete message, the 5G ProSe UE-to-Network Relay responds a Direct Communication Accept message to the 5G ProSe Remote UE to finish the PC5 connection establishment procedures.

[0510] V. Case 4: The Remote UE use SUCI and 5G PRUK ID. PAnF involved to store the 5G PRUK.

[0511] V.(a) Case 4.1 AUSF find PAnF. AUSF generate K_{NR_Prose}

[0512] FIGS. 14A-14B show an example flowchart of a security procedure where AUSF finds PAnF, and AUSF generate K_{NR_Prose} . FIG. 14B is a continuation of the process in FIG. 14A.

[0513] 0. The Remote UE and relay UE can be registered with the network. The UE-to-Network relay can be authenticated and authorized by the network to support as a relay UE. Remote UE can be authenticated and authorized by the network to act as a Remote UE.

[0514] 1. The remote UE can initiate discovery procedure using any of Model A or Model B method.

[0515] 2. After the discovery of the UE-to-Network relay, the Remote UE can send a Direct Communication Request to the relay UE for establishing secure PC5 unicast link. The Remote UE can include its security capabilities and security policy in the DCR message. The message can also include SUCI and 5GPRUK ID if available, Relay Service Code, Nonce_1.

[0516] 3. Upon receiving the DCR message, the Relay UE can send the relay key request to the relay AMF, including the parameters received in the DCR message.

- [0517] 4. The Relay AMF can verify whether the relay UE is authorized to act as U2N relay. The Relay AMF decides to whether to authenticate the Remote UE.
- [0518] 5a. The relay AMF sends a Nausf_UEAuthentication_ProseAuthenticate Request to AUSF. The request message include 5GPRUK ID, RSC, Nonce1, SN name.
- [0519] 5b. The AUSF can select PAnF based on 5GPRUK ID and sends a Npanf_ProseKey_Get Request to PAnF. The request message include 5GPRUK ID, RSC.
- [0520] If AUSF can use 5G PRUK ID to find a PAnF instance ID which is stored in the AUSF, then the AUSF select the PAnF.
- [0521] If RID is included in the 5G PRUK ID, the PAnF selection should consider the RID.
- [0522] The 5GPRUK ID may be generated as follows:
- [0523] 5GPRUK ID is in NAI format as specified in clause 2.2 of IETF RFC 7542, e.g. username@realm. The username part can include the RID and the P-TID (Prose Temporary UE Identifier), and the realm part can include Home Network Identifier.
- [0524] The P-TID is derived from KAUSF or Kausf_p.
- [0525] 5c. If the PAnF can find the 5G PRUK, then sends a Npanf_ProseKey_Get Response with 5G PRUK to the AUSF. The response may also include the Nonce_2. Then go to step 10.
- [0526] If the PAnF can not find the 5G PRUK, then sends a Reject Response to the AUSF. Then go to step 6a.
- [0527] 6a~6b. As shown in FIG. 14B, which is a continuation of the process in FIG. 14A, the AUSF can retrieve the Authentication Vectors from the UDM via Nudm_UEAuthentication_GetProseAv Request message and trigger authentication of the remote UE.
- [0528] 7a. If EAP-AKA' is selected by UDM, the AUSF of the 5G ProSe Remote UE can trigger authentication of the 5G ProSe Remote UE based on EAP-AKA'. The AUSF of the 5G ProSe Remote UE generates the EAP-Request/AKA'-Challenge message and send EAP-Request/AKA'-Challenge message to the AMF of the 5G ProSe UE-to-Network Relay in a Nausf_UEAuthentication_ProSeAuthenticate Response message.
- [0529] 7b. The AMF of the 5G ProSe UE-to-Network Relay can forward the Relay Authentication Request (including the EAP-Request/AKA'-Challenge) to the 5G ProSe UE-to-Network Relay over NAS message, including transaction identifier of the 5G ProSe Remote UE

in the message. The NAS message is protected using the NAS security context created for the 5G ProSe UE-to-Network Relay.

[0530] 7c. Based on the transaction identifier, the 5G ProSe UE-to-Network Relay can forwards the EAP-Request/AKA'-Challenge to the 5G ProSe Remote UE over PC5 messages.

[0531] The USIM in the 5G ProSe Remote UE verifies the freshness of the received values by checking whether AUTN can be accepted.

[0532] For EAP-AKA', the USIM computes a response RES. The USIM can return RES, CK, IK to the ME. The ME can derive CK' and IK'.

[0533] 7d. The 5G ProSe Remote UE can return EAP-Response/AKA'-Challenge to the 5G ProSe UE-to-Network Relay over PC5 messages.

[0534] 7e. The 5G ProSe UE-to-Network Relay forwards the EAP-Response/AKA'-Challenge together with the transaction identifier of the 5G ProSe Remote UE to the AMF of the 5G ProSe UE-to-Network Relay in a NAS message Relay Authentication Response.

[0535] 7f. The AMF of the 5G ProSe UE-to-Network Relay forwards EAP-Response/AKA'-Challenge to the AUSF of the 5G ProSe Remote UE via Nausf_UEAuthentication_ProSeAuthenticate Request.

[0536] The AUSF of the 5G ProSe Remote UE performs the UE authentication by verifying the received information.

[0537] For EAP-AKA', the AUSF of the 5G ProSe Remote UE and the 5G ProSe Remote UE may exchange EAP-Request/AKA'-Notification and EAP-Response /AKA'-Notification messages via the AMF of the 5G ProSe UE-to-Network Relay. After the exchanges, the AUSF of the 5G ProSe Remote UE derives K_{AUSF} without calculating the K_{SEAF} .

[0538] The AUSF of the 5G ProSe Remote UE and the 5G ProSe Remote UE can derive a new K_{AUSF_P} (different from K_{AUSF}). NAS SMC procedure is not performed between 5G ProSe Remote UE and AMF of the 5G ProSe UE-to-Network Relay.

[0539] 8. On successful authentication, the AUSF of the 5G ProSe Remote UE and the 5G ProSe Remote UE can generate 5GPRUK and 5GPRUK ID using the newly derived K_{AUSF_P} .

[0540] 9. AUSF sends a Nudm_UEAuthentication_ProseResultConfirmation to the UDM.

[0541] 10a. The AUSF select a PAnF and sends a Npanf_ProseKey_Register Request to the PAnF. This message include 5GPRUK ID, 5GPRUK, RSC.

[0542] 10b. The PAnF sends a Npanf_ProseKey_Register Response to AUSF. The Response may include the PAnF instance ID. The Response may also include Nonce_2.

[0543] 10. The AUSF of the 5G ProSe Remote UE can generate the K_{NR_ProSe} key.

[0544] 11. The AUSF of the 5G ProSe Remote UE can send the K_{NR_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. When receiving a K_{NR_ProSe} from the AUSF of the 5G ProSe Remote UE, the AMF of the 5G ProSe UE-to-Network Relay can not attempt to trigger NAS SMC procedure with the 5G ProSe Remote UE. The 5G ProSe UE-to-Network Relay derives PC5 session key Krelay-sess and confidentiality and integrity keys from K_{NR_ProSe} .

[0545] 12. The 5G ProSe UE-to-Network Relay can send the received Nonce_2 to the 5G ProSe Remote UE in Direct Security mode command message, which is protected using Krelay-int or/and Krelay-enc derived from Krelay-sess according to the negotiated PC5 signalling policies between the 5G ProSe Remote UE and the 5G ProSe UE-to-Network Relay.

[0546] 13-15b. The 5G ProSe Remote UE can use the 5GPRUK ID to locate the $K_{AUSF_P/5GPRUK}$ to be used for the PC5 link security. The 5G ProSe Remote UE can generate the K_{NR_ProSe} key to be used for Remote access via the 5G ProSe UE-to-Network Relay. The 5G ProSe Remote UE can derive PC5 session key Krelay-sess and confidentiality and integrity keys from K_{NR_ProSe} . The 5G ProSe Remote UE can send the Direct Security Mode Complete message containing its PC5 user plane security policies to the 5G ProSe UE-to-Network relay, which is protected by Krelay-int or/and Krelay-enc derived from Krelay-sess according to the negotiated PC5 signalling policies between the 5G ProSe Remote UE and the 5G ProSe UE-to-Network Relay. After the successful verification of the Direct Security Mode complete message, the 5G ProSe UE-to-Network Relay responds a Direct Communication Accept message to the 5G ProSe Remote UE to finish the PC5 connection establishment procedures.

[0547] V.(b) Case 4.2 AMF find PAnF. PAnF generate K_{NR_Prose}

[0548] FIGS. 15A-15B show an example flowchart of a security procedure where AMF finds PAnF, and PAnF generate K_{NR_Prose} . FIG. 15B is a continuation of the process in FIG. 15A.

[0549] 0. The Remote UE and relay UE can be registered with the network. The UE-to-Network relay can be authenticated and authorized by the network to support as a relay UE. Remote UE can be authenticated and authorized by the network to act as a Remote UE.

- [0550] 1. The remote UE can initiate discovery procedure using any of Model A or Model B method.
- [0551] 2. After the discovery of the UE-to-Network relay, the Remote UE can send a Direct Communication Request to the relay UE for establishing secure PC5 unicast link. The Remote UE can include its security capabilities and security policy in the DCR message. The message can also include SUCI and 5GPRUK ID if available, Relay Service Code, Nonce₁.
- [0552] 3. Upon receiving the DCR message, the Relay UE can send the relay key request to the relay AMF, including the parameters received in the DCR message.
- [0553] 4. The Relay AMF can verify whether the relay UE is authorized to act as U2N relay. The Relay AMF decides to whether to authenticate the Remote UE.
- [0554] 5a. The relay AMF select PAnF based on 5GPRUK ID and sends a Npanf_ProseKey_Get Request to PAnF. The request message include 5GPRUK ID, RSC, Nonce₁.
- [0555] If the PAnF can find the 5G PRUK, then go to Step 11a
- [0556] If AMF can use 5G PRUK ID to find a PAnF instance ID which is stored in the AMF, then the AMF select the PAnF.
- [0557] If RID is included in the 5G PRUK ID, the PAnF selection should consider the RID.
- [0558] The 5GPRUK ID may be generated as follows:
- [0559] 5GPRUK ID is in NAI format as specified in clause 2.2 of IETF RFC 7542, e.g. username@realm. The username part can include the RID and the P-TID (Prose Temporary UE Identifier), and the realm part can include Home Network Identifier.
- [0560] The P-TID is derived from K_{AUSF} or Kausf_p.
- [0561] 5b. As shown in FIG. 15B, which is a continuation of the process in FIG. 15A, if the PAnF can not find the 5G PRUK, then sends a Reject Response to the AMF.
- [0562] 5. The relay AMF sends a Nausf_UEAuthentication_ProseAuthenticate Request to AUSF. The request message include SUCI, RSC, Nonce₁, SN name.
- [0563] 6a~6b. The AUSF can retrieve the Authentication Vectors from the UDM via Nudm_UEAuthentication_GetProseAv Request message and trigger authentication of the remote UE.
- [0564] 7a. If EAP-AKA' is selected by UDM, the AUSF of the 5G ProSe Remote UE can trigger authentication of the 5G ProSe Remote UE based on EAP-AKA'. The AUSF of the 5G

ProSe Remote UE generates the EAP-Request/AKA'-Challenge message and send EAP-Request/AKA'-Challenge message to the AMF of the 5G ProSe UE-to-Network Relay in a Nausf_UEAuthentication_ProSeAuthenticate Response message.

[0565] 7b. The AMF of the 5G ProSe UE-to-Network Relay can forward the Relay Authentication Request (including the EAP-Request/AKA'-Challenge) to the 5G ProSe UE-to-Network Relay over NAS message, including transaction identifier of the 5G ProSe Remote UE in the message. The NAS message is protected using the NAS security context created for the 5G ProSe UE-to-Network Relay.

[0566] 7c. Based on the transaction identifier, the 5G ProSe UE-to-Network Relay can forwards the EAP-Request/AKA'-Challenge to the 5G ProSe Remote UE over PC5 messages.

[0567] The USIM in the 5G ProSe Remote UE verifies the freshness of the received values by checking whether AUTN can be accepted.

[0568] For EAP-AKA', the USIM computes a response RES. The USIM can return RES, CK, IK to the ME. The ME can derive CK' and IK'.

[0569] 7d. The 5G ProSe Remote UE can return EAP-Response/AKA'-Challenge to the 5G ProSe UE-to-Network Relay over PC5 messages.

[0570] 7e. The 5G ProSe UE-to-Network Relay forwards the EAP-Response/AKA'-Challenge together with the transaction identifier of the 5G ProSe Remote UE to the AMF of the 5G ProSe UE-to-Network Relay in a NAS message Relay Authentication Response.

[0571] 7f. The AMF of the 5G ProSe UE-to-Network Relay forwards EAP-Response/AKA'-Challenge to the AUSF of the 5G ProSe Remote UE via Nausf_UEAuthentication_ProSeAuthenticate Request.

[0572] The AUSF of the 5G ProSe Remote UE performs the UE authentication by verifying the received information.

[0573] For EAP-AKA', the AUSF of the 5G ProSe Remote UE and the 5G ProSe Remote UE may exchange EAP-Request/AKA'-Notification and EAP-Response /AKA'-Notification messages via the AMF of the 5G ProSe UE-to-Network Relay. After the exchanges, the AUSF of the 5G ProSe Remote UE derives KAUSF without calculating the KSEAF.

[0574] The AUSF of the 5G ProSe Remote UE and the 5G ProSe Remote UE can derive a new KAUSF_P (different from KAUSF). NAS SMC procedure is not performed between 5G ProSe Remote UE and AMF of the 5G ProSe UE-to-Network Relay.

- [0575] 8. On successful authentication, the AUSF of the 5G ProSe Remote UE and the 5G ProSe Remote UE can generate 5GPRUK and 5GPRUK ID using the newly derived K_{AUSF_P} .
- [0576] 9. AUSF sends a Nudm_UEAuthentication_ProseResultConfirmation to the UDM.
- [0577] 10a. The AUSF select a PAnF and sends a Npanf_ProseKey_Register Request to the PAnF. This message include 5GPRUK ID, 5GPRUK, RSC.
- [0578] 10b. The PAnF sends a Npanf_ProseKey_Register Response to AUSF. The Response may include the PAnF instance ID.
- [0579] 10c. The AUSF sends a Nausf_UEAuthentication_ProseAuthenticate Response to AMF. The message include 5G PRUK ID. The message may also include PAnF ID.
- [0580] 10d. The AMF select the PAnF based on the 5G PRUK ID. If AMF received PAnF ID from AUSF, the AMF select the PAnF. The AMF sends a Npanf_ProseKey_Get Request to PAnF, the message include 5GPRUK ID, RSC, Nonce_1.
- [0581] 11a. The PAnF can generate the K_{NR_ProSe} key.
- [0582] 11b. The PAnF sends a Npanf_ProseKey_Get Response to the AMF.
- [0583] 12. The 5G ProSe UE-to-Network Relay can send the received Nonce_2 to the 5G ProSe Remote UE in Direct Security mode command message, which is protected using Krelay-int or/and Krelay-enc derived from Krelay-sess according to the negotiated PC5 signalling policies between the 5G ProSe Remote UE and the 5G ProSe UE-to-Network Relay.
- [0584] 13-15b. The 5G ProSe Remote UE can use the 5GPRUK ID to locate the $K_{AUSF_P}/5GPRUK$ to be used for the PC5 link security. The 5G ProSe Remote UE can generate the K_{NR_ProSe} key to be used for Remote access via the 5G ProSe UE-to-Network Relay. The 5G ProSe Remote UE can derive PC5 session key Krelay-sess and confidentiality and integrity keys from K_{NR_ProSe} . The 5G ProSe Remote UE can send the Direct Security Mode Complete message containing its PC5 user plane security policies to the 5G ProSe UE-to-Network relay, which is protected by Krelay-int or/and Krelay-enc derived from Krelay-sess according to the negotiated PC5 signalling policies between the 5G ProSe Remote UE and the 5G ProSe UE-to-Network Relay. After the successful verification of the Direct Security Mode complete message, the 5G ProSe UE-to-Network Relay responds a Direct Communication Accept message to the 5G ProSe Remote UE to finish the PC5 connection establishment procedures
- [0585] V.(c) Case 4.3 AUSF find PAnF. PAnF generate K_{NR_Prose}

[0586] FIGS. 16A-16B show an example flowchart of a security procedure where AUSF finds PAnF, and PAnF generate K_{NR_Prose} . FIG. 16B is a continuation of the process in FIG. 16A.

[0587] 0. The Remote UE and relay UE can be registered with the network. The UE-to-Network relay can be authenticated and authorized by the network to support as a relay UE. Remote UE can be authenticated and authorized by the network to act as a Remote UE.

[0588] 1. The remote UE can initiate discovery procedure using any of Model A or Model B method.

[0589] 2. After the discovery of the UE-to-Network relay, the Remote UE can send a Direct Communication Request to the relay UE for establishing secure PC5 unicast link. The Remote UE can include its security capabilities and security policy in the DCR message. The message can also include SUCI and 5GPRUK ID if available, Relay Service Code, Nonce_1.

[0590] 3. Upon receiving the DCR message, the Relay UE can send the relay key request to the relay AMF, including the parameters received in the DCR message.

[0591] 4. The Relay AMF can verify whether the relay UE is authorized to act as U2N relay.

[0592] 5a. The relay AMF sends a Nausf_UEAuthentication_ProseAuthenticate Request to AUSF. The request message include 5GPRUK ID, RSC, Nonce1, SN name.

[0593] 5b. The AUSF can select PAnF based on 5GPRUK ID and sends a Npanf_ProseKey_Get Request to PAnF. The request message include 5GPRUK ID, RSC, Nonce_1. The request may also include the Nonce_2.

[0594] If AUSF can use 5G PRUK ID to find a PAnF instance ID which is stored in the AUSF, then the AUSF select the PAnF.

[0595] If RID is included in the 5G PRUK ID, the PAnF selection should consider the RID.

[0596] The 5GPRUK ID may be generated as follows:

[0597] 5GPRUK ID is in NAI format as specified in clause 2.2 of IETF RFC 7542, e.g. username@realm. The username part can include the RID and the P-TID (Prose Temporary UE Identifier), and the realm part can include Home Network Identifier.

[0598] The P-TID is derived from KAUSF or Kausf_p.

[0599] 5c. If the PAnF can find the 5G PRUK, then sends a Npanf_ProseKey_Get Response with K_{NR_Prose} to the AUSF. If the PAnF received Nonce_2 from AUSF, the PAnF use the

Nonce_2 to generate K_{NR_Prose} . Otherwise, the PAnF generate the Nonce_2 itself and include the Nonce_2 in the response. Then go to step 11.

[0600] If the PAnF can not find the 5G PRUK, then sends a Reject Response to the AUSF. Then go to step 6a.

[0601] 6a~6b. As shown in FIG. 16B, which is a continuation of the process in FIG. 16A, the AUSF can retrieve the Authentication Vectors from the UDM via Nudm_UEAuthentication_GetProseAv Request message and trigger authentication of the remote UE.

[0602] 7a. If EAP-AKA' is selected by UDM, the AUSF of the 5G ProSe Remote UE can trigger authentication of the 5G ProSe Remote UE based on EAP-AKA'. The AUSF of the 5G ProSe Remote UE generates the EAP-Request/AKA'-Challenge message and send EAP-Request/AKA'-Challenge message to the AMF of the 5G ProSe UE-to-Network Relay in a Nausf_UEAuthentication_ProSeAuthenticate Response message.

[0603] 7b. The AMF of the 5G ProSe UE-to-Network Relay can forward the Relay Authentication Request (including the EAP-Request/AKA'-Challenge) to the 5G ProSe UE-to-Network Relay over NAS message, including transaction identifier of the 5G ProSe Remote UE in the message. The NAS message is protected using the NAS security context created for the 5G ProSe UE-to-Network Relay.

[0604] 7c. Based on the transaction identifier, the 5G ProSe UE-to-Network Relay can forwards the EAP-Request/AKA'-Challenge to the 5G ProSe Remote UE over PC5 messages.

[0605] The USIM in the 5G ProSe Remote UE verifies the freshness of the received values by checking whether AUTN can be accepted.

[0606] For EAP-AKA', the USIM computes a response RES. The USIM can return RES, CK, IK to the ME. The ME can derive CK' and IK'.

[0607] 7d. The 5G ProSe Remote UE can return EAP-Response/AKA'-Challenge to the 5G ProSe UE-to-Network Relay over PC5 messages.

[0608] 7e. The 5G ProSe UE-to-Network Relay forwards the EAP-Response/AKA'-Challenge together with the transaction identifier of the 5G ProSe Remote UE to the AMF of the 5G ProSe UE-to-Network Relay in a NAS message Relay Authentication Response.

[0609] 7f. The AMF of the 5G ProSe UE-to-Network Relay forwards EAP-Response/AKA'-Challenge to the AUSF of the 5G ProSe Remote UE via Nausf_UEAuthentication_ProSeAuthenticate Request.

[0610] The AUSF of the 5G ProSe Remote UE performs the UE authentication by verifying the received information as described in TS33.501.

[0611] For EAP-AKA', the AUSF of the 5G ProSe Remote UE and the 5G ProSe Remote UE may exchange EAP-Request/AKA'-Notification and EAP-Response /AKA'-Notification messages via the AMF of the 5G ProSe UE-to-Network Relay. After the exchanges, the AUSF of the 5G ProSe Remote UE derives K_{AUSF} without calculating the K_{SEAF} .

[0612] The AUSF of the 5G ProSe Remote UE and the 5G ProSe Remote UE can derive a new K_{AUSF_P} (different from K_{AUSF}). NAS SMC procedure is not performed between 5G ProSe Remote UE and AMF of the 5G ProSe UE-to-Network Relay.

[0613] 8. On successful authentication, the AUSF of the 5G ProSe Remote UE and the 5G ProSe Remote UE can generate 5GPRUK and 5GPRUK ID using the newly derived K_{AUSF_P} .

[0614] 9. AUSF sends a Nudm_UEAuthentication_ProseResultConfirmation to the UDM.

[0615] 10a. The AUSF select a PAnF and sends a Npanf_ProseKey_Register Request to the PAnF. This message include 5GPRUK ID, 5GPRUK, RSC, Nonce_1. The Request may also include Nonce_2.

[0616] 10b. The PAnF generate the K_{NR_Prose} Key.

[0617] 10c. The PAnF sends a Npanf_ProseKey_Register Response with K_{NR_Prose} to AUSF. The Response may include the PAnF instance ID. The Response may also include Nonce_2.

[0618] 11. The AUSF of the 5G ProSe Remote UE can send the K_{NR_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. When receiving a K_{NR_ProSe} from the AUSF of the 5G ProSe Remote UE, the AMF of the 5G ProSe UE-to-Network Relay can not attempt to trigger NAS SMC procedure with the 5G ProSe Remote UE. The 5G ProSe UE-to-Network Relay derives PC5 session key K_{relay_sess} and confidentiality and integrity keys from K_{NR_ProSe} .

[0619] 12. The 5G ProSe UE-to-Network Relay can send the received Nonce_2 to the 5G ProSe Remote UE in Direct Security mode command message, which is protected using K_{relay} -

int or/and Krelay-enc derived from Krelay-sess according to the negotiated PC5 signalling policies between the 5G ProSe Remote UE and the 5G ProSe UE-to-Network Relay.

[0620] 13-15b. The 5G ProSe Remote UE can use the 5GPRUK ID to locate the $K_{AUSF_P/5GPRUK}$ to be used for the PC5 link security. The 5G ProSe Remote UE can generate the K_{NR_ProSe} key to be used for Remote access via the 5G ProSe UE-to-Network Relay. The 5G ProSe Remote UE can derive PC5 session key Krelay-sess and confidentiality and integrity keys from K_{NR_ProSe} . The 5G ProSe Remote UE can send the Direct Security Mode Complete message containing its PC5 user plane security policies to the 5G ProSe UE-to-Network relay, which is protected by Krelay-int or/and Krelay-enc derived from Krelay-sess according to the negotiated PC5 signalling policies between the 5G ProSe Remote UE and the 5G ProSe UE-to-Network Relay. After the successful verification of the Direct Security Mode complete message, the 5G ProSe UE-to-Network Relay responds a Direct Communication Accept message to the 5G ProSe Remote UE to finish the PC5 connection establishment procedures.

[0621] The 6a-7f all above is about Prose authentication based on EAP-AKA' authentication. However, it may be replaced by 5G-AKA based Prose authentication.

[0622] FIG. 17 shows an example flowchart for an authentication technique.

[0623] 6a~6b. The AUSF can retrieve the Authentication Vectors from the UDM via Nudm_UEAuthentication_GetProseAv Request message and trigger authentication of the remote UE.

[0624] 7a. If 5G-AKA is selected by UDM, the AUSF of the 5G ProSe Remote UE can trigger authentication of the 5G ProSe Remote UE based on 5G-AKA.

[0625] 7b. The AMF of the 5G ProSe UE-to-Network Relay can forward the Relay Authentication Request to the 5G ProSe UE-to-Network Relay over NAS message, including transaction identifier of the 5G ProSe Remote UE in the message. The NAS message is protected using the NAS security context created for the 5G ProSe UE-to-Network Relay.

[0626] 7c. Based on the transaction identifier, the 5G ProSe UE-to-Network Relay can forwards the Authentication Request to the 5G ProSe Remote UE over PC5 messages.

[0627] 7d. The 5G ProSe Remote UE can return Authentication Response to the 5G ProSe UE-to-Network Relay over PC5 messages.

[0628] 7e. The 5G ProSe UE-to-Network Relay forwards the Authentication Response together with the transaction identifier of the 5G ProSe Remote UE to the AMF of the 5G ProSe UE-to-Network Relay in a NAS message Relay Authentication Response.

[0629] 7f. The AMF of the 5G ProSe UE-to-Network Relay forwards Authentication Response to the AUSF of the 5G ProSe Remote UE via Nausf_UEAuthentication_ProSeAuthenticate Request.

[0630] The AUSF of the 5G ProSe Remote UE performs the UE authentication by verifying the received information.

[0631] This patent document describes several techniques that may be used a security or authentication. Some example techniques described in this patent document include:

- The AMF can reject the request or ask for Remote UE's SUCI.
 - If the Remote UE use SUCI or 5G PRUK ID. When 5G PRUK ID is used, based on local policy or the 5G PRUK ID may not be used to find a 5G PRUK, AMF can reject the request or ask for Remote UE's SUCI.
- NF selection, RID and/or NF instance ID is used.
 - AMF may need to find a network function (NF) which store the 5G PRUK. NF can be AUSF (if no PAnF) or PAnF.
 - If AUSF perform the NF selection, which means AMF find AUSF then AUSF need to find the network function (NF) which store the 5G PRUK, PAnF or UDM if PAnF is not used or co-located with UDM.
 - AMF/AUSF can use 5G PRUK ID to find a NF instance ID which is stored in local database
 - If RID is included in the 5G PRUK ID, the AUSF selection should consider the RID.
 - The 5GPRUK ID may be generated as follows:
 - 5GPRUK ID is in NAI format as specified in clause 2.2 of IETF RFC 7542, e.g. username@realm. The username part (or the first part) can include the RID and the P-TID (Prose Temporary UE Identifier), and the realm part (or the second part) can include Home Network Identifier.
 - The P-TID is derived from KAUSF or Kausf_p.

- If both SUCI and 5G PRUK ID is used, use 5G PRUK ID first. If 5G PRUK ID can not be used to find a 5G PRUK, then NF use SUCI to trigger prose authentication.
- Different NF (AUSF, UDM, PAnF) may have the functionality to generate 5G PRUK and/or K_{NR_Prose} and Nonce_2, which result in different flows.

[0632] FIG. 18 shows an exemplary block diagram of a hardware platform 1800 that may be a part of a network device (e.g., base station) or a communication device (e.g., a user equipment (UE)). The hardware platform 500 includes at least one processor 1810 and a memory 1805 having instructions stored thereupon. The instructions upon execution by the processor 1810 configure the hardware platform 1800 to perform the operations described in FIGS. 1 to 18 and 19 to 23 and in the various embodiments described in this patent document. The transmitter 1815 transmits or sends information or data to another device. For example, a network device transmitter can send a message to a user equipment. The receiver 1820 receives information or data transmitted or sent by another device. For example, a user equipment can receive a message from a network device.

[0633] The implementations as discussed above will apply to a wireless communication. FIG. 19 shows an example of a wireless communication system (e.g., a 5G or NR cellular network) that includes a base station 1920 and one or more user equipment (UE) 1911, 1912 and 1913. In some embodiments, the UEs access the BS (e.g., the network) using a communication link to the network (sometimes called uplink direction, as depicted by dashed arrows 1931, 1932, 1933), which then enables subsequent communication (e.g., shown in the direction from the network to the UEs, sometimes called downlink direction, shown by arrows 1941, 1942, 1943) from the BS to the UEs. In some embodiments, the BS send information to the UEs (sometimes called downlink direction, as depicted by arrows 1941, 1942, 1943), which then enables subsequent communication (e.g., shown in the direction from the UEs to the BS, sometimes called uplink direction, shown by dashed arrows 1931, 1932, 1933) from the UEs to the BS. The UE may be, for example, a smartphone, a tablet, a mobile computer, a machine to machine (M2M) device, an Internet of Things (IoT) device, and so on.

[0634] In this document the term “exemplary” is used to mean “an example of” and, unless otherwise stated, does not imply an ideal or a preferred embodiment.

[0635] Some of the embodiments described herein are described in the general context of methods or processes, which may be implemented in one embodiment by a computer program

product, embodied in a computer-readable medium, including computer-executable instructions, such as program code, executed by computers in networked environments. A computer-readable medium may include removable and non-removable storage devices including, but not limited to, Read Only Memory (ROM), Random Access Memory (RAM), compact discs (CDs), digital versatile discs (DVD), etc. Therefore, the computer-readable media can include a non-transitory storage media. Generally, program modules may include routines, programs, objects, components, data structures, etc. that perform particular tasks or implement particular abstract data types. Computer- or processor-executable instructions, associated data structures, and program modules represent examples of program code for executing steps of the methods disclosed herein. The particular sequence of such executable instructions or associated data structures represents examples of corresponding acts for implementing the functions described in such steps or processes.

[0636] Some of the disclosed embodiments can be implemented as devices or modules using hardware circuits, software, or combinations thereof. For example, a hardware circuit implementation can include discrete analog and/or digital components that are, for example, integrated as part of a printed circuit board. Alternatively, or additionally, the disclosed components or modules can be implemented as an Application Specific Integrated Circuit (ASIC) and/or as a Field Programmable Gate Array (FPGA) device. Some implementations may additionally or alternatively include a digital signal processor (DSP) that is a specialized microprocessor with an architecture optimized for the operational needs of digital signal processing associated with the disclosed functionalities of this application. Similarly, the various components or sub-components within each module may be implemented in software, hardware or firmware. The connectivity between the modules and/or components within the modules may be provided using any one of the connectivity methods and media that is known in the art, including, but not limited to, communications over the Internet, wired, or wireless networks using the appropriate protocols.

[0637] While this document contains many specifics, these should not be construed as limitations on the scope of an invention that is claimed or of what may be claimed, but rather as descriptions of features specific to particular embodiments. Certain features that are described in this document in the context of separate embodiments can also be implemented in combination in a single embodiment. Conversely, various features that are described in the context of a single

embodiment can also be implemented in multiple embodiments separately or in any suitable sub-combination. Moreover, although features may be described above as acting in certain combinations and even initially claimed as such, one or more features from a claimed combination can in some cases be excised from the combination, and the claimed combination may be directed to a sub-combination or a variation of a sub-combination. Similarly, while operations are depicted in the drawings in a particular order, this should not be understood as requiring that such operations be performed in the particular order shown or in sequential order, or that all illustrated operations be performed, to achieve desirable results.

[0638] Only a few implementations and examples are described and other implementations, enhancements and variations can be made based on what is described and illustrated in this disclosure.

CLAIMS

What is claimed is:

1. A wireless communication method, comprising:
 - receiving, by a network device, a request message that includes an identifier associated with a first communication device;
 - determining, by the network device in response to the receiving, that the first communication device is authenticated based on a local policy of the network device;
 - and
 - sending, by the network device in response to the determining, a message to a second communication device to relay to the first communication device,
 - wherein the message indicates that the identifier is rejected by the network device for communication with the first communication device, or
 - wherein the message indicates that the first communication device is triggered to send another identifier.
2. The method of claim 1,
 - wherein the message is a reject message that includes a cause of a rejection and a transaction identifier,
 - wherein the reject message indicates that the identifier is rejected by the network device for communication with the first communication device, and
 - wherein the method further comprises:
 - receiving, from the first communication device and in response to the sending, a second message that includes a subscription concealed identifier (SUCI).
3. The method of claim 1,
 - wherein the message is an identity request message that includes a transaction identifier, and
 - wherein the method further comprises:

receiving, from the first communication device and in response to the sending, a second message that includes a subscription concealed identifier (SUCI).

4. The method of claim 1, wherein the second communication device is authorized to act as a relay between the first communication device and a communication network that includes the network device.
5. The method of any one of claims 1 to 4, wherein the identifier includes a 5G ProSe Relay User Key (PRUK) identifier (ID).
6. The method of any one of claims 1 to 4, wherein the network device includes a remote access and mobility management function (AMF) device.
7. A wireless communication method, comprising:
 - receiving, by a first network device from a second network device, a first request message that includes an identifier associated with a first communication device;
 - transmitting, by the first network device to a third network device, a second request message that includes the identifier; and
 - receiving, by the first network device and in response to the second request message, a response message from the third network device, wherein the response message indicates whether the third network device identifies a relay key using the identifier.
8. The method of claim 7, wherein the third network device is determined by the first network device based on the identifier.
9. The method of claim 7, wherein after the receiving and prior to the transmitting, the method further comprises:
 - transmitting, by the first network device, a third request to the third network device, wherein the third request includes the identifier; and

- receiving, from the third network device, another identifier that identifies the third network device.
10. The method of claim 7, wherein the identifier includes a 5G ProSe Relay User Key (PRUK) identifier (ID) that includes a routing identifier or a routing indicator (RID), and wherein the relay key includes 5G PRUK.
 11. The method of claim 10,
 - wherein the 5G PRUK ID includes a first part that includes the RID and a prose temporary user equipment identifier (P-TID), and a second part that includes a home network identifier, and
 - wherein the first part precedes the second part.
 12. The method of claim 7, wherein a second communication device is authorized to act as a relay between the first communication device and a communication network that includes any one or more of first network device, the second network device, and the third network device.
 13. The method of any one of claims 7 to 12,
 - wherein the first network device includes an authentication server function (AUSF) device,
 - wherein the second network device includes a remote access and mobility management function (AMF) device, and
 - wherein the third network device includes a prose anchor function (PAnF).
 14. A wireless communication method, comprising:
 - transmitting, by a second network device to a third network device, a request message that includes an identifier associated with a first communication device; and
 - receiving, by the second network device and in response to the request message, a

- response message from the third network device, wherein the response message indicates whether the third network device identifies a relay key using the identifier.
15. The method of claim 14, wherein the third network device is determined by the second network device based on the identifier.
 16. The method of claim 14, wherein prior to the transmitting, the method further comprises:
 - transmitting, by the second network device, a second request to the third network device, wherein the third request includes the identifier; and
 - receiving, from a first network device, another identifier that identifies the third network device, wherein the first network device includes an authentication server function (AUSF) device.
 17. The method of claim 14, wherein the identifier includes a 5G ProSe Relay User Key (PRUK) identifier (ID) that includes a routing identifier or a routing indicator (RID), and wherein the relay key includes 5G PRUK.
 18. The method of claim 17,
 - wherein the 5G PRUK ID includes a first part that includes the RID and a prose temporary user equipment identifier (P-TID), and a second part that includes a home network identifier, and
 - wherein the first part precedes the second part.
 19. The method of claim 14, wherein a second communication device is authorized to act as a relay between the first communication device and a communication network that includes any one or more of the second network device, and the third network device.
 20. The method of any one of claims 14 to 19,
 - wherein the second network device includes a remote access and mobility

- management function (AMF) device, and
wherein the third network device includes a prose anchor function (PAnF).
21. A wireless communication method, comprising:
receiving, by a first network device from a second network device, a first request message that includes first identifier associated with a first communication device and a second identifier;
transmitting, by the first network device to a third network device, a second request message that includes the first identifier; and
receiving, by the first network device and in response to the second request message, a response message from the third network device, wherein the response message indicates whether the third network device authenticated the first communication device.
22. The method of claim 21,
wherein the first identifier includes a 5G ProSe Relay User Key (PRUK) identifier (ID), and
wherein the second identifier includes a subscription concealed identifier (SUCI).
23. The method of claim 21, wherein a second communication device is authorized to act as a relay between the first communication device and a communication network that includes any one or more of the first network device, the second network device, and the third network device.
24. The method of any one of claims 21 to 23,
wherein the first network device includes an authentication server function (AUSF) device,
wherein the second network device includes a remote access and mobility management function (AMF) device, and
wherein the third network device includes a unified data management (UDM).

25. An apparatus for wireless communication comprising a processor, configured to implement a method recited in one or more of claims 1 to 24.
26. A non-transitory computer readable program storage medium having code stored thereon, the code, when executed by a processor, causing the processor to implement a method recited in one or more of claims 1 to 24.