

**METHOD AND APPARATUS FOR SECURITY REALIZATION OF
CONNECTIONS
OVER HETEROGENEOUS ACCESS NETWORKS**

5 TECHNICAL FIELD

[0001] This application relates generally to access networks, and more specifically to session establishment by user equipment over a plurality of heterogeneous access networks

DESCRIPTION OF RELATED ART

[0002] The statements in this section provide a description of related art and are not admissions of prior art. User equipment (UE), such as smart phones, smart tablets, laptops, computers, smart watches, etc., often include capability for both wireless local area network (WLAN) connectivity (such as IEEE 802.11x compliant WLAN connectivity) and radio access network connectivity (such as technologies wholly or partially compliant with the 3rd generation partnership project (3GPP) set of standards including EVDO, UMTS, HSPA, and LTE). The UE may thus connect to the 3GPP evolved packet core (EPC) network using two types of access technologies composed of 3GPP access networks and non-3GPP access networks.

[0003] In general, 3GPP access networks are wholly or partially compliant with technologies specified by the 3GPP set of standards that include, e.g., GPRS, UMTS, EDGE, HSPA, LTE and LTE Advanced. Non-3GPP access networks are wholly or partially compliant with technologies that are not specified by the 3GPP set of standards. They include technologies such as cdma2000, WLAN (such as IEEE 802.11x compliant WLAN) or fixed networks.

[0004] The 3GPP set of standards specifies “non-3GPP” access technologies with different security mechanisms: untrusted access networks and trusted access networks. Untrusted access networks include access networks that may pose a higher security risk (for example, a public WLAN or femtocell access network). Trusted access networks include access networks that the network operator considers have a level of trust from a security stand point and may interface directly with the EPC network.

[0005] In the new set of 5G standards, one of the most important features for the 5G System is that it offers converged core network that is access agnostic. Different access

network types including 3GPP access and non-3GPP access can be supported via a common access network and core network interfaces. A Non-3GPP Access Network (N3AN) is considered as a 5G Access Network and part of the 5G System (5GS).

[0006] For untrusted non-3GPP access, a N3G access node N3IWF provides termination
5 of signaling interfaces for control-plane and user-plane respectively, same as an NG-RAN node. Thus, 5G capable UEs can access 5G core network by connecting to Non-3GPP Access Network as a 5G Access Network via the N3IWF. The N3IWF relays uplink and downlink control-plane signaling between the UE and AMF, such that the UE has a direct control plane signaling connection towards the AMF. In addition, the N3IWF provides user plane
10 connection between the UE and UPF for the PDU sessions over a non-3GPP access network.

[0007] When a UE is registered to the 5G core over both 3GPP access and non-3GPP access networks, multiple Non-Access Stratum (NAS) connections can be active at the same time. The UE can be registered in the same PLMN or different PLMN. If the UE is accessing one PLMN over one type of access (e.g. 3GPP access) and accessing another PLMN over
15 the other type of access (e.g. non-3GPP access), then different primary authentications are performed. After registration, the NAS connections serve different AMFs utilizing different security contexts. However, if the UE requests registration in the same serving network over different types of access networks, a common 5G NAS security context is created during the registration procedure over the first access type, and all NAS connections are served by the
20 same AMF.

[0008] Currently, for 3GPP access, it is assumed that the NAS connection identifier is "0". For non-3GPP access, it is assumed that the NAS connection identifier is "1". A problem arises when additional non-3GPP access network types are added in future releases, e.g. trusted WLAN access, wireline access, MuLTEFire access, etc. These different types of non-
25 3GPP access networks would each need to establish separate NAS connections. However, the currently there is only the one NAS connection identifier of "1" for NAS connections over the different types of non-3GPP access networks.

[0009] Therefore, a need exists to provide a system and method that supports NAS connections over a plurality of different types of non-3GPP access networks. Other needs
30 and benefits are also provided with embodiments described herein.

DETAILED DESCRIPTION

[0010] The description and drawings merely illustrate the principles of various embodiments. It will thus be appreciated that those skilled in the art will be able to devise various arrangements that, although not explicitly described or shown herein, embody the principles herein and in the claims and fall within the spirit and scope of the disclosure. Furthermore, all examples recited herein are principally intended expressly to be only for pedagogical purposes to aid the reader in understanding the principles of the embodiments and the concepts contributed by the inventor to furthering the art, and are to be construed as being without limitation to such specifically recited examples and conditions. Moreover, all statements herein reciting principles, aspects, and embodiments, as well as specific examples thereof, are intended to encompass equivalents thereof.

[0011] Some of the abbreviations that are described herein are expanded below for convenience:

	5GC	5G Core
15	5GS	5G System
	5G-AN	5G Access Network
	5G-GUTI	5G Globally Unique Temporary Identifier
	5G-S-TMSI	5G S-Temporary Mobile Subscription Identifier
	5QI	5G QoS Identifier
20	AKA	Authentication and Key Agreement
	AMF	Core Access and Mobility Management Function
	AUSF	Authentication Server Function
	EAP	Extensible Authentication Protocol
	HPLMN	Home Public Land Mobile Network
25	IKEv2	Internet Key Exchange v2
	IMSI	International Mobile Subscriber Identity
	IMEI	International Mobile Equipment Identity
	IPsec	Internet protocol security
	MCC	Mobile Country Code
30	MCM	Multi-Connection Mode
	MNC	Mobile Network Code
	N3IWF	Non-3GPP Interworking Function

	NAI	Network Access Identifier
	NAS	Non-Access Stratum
	ngKSI	Key Set Identifier in 5G System
	NHN-ID	Neutral Host Network ID
5	PDN	Packet Data Network
	PLMN	Public Land Mobile Network
	QoS	Quality of Service
	SA	Security Association
	SCM	Single-Connection Mode
10	SMC	Security Mode Command
	SUCI	Subscription Concealed Identifier
	SUPI	Subscription Permanent Identifier
	UDM	Unified Data Management
	UE	User Equipment
15	UICC	Universal Integrated Circuit Card
	USIM	UMTS Subscriber Identity Mobile

[0012] One or more embodiments are described herein that provide a system and method for providing network services to unauthenticated user equipment. For example, various methods are described for session establishment for an unauthenticated UE in a trusted non-
 20 3GPP access network.

[0013] FIG. 1 illustrates a schematic block diagram of an embodiment of types of access networks for an evolved packet core that is fully or partially compliant with the 3rd Generation Partnership Project (3GPP) set of standards or other type of internet protocol (IP) data packet core network standards. This architecture is described in more detail in the
 25 technical standard 3GPP TS 23.402 V14.2.0 (December 2016) entitled, "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Architecture enhancements for non-3GPP accesses," which is hereby incorporated by reference herein.

[0014] In 3GPP architecture, the EPC network 100 is communicatively coupled to one
 30 or more access networks 102. In an embodiment, the access networks 102 may include one or more 3GPP access networks 104 or one or more non-3GPP access networks 106. The 3GPP access networks 104 are wholly or partially compliant with technologies specified by

the 3GPP set of standards and include, e.g. GPRS, UMTS, EDGE, HSPA, LTE and LTE Advanced. The non-3GPP access networks 106 are wholly or partially compliant with technologies that are not specified by the 3GPP set of standards. The non-3GPP access networks 106 may be so specified in the 3GPP set of standards. The non-3GPP access
5 networks 106 may include one or more non-3GPP trusted access networks 108 or one or more non-3GPP, non-trusted access networks 110.

[0015] The trusted non-3GPP access networks 108 are operator-built or operator supported wireless local area networks (WLAN), such as an IEEE 802.11x compliant WLAN network, with encryption and a secure authentication method. In one embodiment,
10 the trusted, non-3GPP access network 108 supports the following example features: 802.1x-based authentication which in turn also requires encryption of the radio access network (RAN), 3GPP-based network access using EAP method for authentication, and IPv4 and/or IPv6 protocols. However, an operator may determine that other types of non-3GPP access networks with different types of security are to be considered trusted. The untrusted non-
15 3GPP access networks 110 include non-3GPP access networks that are unknown to an operator or do to not include supported authentication standards. For example, an untrusted non-3GPP access network may include a home or public WLAN, such as an IEEE 802.11x compliant WLAN network that is open to the public, home WLAN or another non-operator originated and managed.

20 [0016] Another set of protocols for Fifth-Generation wireless, or 5G, is the latest iteration of cellular technology, engineered to greatly increase the speed and responsiveness of wireless networks. The term 5G was initially defined by the ITU IMT-2020 standard, which required a theoretical peak download capacity of 20 gigabits. More recently, the industry standards group 3GPP is defining the 5G architecture and protocols. For example,
25 Technical Specification (TS) 23.501 defines Stage-2 System Architecture for the 5G System which includes Network Slicing. Technical Specification (TS) 23.502 defines procedures for the 5G System. Technical Specification (TS) 23.503 defines Policy and Charging Control Framework for the 5G System.

[0017] In 5G systems, 5G access network may include, e.g. a Next Generation (NG)
30 Radio Access Network (NG-RAN) as described in 3GPP TS 38.300. In addition, a 5G access network may include an untrusted non-3GPP Access Network in which the UE may connect to the 5G core network, e.g., via a secured IPSec/IKE tunnel terminated on a Non-

3GPP Interworking Function (N3IWF). The non-3GPP Access Network (N3AN) is considered as a 5G Access Network and part of the 5G System (5GS).

[0018] For untrusted non-3GPP access, the access node including N3IWF provides termination of N2 and N3 signaling interfaces for control-plane and user-plane respectively.

5 The 5G capable UEs access the 5G core network by connecting to the Non-3GPP Access Network (as a 5G Access Network) via the N3IWF. The N3IWF relays uplink and downlink control-plane NAS (N1) signaling between the UE and the 5G core network, makes it possible for the UE to have direct NAS signaling connection towards the core network. In addition, the N3IWF provides user plane connection between the UE and the core network
10 for PDU sessions over the non-3GPP access network.

[0019] FIG. 2 illustrates a schematic block diagram of an embodiment of a 5G System Architecture for non-3GPP access. This architecture is described in more detail in the technical standard 3GPP TS 23.501, Release 15 (December 2017) entitled, "System Architecture for the 5G System," which is incorporated by reference herein.

15 [0020] Non-3GPP access networks are connected to the 5G Core Network via a Non-3GPP Interworking Function (N3IWF). The N3IWF interfaces the 5G Core Network control plane (CP) and user plane (UP) functions via N2 and N3 interfaces, respectively. A UE establishes an IPsec tunnel with the N3IWF to attach to the 5G Core Network over the untrusted non-3GPP access network. The UE is authenticated by and attached to the 5G Core
20 Network during the IPsec tunnel establishment procedure. Further details for UE attachment to 5G Core Network over untrusted non-3GPP access are described in 3GPP TS 23.502, Release 15 (December 2017) entitled, "Procedures for the 5G System," which is hereby incorporated by reference herein.

[0021] The 5G System includes a Home Public Land Mobile Network or Equivalent
25 Home PLMN (HPLMN-5G) including an Access and Mobility Management function (AMF). The AMF provides for the termination of the RAN control plane interface (N2) and termination of NAS (N1) set of protocols and NAS ciphering and integrity protection. The AMF also provides registration and connection management. The AMF may include various functionality to support non-3GPP access networks. For example, the AMF may provide
30 support of N2 interface control protocols with the N3IWF as well as support of NAS signalling with a UE over the N3IWF. In addition, the AMF may provide support of authentication of UEs connected over the N3IWF and management of mobility,

authentication, and separate security context state(s) of a UE connected via the non-3GPP access or connected via 3GPP and non-3GPP accesses simultaneously.

[0022] The Session Management function (SMF) includes session management functionality, e.g. session establishment, modify and release, including tunnel maintenance
5 between the UPF and AN node. The SMF also provides for UE IP address allocation & management (including optional Authorization) and DHCPv4 (server and client) and DHCPv6 (server and client) functions.

[0023] The User plane function (UPF) provides an external PDU Session point of interconnect to Data Network and Packet routing & forwarding. The UPF also supports the
10 User Plane part of policy rule enforcement, e.g. Gating, Redirection, Traffic steering, etc.

[0024] The Policy Control Function (PCF) supports a unified policy framework to govern network behaviour. The Unified Data Management (UDM) includes support for generation of 3GPP AKA Authentication Credentials, Access authorization based on subscription data (e.g. roaming restrictions), and UE's Serving NF Registration Management
15 (e.g. storing serving AMF for UE, storing serving SMF for UE's PDU Session). It also provides SMS and subscription management. To provide this functionality, the UDM uses subscription data (including authentication data) that may be stored in the UDR. The AUSF provides Authentication Server Function (AUSF).

[0025] The functionality of N3IWF in case of untrusted non-3GPP access includes the
20 support of IPsec tunnel establishment with the UE. The N3IWF terminates the IKEv2/IPsec protocols with the UE over NWu and relays over N2 the information needed to authenticate the UE and authorize its access to the 5G Core Network. The N3IWF provides termination of N2 and N3 interfaces to 5G Core Network for control - plane and user-plane respectively. The N3IWF relays uplink and downlink control-plane NAS (N1) signaling between the UE
25 and AMF. The N3IWF provides handling of N2 signaling from SMF (relayed by AMF) related to PDU Sessions and QoS. The N3IWF further provides for the establishment of IPsec Security Association (IPsec SA) to support PDU Session traffic. The N3IWF also provides for relaying uplink and downlink user-plane packets between the UE and UPF.

[0026] FIG. 3 illustrates a schematic block diagram of an embodiment of a UE accessing
30 the 5G system over multiple heterogenous access networks. The multiple heterogenous access networks include, e.g., 3GPP access, untrusted WLAN access and Non-3GPP access. When the UE is registered to the 5G core over both 3GPP access and non-3GPP access

networks, multiple control plane NAS signaling connections are active between the UE and the AMF at the same time.

[0027] When the UE establishes a secure connection, it sends a "Registration Request" message to the AMF/SEAF. The Registration request message includes the 5GS mobile identity IE which contains either the SUCI, 5G-GUTI or IMEI. After receiving the registration request message from the UE, the AMF/SEAF prepares an "Authentication Initiation Request" (5G-AIR) message to the AUSF. The SEAF also includes the serving network name into the 5G-AIR message. After receiving the 5G-AIR message from the SEAF, the AUSF prepares "Auth-Info-Req" message and sends to the UDM/ARPF. The UDM/ARPF first generates an authentication vector with Authentication Management Field (AMF) separation bit = 1. The UDM/ARPF then compute CK' and IK'. After that ARPF sends (RAND, AUTN, XRES, CK', IK') to the AUSF using the Auth-Info-Rsp message. The AUSF responds to the SEAF by sending 5G-AIA message which in turn includes EAP-Request/AKA'-Challenge message. The SEAF transparently forwards the EAP-Request/AKA'-Challenge message to the UE in a NAS message Auth-Req message. After receiving a response from the UE for the Auth-Req message, the SEAF forwards the EAP Response to the AUSF, and the AUSF validates the same with the stored information. In case of successful verification, AUSF sends EAP-SUCCESS and Anchor key to SEAF and then SEAF responds to UE with EAP-SUCCESS. If the AUSF received SUCI from SEAF when the authentication was initiated, then the AUSF also includes the SUPI while sending EAP-SUCCESS message.

[0028] If the UE is accessing one PLMN over one type of access (e.g. 3GPP access) and accessing another PLMN over another type of access (e.g. non-3GPP access), then different primary authentications are performed. After registration, the NAS connections are served by different AMFs utilizing different security contexts. However, as shown in FIG. 3, the UE may request registration in the same serving network (e.g., same HPLMN-5G) over different types of access. All the NAS connections for the UE are then served by the same AMF.

[0029] Currently, when the UE is registered in a serving network over different types of access, the assignment of NAS connection identifiers is hard-coded. For example, the 3GPP TSG #80 Plenary Meeting approved the completion of the standalone (SA) Release 15, 5G specifications, dated July 15, 2018 (REL-15) and incorporated by reference herein. In REL-

15, it is assumed that the NAS connection identifier is "0" for 3GPP access. For non-3GPP access, it is assumed that the NAS connection identifier is "1". This assignment of hard-coded connection identifiers did not present a problem in Rel-15 as only one type of non-3GPP access was supported, e.g. untrusted WLAN access. However, it is foreseen that
5 additional non-3GPP access network types will be added in future releases, e.g. trusted WLAN access, wireline access, MuLteFire access, etc. Different types of non-3GPP access networks each need to establish separate NAS connections. Depending on the network configuration and UE service subscription, the UE may be simultaneously connected to multiple access networks, for example, to 3GPP access and multiple non-3GPP access
10 networks as show in Figure 2. In this situation, using the same NAS connection identifier for connections over different non-3GPP access networks would not work.

[0030] In addition, different access types may be activated in different sequences. For example, it is possible that the UE receives authentication over one of the non-3GPP access networks first and establishes a NAS security context before the UE registers via a 3GPP
15 access network. In another possibility, the UE registers via multiple non-3GPP access networks but not over a 3GPP access network. As such, a more flexible binding between the serving network and access type pair and NAS connection is desired.

[0031] In order for the UE to verify it is connected to a serving network that is authorized to provide services to the UE, the serving network needs to be verified by the home network
20 during authentication (AKA) procedures. The verification is implicit as it is assumed that if primary authentication and key agreement procedure has completed successfully, the serving network is authorized. However, the failure case should not be implicit and needs to be defined explicitly.

[0032] Finally, in a 5G system, a subscriber identifier is called a Subscription permanent
25 identifier (SUPI). The SUPI can be defined in either an IMSI or NAI format. To ensure Subscriber privacy, the SUPI should not be transferred in clear text over a 5G RAN and is concealed over-the-air by using the Subscription Concealed Identifier (SUCI). The SUCI is generated using a protection scheme with the raw public key that was securely provisioned in control of the home network. Only the subscription identifier part of the SUPI is
30 concealed, while the home network identifier part of the SUPI needs to remain clear for routing purpose.

[0033] The routing information may be different for different access network types. For a 3GPP access network, Mobile Country Code (MCC) and Mobile Network Code (MNC) may be part of the routing information. However, for a non-3GPP access network, a different network identifier and routing information may be used. For example, for MuLteFire type access network, the network identifier and routing information are based on a Neutral Host Network ID (NHN-ID), Participating Service Provider ID (PSP-ID) and Neutral Host Access Mode Indicator (NHAMI). NHAMI is a reserved global value that is the same for all MuLteFire networks enabling NHN Access Mode. There is a need to define the coding of the SUCI information element in a generic way for the SUCI to support other types of networks and subscriber identifier formats to be used as a mobile identity during the authentication procedure.

[0034] Also given that both IMSI and NAI formats can be used for SUPI, for SUCI schema output, MSIN corresponds to the representation in case the subscription identifier is in IMSI format and username corresponds to the representation in case the subscription identifier is in NAI format. For IMSI based NAI, the subscriber identifier part of NAI is also made of digits, so additional encoding rules are needed to distinguish the IMSI format, NAI format and potentially other types of subscriber identifier formats within the SUCI information element definition.

[0035] One or more embodiments described herein provide systems and methods for enabling concurrent secure connections over multiple heterogeneous access networks. New methods and protocol enhancements are described to allow the UE to include an access type during registration and to track concurrent NAS connections mapping over heterogeneous access networks. New systems and methods for handling serving network verification failure are also described. New systems and methods and protocol enhancements are further described to support using NAI as one type of subscription identifier as well as future extensibility of subscription identifier for support of MuLteFire access networks and private networks.

1. Embodiment - UE includes access type during registration and Ability for tracking concurrent NAS connections mapping over heterogeneous access networks

a) UE initiates initial registration over Access Type A.

[0036] FIG. 4 illustrates a logical flow diagram of an embodiment of a method for authentication and key agreement message flow between UE and core network functions when the UE initiates initial registration over Access Network Type A. The NAS messages shown between the UE and AMF may be tunneled via an IPsec tunnel in case the Access Network Type A is an untrusted non-3GPP access. For example, the UE may establish an IPsec Security Association (SA) with the selected N3IWF by initiating an Internet Key exchange (IKE) protocol initial exchange, e.g. as described in IETF RFC 7296, "Internet Key Exchange Protocol Version 2 (IKEv2)," (October 2014). In this example, Access Network Type A is a first type of a plurality of types of networks, including 3GPP access, trusted non-3GPP access, untrusted non-3GPP access, untrusted WLAN access, trusted WLAN access, MuLteFire access, etc.

[0037] When the UE initiates the initial registration over Access Network Type A, the UE includes the Access Type in the registration request message. The registration request message is sent by the UE to the AMF. The AMF is collocated with SEcurity Anchor Function (SEAF) which serves as the anchor for security in 5G Systems. Upon receiving the registration request message, the AMF/SEAF invokes the Nausf_UEAuthentication service by sending a Nausf_UEAuthentication_Authenticate Request message to the AUSF to initiate an authentication. The SEAF includes the Subscribe Id, the Serving network name and Access type in the Nausf_UEAuthentication_Authenticate Request.

[0038] After receiving the Nausf_UEAuthentication_Authenticate Request message, the AUSF compares the received Serving network name with the expected serving network name. If the requesting SEAF in the serving network is authorized to use the serving network name, the AUSF sends the Nudm_UEAuthentication_Get Request to the UDM including the Subscribe Id, the Serving network name and Access type.

[0039] After reception of the Nudm_UEAuthentication_Get Request, the UDM/ARPF chooses the authentication method, based on the subscription data. For example, an EAP-AKA' mutual authentication type protocol as modified herein may be executed between the UE and AUSF (such as EAP-AKA' described in IETF RFC 5448, "Improved Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA') March 5, 2018 and incorporated by reference herein).

[0040] The UDM/ARPF generates an authentication vector and sends this authentication vector AV' (RAND, AUTN, XRES, CK', IK') to the AUSF from which it received the

Nudm_UEAuthentication_Get Request. The UDM/ARPF also transmits an indication that the authentication vector AV' is to be used for EAP-AKA' using a Nudm_UEAuthentication_Get Response message.

[0041] The AUSF and the UE then proceed with EAP-Request/AKA'-Challenge exchange. The AUSF derives the KAUSF and the KSEAF keys, and it includes an EAP Success message and the KSEAF inside Nausf_UEAuthentication_Authenticate Response message and sends it to the AMF/SEAF.

[0042] After receiving the Nausf_UEAuthentication_Authenticate Response message, the AMF/SEAF derives the KAMF key. The AMF then initiates Security mode command procedure to send the security context and security algorithm information to the UE. The UE receives the Security mode command and derives NAS security contexts and sends a Security mode command complete message to the AMF.

[0043] At the completion of the procedure, the Serving Network and Access Type to NAS connections mapping table is updated to include connection information for Access Network Type A, as shown in FIG. 5 below.

[0044] FIG. 5 illustrates a schematic block diagram of an embodiment of a Serving Network and Access Type to NAS connections mapping table. In this example, the mapping table is updated to include connection information for a first type of access network, e.g. Access Network Type A. The mapping table is updated after registration by a UE over an access network. The table includes the access network type, network identifier and access network identifier. The mapping table also includes the NAS connection identifier for the NAS connection between the Access Network Type A and the UE. The mapping table thus stores for each NAS connection, the NAS connection identifier, the access network type, network identifier, and access network identifier.

[0045] FIG. 6 illustrates a schematic block diagram of an embodiment of content of a registration request message. The registration request message is transmitted by the UE to the AMF over an access network to begin an initial registration. The registration request message includes an information element "Access Type" of the access network. The purpose of the access type information element is to indicate the access type over which the downlink signaling, or user data is to be sent to the UE.

[0046] FIG. 7 illustrates a schematic block diagram of an embodiment of the access type information element in a registration request message. The access type is a type 1 information element.

[0047] FIG. 8 illustrates a schematic block diagram of an embodiment of the access type values for the access type information element in a registration request message. In an embodiment, the access types include 3GPP access, untrusted non-3GPP access, trusted non-3GPP access, untrusted WLAN access, trusted WLAN access and MuLteFire access. Alternate or additional access types may be included in the access type information element in the registration message.

10

b1) UE initiates subsequent registration over access type C and existing NAS security context is reused

[0048] When the UE initiates subsequent registration over another type of access network, e.g. access type C, and the UE is already authenticated by the network and is served by the same AMF in the same serving network, the AMF may decide not to run a new authentication if it has an available security context to use.

[0049] FIG. 9 illustrates a logical flow diagram of an embodiment of a method for registration by a UE over an Access Network Type C when existing NAS security context is reused. It is assumed in this example, that the UE has established an NAS connection with Access Network Type A and Access Network Type B. Note that NAS messages shown between the UE and AMF are tunnelled via IPsec tunnel in case the Access Network Type C is an untrusted non-3GPP access.

[0050] When the UE initiates subsequent registration over another access network with Access Network Type C, it includes the Access Type in the registration request message. The AMF may decide to reuse the existing security context. A new NAS connection is created using the available common 5G NAS security context. The NAS security context is updated with parameters specific to the new NAS connection. At the completion of the procedure, the Serving Network and Access Type to NAS connections mapping table is updated to include connection information for Access Network C, as shown in FIG. 10.

[0051] FIG. 10 illustrates a schematic block diagram of an embodiment of a Serving Network and Access Type to NAS connections mapping table after registration with an access type A, access type B, and access type C. In this example, the mapping table is

updated to include connection information for the access type C. The mapping table is updated after registration by the UE over an access network. The table includes the access network type, network identifier and access network identifier. The mapping table also includes the NAS connection identifier for the NAS connection between the Access Network
5 Type C and the UE. The NAS connection identifier is "2". The mapping table may be stored in the UE and AMF and/or at other functions or nodes, such as the AUSF.

b2) UE initiates subsequent registration over Access Network Type C and new authentication is initiated

10 [0052] When the UE initiates subsequent registration over access type C, if the UE is already authenticated by the network for the same serving network, the AMF can decide to run the authentication and key agreement procedure again either because the UE is served by a different AMF or due to security algorithm has changed.

[0053] Figure 11 is a logical flow diagram of an embodiment of a method for registration
15 by the UE over an access network type C when new authentication is initiated. It is assumed in this example, that the UE has established an NAS connection with Access Network Type A and Access Network Type B. Note that NAS messages shown between the UE and AMF are tunneled via IPsec tunnel if the Access Network Type C is untrusted non-3GPP access.

[0054] When the UE initiates subsequent registration over Access Network Type C, it
20 includes the Access type in the registration request message. The AMF decides to run the authentication and key agreement procedure again. The AMF may decide to run the authentication and key agreement procedure again either because the UE is served by a different AMF or due to security algorithm has changed. When the authentication and key agreement procedure completes, new NAS security mode command is initiated by the AMF
25 to the UE to activate the new derived 5G NAS security context on Access Type C.

[0055] A new NAS connection is created using the newly derived 5G NAS security context. The NAS security context is updated with parameters specific to the new NAS connection. The AMF then triggers additional NAS SMC procedures for all other Access Types in order to activate the new 5G NAS security context for each existing Access Type.
30 After successful NAS SMC procedures over the other accesses types, both the UE and the AMF delete the old NAS security context. At the completion of the procedure, the Serving

Network and Access Type to NAS connections mapping table is updated to include connection information for Access Network Type C, as shown in FIG. 12.

[0056] FIG. 12 illustrates a schematic block diagram of an embodiment of a Serving Network and Access Type to NAS connections mapping table after registration with an access type A, access type B, and access type C. In this example, the mapping table is updated to include connection information for the access type C. The mapping table is updated after registration by the UE over an access network. The table includes the access network type, network identifier and access network identifier. The mapping table also includes the NAS connection identifier for the NAS connection between the Access Network Type C and the UE. The NAS connection identifier is "2". The mapping table may be stored in the UE and AMF and/or at other functions or nodes, such as the AUSF.

2. Embodiment - Serving Network Authorization Failure

[0057] In order for the UE to verify it is connected to a serving network that is authorized to provide services to the UE, the serving network needs to be verified by the home network during AKA procedures. If the serving network is authorized, the AKA procedure would continue and if primary authentication and key agreement procedure has completed successfully, it would mean the serving network is authorized.

[0058] However, if the serving network is unauthorized, the authentication procedure would stop and the AUSF would send an authentication response to the AMF to indicate authentication failure due to the serving network not being authorized.

[0059] Figure 13 illustrates a logical flow diagram of an embodiment of a method for registration by a UE over an access network type A when a serving network authorization failure has occurred. Note that NAS messages between the UE and AMF are tunneled via IPsec tunnel in case the Access Network Type A is an untrusted non-3GPP access.

[0060] Upon receiving the Nausf_UEAuthentication_Authenticate Request message, the AUSF compares the received serving network name with the expected serving network name. If the requesting SEAF in the serving network is not authorized to use the serving network name, the AUSF responds with "serving network not authorized" in the Nausf_UEAuthentication_Authenticate Response.

[0061] The serving network authorization failure is different from other PLMN related failures. It is not failure due to UE subscription or access restriction, e.g. due to operator

barring, rather it is due to the serving network failure of security verification/authorization. Currently there is no cause code for such a failure case.

[0062] One failure code related to PLMN failure is "PLMN not allowed", but it is for indicating to the UE a rejection due to subscription or due to operator determined barring.

5 This failure code is: Cause #11 – PLMN not allowed. This 5GMM cause is sent to the UE if it requests service, or if the network initiates a de-registration request, in a PLMN where the UE, by subscription or due to operator determined barring, is not allowed to operate.

[0063] When the UE receives a rejection due to "PLMN not allowed", the UE needs to set the 5GS update status to 5U3 ROAMING NOT ALLOWED, reset the registration
10 attempt counter, delete its security context, any 5G-GUTI, last visited registered TAI, TAI list, ngKSI, the list of equivalent PLMNs and also store the PLMN identity in the "forbidden PLMN list".

[0064] However, when the serving network authorization failure occurs, given that the failure is not failure related to UE subscription or access restriction, the UE does not need to
15 reset its update status to 5U3 ROAMING NOT ALLOWED and could immediately attempt to select another PLMN. So, it is more appropriate to define a new cause code for this different situation since the UE may take different actions.

[0065] For example, when the serving network authorization failure occurs, the UE may abort the initial registration procedure with the PLMN, store the PLMN identity in the
20 "forbidden PLMN list", set the 5GS update status to 5U2 NOT UPDATED and enter state 5GMM-DEREGISTERED.PLMN-SEARCH in order to perform a PLMN selection. As such, a new 5GMM rejection cause is needed to indicate "Serving Network Not Authorized".

[0066] FIG. 14 illustrates a schematic block diagram of an embodiment of 5GMM cause information element. The 5GMM cause information element indicates a reason for a
25 rejection by the network of a 5GMM request from the UE. A new 5GMM rejection cause is included in this information element to indicate "Serving Network Not Authorized". For example, the new rejection may be included as new cause code #73 to signal a serving network authorization failure to the UE. The new cause code is used if the authentication process cannot proceed because the serving network is not authorized.

30 [0067] FIG. 15 illustrates a schematic block diagram of an embodiment of cause values for the 5GMM cause information element. The cause values are updated to include new Cause #73 – Serving Network Not Authorized. This 5GMM cause is sent to the UE if the

UE initiates registration towards a serving network and the serving network failed authorization.

[0068] After failure of authentication of the serving network, the UE receives a registration rejection with 5GMM cause "Serving Network Not Authorized" for 3GPP access. The UE then aborts the initial registration procedure, stores the PLMN identity in the "forbidden PLMN list", sets the 5GS update status to 5U2 NOT UPDATED and enters state 5GMM-DEREGISTERED.PLMN-SEARCH in order to perform a PLMN selection. The UE is thus able to select another PLMN.

10 **3. Embodiment - Methods and Protocol enhancements to support using NAI as one type of subscription identifier and future extensibility of subscription identifier for support of MuLteFire and private networks**

15 **a) A new field "SUPI Format" is defined to enable different subscriber identity type/formats to be used as the Subscriber Identifier**

[0069] A globally unique 5G Subscription Permanent Identifier (SUPI) is allocated to each subscriber in the 5G System and provisioned in the UDM/UDR. The SUPI is used only inside the 3GPP system, and its privacy is specified in 3GPP TS 33.501, "Security architecture and procedures for 5G System," Release 15 dated March 26, 2018 and incorporated by reference herein. The following have been identified as valid SUPI types: IMSI and NAI.

[0070] The SUCI is a partially encrypted SUPI used during procedures associated with the 5G System when the device has not been assigned a 5G-GUTI (5G Globally Unique Temporary Identity). The SUCI is generally created by encrypting the MSIN (Mobile Subscriber Identification Number) component of the subscriber's IMSI.

[0071] The UE generates a SUCI using the raw public key that was securely provisioned in control of the home network. The protection scheme uses the raw public key of the home network. The UE constructs a scheme-input from the subscription identifier part of the SUPI, as specified by the protection scheme (e.g., applying some padding-scheme). The UE then executes the protection scheme with the constructed scheme-input as input and take the output as the scheme-output. The UE does not conceal the home network identifier, e.g., Mobile Country Code (MCC) or Mobile Network Code (MNC). The UE then generates the

SUCI including the home network identifier, the identifier of the home network public key, and the scheme-output.

[0072] However, given that both IMSI and NAI formats can be used for SUPI, for SUCI schema output, MSIN corresponds to the representation in case the subscription identifier is in IMSI format and username corresponds to the representation in case the subscription identifier is in NAI format. For IMSI based NAI, the subscriber identifier part of NAI is also made of digits, so additional encoding rules are needed to distinguish the IMSI format, NAI format and potentially other types of subscriber identifier formats within the SUCI information element definition.

10 [0073] FIG. 16 illustrates a schematic block diagram of an embodiment of a new information field for a Subscription Concealed Identifier (SUCI) to enable different SUCI structures. Using a new information field, the mobile identify format for the SUPI and SUCI may be tailored based on the SUPI identity type/format used. For example, for IMSI, the network identifier is based on MNC/MCC. For IMSI based NAI, the network identifier is also based on MNC/MCC. For non-IMSI based NAI, the network identifier is based on a generic network type indicator and operator or enterprise specific network identifier, where the network type indicator can be based on a special reserved/hard-coded global MCC/MNC value. For MuLteFire NAI (MF-NAI), the network identifier is based on special reserved/hard-coded global MCC/MNC, Neutral Host Network ID (NHN-ID), and
15 Participating service provider ID (PSP-ID).

[0074] FIG. 17 illustrates a schematic block diagram of an embodiment of identity types supported by the new information field for the Subscription Concealed Identifier (SUCI). The new SUCI information field enables different identity types for the Subscriber Identifier. The identity types may include SUCI, 5G-GUTI, IMEI, 5G-S-TMSI, IMEISV, MAC address, or a device identify. The device identity may include for example, UDI, ODIN, Bluetooth id, serial number, etc. Alternate or additional identity types may also be defined.

25 [0075] FIG. 18 illustrates a schematic block diagram of an embodiment of a generic SUCI subscriber identity format. The SUCI subscriber identity structure includes a network type indicator (NTI). A home network identifier and the routing identifier may be different for different access network types. The scheme output field contains the concealed subscriber identifier generated using a protection scheme.

[0076] FIG. 19 illustrates a schematic block diagram of an embodiment of a SUCI subscriber identity format when the SUPI format is IMSI or IMSI based NAI. This illustrates the 5GS mobile identity information element format when type of identity is "SUCI" and SUPI format is "IMSI" or "IMSI based NAI". For 3GPP access network, the home network identifier contains the PLMN ID (MCC and MNC). The Mobile Country Code (MCC) and Mobile Network Code (MNC) may be part of the routing information.

[0077] FIG. 20 illustrates a schematic block diagram of an embodiment of a SUCI subscriber identity format when the SUPI format is Non-IMSI based NAI and the type of identity is "SUCI". This illustrates an example of the 5GS mobile identity information element format when the type of identity is "SUCI" and the SUPI format is "non-IMSI based NAI". The network identifier and routing information are network specific. The values in the Network Type Indicator (NTI) field are used to indicate the type of network.

[0078] FIG. 21 illustrates a schematic block diagram of an embodiment of a SUCI subscriber identity format when the SUPI format is Non-IMSI based NAI" and the NTI is assigned a reserved global PLMN ID. When the SUPI format is "Non-IMSI based NAI", the Network Type Indicator may be a reserved global value in PLMN ID (MCC/MNC).

[0079] FIG. 22 illustrates a schematic block diagram of an embodiment of a SUCI subscriber identity format when the type of identity is "SUCI" and the SUPI format is "MF-NAI". For MuLteFire networks, the network identifier and routing information are based on a Neutral Host Network ID (NHN-ID), Participating Service Provider ID (PSP-ID) and Neutral Host Access Mode Indicator (NHAMI). NHAMI is a reserved global value that is the same for all MuLteFire networks enabling NHN Access Mode.

[0080] FIG. 23 illustrates a schematic block diagram of an embodiment of the SUCI identity type. The table illustrates various examples of additional encoding for the SUCI identity type.

[0081] FIG. 24 illustrates a schematic block diagram of an embodiment of example user equipment 220. The user equipment (UE) 220 may include a smart phone, smart tablet, laptop, smart watch, PC, TV or other device. Additional or alternative components and functions may be included within the UE 220. In addition, one or more of the functions and components shown herein may not be present or combined with other components or functions.

[0082] The UE 220 includes a processing device 2600 and memory device 2602 that are configured to perform one or more of the functions described herein with respect to the UE 220. The memory device 2602 may include a managed object 2604 that stores applications and operational instructions that controls the processing device 2600 to perform various functions described herein. The memory device 2602 may also store the Serving Network and Access Type to NAS connections mapping table 2650. The UE 220 may also include a UICC 2606 that includes a USIM 2608 for storage of the IMSI.

[0083] The UE 220 may further include a Bluetooth transceiver 2610, a WLAN (IEEE 802.11x compliant) transceiver 2612, mobile RF (3G/4G/5G) transceiver 2614 and GPS 2616. The WLAN transceiver 2612 may operate as a non-3GPP access interface to a WLAN network. The UE 220 may further include user interfaces 2618, AC adapter 2620, battery module 2622, USB transceiver 2624 and Ethernet Port 2628.

[0084] The UE 220 may further include a digital camera 2630, touch screen controller 2632, speaker 2634 and microphone 2636. The UE 220 may also include a power management unit 2638. One or more internal communication buses (not shown) may communicatively couple one or more of the components of the UE 220.

[0085] FIG. 25 illustrates a schematic block diagram of an embodiment of an example AMF Node. The AMF node may be integrated with other nodes in the 5G core network. Additional or alternative components and functions may be included within the AMF node. In addition, one or more of the functions and components shown herein may not be present or combined with other components or functions or nodes. The AMF node includes a processing device 2700 and memory device 2702 that are configured to perform one or more of the functions described herein. The AMF node may include a network interface 2704 that includes ports for interfacing to other network nodes in the 5GC network.

[0086] FIG. 26 illustrates a schematic block diagram of an embodiment of an example N3IWF. The N3IWF may be an access point in a wireless local area network, a gateway in a local area network, etc. The N3IWF may be integrated with other nodes in an access network. Additional or alternative components and functions may be included within the N3IWF. In addition, one or more of the functions and components shown herein may not be present or combined with other components or functions. The N3IWF includes a processing device 2800 and memory device 2802 that are configured to perform one or more of the functions described herein. The N3IWF may include a first network interface 2804

(e.g. Ethernet ports, IP ports) for interfacing to other network nodes in the 5GC network. The N3IWF may also include one or more other types of interfaces to communicate with the UE, such as a WLAN transceiver 2806 (e.g., compliant with IEEE 802.1x WLAN type networks). The N3IWF may also include a mobile RF transceiver 2808 compliant with a cellular air interface. The UE 220 may communicate with the N3IWF using one or more of the WLAN transceiver 2806 or Mobile RF transceiver 2808.

[0087] A processing device as described herein includes at least one processing device, such as a microprocessor, micro-controller, digital signal processor, microcomputer, central processing unit, field programmable gate array, programmable logic device, state machine, logic circuitry, analog circuitry, digital circuitry, and/or any device that manipulates signals (analog and/or digital) based on hard coding of the circuitry and/or operational instructions. A memory device is a non-transitory memory device and may be an internal memory or an external memory, and the memory may be a single memory device or a plurality of memory devices. The memory device may be a read-only memory, random access memory, volatile memory, non-volatile memory, static memory, dynamic memory, flash memory, cache memory, and/or any non-transitory memory device that stores digital information. The term “module” is used in the description of one or more of the embodiments of elements herein. A module includes one or more processing devices and/or one or more non-transitory memory devices operable to perform one or more functions as may be described herein. A module may operate independently and/or in conjunction with other modules and may utilize the processing device and/or memory of other modules and/or operational instructions of other modules. As also used herein, a module may contain one or more sub-modules, each of which may be one or more modules.

[0088] As may be used herein, the term “operable to” or “configurable to” indicates that an element includes one or more of circuits, instructions, modules, data, input(s), output(s), etc., to perform one or more of the described or necessary corresponding functions and may further include inferred coupling to one or more other items to perform the described or necessary corresponding functions. As may also be used herein, the term(s) “coupled”, “coupled to”, “connected to” and/or “connecting” or “interconnecting” includes direct connection or link between nodes/devices and/or indirect connection between nodes/devices via an intervening item (e.g., an item includes, but is not limited to, a component, an element, a circuit, a module, a node, device, network element, etc.). As may further be used herein,

inferred connections (i.e., where one element is connected to another element by inference) includes direct and indirect connection between two items in the same manner as “connected to”.

[0089] Note that the aspects of the present disclosure may be described herein as a process that is depicted as a schematic, a flowchart, a flow diagram, a structure diagram, or a block diagram. Although a flowchart may describe the operations as a sequential process, many of the operations can be performed in parallel or concurrently. In addition, the order of the operations may be re-arranged. A process is terminated when its operations are completed. A process may correspond to a method, a function, a procedure, a subroutine, a subprogram, etc. When a process corresponds to a function, its termination corresponds to a return of the function to the calling function or the main function.

[0090] The various features of the disclosure described herein can be implemented in different systems and devices without departing from the disclosure. It should be noted that the foregoing aspects of the disclosure are merely examples and are not to be construed as limiting the disclosure. The description of the aspects of the present disclosure is intended to be illustrative, and not to limit the scope of the claims. As such, the present teachings can be readily applied to other types of apparatuses and many alternatives, modifications, and variations will be apparent to those skilled in the art.

[0091] In the foregoing specification, certain representative aspects of the invention have been described with reference to specific examples. Various modifications and changes may be made, however, without departing from the scope of the present invention as set forth in the claims. The specification and figures are illustrative, rather than restrictive, and modifications are intended to be included within the scope of the present invention. Accordingly, the scope of the invention should be determined by the claims and their legal equivalents rather than by merely the examples described. For example, the components and/or elements recited in any apparatus claims may be assembled or otherwise operationally configured in a variety of permutations and are accordingly not limited to the specific configuration recited in the claims.

[0092] Furthermore, certain benefits, other advantages and solutions to problems have been described above with regard to particular embodiments; however, any benefit, advantage, solution to a problem, or any element that may cause any particular benefit,

advantage, or solution to occur or to become more pronounced are not to be construed as critical, required, or essential features or components of any or all the claims.

[0093] As used herein, the terms “comprise,” “comprises,” “comprising,” “having,” “including,” “includes” or any variation thereof, are intended to reference a nonexclusive inclusion, such that a process, method, article, composition or apparatus that comprises a list of elements does not include only those elements recited, but may also include other elements not expressly listed or inherent to such process, method, article, composition, or apparatus. Other combinations and/or modifications of the above-described structures, arrangements, applications, proportions, elements, materials, or components used in the practice of the present invention, in addition to those not specifically recited, may be varied or otherwise particularly adapted to specific environments, manufacturing specifications, design parameters, or other operating requirements without departing from the general principles of the same.

[0094] Moreover, reference to an element in the singular is not intended to mean “one and only one” unless specifically so stated, but rather “one or more.” Unless specifically stated otherwise, the term “some” refers to one or more. All structural and functional equivalents to the elements of the various aspects described throughout this disclosure that are known or later come to be known to those of ordinary skill in the art are expressly incorporated herein by reference and are intended to be encompassed by the claims. Moreover, nothing disclosed herein is intended to be dedicated to the public regardless of whether such disclosure is explicitly recited in the claims. No claim element is intended to be construed under the provisions of 35 U.S.C. §112(f) as a “means-plus-function” type element, unless the element is expressly recited using the phrase “means for” or, in the case of a method claim, the element is recited using the phrase “step for.”

CLAIMS

1. User equipment (UE), comprising:
 - one or more transceivers configured to access a serving network over a plurality of access network types;
 - 5 a memory device configured to store a mapping table; and
 - a processing device configured to:
 - generate a request for registration to the serving network over a first access network, wherein the request includes a first access network type of the first access network;
 - 10 receive a response indicating NAS connection establishment is accepted by the serving network, wherein the response includes the first access network type and NAS connection identifier; and
 - update the mapping table to include the first access network type and NAS connection identifier.
- 15 2. The UE of claim 1, wherein the first access network type includes a value indicating at least one of: 3GPP access, untrusted non-3GPP access, trusted non-3GPP access, untrusted WLAN access, trusted WLAN access or MuLteFire access.
- 20 3. The UE of claim 2, wherein the processing device is further configured to:
 - update the mapping table to include the first access network type, NAS connection identifier, access network identifier and serving network identifier.
- 25 4. The UE of claim 3, wherein processing device is further configured to:
 - generate a second request for registration to the serving network over a second access network having a second access network type, wherein the second request includes the second access network type of the second access network;
 - receive a response indicating connection establishment is accepted by the serving network, wherein the response includes the second access network type and
 - 30 a second NAS connection identifier; and
 - update the mapping table to include the second access network type and the second NAS connection identifier.

5. The UE of claim 4, wherein the second access network type is different from the first access network type and wherein the second access network type indicates a second different one of: 3GPP access, untrusted non-3GPP access, trusted non-3GPP access,
5 untrusted WLAN access, trusted WLAN access or MuLteFire access.
6. The UE of claim 5, wherein processing device is further configured to:
generate a third request for registration to the serving network over a third
access network having a third access network type, wherein the third request
10 includes the third access network type of the third access network;
receive a response indicating connection establishment is accepted by the
serving network, wherein the response includes the third access network type and a
third NAS connection identifier; and
update the mapping table to include the third access network type and the
15 third NAS connection identifier.
7. The UE of claim 6, wherein the third access network type is different from the first and second access network types and wherein the third access network type indicates a third different one of: 3GPP access, untrusted non-3GPP access, trusted non-3GPP access,
20 untrusted WLAN access, trusted WLAN access or MuLteFire access.
8. The UE of claim 7, wherein the processing device is further configured to:
use existing NAS security context established over the first access network with the
serving network.

9. The UE of claim 7, wherein the processing device is further configured to:
receive a request to perform authentication for connection over the third access
network;
obtain a new NAS security context from the serving network over the third access
5 network;
establish the NAS connection using the new NAS security context over the third
access network;
activate the new NAS security context for the first and second access networks; and
delete the prior NAS security context.
- 10
10. User equipment (UE), comprising:
one or more transceivers configured to access a serving network over a plurality of
access network types;
a processing device configured to:
15 generate a request for registration to the serving network over an access
network; and
receive a registration reject message, wherein the registration reject message
indicates that the serving network is not authorized.
- 20
11. The UE of claim 10, wherein the registration reject message includes a cause
information element, wherein the cause information element includes a value
corresponding to "Serving Network Not Authorized."
- 25
12. The UE of claim 10, wherein the processing device is further configured to:
abort registration with the serving network;
store an identity of the serving network in a list of unauthorized serving
networks [the "forbidden PLMN list"].
- 30
13. The UE of claim 12, wherein the processing device is further configured to select
another serving network for registration.

14. An authentication server function in a node of a core network, comprising:
a transceiver configured to communicate with one or more other nodes in the core network;
a processing device configured to:
5 receive an authentication request for a UE requesting access to a serving network, wherein the authentication request includes an identifier of the serving network and a subscriber identity; and
determine the serving network is not authorized; and
generate an authentication response, wherein the authentication response
10 indicates that the serving network is not authorized.
15. The authentication server function in the node of the core network of claim 14, wherein the authentication response includes a cause information element, wherein the cause information element includes a value corresponding to “Serving Network Not
15 Authorized.”
16. A UE, comprising:
a transceiver configured to communicate with one or more types of access networks;
20 a processing device configured to generate a SUCI by:
determine one of a plurality of SUPI formats;
determine one of a plurality of types of identity for a subscriber identifier;
determine a scheme output from the subscriber identifier using a protection scheme; and
25 construct the SUCI including a SUPI format value, a type of identity value and the scheme-output.
17. The UE of claim 16, wherein the one of the plurality of types of identity for the subscriber identifier includes one of: SUCI, 5G-GUTI, IMEI, 5G-S-TMSI, IMEISV, MAC
30 address, or a device identify.

18. The UE of claim 16, wherein the one of the plurality of SUPI formats includes at least one of: IMSI, IMSI based NAI, NON-IMSI based NAI or MF-NAI.
19. The UE of claim 16, wherein the processing device is further configured to
- 5 generate the SUCI by selecting one of a plurality of network types and including a network type indicator for the selected network type in the SUCI structure.