SUBSCRIBER IDENTIFIER PROTECTION IN A HOSTED NETWORK

RELATED APPLICATION

[0001] This application claims priority to U.S. Patent Application Serial No. 63/635,602 filed April 17, 2024, entitled "SUBSCRIBER IDENTIFIER PROTECTION IN A HOSTED NETWORK," the disclosure of which is incorporated by reference herein in its entirety.

TECHNICAL FIELD

[0002] The present disclosure relates to wireless communications, and more specifically to subscriber identifier protection in a hosted network.

BACKGROUND

[0003] A wireless communications system may include one or multiple network communication devices, which may be otherwise known as network equipment (NE), supporting wireless communications for one or multiple user communication devices, which may be otherwise known as user equipment (UE), or other suitable terminology. The wireless communications system may support wireless communications with one or multiple user communication devices by utilizing resources of the wireless communication system (e.g., time resources (e.g., symbols, slots, subframes, frames, or the like) or frequency resources (e.g., subcarriers, carriers, or the like)). Additionally, the wireless communications system may support wireless communications across various radio access technologies including third generation (3G) radio access technology, fourth generation (4G) radio access technology, fifth generation (5G) radio access technology, among other suitable radio access technologies beyond 5G (e.g., sixth generation (6G)).

SUMMARY

[0004] An article "a" before an element is unrestricted and understood to refer to "at least one" of those elements or "one or more" of those elements. The terms "a," "at least one," "one or more," and "at least one of one or more" may be interchangeable. As used herein, including in the claims, "or" as used in a list of items (e.g., a list of items prefaced by a phrase such as "at least one of" or "one or more of" or "one or both of") indicates an inclusive list such that, for example, a list of at least one of A, B, or C means A or B or C or AB or AC or BC or ABC (i.e., A and B and C). By

way of another example, a list of at least one of A; B; or C means A or B or C or AB or AC or BC or ABC (i.e., A and B and C). Also, as used herein, the phrase "based on" shall not be construed as a reference to a closed set of conditions. For example, an example step that is described as "based on condition A" may be based on both a condition A and a condition B without departing from the scope of the present disclosure. In other words, as used herein, the phrase "based on" shall be construed in the same manner as the phrase "based at least in part on". Further, as used herein, including in the claims, a "set" may include one or more elements.

[0005] An NE (e.g., a base station) for wireless communication is described. The NE may be configured to, capable of, or operable to perform one or more operations as described herein. For example, the NE may be configured to, capable of, or operable to receive an authentication request message that includes a subscription permanent identifier (SUPI) for a UE in a non-public network (NPN) hosted by a public land mobile network (PLMN); limit, based at least in part on a SUPI usage policy, usage of the SUPI in the NPN hosted by the PLMN.

[0006] A processor (e.g., a standalone processor chipset, or a component of a NE (e.g., a base station)) for wireless communication is described. The processor may be configured to, capable of, or operable to perform one or more operations as described herein. For example, the processor may be configured to, capable of, or operable to receive an authentication request message that includes a SUPI for a UE in a NPN hosted by a PLMN; limit, based at least in part on a SUPI usage policy, usage of the SUPI in the NPN hosted by the PLMN.

[0007] A method performed or performable by an NE (e.g., a base station) for wireless communication is described. The method may include receiving an authentication request message that includes a SUPI for a UE in a NPN hosted by a PLMN; and limiting, based at least in part on a SUPI usage policy, usage of the SUPI in the NPN hosted by the PLMN.

[0008] In some implementations of the NE, the processor, and the method described herein, to limit usage of the SUPI in the NPN, the NE, processor, and method may further be configured to, capable of, performed, performable, or operable to: generate or assign a generic public subscription identifier (GPSI) for the UE for use in place of the SUPI. In some implementations of the NE, processor, and method described herein, the NE, processor, and method may further be configured to, capable of, performed, performable, or operable to receive the authentication request message

from an authentication server function (AUSF); and transmit, to the AUSF, the GPSI and an SUPI usage restriction indication.

[0009] In some implementations of the NE, the processor, and the method described herein, the GPSI is specific to the NPN. In some implementations of the NE, processor, and method described herein, the NE, processor, and method may further be configured to, capable of, performed, performable, or operable to determine, based at least in part on the SUPI usage policy, to not disclose the SUPI. In some implementations of the NE, the processor, and the method described herein, the NE implements a unified data management (UDM) function.

[0010] An NE (e.g., a base station) for wireless communication is described. The NE may be configured to, capable of, or operable to perform one or more operations as described herein. For example, the NE may be configured to, capable of, or operable to receive an authentication response message that includes a GPSI for a UE in a NPN hosted by a PLMN and a SUPI usage restriction indication; receive, from a security anchor function (SEAF) an authentication request; transmit, to the SEAF based at least in part on the SUPI usage restriction indication, an authentication response that includes the GPSI for the UE and the SUPI for the UE.

[0011] A processor (e.g., a standalone processor chipset, or a component of a NE (e.g., a base station)) for wireless communication is described. The processor may be configured to, capable of, or operable to perform one or more operations as described herein. For example, the processor may be configured to, capable of, or operable to receive an authentication response message that includes a GPSI for a UE in a NPN hosted by a PLMN and a SUPI usage restriction indication; receive, from a SEAF an authentication request; transmit, to the SEAF based at least in part on the SUPI usage restriction indication, an authentication response that includes the GPSI for the UE and the SUPI for the UE.

[0012] A method performed or performable by an NE (e.g., a base station) for wireless communication is described. The method may include receiving an authentication response message that includes a GPSI for a UE in a NPN hosted by a PLMN and a SUPI usage restriction indication; receiving, from a SEAF an authentication request; transmitting, to the SEAF based at least in part on the SUPI usage restriction indication, an authentication response that includes the GPSI for the UE and the SUPI for the UE.

[0013] In some implementations of the NE, the processor, and the method described herein, the authentication response includes the SUPI usage restriction indication. In some implementations of the NE, the processor, and the method described herein, to receive the authentication response message, the NE, processor, and method may further be configured to, capable of, performed, performable, or operable to receive the authentication response message from a UDM function. In some implementations of the NE, the processor, and the method described herein, the NE implements an AUSF.

[0014] An NE (e.g., a base station) for wireless communication is described. The NE may be configured to, capable of, or operable to perform one or more operations as described herein. For example, the NE may be configured to, capable of, or operable to transmit, to an AUSF, a authentication request for a UE in a NPN hosted by a PLMN; receive, from the AUSF, an authentication response that includes a GPSI for the UE and a SUPI for the UE.

[0015] A processor (e.g., a standalone processor chipset, or a component of a NE (e.g., a base station)) for wireless communication is described. The processor may be configured to, capable of, or operable to perform one or more operations as described herein. For example, the processor may be configured to, capable of, or operable to transmit, to an AUSF, a authentication request for a UE in a NPN hosted by a PLMN; receive, from the AUSF, an authentication response that includes a GPSI for the UE and a SUPI for the UE.

[0016] A method performed or performable by an NE (e.g., a base station) for wireless communication is described. The method may include transmit, to an AUSF, an authentication request for a UE in a NPN hosted by a PLMN; receive, from the AUSF, an authentication response that includes a GPSI for the UE and a SUPI for the UE.

[0017] In some implementations of the NE, processor, and method described herein, the authentication response includes an SUPI usage restriction indication for the SUPI. In some implementations of the NE, processor, and method described herein, the NE, processor, and method may further be configured to, capable of, performed, performable, or operable to use the GPSI rather than the SUPI for context identification and management for the UE. In some implementations of the NE, processor, and method described herein, the NE implements a SEAF.

BRIEF DESCRIPTION OF THE DRAWINGS

[0018] Figure 1 illustrates an example of a wireless communications system in accordance with aspects of the present disclosure.

[0019] Figure 2 illustrates an example of an authentication procedure in accordance with aspects of the present disclosure.

[0020] Figure 3 illustrates an example of an authentication procedure in accordance with aspects of the present disclosure.

[0021] Figure 4 illustrates an example of a UE ID privacy support capability exchange in accordance with aspects of the present disclosure.

[0022] Figures 5A and 5B illustrate an example of SUPI disclosure restriction and privacy protected UE ID usage in accordance with aspects of the present disclosure.

[0023] Figures 6A and 6B illustrate an example of SUPI disclosure restriction and privacy protected UE ID usage in accordance with aspects of the present disclosure.

[0024] Figure 7 illustrates an example of a UE in accordance with aspects of the present disclosure.

[0025] Figure 8 illustrates an example of a processor in accordance with aspects of the present disclosure.

[0026] Figure 9 illustrates an example of a NE in accordance with aspects of the present disclosure.

[0027] Figures 10 through 12 illustrate flowcharts of methods performed by one or more NEs in accordance with aspects of the present disclosure.

DETAILED DESCRIPTION

[0028] When non-public network (NPN) is hosted by a public land mobile network (PLMN), there is a possible deployment scenario, where dedicated user plane function (UPF) and part of control plane (CP) functions (e.g., access and mobility management function (AMF) or security anchor function (SEAF)) are deployed in customer premises with service based architecture (SBA)

interface with operator premises. Considering primary authentication and authorization procedure, e.g., specified in clause 6.1.3 in 3rd Generation Partnership Project (3GPP) Technical Specification (TS) 33.501, if a subscription permanent identifier (SUPI) is available in clear text to the network functions (NFs) in customer premises then it can potentially lead to security threats, privacy breach, UE location tracking, targeted attacks, and so forth, if SUPI in transit and at rest is not protected. There are currently no solutions to protect the SUPI in rest at the customer premise.

[0029] The techniques discussed herein describe a method for the UDM to enforce SUPI usage restrictions, for example, to protect SUPI at rest in the control plane functions deployed at the customer premise in a hosted NPN/serving network scenario. The control plane function (e.g., AMF/SEAF) deployed at the customer premise can be treated as more prone to illegitimate access, attacks, or security threats and this control plane function can be treated as an external function (e.g., like an external application function (AF)). The GPSI (e.g., with an external identifier) or a privacy protected UE ID can be provided by the UDM to let the control plane function at the customer premise (e.g., a hosted NPN or serving network) use the GPSI or privacy protected ID for the UE context fetching and management both locally (in the hosted NPN or serving network) and from the home network (or UDM/UDR).

[0030] The techniques discussed herein also describe a process of SUPI usage restriction during the EAP-AKA' based primary authentication run that includes providing a GPSI or privacy protected UE ID (instead of SUPI) to the serving network or NPN. This allows the serving network (or NPN) and the UE to use the GPSI or privacy protected UE ID in UE context identification and management aspects during primary authentication and key establishment processes (e.g., Kamf derivation).

[0031] The techniques discussed herein also describes a process of SUPI usage restriction during the 5G authentication and key agreement (5G-AKA) based primary authentication run that includes providing a GPSI or privacy protected UE ID (instead of SUPI) to the serving network or NPN. This allows the serving network (or NPN) and the UE to use the GPSI or privacy protected UE ID in UE context identification and management aspects during primary authentication and key establishment processes (e.g., for UE security context fetching for right key derivations such as Kamf /Kamf* derivation).

[0032] The techniques discussed herein allow for the use of a GPSI or privacy protected ID, instead of SUPI, in a serving network or NPN, allowing the SUPI to be protected while an identifier (e.g., GPSI or privacy protected UE ID) is at rest at the customer premise.

[0033] Reference is made herein to receiving, transmitting, or communicating data or information, such as signaling communication resources and/or communications that are transmitted or received between devices. It is to be appreciated that other terms may be used interchangeably with communicating, such as signaling, transmitting, receiving, outputting, forwarding, retrieving, obtaining, and so forth. Similarly, other terms may be used interchangeably with transmitting (e.g., communicating, signaling, outputting, forwarding, and so forth), and other terms may be used interchangeably with receiving (e.g., communicating, retrieving, obtaining, and so forth).

[0034] Aspects of the present disclosure are described in the context of a wireless communications system.

[0035] Figure 1 illustrates an example of a wireless communications system 100 in accordance with aspects of the present disclosure. The wireless communications system 100 may include one or more NE 102, one or more UE 104, and a core network (CN) 106. The wireless communications system 100 may support various radio access technologies. In some implementations, the wireless communications system 100 may be a 4G network, such as an LTE network or an LTE-Advanced (LTE-A) network. In some other implementations, the wireless communications system 100 may be a new radio (NR) network, such as a 5G network, a 5G-Advanced (5G-A) network, or a 5G ultrawideband (5G-UWB) network. In other implementations, the wireless communications system 100 may be a combination of a 4G network and a 5G network, or other suitable radio access technology including Institute of Electrical and Electronics Engineers (IEEE) 802.11 (Wi-Fi), IEEE 802.16 (WiMAX), IEEE 802.20. The wireless communications system 100 may support radio access technologies beyond 5G, for example, 6G. Additionally, the wireless communications system 100 may support technologies, such as time division multiple access (TDMA), frequency division multiple access (FDMA), or code division multiple access (CDMA), etc.

[0036] The one or more NE 102 may be dispersed throughout a geographic region to form the wireless communications system 100. One or more of the NE 102 described herein may be or include or may be referred to as a network node, a base station, a network element, a network

function, a network entity, a radio access network (RAN), a NodeB, an eNodeB (eNB), a next-generation NodeB (gNB), or other suitable terminology. An NE 102 and a UE 104 may communicate via a communication link, which may be a wireless or wired connection. For example, an NE 102 and a UE 104 may perform wireless communication (e.g., receive signaling, transmit signaling) over a Uu interface.

[0037] An NE 102 may provide a geographic coverage area for which the NE 102 may support services for one or more UEs 104 within the geographic coverage area. For example, an NE 102 and a UE 104 may support wireless communication of signals related to services (e.g., voice, video, packet data, messaging, broadcast, etc.) according to one or multiple radio access technologies. In some implementations, an NE 102 may be moveable, for example, a satellite associated with a non-terrestrial network (NTN). In some implementations, different geographic coverage areas associated with the same or different radio access technologies may overlap, but the different geographic coverage areas may be associated with different NE 102.

[0038] The one or more UE 104 may be dispersed throughout a geographic region of the wireless communications system 100. A UE 104 may include or may be referred to as a remote unit, a mobile device, a wireless device, a remote device, a subscriber device, a transmitter device, a receiver device, or some other suitable terminology. In some implementations, the UE 104 may be referred to as a unit, a station, a terminal, or a client, among other examples. Additionally, or alternatively, the UE 104 may be referred to as an Internet-of-Things (IoT) device, an Internet-of-Everything (IoE) device, or machine-type communication (MTC) device, among other examples.

[0039] A UE 104 may be able to support wireless communication directly with other UEs 104 over a communication link. For example, a UE 104 may support wireless communication directly with another UE 104 over a device-to-device (D2D) communication link. In some implementations, such as vehicle-to-vehicle (V2V) deployments, vehicle-to-everything (V2X) deployments, or cellular-V2X deployments, the communication link may be referred to as a sidelink. For example, a UE 104 may support wireless communication directly with another UE 104 over a PC5 interface.

[0040] An NE 102 may support communications with the CN 106, or with another NE 102, or both. For example, an NE 102 may interface with other NE 102 or the CN 106 through one or more backhaul links (e.g., S1, N2, N6, or other network interface). In some implementations, the NE 102

may communicate with each other directly. In some other implementations, the NE 102 may communicate with each other indirectly (e.g., via the CN 106). In some implementations, one or more NE 102 may include subcomponents, such as an access network entity, which may be an example of an access node controller (ANC). An ANC may communicate with the one or more UEs 104 through one or more other access network transmission entities, which may be referred to as a radio heads, smart radio heads, or transmission-reception points (TRPs).

[0041] The CN 106 may support user authentication, access authorization, tracking, connectivity, and other access, routing, or mobility functions. The CN 106 may be an evolved packet core (EPC), or a 5G core (5GC), which may include a control plane entity that manages access and mobility (e.g., a mobility management entity (MME), an access and mobility management functions (AMF)) and a user plane entity that routes packets or interconnects to external networks (e.g., a serving gateway (S-GW), a packet data network (PDN) gateway (P-GW), or a user plane function (UPF)). In some implementations, the control plane entity may manage non-access stratum (NAS) functions, such as mobility, authentication, and bearer management (e.g., data bearers, signal bearers, etc.) for the one or more UEs 104 served by the one or more NE 102 associated with the CN 106.

[0042] The CN 106 may communicate with a packet data network over one or more backhaul links (e.g., via an S1, N2, N6, or other network interface). The packet data network may include an application server. In some implementations, one or more UEs 104 may communicate with the application server. A UE 104 may establish a session (e.g., a protocol data unit (PDU) session, or the like) with the CN 106 via an NE 102. The CN 106 may route traffic (e.g., control information, data, and the like) between the UE 104 and the application server using the established session (e.g., the established PDU session). The PDU session may be an example of a logical connection between the UE 104 and the CN 106 (e.g., one or more network functions of the CN 106).

[0043] In the wireless communications system 100, the NEs 102 and the UEs 104 may use resources of the wireless communications system 100 (e.g., time resources (e.g., symbols, slots, subframes, frames, or the like) or frequency resources (e.g., subcarriers, carriers)) to perform various operations (e.g., wireless communications). In some implementations, the NEs 102 and the UEs 104 may support different resource structures. For example, the NEs 102 and the UEs 104 may support different frame structures. In some implementations, such as in 4G, the NEs 102 and the

UEs 104 may support a single frame structure. In some other implementations, such as in 5G and among other suitable radio access technologies, the NEs 102 and the UEs 104 may support various frame structures (i.e., multiple frame structures). The NEs 102 and the UEs 104 may support various frame structures based on one or more numerologies.

[0044] One or more numerologies may be supported in the wireless communications system 100, and a numerology may include a subcarrier spacing and a cyclic prefix. A first numerology (e.g., μ=0) may be associated with a first subcarrier spacing (e.g., 15 kHz) and a normal cyclic prefix. In some implementations, the first numerology (e.g., μ=0) associated with the first subcarrier spacing (e.g., 15 kHz) may utilize one slot per subframe. A second numerology (e.g., μ=1) may be associated with a second subcarrier spacing (e.g., 30 kHz) and a normal cyclic prefix. A third numerology (e.g., μ=2) may be associated with a third subcarrier spacing (e.g., 60 kHz) and a normal cyclic prefix or an extended cyclic prefix. A fourth numerology (e.g., μ=3) may be associated with a fourth subcarrier spacing (e.g., 120 kHz) and a normal cyclic prefix. A fifth numerology (e.g., μ=4) may be associated with a fifth subcarrier spacing (e.g., 240 kHz) and a normal cyclic prefix.

[0045] A time interval of a resource (e.g., a communication resource) may be organized according to frames (also referred to as radio frames). Each frame may have a duration, for example, a 10 millisecond (ms) duration. In some implementations, each frame may include multiple subframes. For example, each frame may include 10 subframes, and each subframe may have a duration, for example, a 1 ms duration. In some implementations, each frame may have the same duration. In some implementations, each subframe of a frame may have the same duration.

[0046] Additionally, or alternatively, a time interval of a resource (e.g., a communication resource) may be organized according to slots. For example, a subframe may include a number (e.g., quantity) of slots. The number of slots in each subframe may also depend on the one or more numerologies supported in the wireless communications system 100. For instance, the first, second, third, fourth, and fifth numerologies (i.e., μ=0, μ=1, μ=2, μ=3, μ=4) associated with respective subcarrier spacings of 15 kHz, 30 kHz, 60 kHz, 120 kHz, and 240 kHz may utilize a single slot per subframe, two slots per subframe, four slots per subframe, eight slots per subframe, and 16 slots per subframe, respectively. Each slot may include a number (e.g., quantity) of symbols (e.g., OFDM symbols). In some implementations, the number (e.g., quantity) of slots for a subframe may depend

on a numerology. For a normal cyclic prefix, a slot may include 14 symbols. For an extended cyclic prefix (e.g., applicable for 60 kHz subcarrier spacing), a slot may include 12 symbols. The relationship between the number of symbols per slot, the number of slots per subframe, and the number of slots per frame for a normal cyclic prefix and an extended cyclic prefix may depend on a numerology. It should be understood that reference to a first numerology (e.g., μ=0) associated with a first subcarrier spacing (e.g., 15 kHz) may be used interchangeably between subframes and slots.

[0047] In the wireless communications system 100, an electromagnetic (EM) spectrum may be split, based on frequency or wavelength, into various classes, frequency bands, frequency channels, etc. By way of example, the wireless communications system 100 may support one or multiple operating frequency bands, such as frequency range designations FR1 (410 MHz – 7.125 GHz), FR2 (24.25 GHz – 52.6 GHz), FR3 (7.125 GHz – 24.25 GHz), FR4 (52.6 GHz – 114.25 GHz), FR4a or FR4-1 (52.6 GHz – 71 GHz), and FR5 (114.25 GHz – 300 GHz). In some implementations, the NEs 102 and the UEs 104 may perform wireless communications over one or more of the operating frequency bands. In some implementations, FR1 may be used by the NEs 102 and the UEs 104, among other equipment or devices for cellular communications traffic (e.g., control information, data). In some implementations, FR2 may be used by the NEs 102 and the UEs 104, among other equipment or devices for short-range, high data rate capabilities.

[0048] FR1 may be associated with one or multiple numerologies (e.g., at least three numerologies). For example, FR1 may be associated with a first numerology (e.g., μ=0), which includes 15 kHz subcarrier spacing; a second numerology (e.g., μ=1), which includes 30 kHz subcarrier spacing; and a third numerology (e.g., μ=2), which includes 60 kHz subcarrier spacing. FR2 may be associated with one or multiple numerologies (e.g., at least 2 numerologies). For example, FR2 may be associated with a third numerology (e.g., μ=2), which includes 60 kHz subcarrier spacing; and a fourth numerology (e.g., μ=3), which includes 120 kHz subcarrier spacing.

[0049] A scenario for NPN security considerations is the wireless communications system (e.g., 5G system) is expected to enable a PLMN to host an NPN without compromising the security of that PLMN. It should be noted that dedicated network entities of NPN can be deployed in customer premises that are outside the control of the PLMN operator. When NPN is hosted by a PLMN, two possible deployment scenarios include: scenario 1, where dedicated UPF is deployed in customer

premises, with N4 interface (non-SBA interface) with the operator premises; scenario 2, where dedicated UPF and part of CP functions are deployed in customer premises with SBA interface with operator premises.

[0050] Considering primary authentication and authorization procedure specified in clause in 3GPP TS 33.501, if a SUPI is available in clear text to the NFs in customer premises, then it may potentially lead to security threats, privacy breach, UE location tracking, targeted attacks, and so forth. The privacy sensitive SUPI is the home network operator provided identifier is used exclusively to identify its subscribers and related subscription information to handle the related services. It is not a security best practice to expose the privacy sensitive SUPI external to the operator's trust domain. Especially in case of PLMN hosting NPN scenarios, exposing SUPI beyond operator trust domain (e.g., PLMN) to NFs in the NPN (which is in different trust domain) is to be avoided. The techniques discussed herein protect the SUPI by using a GPSI or privacy protected UE ID instead of the SUPI.

[0051] One issue is how to avoid exposure of the sensitive parameters (e.g., permanent identifier) to the entities outside the mobile network operator (MNO) premises (in other security domains). With respect to security threats, as the security at the customer premise might be weaker than that of operator premise even with the existing network domain security (NDS)/IP or SBA security, an attacker can compromise NFs in customer premise and can retrieve the SUPI to launch targeted attacks. If the dedicated NFs could be compromised in customer premises, then SUPI is available to the attacker, it can potentially lead to security threats, like privacy breach, UE location tracking, mapping of the user to the identifiers, targeted DoS, like so. With respect to potential security requirements, the wireless communications system (e.g., 5G system) is expected to support a mechanism to ensure protection of the sensitive parameters (specifically, SUPI) against the risk caused by PLMN hosting NPN.

[0052] Figure 2 illustrates an example 200 of an authentication procedure in accordance with aspects of the present disclosure. Example 200 is an example of an authentication procedure for extensible authentication protocol - authentication and key agreement (EAP-AKA). In the example 200, in case of roaming, the SUPI is sent from the home network UDM and AUSF to the serving network's SEAF (co-located with AMF), in step 10, following the successful primary authentication of the UE. This allows SUPI's exposure to the AMF/SEAF.

[0053] Figure 3 illustrates an example 300 of an authentication procedure in accordance with aspects of the present disclosure. Example 300 is an example of an authentication procedure for 5G AKA. In the example 300, in case of roaming, the SUPI is sent from the home network UDM and AUSF to the serving network's SEAF (co-located with AMF), in step 12, following the successful primary authentication of the UE. This allows SUPI's exposure to the AMF/SEAF.

[0054] In case of PLMN hosting an NPN in the customer premise (which is outside the trust domain or control of the PLMN operator), if the primary authentication procedure using example 200 of Figure 2 or example 300 of Figure 3 are applied, the UE's privacy sensitive SUPI will be exposed to the AMF/SEAF in NPN leading to privacy risks. With respect to securing sensitive data with trusted environment one solution is a trusted environment is used for the execution of sensitive functions and the storage of sensitive data in the NFs deployed in customer premise.

[0055] A trusted environment (TrE) is a logical entity that provides a trustworthy environment for the execution of sensitive functions and the storage of sensitive data. All data produced through execution of functions within the TrE is unknowable to unauthorized external entities, which protects data it holds from unauthorized access and tampering.

[0056] The TrE is built from an irremovable, hardware-based root of trust by way of a secure boot process, which occurs whenever an NF in customer premises is turned on or goes through a hard reset. The root of trust is physically bound to the NF. The secure boot process includes checks of the integrity of the TrE performed by the root of trust. Only successfully verified components can be loaded or started. The TrE, after having been successfully started, proceeds to verify other components of the hosting NF (e.g., operating system and further programs) that are necessary for trusted operation of the NF.

[0057] The TrE is used to provide the following protections to secure the sensitive data in customer premise: sensitive data such as SUPI and security context in UE context should be stored in the TrE of the NF in customer premise; sensitive functions such as key derivation functions should be performed within TrE; all signaling messages are expected to be confidentiality, integrity and replay protected while being transmitted in the customer premise; SUIP is expected to be confidentiality protected when being sent between the NF in dedicated network and 5G core

network (5GC). This TrE protects the SUPI in transit and does not impact UE, but it cannot protect the SUPI at rest.

[0058] In one or more implementations, a method for the UDM based on the secondary node (SN) ID or NPN ID, and based on operator policy determines to enforce SUPI usage restrictions. Where the GPSI (e.g., with an external identifier) or a privacy protected UE ID provided by the UDM can be used to identify and management UE context in the hosted NPN/serving network.

[0059] Additionally, or alternatively, the process of SUPI usage restriction (during the EAP-AKA' based primary authentication run) includes providing a GPSI/privacy protected UE ID (instead of SUPI) to the serving network or NPN, to enable the serving network or NPN, and UE, to use the GPSI/privacy protected UE ID in the further UE context identification and management aspects during primary authentication and key establishment process (e.g., Kamf derivation). The GPSI usage/privacy protected UE ID generation and usage is discussed in more detail below.

[0060] Additionally, or alternatively, the process of SUPI usage restriction (during the 5G AKA based primary authentication run) includes providing a GPSI/privacy protected UE ID (instead of SUPI) to the Serving network or NPN, to enable the serving network or NPN and UE to use the GPSI/privacy protected UE ID in the further primary authentication and key establishment process (e.g., Kamf derivation). The GPSI usage/privacy protected UE ID generation and usage is discussed in more detail below.

[0061] With respect to determining the usage of privacy protected UE ID in the hosted NPN/serving PLMN, the technique for the UDM based on the SN ID/NPN ID/ and based on operator policy determines to enforce SUPI usage restrictions (e.g., to protect SUPI at rest in the control plane functions deployed at the customer premise in case of hosted NPN/serving network scenario). Here the control plane function (e.g., AMF/SEAF) deployed in the customer premise can be treated as more prone to illegitimate access, attacks, or security threats and this control plane function can be treated as an external function (e.g., like external application function (AF)). Where the GPSI (e.g., with an external identifier) or a privacy protected UE ID can be determined to use provided by the UDM to let the control plane function at the customer premise (e.g., hosted NPN or serving network) to use the GPSI/privacy protected ID for the UE context fetching and management

both locally (in the hosted NPN/serving network) and from the home network (or UDM/unified data repository (UDR)) as detailed in example 400 of Figure 4.

[0062] Figure 4 illustrates an example 400 of a UE ID privacy support capability exchange in accordance with aspects of the present disclosure. Example 400 is an example of a UE ID privacy support capability exchange during the primary authentication initiation procedure.

[0063] The acts in the example 400 are described below. At 402 (1.), the UE sends any NAS message/N1 transport (e.g., Registration Request/Mobility Registration update/Periodic Registration update/any initial NAS message/PDU session establishment/modification request message etc.,) along with UE identifier (SUCI/5G-globally unique temporary UE identity (GUTI)).

[0064] At 404 (2.), the SEAF may initiate an authentication with the UE during any procedure establishing a signaling connection with the UE, according to the SEAF's policy. The UE can use subscription concealed identifier (SUCI) or 5G-GUTI in the Registration Request. The SEAF invokes the Nausf_UEAuthentication service by sending a Nausf_UEAuthentication_Authenticate Request message to the AUSF whenever the SEAF wishes to initiate an authentication.

[0065] The Nausf_UEAuthentication_Authenticate Request message contains the serving network name (e.g., related to hosted NPN or a serving network) and either SUCI or SUPI. The SEAF includes the SUPI in the Nausf_UEAuthentication_Authenticate Request message in case the SEAF has a valid 5G-GUTI and re-authenticates the UE. Otherwise, the SUCI is included in Nausf_UEAuthentication_Authenticate Request.

[0066] It should be noted that the local policy for the selection of the authentication method does not need to be on a per-UE basis but can be the same for all UEs. The Nausf_UEAuthentication_Authenticate Request may furthermore contain Disaster Roaming service indication.

[0067] At 406 (3.), upon receiving the Nausf_UEAuthentication_Authenticate Request message, the AUSF checks that the requesting SEAF in the serving network identified by the 3gpp-Sbi-Originating-Network-Id header specified in 3GPP TS 29.500 is entitled to use the serving network name in the Nausf_UEAuthentication_Authenticate Request. For the Disaster Roaming, the AUSF checks the local configuration and, if allowed, the AUSF sends Nudm_UEAuthentication_Get Request to the UDM. The Nudm_UEAuthentication_Get Request

sent from AUSF to UDM includes the following information: - SUCI or SUPI; the serving network name; if received from SEAF, Disaster Roaming service indication.

[0068] At 408 (4.), upon reception of the Nudm_UEAuthentication_Get Request, the UDM invoke subscription identifier de-concealing function (SIDF) if a SUCI is received. SIDF de-conceals SUCI to gain SUPI before UDM can process the request. Based on SUPI, the UDM/ authentication credential repository and processing function (ARPF) choose the authentication method.

[0069] It should be noted that the Nudm_UEAuthentication_Get Response in reply to the Nudm_UEAuthentication_Get Request and the Nausf_UEAuthentication_Authenticate Response message in reply to the Nausf_UEAuthentication_Authenticate Request message are described as part of the authentication procedures below. For the Disaster Roaming, the UDM checks the local configuration and, if allowed, the UDM proceeds with the chosen authentication method.

[0070] The UDM manages the SUPI usage restriction information/policies for one or more of hosted NPNs/serving networks (identified with their NPN ID or SN ID etc.,). SUPI usage restriction or limitation information/policies states if a SUPI usage is allowed or not allowed for the UE context management external to operator's security domain/network domain (e.g., for the UE during a hosted NPNs/serving networks access).

[0071] Based on the SUPI usage restriction information/policies/operator policy, and SN ID/NPN ID, the UDM determines to additionally provide a GPSI or a privacy protected UE for the UE context management at the hosted NPN/visited public land mobile network (VPLMN)/serving network, thereby limiting or restricting usage of the SUPI at the NPN/VPLMN. Additionally, or alternatively, the SUPI usage restriction information/policies is referred to as a 'SUPI disclosure policy'.

[0072] Further if the UDM determines not to disclose the SUPI (e.g., to not use for UE context management purpose external to operator network or security domain), the UDM generates or assigns GPSI (with external identifier) specific to (e.g., for use only by or communicated only to) the hosted NPN/VPLMN/serving network for the UE or the serving network UE ID (S-UEID) for the SUPI. Store SUPI and S-UEID pair in the UDM/UDR.

[0073] Serving network UE ID (S-UEID) Generation/constructed can be based on any one of the following: Option1: S-UEID: ID Type, Privacy protected UE identifier (P-IMSI/P-NSI/P-GLI/P-GCI), where P stands for 'privacy protected'; Option2: S-UEID: ID Type, privacy protected Equivalent UE identifier (E-IMSI/E-NSI/E-GLI/E-GCI), where E stands for 'privacy protected equivalent'; E-IMSI: mobile country code (MCC), mobile network code (MNC), secondary network name (SNN)/SN ID, EMSIN, where EMSIN identifies the UE subscription data within the serving network and it is a privacy protected mobile subscriber identification number (MSIN); E-NSI: equivalent username @ MCC, MNC and SNN/Serving network identification (NID)/NPN ID. E-GLI and E-GCI can be constructed with equivalent username and realm information same as E-NSI.

[0074] Additionally, or alternatively, UDM computes the S-UEID as follows: S-UE ID can include the E-IMSI/E-NSI/E-GLI/E-GCI are derived and composed as follows. E-MSIN part of E-IMSI = MAC (SUPI, SNN/SN ID/NPN ID, a freshness parameter (e.g., Nonce, RAND, Counter). Rest of E-IMSI are same as described above e.g., MCC, MNC, SNN/SN ID. E-IMSI composition can be as MCC, MNC, SNN/SN ID/NPN ID, EMSIN.

[0075] E-username part of E-NSI/E-GLI/E-GCI = MAC (Username/SUPI, SNN/SN ID/NPN ID, a freshness parameter (e.g., Nonce, RAND, Counter)). Rest of E-NSI/E-GLI/E-GCI are same as described above e.g., @ MCC, MNC, SNN/SN ID. E-IMSI composition can be as E-username@MCC, MNC, SNN/SN ID/NPN ID.

[0076] With respect to a technique to provide and use the privacy protected UE ID for the UE and the hosted NPN/serving PLMN during EAP-AKA', the technique describes the process of SUPI usage restriction (during the EAP-AKA' based primary authentication run) includes providing a GPSI/privacy protected UE ID (instead of SUPI) to the Serving network/NPN, to enable the serving network/NPN and UE to use the GPSI/privacy protected UE ID in the further UE context identification and management aspects during primary authentication and key establishment process (e.g., for UE security context fetching for right key derivations such as Kamf /Kamf* derivation) as shown in Figures 5A and 5B. The GPSI usage/privacy protected UE ID generation and usage is detailed in the discussions herein.

[0077] Figures 5A and 5B illustrate an example 500 of SUPI disclosure restriction and privacy protected UE ID usage in accordance with aspects of the present disclosure. Example 500 is an

example SUPI disclosure restriction and privacy protected UE ID usage in the hosted NPN/serving networking scenario during primary authentication with EAP-AKA'.

[0078] The acts in the example 500 are described below. At 502 (1.), the UDM/ARPF first generates an authentication vector with Authentication Management Field (AMF) separation bit = 1 as defined in 3GPP TS 33.102. The UDM/ARPF then computes cipher key (CK') and integrity key (IK') as per the normative Annex A and replace CK and IK by CK' and IK'.

[0079] At 504 (2.), the UDM subsequently sends this transformed authentication vector (AV') (RAND, authentication token (AUTN), expected response (XRES), CK', IK') to the AUSF from which it received the Nudm_UEAuthentication_Get Request together with an indication that the AV' is to be used for EAP-AKA' using a Nudm_UEAuthentication_Get Response message. It should be noted that the exchange of a Nudm_UEAuthentication_Get Request message and an Nudm_UEAuthentication_Get Response message between the AUSF and the UDM/ARPF described in the preceding paragraph is the same as for trusted access using EAP-AKA' described in 3GPP TS 33.402, sub-clause 6.2, step 10, except for the input parameter to the key derivation, which is the value of <network name>. The "network name" is carried in the AT_KDF_INPUT attribute in EAP-AKA'. For evolved packet system (EPS), the value of <network name> is defined as "access network identity", and for 5G, it is defined as "serving network name".

[0080] In case SUCI was included in the Nudm_UEAuthentication_Get Request, UDM if determines not to allow SUPI for UE context management at the hosted NPN/VPLMN/serving network (e.g., as discussed above and if it has a GPSI or constructs a S-UEID), the UDM will include the GPSI (or) S-UEID in addition to SUPI and SUPI usage restriction indication in the Nudm_UEAuthentication_Get Response. If a subscriber has an authentication and key management for application (AKMA) subscription, the UDM includes the AKMA indication and Routing indicator in the Nudm_UEAuthentication_Get Response.

[0081] At 506 (3.), the AUSF send the EAP-Request/AKA'-Challenge message to the SEAF in a Nausf_UEAuthentication_Authenticate Response message and stores GPSI or S-UEID in addition to SUPI and SUPI usage restriction indication if received from the UDM (along with serving network name or serving network id related to the hosted NPN/serving network).

[0082] At 508 (4.), the SEAF transparently forwards the EAP-Request/AKA'-Challenge message to the UE in a NAS message Authentication Request message. The mobile equipment (ME) forwards the RAND and AUTN received in EAP-Request/AKA'-Challenge message to the universal subscriber identity module (USIM). This message includes the ngKSI and anti-bidding down between architectures (ABBA) parameter. SEAF includes the ngKSI and ABBA parameter in all EAP-Authentication request message. The ngKSI will be used by the UE and AMF to identify the partial native security context that is created if the authentication is successful. The SEAF sets the ABBA parameter. During an EAP authentication, the value of the ngKSI and the ABBA parameter sent by the SEAF to the UE is not to be changed. It should be noted that the SEAF is expected to understand that the authentication method used is an EAP method by evaluating the type of authentication method based on the Nausf_UEAuthentication_Authenticate Response message.

[0083] At 510 (5.), at receipt of the RAND and AUTN, the USIM verifies the freshness of the AV' by checking whether AUTN can be accepted as described in 3GPP TS 33.102. If so, the USIM computes a response (RES). The USIM returns RES, CK, IK to the ME. If the USIM computes a Kc (e.g., general packet radio services (GPRS) Kc) from CK and IK using conversion function c3 as described in 3GPP TS 33.102, and sends it to the ME, then the ME ignores such GPRS Kc and not store the GPRS Kc on USIM or in ME. The ME derives CK' and IK' according to Annex A.3. If the verification of the AUTN fails on the USIM, then the USIM and ME proceeds as described in 3GPP TS 33.102 sub-clause 6.1.3. 3.

[0084] At 512 (6.), the UE sends the EAP-Response/AKA'-Challenge message to the SEAF in a NAS message Auth-Resp message. At 514 (7.), the SEAF transparently forwards the EAP-Response/AKA'-Challenge message to the AUSF in Nausf_UEAuthentication_Authenticate Request message. At 516 (8.), the AUSF verifies the message by comparing the XRES and RES, and if the AUSF has successfully verified this message it continues as follows, otherwise it returns an error to the SEAF. AUSF informs UDM about the authentication result.

[0085] At 518 (9.), the AUSF and the UE may exchange EAP-Request/AKA'-Notification and EAP-Response /AKA'-Notification messages via the SEAF. The SEAF transparently forwards these messages. It should be noted that EAP Notifications can be used at any time in the EAP-AKA

exchange. These notifications can be used e.g., for protected result indications or when the EAP server detects an error in the received EAP-AKA response.

[0086] At 520 (10a.), the AUSF derives extended master session key (EMSK) from CK' and IK'. The AUSF uses the most significant 256 bits of EMSK as the K_{AUSF} and then calculates K_{SEAF} from K_{AUSF}. The AUSF based on SUPI usage restriction indication and/or GPSI/ S-UEID received in step 2 (at 504) from the UDM, the AUSF determines to provide the GPSI/S-UEID in addition to SUPI.

[0087] At 522 (10b.), the AUSF sends an EAP Success message to the SEAF inside Nausf_UEAuthentication_Authenticate Response along with along with GPSI/S-UEID, which forwards it transparently to the UE. Nausf_UEAuthentication_Authenticate Response message contains the K_{SEAF}. If the AUSF received a SUCI from the SEAF when the authentication was initiated, then the AUSF also includes the GPSI/S-UEID in addition to SUPI in the Nausf_UEAuthentication_Authenticate Response message. The AUSF stores the K_{AUSF} and SUPI along with GPSI/S-UEID based on the home network operator's policy.

[0088] It should be noted that, for lawful interception, the AUSF sending GPSI/S-UEID in addition to SUPI to SEAF is expected but not sufficient. By including the GPSI/S-UEID / SUPI as input parameter to the key derivation of K_{AMF} from K_{SEAF}, additional assurance on the correctness of GPSI/S-UEID/SUPI, which is indirectly related to GPSI/S-UEID) is achieved by the serving network from both, home network and UE side.

[0089] At 524 and 526 (11a. and 11b.), the SEAF sends the EAP Success message to the UE in the N1 message. This message also includes the ngKSI and the ABBA parameter. The SEAF sets the ABBA parameter.

[0090] It should be noted that 11a. and 11b. can be NAS Security Mode Command or Authentication Result. It should also be noted that the ABBA parameter is included to enable the bidding down protection of security features that may be introduced later.

[0091] The key received in the Nausf_UEAuthentication_Authenticate Response message becomes the anchor key, K_{SEAF} in the sense of the key hierarchy. The SEAF then derives the K_{AMF} from the K_{SEAF}, the ABBA parameter and the SUPI and sends it to the AMF. On receiving the EAP-

Success message, the UE derives EMSK from CK' and IK'. The ME uses the most significant 256 bits of the EMSK as the K_{AUSF} and then calculates K_{SEAF} in the same way as the AUSF.

[0092] At 528 (11c.), the UE derives the K_{AMF} from the K_{SEAF}, the ABBA parameter and the SUPI. It should be noted that, as an implementation option, the UE creates the temporary security context as described in 524, 526, and 528 after receiving the EAP message that allows EMSK to be calculated. The UE turns this temporary security context into a partial security context when it receives the EAP Success. The UE removes the temporary security context if the EAP authentication fails.

[0093] Further actions can be taken by the AUSF upon receiving a successfully verified EAP-Response/AKA'-Challenge message. If the EAP-Response/AKA'-Challenge message is not successfully verified, the subsequent AUSF behavior is determined according to the home network's policy. If AUSF and SEAF determine that the authentication was successful, then the SEAF provides the ngKSI and the K_{AMF} to the AMF.

[0094] The SEAF and AMF uses GPSI/S-UEID (instead of SUPI) received from the UDM (via AUSF) as the identifier to use for the UE context identification and management. Moreover, the AMF/SEAF based on the received GPSI/S-UEID or SUPI usage restriction indication, deletes the received SUPI soon after Kseaf derivation. Whenever the UE provides 5G-GUTI, if the AMF/SEAF in the hosted NPN/serving network which uses GPSI/S-UEID (instead of SUPI) to manage UE context and subscription related data wants to initiate primary authentication, it sends an identity request to the UE and received SUCI and sends SUCI in the authentication request message sent to AUSF (e.g., at 404 in the example 400 of Figure 4). In the rest of the cases when the AMF wants to fetch any UE context or subscription data from UDM/UDR, the AMF uses GPSI/S-UEID instead of SUPI (in any Nudm service operation message). Additionally, or alternatively, AMF may send GPSI/S-UEID instead of SUPI in message 2 and 3 (via AUSF) in the procedure shown in the example 400 of Figure 4.

[0095] An example GPSI used for hosted NPN case/serving network case is as follows. An External Identifier identifies a subscription/UE's external security/network domain context associated to an international mobile subscriber identity (IMSI). A subscription or UE's external

security/network domain context associated to an IMSI may have one or several External Identifier(s). The External Identifier has the form username@realm.

[0096] The username part format of the External Identifier contains a Local Identifier as specified in 3GPP TS 23.682. The realm part format of the External Identifier contains a Domain Identifier as specified in 3GPP TS 23.682. The Domain Identifier is, for example, a registered Internet domain name. The combination of Local Identifier and Domain Identifier makes the External Identifier globally unique. The result of the External Identifier form is: "<Local Identifier>@<Domain Identifier>"

[0097] An example of an External Identifier is:

Local Identifier in use: "123456789"; this identifier may be extended to include hosted NPN case/serving network specific id or codes in addition.

Domain Identifier = "domain.com".

Which gives the External Identifier as: 123456789@domain.com.

[0098] External Identifier is expected to be globally unique and includes a Domain Identifier and a Local Identifier. The Domain Identifier identifies a domain that is under the control of a Mobile Network Operator (MNO). The Domain Identifier is used to identify where services provided by the operator network can be accessed (e.g., MTC-IWF or service capability exposure function (SCEF) provided services). An operator may use different domain identifiers to provide access to different services and/or MTC Service Providers. The Local Identifier is used to derive or obtain the IMSI. The Local Identifier is expected to be unique within the applicable domain. It is managed by the Mobile Network Operator.

[0099] Additionally, or alternatively, UDM computes the S-UEID as follows. S-UE ID can include the E-IMSI/E-NSI/E-GLI/E-GCI where are derived and composed as follows.

[0100] E-MSIN part of E-IMSI = MAC (SUPI, SNN/SN ID/NPN ID, a freshness parameter (e.g., Nonce, RAND, Counter) known to UE and network or provided by the network to the UE). Rest of E-IMSI are same as described above e.g., MCC, MNC, SNN/SN ID. E-IMSI composition can be as MCC, MNC, SNN/SN ID/NPN ID, EMSIN.

[0101] E-username part of E-NSI/E-GLI/E-GCI = MAC (Username/SUPI, SNN/SN ID/NPN ID, a freshness parameter (e.g., Nonce, RAND, Counter) known to UE and network or provided by the network to the UE). Rest of E-NSI/E-GLI/E-GCI are same as described above e.g., @ MCC, MNC, SNN/SN ID. E-IMSI composition can be as E-username@MCC, MNC, SNN/SN ID/NPN ID.

[0102] Some of the scenarios in UE general registration process where the GPSI/S-UEID (which can be used instead of SUPI) includes the following:

- old AMF to new AMF: Response to Namf_Communication_UEContextTransfer (GPSI/S-UEID or SUPI, UE Context in AMF (as per Table 5.2.2.2.2-1)) or unstructured data storage function (UDSF) to new AMF: Nudsf_Unstructured Data Management_Query().
- The AMF may decide to initiate UE authentication by invoking an AUSF. In that case, the AMF selects an AUSF based on GPSI/S-UEID or SUPI or SUCI.
- The GPSI is provided to the AMF in the Access and Mobility Subscription data from the UDM if the GPSI is available in the UE subscription data for hosted NPN access or serving network access or for UE context management at the different network domains or security domains.
- UDM discovery and selection - GPSI or External Group ID/S-UEID; UDM NF consumers which manage network signaling not based on SUPI/SUCI (e.g., the network exposure function (NEF)) select a UDM instance based on the S-UEID/GPSI or External Group ID range the UE's GPSI or External Group ID belongs to or based on the results of a discovery procedure with network repository function (NRF) using the UE's GPSI or External Group ID as input for UDM discovery.

[0103] With respect to providing and using the privacy protected UE ID for the UE and the hosted NPN/serving PLMN during 5G-AKA, the process of SUPI usage restriction (during the 5G-AKA based primary authentication run) includes providing a GPSI/privacy protected UE ID (instead of SUPI) to the Serving network/NPN, to enable the serving network/NPN and UE to use the GPSI/privacy protected UE ID in the further UE context identification and management aspects during primary authentication and key establishment process (e.g., for UE security context fetching for right key derivations such as Kamf /Kamf* derivation) as shown in Figures 6A and 6B. The GPSI usage/privacy protected UE ID generation and usage is detailed in the discussions herein.

[0104] Figures 6A and 6B illustrate an example 600 of SUPI disclosure restriction and privacy protected UE ID usage in accordance with aspects of the present disclosure. Example 600 is an example SUPI disclosure restriction and privacy protected UE ID usage in the hosted NPN/serving networking scenario during primary authentication with 5G AKA.

[0105] The acts in the example 600 are described below. At 602 (1.), for each Nudm_Authenticate_Get Request, the UDM/ARPF creates a 5G HE AV. The UDM/ARPF does this by generating an AV with the Authentication Management Field (AMF) separation bit set to "1". The UDM/ARPF then derives K_{AUSF} (as per Annex A.2) and calculates XRES* (as per Annex A.4). Finally, the UDM/ARPF creates a 5G HE AV from RAND, AUTN, XRES*, and K_{AUSF}.

[0106] At 604 (2.), the UDM then returns the 5G HE AV to the AUSF together with an indication that the 5G HE AV is to be used for 5G AKA in a Nudm_UEAuthentication_Get Response. In case SUCI was included in the Nudm_UEAuthentication_Get Request, UDM if determines not to allow SUPI for UE context management at the hosted NPN/VPLMN/serving network (based on example 400 of Figure 4 and if it has a GPSI or constructs a S-UEID), the UDM includes GPSI (or) S-UEID in addition to SUPI and SUPI usage restriction indication in the Nudm_UEAuthentication_Get Response after deconcealment of SUCI by SIDF. If a subscriber has an AKMA subscription, the UDM includes the AKMA indication and Routing indicator in the Nudm_UEAuthentication_Get Response.

[0107] At 606 (3.), the AUSF stores the XRES* temporarily together with the received SUCI or SUPI. The AUSF also stores the GPSI (or) S-UEID (along with serving network name or serving network id related to the hosted NPN/serving network) in addition to SUPI and SUPI usage restriction indication if received. Also at 606 (4.), the AUSF then generates the 5G AV from the 5G HE AV received from the UDM/ARPF by computing the HXRES* from XRES* (according to Annex A.5) and K_{SEAF} from K_{AUSF} (according to Annex A.6), and replacing the XRES* with the HXRES* and K_{AUSF} with K_{SEAF} in the 5G HE AV.

[0108] At 608 (5.), the AUSF then removes the K_{SEAF} and return the 5G SE AV (RAND, AUTN, HXRES*) to the SEAF in a Nausf_UEAuthentication_UEAuthentication Response. At 610 (6.), the SEAF sends RAND, AUTN to the UE in a NAS message Authentication Request. This message also includes the ngKSI that will be used by the UE and AMF to identify the K_{AMF} and the

partial native security context that is created if the authentication is successful. This message also includes the ABBA parameter. The SEAF sets the ABBA parameter as defined in Annex A.7.1. The ME forwards the RAND and AUTN received in NAS message Authentication Request to the USIM. It should be noted that the ABBA parameter is included to enable the bidding down protection of security features.

[0109] At 612 (7. or 7a.), at receipt of the RAND and AUTN, the USIM verifies the freshness of the received values by checking whether AUTN can be accepted as described in 3GPP TS 33.102. If so, the USIM computes a response RES. The USIM returns RES, CK, IK to the ME. If the USIM computes a Kc (e.g., GPRS Kc) from CK and IK using conversion function c3 as described in 3GPP TS 33.102, and sends it to the ME, then the ME ignores such GPRS Kc and does not store the GPRS Kc on USIM or in ME. The ME then computes RES* from RES according to Annex A.4. The ME calculates K_{AUSF} from CK||IK according to clause A.2. The ME calculates K_{SEAF} from K_{AUSF} according to clause A.6. An ME accessing 5G checks during authentication that the "separation bit" in the AMF field of AUTN is set to 1. The "separation bit" is bit 0 of the AMF field of AUTN.

[0110] It should be noted that this separation bit in the AMF field of AUTN cannot be used anymore for operator specific purposes as described by 3GPP TS 33.102, Annex F. At 614 (8.), the UE returns RES* to the SEAF in a NAS message Authentication Response. At 616 (9.), the SEAF then computes hash response (HRES*) from RES* according to Annex A.5, and the SEAF compares HRES* and hash expected response (HXRES*). If they coincide, the SEAF considers the authentication successful from the serving network point of view. If not, the SEAF proceeds as described in sub-clause 6.1.3.2.2. If the UE is not reached, and the RES* is never received by the SEAF, the SEAF considers authentication as failed, and indicates a failure to the AUSF.

[0111] At 618 (10.), the SEAF sends RES*, as received from the UE, in a Nausf_UEAuthentication_Authenticate Request message to the AUSF. At 620 (11a.), when the AUSF receives as authentication confirmation the Nausf_UEAuthentication_Authenticate Request message including a RES* it may verify whether the 5G AV has expired. If the 5G AV has expired, the AUSF may consider the authentication as unsuccessful from the home network point of view. Upon successful authentication, the AUSF stores the K_{AUSF} based on the home network operator's policy. AUSF compares the received RES* with the stored XRES*. If the RES* and XRES* are

equal, the AUSF considers the authentication as successful from the home network point of view. AUSF informs UDM about the authentication result.

[0112] At 622 (11b.), the AUSF based on SUPI usage restriction indication and/or GPSI/ S-UEID received at 604 (2.) from the UDM, the AUSF determines to provide the GPSI/S-UEID in addition to SUPI. It should be noted that it is left to implementation to temporarily store the K_{AUSF} received at 604 (2.) in AUSF until the RES* verification is done successfully (e.g., at 620 (11a.)).

[0113] At 624 (12.), the AUSF indicates to the SEAF in the Nausf_UEAuthentication_Authenticate Response whether the authentication was successful or not from the home network point of view. If the authentication was successful, the K_{SEAF} is sent to the SEAF in the Nausf_UEAuthentication_Authenticate Response along with GPSI/S-UEID in addition to SUPI. In case the AUSF received a SUCI from the SEAF in the authentication request, and if the authentication was successful, then the AUSF also includes the GPSI/S-UEID in addition to SUPI in the Nausf_UEAuthentication_Authenticate Response message. The AUSF may store the SUPI along with GPSI/S-UEID in addition if not done earlier.

[0114] If the authentication was successful, the key K_{SEAF} received in the Nausf_UEAuthentication_Authenticate Response message becomes the anchor key in the sense of the key hierarchy as specified in sub-clause 6.2 of the present document. Then at 626 (13.), the SEAF derives the K_{AMF} from the K_{SEAF}, the ABBA parameter and the SUPI. The SEAF provides the ngKSI and the K_{AMF} to the AMF. If the AUSF indicates that the authentication was successful from the home network point of view, then the AMF initiates NAS security mode command procedure (as described in 3GPP TS 33.501 clause 6.7.2) with the UE, to take the newly generated partial native 5G NAS security context into use. Upon receiving the valid NAS Security Mode Command message from the AMF, the UE considers the performed primary authentication as successful.

[0115] If a SUCI was used for this authentication, then the SEAF only provides ngKSI and K_{AMF} to the AMF after it has received the Nausf_UEAuthentication_Authenticate Response message containing K_{SEAF} and GPSI/S-UEID in addition to SUPI/SUPI; no communication services will be provided to the UE until the GPSI/S-UEID in addition to SUPI/SUPI is known to the serving

network. The further steps taken by the AUSF after the authentication procedure are described in sub-clause 6.1.4 of the present document.

[0116] The SEAF and AMF uses GPSI/S-UEID (instead of SUPI) received from the UDM (via AUSF) as the identifier to use for the UE context identification and management. Moreover, the AMF/SEAF based on the received GPSI/S-UEID or SUPI usage restriction indication, deletes the received SUPI soon after the Kseaf generation. Whenever the UE provides 5G-GUTI in any NAS message or registration request/update message, if the AMF/SEAF in the hosted NPN/serving network which uses GPSI/S-UEID (instead of SUPI) to manage UE context and subscription related data wants to initiate primary authentication, it sends an identity request to the UE and receives SUCI and sends SUCI in the authentication request message sent to AUSF in step 2 of example 400 of Figure 4. Rest of the cases when the AMF wants to fetch any UE context or subscription data from UDM/UDR, the AMF uses GPSI/S-UEID instead of SUPI (in any Nudm service operation message).

[0117] Additionally, or alternatively, AMF may send GPSI/S-UEID instead of SUPI in message 2 and 3 (via AUSF) in the procedure shown in the example 400 of Figure 4.

[0118] An example GPSI used for hosted NPN case/serving network case is as follows. An External Identifier identifies a subscription/UE's external security/network domain context associated to an IMSI. A subscription or UE's external security/network domain context associated to an IMSI may have one or several External Identifier(s). The External Identifier has the form username@realm. The username part format of the External Identifier contain a Local Identifier as specified in 3GPP TS 23.682. The realm part format of the External Identifier contains a Domain Identifier as specified in 3GPP TS 23.682. The Domain Identifier is, for example, a registered Internet domain name. The combination of Local Identifier and Domain Identifier makes the External Identifier globally unique. The result of the External Identifier form is: "<Local Identifier>@<Domain Identifier>".

[0119] An example of an External Identifier is:

Local Identifier in use: "123456789"; this identifier may be extended to include hosted NPN case/serving network specific id or codes in addition.

Domain Identifier = "domain.com".

Which gives the External Identifier as: 123456789@domain.com.

[0120] External Identifier is expected to be globally unique and includes a Domain Identifier and a Local Identifier. The Domain Identifier identifies a domain that is under the control of a Mobile Network Operator (MNO). The Domain Identifier is used to identify where services provided by the operator network can be accessed (e.g., MTC-IWF or SCEF provided services). An operator may use different domain identifiers to provide access to different services and/or MTC Service Providers. The Local Identifier is used to derive or obtain the IMSI. The Local Identifier is expected to be unique within the applicable domain. It is managed by the Mobile Network Operator.

[0121] Additionally, or alternatively, UDM computes the S-UEID as follows. S-UE ID can include the E-IMSI/E-NSI/E-GLI/E-GCI which are derived and composed as follows. E-MSIN part of E-IMSI = MAC (SUPI, SNN/SN ID/NPN ID, a freshness parameter (e.g., Nonce, RAND, Counter) known to UE and network or provided by the network to the UE). The rest of E-IMSI are same as described above e.g., MCC, MNC, SNN/SN ID. E-IMSI composition can be as MCC, MNC, SNN/SN ID/NPN ID, EMSIN.

[0122] E-username part of E-NSI/E-GLI/E-GCI = MAC (Username/SUPI, SNN/SN ID/NPN ID, a freshness parameter (e.g., Nonce, RAND, Counter) known to UE and network or provided by the network to the UE). Rest of E-NSI/E-GLI/E-GCI are same as described above e.g., @ MCC, MNC, SNN/SN ID. E-IMSI composition can be as E-username@MCC, MNC, SNN/SN ID/NPN ID.

[0123] Some of the scenarios in UE general registration process where the GPSI/S-UEID (which can be used instead of SUPI) includes the following:

- old AMF to new AMF: Response to Namf_Communication_UEContextTransfer (GPSI/S-UEID or SUPI, UE Context in AMF (as per Table 5.2.2.2.2-1)) or UDSF to new AMF: Nudsf_Unstructured Data Management_Query().
- The AMF may decide to initiate UE authentication by invoking an AUSF. In that case, the AMF selects an AUSF based on GPSI/S-UEID or SUPI or SUCI.
- The GPSI is provided to the AMF in the Access and Mobility Subscription data from the UDM if the GPSI is available in the UE subscription data for hosted NPN access or serving

network access or for UE context management at the different network domains or security domains.

- UDM discovery and selection - GPSI or External Group ID/S-UEID; UDM NF consumers which manage network signaling not based on SUPI/SUCI (e.g., the NEF) select a UDM instance based on the S-UEID/GPSI or External Group ID range the UE's GPSI or External Group ID belongs to or based on the results of a discovery procedure with NRF using the UE's GPSI or External Group ID as input for UDM discovery.

[0124] Based on operator policy GPSI lifetime and usage can be restricted and as required, the UDM may issue fresh GPSI/S-UEID for the aspects described in example 500 of Figure 5 and example 600 of Figure 6.

[0125] Figure 7 illustrates an example of a UE 700 in accordance with aspects of the present disclosure. The UE 700 may include a processor 702, a memory 704, a controller 706, and a transceiver 708. The processor 702, the memory 704, the controller 706, or the transceiver 708, or various combinations thereof or various components thereof may be examples of means for performing various aspects of the present disclosure as described herein. These components may be coupled (e.g., operatively, communicatively, functionally, electronically, electrically) via one or more interfaces.

[0126] The processor 702, the memory 704, the controller 706, or the transceiver 708, or various combinations or components thereof may be implemented in hardware (e.g., circuitry). The hardware may include a processor, a digital signal processor (DSP), an application-specific integrated circuit (ASIC), or other programmable logic device, or any combination thereof configured as or otherwise supporting a means for performing the functions described in the present disclosure.

[0127] The processor 702 may include an intelligent hardware device (e.g., a general-purpose processor, a DSP, a CPU, an ASIC, an FPGA, or any combination thereof). In some implementations, the processor 702 may be configured to operate the memory 704. In some other implementations, the memory 704 may be integrated into the processor 702. The processor 702 may be configured to execute computer-readable instructions stored in the memory 704 to cause the UE 700 to perform various functions of the present disclosure.

[0128] The memory 704 may include volatile or non-volatile memory. The memory 704 may store computer-readable, computer-executable code including instructions when executed by the processor 702 cause the UE 700 to perform various functions described herein. The code may be stored in a non-transitory computer-readable medium such as the memory 704 or another type of memory. Computer-readable media includes both non-transitory computer storage media and communication media including any medium that facilitates transfer of a computer program from one place to another. A non-transitory storage medium may be any available medium that may be accessed by a general-purpose or special-purpose computer.

[0129] In some implementations, the processor 702 and the memory 704 coupled with the processor 702 may be configured to cause the UE 700 to perform one or more of the functions described herein (e.g., executing, by the processor 702, instructions stored in the memory 704). For example, the processor 702 may support wireless communication at the UE 700 in accordance with examples as disclosed herein.

[0130] The controller 706 may manage input and output signals for the UE 700. The controller 706 may also manage peripherals not integrated into the UE 700. In some implementations, the controller 706 may utilize an operating system such as iOS®, ANDROID®, WINDOWS®, or other operating systems. In some implementations, the controller 706 may be implemented as part of the processor 702.

[0131] In some implementations, the UE 700 may include at least one transceiver 708. In some other implementations, the UE 700 may have more than one transceiver 708. The transceiver 708 may represent a wireless transceiver. The transceiver 708 may include one or more receiver chains 710, one or more transmitter chains 712, or a combination thereof.

[0132] A receiver chain 710 may be configured to receive signals (e.g., control information, data, packets) over a wireless medium. For example, the receiver chain 710 may include one or more antennas to receive a signal over the air or wireless medium. The receiver chain 710 may include at least one amplifier (e.g., a low-noise amplifier (LNA)) configured to amplify the received signal. The receiver chain 710 may include at least one demodulator configured to demodulate the receive signal and obtain the transmitted data by reversing the modulation technique applied during

transmission of the signal. The receiver chain 710 may include at least one decoder for decoding the demodulated signal to receive the transmitted data.

[0133] A transmitter chain 712 may be configured to generate and transmit signals (e.g., control information, data, packets). The transmitter chain 712 may include at least one modulator for modulating data onto a carrier signal, preparing the signal for transmission over a wireless medium. The at least one modulator may be configured to support one or more techniques such as amplitude modulation (AM), frequency modulation (FM), or digital modulation schemes like phase-shift keying (PSK) or quadrature amplitude modulation (QAM). The transmitter chain 712 may also include at least one power amplifier configured to amplify the modulated signal to an appropriate power level suitable for transmission over the wireless medium. The transmitter chain 712 may also include one or more antennas for transmitting the amplified signal into the air or wireless medium.

[0134] Figure 8 illustrates an example of a processor 800 in accordance with aspects of the present disclosure. The processor 800 may be an example of a processor configured to perform various operations in accordance with examples as described herein. The processor 800 may include a controller 802 configured to perform various operations in accordance with examples as described herein. The processor 800 may optionally include at least one memory 804, which may be, for example, an L1/L2/L3 cache. Additionally, or alternatively, the processor 800 may optionally include one or more arithmetic-logic units (ALUs) 806. One or more of these components may be in electronic communication or otherwise coupled (e.g., operatively, communicatively, functionally, electronically, electrically) via one or more interfaces (e.g., buses).

[0135] The processor 800 may be a processor chipset and include a protocol stack (e.g., a software stack) executed by the processor chipset to perform various operations (e.g., receiving, obtaining, retrieving, transmitting, outputting, forwarding, storing, determining, identifying, accessing, writing, reading) in accordance with examples as described herein. The processor chipset may include one or more cores, one or more caches (e.g., memory local to or included in the processor chipset (e.g., the processor 800) or other memory (e.g., random access memory (RAM), read-only memory (ROM), dynamic RAM (DRAM), synchronous dynamic RAM (SDRAM), static RAM (SRAM), ferroelectric RAM (FeRAM), magnetic RAM (MRAM), resistive RAM (RRAM), flash memory, phase change memory (PCM), and others).

[0136] The controller 802 may be configured to manage and coordinate various operations (e.g., signaling, receiving, obtaining, retrieving, transmitting, outputting, forwarding, storing, determining, identifying, accessing, writing, reading) of the processor 800 to cause the processor 800 to support various operations in accordance with examples as described herein. For example, the controller 802 may operate as a control unit of the processor 800, generating control signals that manage the operation of various components of the processor 800. These control signals include enabling or disabling functional units, selecting data paths, initiating memory access, and coordinating timing of operations.

[0137] The controller 802 may be configured to fetch (e.g., obtain, retrieve, receive) instructions from the memory 804 and determine subsequent instruction(s) to be executed to cause the processor 800 to support various operations in accordance with examples as described herein. The controller 802 may be configured to track memory addresses of instructions associated with the memory 804. The controller 802 may be configured to decode instructions to determine the operation to be performed and the operands involved. For example, the controller 802 may be configured to interpret the instruction and determine control signals to be output to other components of the processor 800 to cause the processor 800 to support various operations in accordance with examples as described herein. Additionally, or alternatively, the controller 802 may be configured to manage flow of data within the processor 800. The controller 802 may be configured to control transfer of data between registers, ALUs 806, and other functional units of the processor 800.

[0138] The memory 804 may include one or more caches (e.g., memory local to or included in the processor 800 or other memory, such as RAM, ROM, DRAM, SDRAM, SRAM, MRAM, flash memory, etc. In some implementations, the memory 804 may reside within or on a processor chipset (e.g., local to the processor 800). In some other implementations, the memory 804 may reside external to the processor chipset (e.g., remote to the processor 800).

[0139] The memory 804 may store computer-readable, computer-executable code including instructions that, when executed by the processor 800, cause the processor 800 to perform various functions described herein. The code may be stored in a non-transitory computer-readable medium such as system memory or another type of memory. The controller 802 and/or the processor 800 may be configured to execute computer-readable instructions stored in the memory 804 to cause the processor 800 to perform various functions. For example, the processor 800 and/or the controller

802 may be coupled with or to the memory 804, the processor 800, and the controller 802, and may be configured to perform various functions described herein. In some examples, the processor 800 may include multiple processors and the memory 804 may include multiple memories. One or more of the multiple processors may be coupled with one or more of the multiple memories, which may, individually or collectively, be configured to perform various functions herein.

[0140] The one or more ALUs 806 may be configured to support various operations in accordance with examples as described herein. In some implementations, the one or more ALUs 806 may reside within or on a processor chipset (e.g., the processor 800). In some other implementations, the one or more ALUs 806 may reside external to the processor chipset (e.g., the processor 800). One or more ALUs 806 may perform one or more computations such as addition, subtraction, multiplication, and division on data. For example, one or more ALUs 806 may receive input operands and an operation code, which determines an operation to be executed. One or more ALUs 806 may be configured with a variety of logical and arithmetic circuits, including adders, subtractors, shifters, and logic gates, to process and manipulate the data according to the operation. Additionally, or alternatively, the one or more ALUs 806 may support logical operations such as AND, OR, exclusive-OR (XOR), not-OR (NOR), and not-AND (NAND), enabling the one or more ALUs 806 to handle conditional operations, comparisons, and bitwise operations.

[0141] The processor 800 may support wireless communication in accordance with examples as disclosed herein. The processor 800 may be configured to or operable to support at least one controller (e.g., the controller 802) coupled with at least one memory (e.g., the memory 804) and configured to cause the processor to: receive an authentication request message that includes a SUPI for a UE in a NPN hosted by a PLMN; limit, based at least in part on a SUPI usage policy, usage of the SUPI in the NPN hosted by the PLMN.

[0142] Additionally, the processor 800 may be configured to or configured to or operable to support any one or combination of where to limit usage of the SUPI in the NPN, the at least one processor is further configured to or operable to cause the NE to generate or assign a GPSI for the UE for use in place of the SUPI.; where the at least one processor is further configured to or operable to cause the NE to: receive the authentication request message from an AUSF; and transmit, to the AUSF, the GPSI and an SUPI usage restriction indication; where the GPSI is specific to the NPN; where the at least one processor is further configured to or operable to cause

the NE to determine, based at least in part on the SUPI usage policy, to not disclose the SUPI; where the NE implements a UDM function.

[0143] The processor 800 may support wireless communication in accordance with examples as disclosed herein. The processor 800 may be configured to or operable to support at least one controller (e.g., the controller 802) coupled with at least one memory (e.g., the memory 804) and configured to cause the processor to: receive an authentication response message that includes a GPSI for a UE in a NPN hosted by a PLMN and a SUPI usage restriction indication; receive, from a SEAF an authentication request; transmit, to the SEAF based at least in part on the SUPI usage restriction indication, an authentication response that includes the GPSI for the UE and the SUPI for the UE.

[0144] Additionally, the processor 800 may be configured to or operable to support any one or combination of where the authentication response includes the SUPI usage restriction indication; where to receive the authentication response message, the at least one processor is further configured to receive the authentication response message from a UDM function; where the NE implements an AUSF.

[0145] The processor 800 may support wireless communication in accordance with examples as disclosed herein. The processor 800 may be configured to or operable to support at least one controller (e.g., the controller 802) coupled with at least one memory (e.g., the memory 804) and configured to cause the processor to: transmit, to an AUSF, a authentication request for a UE in a NPN hosted by a PLMN; receive, from the AUSF, an authentication response that includes a GPSI for the UE and a SUPI for the UE.

[0146] Additionally, the processor 800 may be configured to or operable to support any one or combination of where the authentication response includes an SUPI usage restriction indication for the SUPI; where the at least one processor is further configured to or operable to cause the NE to use the GPSI rather than the SUPI for context identification and management for the UE; where the NE implements a SEAF.

[0147] Figure 9 illustrates an example of a NE 900 in accordance with aspects of the present disclosure. The NE 900 may include a processor 902, a memory 904, a controller 906, and a transceiver 908. The processor 902, the memory 904, the controller 906, or the transceiver 908, or

various combinations thereof or various components thereof may be examples of means for performing various aspects of the present disclosure as described herein. These components may be coupled (e.g., operatively, communicatively, functionally, electronically, electrically) via one or more interfaces. The NE 900 optionally hosts or implements any of various network functions, such as an AMF, an SEAF, an AUSF, a UDM, an ARPF, an SIDF, and so forth.

[0148] The processor 902, the memory 904, the controller 906, or the transceiver 908, or various combinations or components thereof may be implemented in hardware (e.g., circuitry). The hardware may include a processor, a digital signal processor (DSP), an application-specific integrated circuit (ASIC), or other programmable logic device, or any combination thereof configured as or otherwise supporting a means for performing the functions described in the present disclosure.

[0149] The processor 902 may include an intelligent hardware device (e.g., a general-purpose processor, a DSP, a CPU, an ASIC, an FPGA, or any combination thereof). In some implementations, the processor 902 may be configured to operate the memory 904. In some other implementations, the memory 904 may be integrated into the processor 902. The processor 902 may be configured to execute computer-readable instructions stored in the memory 904 to cause the NE 900 to perform various functions of the present disclosure.

[0150] The memory 904 may include volatile or non-volatile memory. The memory 904 may store computer-readable, computer-executable code including instructions when executed by the processor 902 cause the NE 900 to perform various functions described herein. The code may be stored in a non-transitory computer-readable medium such as the memory 904 or another type of memory. Computer-readable media includes both non-transitory computer storage media and communication media including any medium that facilitates transfer of a computer program from one place to another. A non-transitory storage medium may be any available medium that may be accessed by a general-purpose or special-purpose computer.

[0151] In some implementations, the processor 902 and the memory 904 coupled with the processor 902 may be configured to cause the NE 900 to perform one or more of the functions described herein (e.g., executing, by the processor 902, instructions stored in the memory 904). For example, the processor 902 may support wireless communication at the NE 900 in accordance with

examples as disclosed herein. The NE 900 may be configured to support a means for receiving an authentication request message that includes a SUPI for a UE in a NPN hosted by a PLMN; and limiting, based at least in part on a SUPI usage policy, usage of the SUPI in the NPN hosted by the PLMN.

[0152] Additionally, the NE 900 may be configured to support any one or combination of where limiting usage of the SUPI in the NPN comprises generating or assigning a GPSI for the UE for use in place of the SUPI; receiving the authentication request message from an AUSF; and transmitting, to the AUSF, the GPSI and an SUPI usage restriction indication; where the GPSI is specific to the NPN; determining, based at least in part on the SUPI usage policy, to not disclose the SUPI; where the network equipment implements a UDM function.

[0153] In some implementations, the processor 902 and the memory 904 coupled with the processor 902 may be configured to cause the NE 900 to perform one or more of the functions described herein (e.g., executing, by the processor 902, instructions stored in the memory 904). For example, the processor 902 may support wireless communication at the NE 900 in accordance with examples as disclosed herein. The NE 900 may be configured to support a means receiving, from a UDM function, an authentication response message that includes a GPSI for a UE in a NPN hosted by a PLMN and a SUPI usage restriction indication; receiving, from a SEAF an authentication request; and transmitting, to the SEAF based at least in part on the SUPI usage restriction indication, an authentication response that includes the GPSI for the UE and the SUPI for the UE.

[0154] Additionally, the NE 900 may be configured to support any one or combination of where the authentication response includes the SUPI usage restriction indication; where the network equipment implements an AUSF.

[0155] In some implementations, the processor 902 and the memory 904 coupled with the processor 902 may be configured to cause the NE 900 to perform one or more of the functions described herein (e.g., executing, by the processor 902, instructions stored in the memory 904). For example, the processor 902 may support wireless communication at the NE 900 in accordance with examples as disclosed herein. The NE 900 may be configured to support a means for transmitting, to an AUSF, an authentication request for a UE in a NPN hosted by a PLMN; and receiving, from the AUSF, an authentication response that includes a GPSI for the UE and a SUPI for the UE.

[0156] Additionally, the NE 900 may be configured to support any one or combination of where the authentication response includes an SUPI usage restriction indication for the SUPI; using the GPSI rather than the SUPI for context identification and management for the UE; where the network equipment implements a SEAF.

[0157] Additionally, or alternatively, the NE 900 may support at least one memory (e.g., the memory 904) and at least one processor (e.g., the processor 902) coupled with the at least one memory and configured to or operable to cause the NE to receive an authentication request message that includes a SUPI for a UE in a NPN hosted by a PLMN; limit, based at least in part on a SUPI usage policy, usage of the SUPI in the NPN hosted by the PLMN.

[0158] Additionally, the NE 900 may be configured to support any one or combination of where to limit usage of the SUPI in the NPN, the at least one processor is further configured to or operable to cause the NE to generate or assign a GPSI for the UE for use in place of the SUPI; where the at least one processor is further configured to or operable to cause the NE to receive the authentication request message from an AUSF; and transmit, to the AUSF, the GPSI and an SUPI usage restriction indication; where the GPSI is specific to the NPN; where the at least one processor is further configured to or operable to cause the NE to determine, based at least in part on the SUPI usage policy, to not disclose the SUPI; where the NE implements a UDM function.

[0159] Additionally, or alternatively, the NE 900 may support at least one memory (e.g., the memory 904) and at least one processor (e.g., the processor 902) coupled with the at least one memory and configured to or operable to cause the NE to receive an authentication response message that includes a GPSI for a UE in a NPN hosted by a PLMN and a SUPI usage restriction indication; receive, from a SEAF an authentication request; transmit, to the SEAF based at least in part on the SUPI usage restriction indication, an authentication response that includes the GPSI for the UE and the SUPI for the UE.

[0160] Additionally, the NE 900 may be configured to support any one or combination of where the authentication response includes the SUPI usage restriction indication; where to receive the authentication response message, the at least one processor is further configured to receive the authentication response message from a UDM function; where the NE implements an AUSF.

[0161] Additionally, or alternatively, the NE 900 may support at least one memory (e.g., the memory 904) and at least one processor (e.g., the processor 902) coupled with the at least one memory and configured to or operable to cause the NE to transmit, to an AUSF, a authentication request for a UE in a NPN hosted by a PLMN; receive, from the AUSF, an authentication response that includes a GPSI for the UE and a SUPI for the UE.

[0162] Additionally, the NE 900 may be configured to support any one or combination of where the authentication response includes an SUPI usage restriction indication for the SUPI; where the at least one processor is further configured to or operable to cause the NE to use the GPSI rather than the SUPI for context identification and management for the UE; where the NE implements a SEAF.

[0163] The controller 906 may manage input and output signals for the NE 900. The controller 906 may also manage peripherals not integrated into the NE 900. In some implementations, the controller 906 may utilize an operating system such as iOS®, ANDROID®, WINDOWS®, or other operating systems. In some implementations, the controller 906 may be implemented as part of the processor 902.

[0164] In some implementations, the NE 900 may include at least one transceiver 908. In some other implementations, the NE 900 may have more than one transceiver 908. The transceiver 908 may represent a wireless transceiver. The transceiver 908 may include one or more receiver chains 910, one or more transmitter chains 912, or a combination thereof.

[0165] A receiver chain 910 may be configured to receive signals (e.g., control information, data, packets) over a wireless medium. For example, the receiver chain 910 may include one or more antennas to receive a signal over the air or wireless medium. The receiver chain 910 may include at least one amplifier (e.g., a low-noise amplifier (LNA)) configured to amplify the received signal. The receiver chain 910 may include at least one demodulator configured to demodulate the receive signal and obtain the transmitted data by reversing the modulation technique applied during transmission of the signal. The receiver chain 910 may include at least one decoder for decoding the demodulated signal to receive the transmitted data.

[0166] A transmitter chain 912 may be configured to generate and transmit signals (e.g., control information, data, packets). The transmitter chain 912 may include at least one modulator for modulating data onto a carrier signal, preparing the signal for transmission over a wireless medium.

The at least one modulator may be configured to support one or more techniques such as amplitude modulation (AM), frequency modulation (FM), or digital modulation schemes like phase-shift keying (PSK) or quadrature amplitude modulation (QAM). The transmitter chain 912 may also include at least one power amplifier configured to amplify the modulated signal to an appropriate power level suitable for transmission over the wireless medium. The transmitter chain 912 may also include one or more antennas for transmitting the amplified signal into the air or wireless medium.

[0167] Figure 10 illustrates a flowchart of a method in accordance with aspects of the present disclosure. The operations of the method may be implemented by a NE as described herein. In some implementations, the NE may execute a set of instructions to control the function elements of the NE to perform the described functions.

[0168] At 1002, the method may include receiving an authentication request message that includes a SUPI for a UE in a NPN hosted by a PLMN. The operations of 1002 may be performed in accordance with examples as described herein. In some implementations, aspects of the operations of 1002 may be performed by a NE as described with reference to Figure 9.

[0169] At 1004, the method may include limiting, based at least in part on a SUPI usage policy, usage of the SUPI in the NPN hosted by the PLMN. The operations of 1004 may be performed in accordance with examples as described herein. In some implementations, aspects of the operations of 1004 may be performed by a NE as described with reference to Figure 9.

[0170] Figure 11 illustrates a flowchart of a method in accordance with aspects of the present disclosure. The operations of the method may be implemented by a NE as described herein. In some implementations, the NE may execute a set of instructions to control the function elements of the NE to perform the described functions.

[0171] At 1102, the method may include receiving, from a UDM function, an authentication response message that includes a GPSI for a UE in a NPN hosted by a PLMN and a SUPI usage restriction indication. The operations of 1102 may be performed in accordance with examples as described herein. In some implementations, aspects of the operations of 1102 may be performed by a NE as described with reference to Figure 9.

[0172] At 1104, the method may include receiving, from a SEAF, an authentication request. The operations of 1104 may be performed in accordance with examples as described herein. In

some implementations, aspects of the operations of 1104 may be performed by a NE as described with reference to Figure 9.

[0173] At 1106, the method may include transmitting, to the SEAF based at least in part on the SUPI usage restriction indication, an authentication response that includes the GPSI for the UE and the SUPI for the UE. The operations of 1106 may be performed in accordance with examples as described herein. In some implementations, aspects of the operations of 1106 may be performed a NE as described with reference to Figure 9.

[0174] Figure 12 illustrates a flowchart of a method in accordance with aspects of the present disclosure. The operations of the method may be implemented by a NE as described herein. In some implementations, the NE may execute a set of instructions to control the function elements of the NE to perform the described functions.

[0175] At 1202, the method may include transmitting, to an AUSF, an authentication request for a UE in a NPN hosted by a PLMN. The operations of 1202 may be performed in accordance with examples as described herein. In some implementations, aspects of the operations of 1202 may be performed by a NE as described with reference to Figure 9.

[0176] At 1204, the method may include receiving, from the AUSF, an authentication response that includes a GPSI for the UE and a SUPI for the UE. The operations of 1204 may be performed in accordance with examples as described herein. In some implementations, aspects of the operations of 1204 may be performed by a NE as described with reference to Figure 9.

[0177] It should be noted that the method described herein describes a possible implementation, and that the operations and the steps may be rearranged or otherwise modified and that other implementations are possible.

[0178] The description herein is provided to enable a person having ordinary skill in the art to make or use the disclosure. Various modifications to the disclosure will be apparent to a person having ordinary skill in the art, and the generic principles defined herein may be applied to other variations without departing from the scope of the disclosure. Thus, the disclosure is not limited to the examples and designs described herein but is to be accorded the broadest scope consistent with the principles and novel features disclosed herein.

CLAIMS

What is claimed is:

1. A network equipment (NE) for wireless communication, comprising:
at least one memory; and
at least one processor coupled with the at least one memory and operable to cause the NE to:
receive an authentication request message that includes a subscription permanent identifier (SUPI) for a user equipment (UE) in a non-public network (NPN) hosted by a public land mobile network (PLMN);
limit, based at least in part on a SUPI usage policy, usage of the SUPI in the NPN hosted by the PLMN.

2. The NE of claim 1, wherein to limit usage of the SUPI in the NPN, the at least one processor is further operable to cause the NE to:
generate or assign a generic public subscription identifier (GPSI) for the UE for use in place of the SUPI.

3. The NE of claim 2, wherein the at least one processor is further operable to cause the NE to:
receive the authentication request message from an authentication server function (AUSF); and
transmit, to the AUSF, the GPSI and an SUPI usage restriction indication.

4. The NE of claim 2, wherein the GPSI is specific to the NPN.

5. The NE of claim 2, wherein the at least one processor is further operable to cause the NE to determine, based at least in part on the SUPI usage policy, to not disclose the SUPI.

6. The NE of claim 1, wherein the NE implements a unified data management (UDM) function.

7. A network equipment (NE) for wireless communication, comprising:
at least one memory; and
at least one processor coupled with the at least one memory and operable to cause the NE to:

receive an authentication response message that includes a generic public subscription identifier (GPSI) for a user equipment (UE) in a non-public network (NPN) hosted by a public land mobile network (PLMN) and a subscription permanent identifier (SUPI) usage restriction indication;

receive, from a security anchor function (SEAF) an authentication request;

transmit, to the SEAF based at least in part on the SUPI usage restriction indication, an authentication response that includes the GPSI for the UE and the SUPI for the UE.

8. The NE of claim 7, wherein the authentication response includes the SUPI usage restriction indication.

9. The NE of claim 7, wherein to receive the authentication response message, the at least one processor is further configured to receive the authentication response message from a unified data management (UDM) function.

10. The NE of claim 7, wherein the NE implements an authentication server function (AUSF).

11. A network equipment (NE) for wireless communication, comprising:

at least one memory; and

at least one processor coupled with the at least one memory and operable to cause the NE to:

transmit, to an authentication server function (AUSF), an authentication request for a user equipment (UE) in a non-public network (NPN) hosted by a public land mobile network (PLMN);

receive, from the AUSF, an authentication response that includes a generic public subscription identifier (GPSI) for the UE and a subscription permanent identifier (SUPI) for the UE.

12. The NE of claim 11, wherein the authentication response includes an SUPI usage restriction indication for the SUPI.

13. The NE of claim 11, wherein the at least one processor is further operable to cause the NE to:

use the GPSI rather than the SUPI for context identification and management for the UE.

14. The NE of claim 11, wherein the NE implements a security anchor function (SEAF).

15. A method performed by a network equipment, the method comprising:

receiving an authentication request message that includes a subscription permanent identifier (SUPI) for a user equipment (UE) in a non-public network (NPN) hosted by a public land mobile network (PLMN); and

limiting, based at least in part on a SUPI usage policy, usage of the SUPI in the NPN hosted by the PLMN.

16. The method of claim 15, wherein limiting usage of the SUPI in the NPN comprises:

generating or assigning a generic public subscription identifier (GPSI) for the UE for use in place of the SUPI.

17. The method of claim 16, further comprising:

receiving the authentication request message from an authentication server function (AUSF); and

transmitting, to the AUSF, the GPSI and an SUPI usage restriction indication.

18. The method of claim 16, wherein the GPSI is specific to the NPN.

19. The method of claim 16, further comprising determining, based at least in part on the SUPI usage policy, to not disclose the SUPI.

20. The method of claim 15, wherein the network equipment implements a unified data management (UDM) function.