

CERTIFICATE OF AVAILABILITY OF A CERTIFIED PATENT DOCUMENT IN A DIGITAL LIBRARY

The International Bureau certifies that a copy of the patent application indicated below has been available to the WIPO Digital Access Service since the date of availability indicated, and that the patent application has been available to the indicated Office(s) as of the date specified following the relevant Office code:

Document details: Country/Office: US

Filing date: 25 Jul 2017 (25.07.2017)

Application number: 62536632

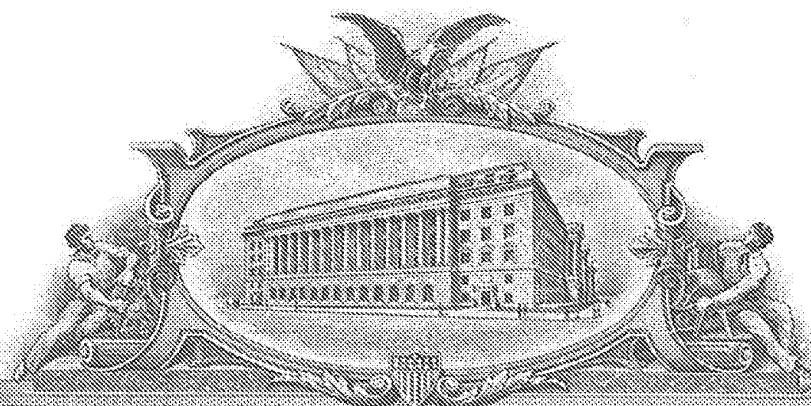
Date of availability of document: 22 Aug 2017 (22.08.2017)

The following Offices can retrieve this document by using the access code:

JP, US, SE, NZ, KR, EA, IN, BR, GB, AU, ES, NL, IB, EE, CN, MA,
FI, DK

Date of issue of this certificate: 06 Aug 2018 (06.08.2018)

34, chemin des Colombettes
1211 Geneva 20, Switzerland
www.wipo.int



THE UNITED STATES OF AMERICA

TO ALL TO WHOM THESE PRESENTS SHALL COME:

UNITED STATES DEPARTMENT OF COMMERCE

United States Patent and Trademark Office

August 06, 2018

THIS IS TO CERTIFY THAT ANNEXED HERETO IS A TRUE COPY FROM THE RECORDS OF THE UNITED STATES PATENT AND TRADEMARK OFFICE OF THOSE PAPERS OF THE BELOW IDENTIFIED PATENT APPLICATION THAT MET THE REQUIREMENTS TO BE GRANTED A FILING DATE UNDER 35 USC 111.

APPLICATION NUMBER: 62/536,632
FILING DATE: *July 25, 2017*

THE COUNTRY CODE AND NUMBER OF YOUR PRIORITY APPLICATION, TO BE USED FOR FILING ABROAD UNDER THE PARIS CONVENTION, IS *US62/536,632*



Certified by

Andres Ibarra

Under Secretary of Commerce
for Intellectual Property
and Director of the United States
Patent and Trademark Office

ENABLING SUBSCRIPTION IDENTIFIER PRIVACY

TECHNICAL FIELD

[0001] Embodiments of the present disclosure generally relate to the field of wireless communication network security, and more particularly to ensuring that a subscription identifier of a user equipment can be communicated securely within the wireless communication network.

BACKGROUND

[0002] It is important to maintain the confidentiality of a user equipment's (UE's) long-term subscription identifier (e.g., an IMSI (International Mobile Subscriber Identity)). Early generation 3GPP systems (e.g., 4G/LTE, 3G/UMTS, 2G/GSM) included a partial mechanism for long-term subscription identifier confidentiality using one or more short-term subscription identifiers. GUTI (Globally Unique Temporary ID) and C-RNTI (Cell-Radio Network Temporary Identifier) are examples of short-term subscription identifiers in 4G/LTE systems. However, the legacy partial mechanism may expose the long-term subscription identifier in clear text over the air interface. For example, so-called "IMSI catchers" could simply ask the long-term identifier from the UE, e.g., using identifier request/response messages.

DETAILED DESCRIPTION

[0003] Figure 0 illustrates an example wireless communication network that includes a UE, a serving network, and a home network. The UE and home network are both communicatively connected to, and exchange signals with each other via, the serving network. The UE is configured with a subscription identifier identifying a subscription supported by the home network, and accesses the home network using the serving network.



FIG. 0

[0004] Typical examples of the UE include a mobile equipment (ME), mobile terminal, smartphone, personal computer, a laptop computer, a desktop computer, a workstation, a tablet computer, a wearable computer, and/or a smart appliance. According to particular embodiments of the UE, the UE may comprise a general memory storage as part of an ME, and a tamper resistant secure hardware component providing secure storage, such as a 5G-USIM (Universal Subscriber Identity Module), a UICC (Universal Integrated Circuit Card) and/or other secure storage device. According to such embodiments, any of the capabilities attributed to the UE, generally, may be performed using the tamper resistant secure hardware component of the UE.

[0005] The serving network includes one or more physical devices and/or signaling mediums capable of exchanging communication signals with the UE and the home network. In particular, the serving network may include hardware that provides one or more: access points (e.g., a base station, eNodeB, femtocell, and/or wireless access point), access networks, authentication servers, Access and Mobility management Functions (AMFs), Security Anchor Functions (SEAFs), Authentication Server Functions (AUSFs), and/or any combination thereof (not shown). In particular, an authentication server may provide one or more AMFs, SEAFs, AUSFs, and/or any combination thereof. Particular of these network entities will be discussed in further detail below.

[0006] The home network includes one or more physical devices and/or signaling mediums capable of exchanging communication signals with the UE via the serving network. In particular, the home network may include one or more: de-concealing servers, authentication servers (e.g., as described above), key provisioning servers, Subscription Identifier De-concealing Functions (SIDFs), Privacy Key Provisioning Functions (PKPFs), Unified Data Management (UDM) and/or any combination thereof (not shown). In particular, a de-concealing server may provide one or more SIDFs, PKPFs, and/or any combination thereof. Particular of these network entities will also be discussed in further detail below.

[0007] Examples of the serving and/or home network include (but are not limited to) one or more: local area networks, wireless networks; cellular networks; Internet Protocol-based networks; Ethernet networks; optical networks; and/or circuit switched networks. Such networks may comprise any number of networking devices such as routers, gateways, switches, hubs, firewalls, and the like (not shown) supporting the exchange of such communication signals.

[0008] Although Figure 0 illustrates separate serving and home networks, in some embodiments of the present disclosure, the home network is the serving network. Further, although examples of particular functions in either the home network or the serving network were specified above, those particular functions may be in the other of the home network or serving network according to particular embodiments. Further still, although only one UE is illustrated in Figure 0, the serving and home networks may support a plurality of UEs, according to particular embodiments.

[0009] One example way to maintain the confidentiality of a UE's long-term subscription identifier is to protect the long-term subscription identifier using the home network public key. The home network public key may be provisioned within the UE without a certificate, such that a global public key infrastructure (PKI) or certificate authority (CA) is not required (i.e., because the technique is used asymmetrically between the UE and a function in the home network). In

such an example, the UE may be expected to encrypt the long-term subscription identifier, when transmitted towards the home network, using the home network public key.

[0010] Figure 1 illustrates one such particular example in which the UE encrypts its long-term subscription identifier as part of an attachment procedure. According to the example of Figure 1, the UE encrypts its IMSI, leaving its MCC (Mobile Country Code) and MNC (Mobile Network Code) parts in clear-text, and sends an Attach Request to the serving network with the encrypted IMSI as its identifier (step 1). The serving network identifies the UE's home network using clear-text MCC/MNC and requests authentication information from the UE's home network using the encrypted IMSI as the UE's identifier (step 2). The home network decrypts the IMSI from the encrypted IMSI and fetches the corresponding authentication information. In response to the authentication information request, the home network sends the UE's authentication information along with the clear-text IMSI to the serving network (step 3). The serving network performs an authentication procedure with the UE to authenticate the UE (step 4). If the authentication procedure succeeds, the serving network sends an Attach Accept message to the UE (step 5).

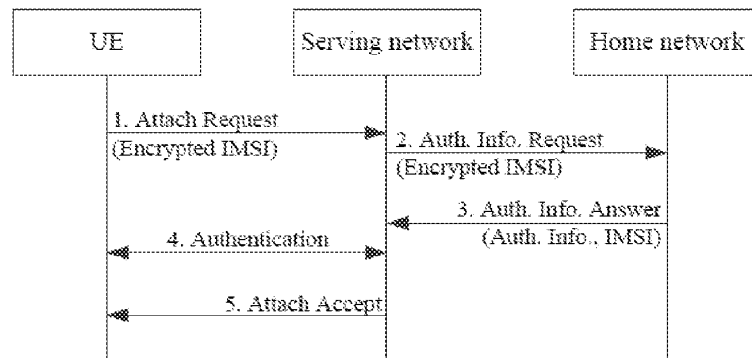


FIG. 1

[0011] In such an approach, the home network public key may be pre-provisioned in a USIM and/or may be provisioned using an OTA (Over-the-Air) provisioning procedure. Although the approach illustrated in Figure 1 does protect the long-term subscription identifier in at least

some embodiments, some such embodiments may include one or more deficiencies. For example, the approach illustrated in Figure 1 may be frustrated by legacy USIMs that cannot be feasibly changed, certain home operators that may not support OTA provisioning, and/or USIMs that may not be updatable (e.g., due to technical limitations, lack of storage space, or other limitations).

[0012] Various embodiments of the present disclosure provide alternatives to at least some aspects of the particular embodiment illustrated in Figure 1. Particular embodiments enable the public key of the home network to be provisioned (e.g., newly or refreshed) and stored in the UE, such that the UE is able to encrypt its subscription identifier with this public key. Moreover, in particular embodiments, the core network (such as a 5GC (5G core) network) triggers the provisioning of the home network public key over existing traffic procedures defined by 3GPP (e.g., registration/authentication signaling) without the need to rely on additional infrastructure and out-of-band procedures such as performing an OTA update procedure.

[0013] Although various embodiments herein will describe certain features or actions performed by a UE, it should not be presumed that such features or actions are performed by any particular component of the UE unless otherwise specified. For example, such functions may or may not be performed by a UICC, USIM, or other circuitry and/or software of the UE, depending on the particular embodiment.

[0014] Particular embodiments include a Subscription Permanent Identifier (SUPI). A SUPI is a clear-text, globally unique, 5G, permanent identifier allocated to each subscriber in a 5G system. The SUPI may be IMSI-based or non-IMSI based. Embodiments that include an IMSI-based SUPI may use the IMSI as described in 3GPP TS 23.003, for example. Embodiments that include a non-IMSI based SUPI may be based on a Network Access Identifier (NAI) according to the NAI IETF RFC 4282 based user identification described in 3GPP TS 23.003. In some embodiments, the the SUPI contains the address of the home network (e.g. the MCC and MNC in the case of an IMSI based SUPI). Such embodiments

may enable certain roaming scenarios, e.g., by providing the serving network with information useful for identifying the UE's home network.

[0015] Particular embodiments additionally or alternatively include a Subscription Concealed Identifier (SUCI), such as illustrated in the example of Figure 2. A SUCI is a protected version of a SUPI. The SUCI includes a clear-text part and an encrypted part.

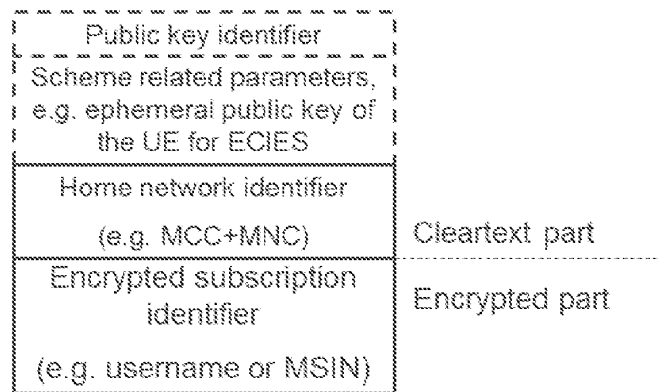


FIG. 2

[0016] The clear-text part includes a home network identifier that identifies the home network of the UE. For example, the SUCI may include an MCC and MNC of the home network. The clear-text part may also include a public key identifier, an encryption scheme identifier, and/or scheme related parameters useful for decrypting the encrypted part of the SUCI according to an encryption scheme, such as an ephemeral public key of the UE or other parameters for use in Elliptic Curve Integrated Encryption Scheme (ECIES) or other encryption scheme. As will be discussed below, the public key identifier is an identifier that may be used within the home network to identify the correct SIDF (Subscription Identifier De-concealing Function) in a home network that includes a plurality of SIDFs. The ECIES, the public key identifier, and SIDFs will be described in greater detail below.

[0017] When the encrypted part is included in the SUCI, the SUCI is a protected version of SUPI. The encrypted part includes an encrypted subscription identifier, such as an MSIN

(Mobile Subscription Identification Number) or username. Thus, decrypting the encrypted part of the SUPI may be performed to learn the corresponding SUPI. ECIES is an example of a public key encryption scheme that may be used to generate a SUCI from a SUPI and/or a SUPI from a SUCI. As will be discussed further below, the encrypted part of the SUCI may use a null encryption scheme, e.g., if the UE has not been provisioned with the public key of the home network.

[0018] A SIDF is a function located in the home network that is responsible for decrypting the SUCI. Particularly in 5G architecture, a SIDF may be co-located in UDM (Unified Data Management). Additionally or alternatively, a SIDF may be an entity separate from UDM and/or co-located with an AUSF (Authentication Server Function).

[0019] Figure 3 illustrates an example of a privacy key. This particular example of the privacy key includes a public key of the home network. In some embodiments, the privacy key also includes one or more public key scheme related parameters, the long-term subscription identifier, a subject field indicating a network, domain, or context to which the privacy key pertains (e.g., the subject may be a home network identifier, such as an MCC/MNC), a public key scheme identifier, public key scheme related domain specific values (e.g. values for the elliptic curve domain in case of ECIES scheme), the public key identifier as will be discussed in greater detail below, validity times indicating specifying when the privacy key is valid (e.g., not valid before and/or not valid after times), a key usage field indicating one or more ways the key may be used (e.g., subscription identifier privacy, slice selection privacy, etc.), and/or a digital signature calculated over some or all of the privacy key.

[subscription identifier]
(e.g. username or MSIN)
Subject (e.g. MCC/MNC or SDF identifier)
Scheme identifier: e.g. 0 (null-scheme), 1 (ECIES), etc
Public key scheme related domain specific values
Public key
Public key ID
Validity (not before)
Validity (not after)
Key usage (subscription privacy)
[Digital Signature]

FIG. 3

[0020] In particular, the key usage field may be set to indicate that the key is useful for "subscription privacy," in accordance with embodiments of the present disclosure. Uses of the privacy that are beyond the scope of the present disclosure may additionally or alternatively indicate other uses for the privacy key. For example, the private key may be used for "Network Slice Selection Assistance Information (NSSAI) privacy" purposes instead of, or in addition to, "subscription privacy" purposes. Indeed, such other purposes may include similar methods, devices, and systems in the UE and/or in the home network for initial provisioning, refresh, and other features as described herein. Although one privacy key may, in some embodiments, indicate multiple usages, other embodiments may include respective privacy keys for respective usages, the key usage field of each privacy key indicating a single key usage (e.g., one of the privacy keys may indicate "subscription privacy" and the other may indicated "NSSAI privacy"). The key usage field may be formatted as an integer, one or more

enumerated values, an alphanumeric string, a bit string, a delimited string, and/or an array of any of the above-mentioned formats, among other things.

[0021] A 3GPP public key privacy scheme (3GPK schemes) is a standardized public key scheme that a UE may support for interoperability between the UE and, e.g., a mobile operator. In absence of a standardized scheme, UE vendors would likely need to coordinate with such operators to implement privacy mechanisms. According to particular embodiments, the UE should support whichever schemes are allowed and/or standardized so that the home network is able to freely choose a scheme without creating any interoperability difficulties. One such scheme in particular is, for example, ECIES. Particular schemes may be adopted by as standard, and given an identifier (also called a "register") for interoperability. For each such scheme, any specific algorithms that need to be supported may also be specified. For example, in the case of ECIES, key agreement (KA), key derivation (KD) function (KDF), symmetric integrity, and symmetric encryption may be specified. One or more parameters relating to such a scheme, as well as (in one or more cases) their potential static values may also be specified. For example, in ECIES, elliptic curve domain parameters (p, a, b, G, n, h) for a curve over a prime field and/or $(m, f(x), a, b, G, n, h)$ for a curve over a binary field may be specified.

[0022] Figure 4 illustrates an example 3GPK scheme. Each scheme adopted as standard may be assigned a specific identifier. For example, the null-scheme may be assigned a 0, ECIES may be assigned a 1, and so on. Other embodiments may format the scheme identifier in other ways, including but not limited to one or more integers, numeric strings, alphanumeric strings, bit strings, and/or other data types.

Scheme identifier: e.g. 0 (null-scheme), 1 (ECIES), etc
Scheme specific algorithms: e.g. KA, KDF, symmetric integrity algorithm, symmetric encryption algorithm
Public key scheme related parameters and their static values

FIG. 4

[0023] According to embodiments herein, the UE registers with the wireless communication network according to a registration procedure, such as the example registration procedure illustrated in Figure 5. According to the example registration procedure illustrated in Figure 5, the UE uses a public key of the home network to conceal a long-term subscription identifier. Although one or more particular interfaces illustrated in Figure 5, such as those specified by an N followed by a numerical designation (e.g., N1, N12, N13), are in accordance with 3GPP TS 23.501, the signaling performed over such interfaces as described herein, as well as other of the interfaces themselves (e.g., Nxx), are not known or described in any known art.

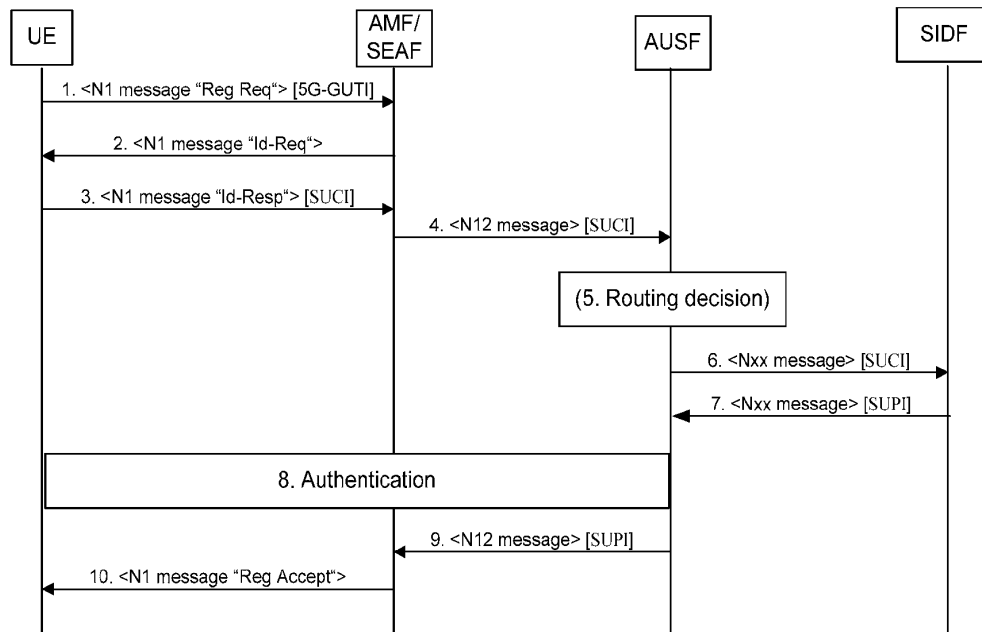


FIG. 5

[0024] According to the example of Figure 5, the UE includes a temporary identifier (e.g., a 5G-GUTI) in a registration request and sends the registration request to an AMF/SEAF (step 1). The AMF/SEAF, failing to recognize the 5G-GUTI, transmits an identifier request message to the UE to request the UE's identifier (step 2). The UE responds to the identifier request message with an identifier response message comprising a SUCI (step 3). The AMF/SEAF requests authentication of the UE from the AUSF in the home network, and includes the SUCI in the authentication request (step 4). The AUSF uses information encoded in the SUCI to determine which of a plurality of SDFs to use to decrypt at least part of the SUCI (step 5). In particular, the AUSF may use the public key identifier carried in the SUCI (or otherwise present in the authentication request message) to identify the correct SDF. In some embodiments, the AUSF may additionally or alternatively use the scheme identifier to identify the correct SDF. In other words, different SDFs may handle different encryption schemes

(e.g., a first SIDF may handle ECIES and a second SIDF may handle RSA), and the AUSF may choose an appropriate SIDF based on which scheme is identified by the SUCI.

[0025] Embodiments of the present disclosure may include multiple SIDFs to avoid having a single point of failure for networks having a large number of subscribers, for example. Consequently, distributed SIDF deployments may be advantageous to improve the fault tolerance, load balancing, and/or overall capacity of the network. Additionally or alternatively, different SDIF instances may be deployed to handle different sets of home network public keys. Accordingly, the public key identifier in the SUCI may be used to select the proper SDIF instance(s), according to one or more embodiments herein. Alternatively, in particular embodiments that only have one SIDF deployed, the public key identifier may be omitted from the SUCI.

[0026] The AUSF sends the SUCI to the selected SIDF (step 6). If the SIDF is co-located in UDM (such that the Nxx message is a N13 message, for example), then the same message may be used to request an authentication vector or authentication credentials from the UDM. The SIDF decrypts the SUCI to obtain a corresponding SUPI, and returns the SUPI to the AUSF (step 7). If the SIDF is co-located in UDM, then the same message may be used to return authentication vector/credentials to AUSF.

[0027] AUSF and UE exchange authentication messages using authentication vectors/credentials received from UDM (step 8). If the AUSF has not already received the required authentication vector/credentials from UDM (e.g., in step 7 discussed above), the AUSF may request authentication vector/credentials from UDM before initiating authentication with the UE (not shown). Alternatively, the AUSF may have delegated the authentication to SEAF. In such embodiments, the AUSF may simply forward the SUPI to the SEAF in this step, and rely on the SEAF to perform the authentication in the next step.

[0028] Continuing with the example in which the AUSF successfully authenticates the UE, the AUSF returns the SUPI to the AMF/SEAF (step 9). The AMF/SEAF accepts the registration of the UE and transmits a registration acceptance message to the UE (step 10).

[0029] As briefly discussed above, particular features of the UE may be performed by a tamper resistant secure hardware component of the UE. Figure 6 illustrates a particular example in which a 5G-USIM/UICC of an ME generates the SUCI. Although this particular example uses the term 5G-USIM/UICC, this term should not be considered as limiting with respect to any version or vendor of USIM or UICC technology, nor should this term be considered as limiting with respect to any generation of mobile network, e.g., 2G/3G/4G/5G.

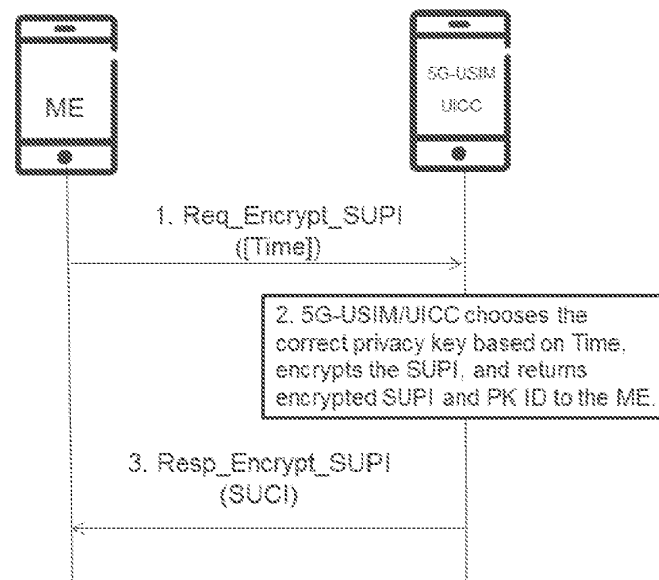


FIG. 6

[0030] According to the example of Figure 6, the ME requests a SUCI (step 1). In some such embodiments, this SUCI request may include the time. In other such embodiments, the request may simply be a read operation from the UICC. According to such embodiments in which there are multiple home network public keys, the 5G-USIM/UICC chooses the correct corresponding privacy key (e.g., based on the time), and generates the SUCI using the selected

privacy key (step 2). Alternatively, if such embodiments in which there is only one privacy key, the 5G-USIM/UICC simply uses that privacy key. The 5G-USIM/UICC then returns the SUCI to the ME (step 3).

[0031] Figure 7 illustrates an example in which the 5G-USIM/UICC does not have a privacy key, or does not support the feature.

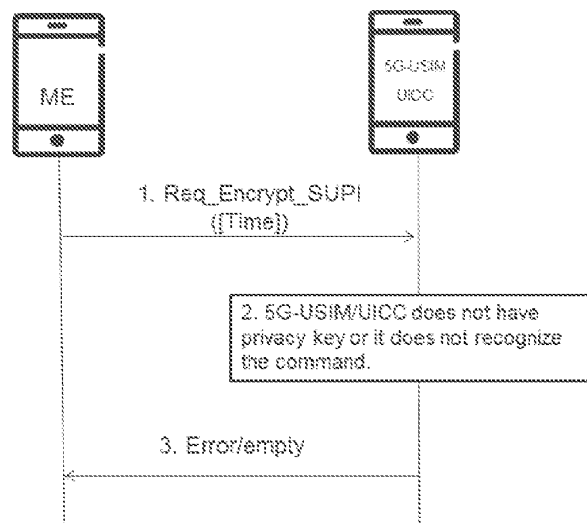


FIG. 7

[0032] According to the example of Figure 7, the ME requests a SUCI with a request (which may include the time, in some embodiments) in similar fashion as described above with respect to Figure 6. In this example, however, the 5G-USIM/UICC does not have privacy key or does not recognize the command because it does support the feature (step 2). Accordingly, the 5G-USIM/UICC returns an error message (or empty data) to the ME (step 3).

[0033] Alternatively to the example of Figure 7, the ME may know that 5G-USIM/UICC does not have privacy key or does not support privacy key by other means, according to particular embodiments. For example, the ME may obtain the version and or vendor information of 5G-USIM/UICC and determine, based on this information, that a privacy key is not supported or

present. As another example, the ME may determine that a privacy key is not supported or present in 5G-USIM/UICC based on some other response message from the 5G-USIM/UICC.

[0034] Figure 8 illustrates an example in which the ME generates the SUCI, but the privacy key itself is stored in the 5G-USIM/UICC.

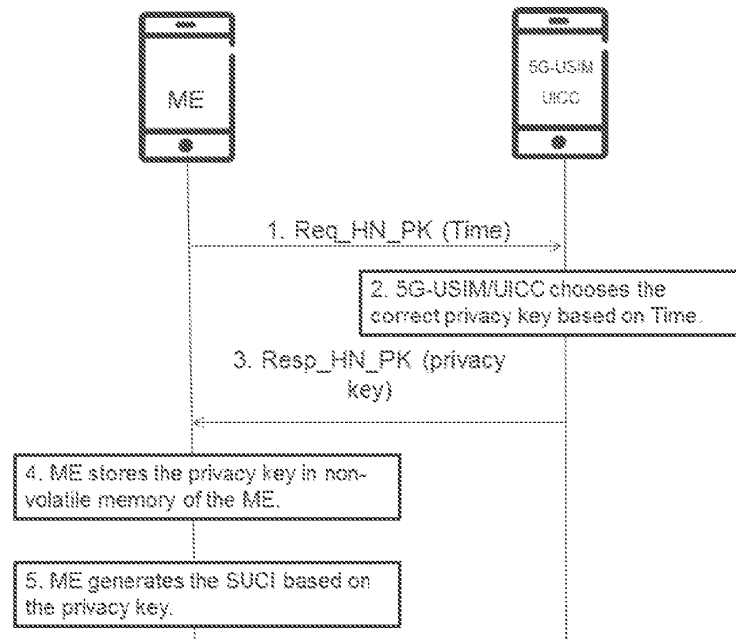


FIG. 8

[0035] According to the example of Figure 8, the ME has no privacy key and requests one from the 5G-USIM/UICC (step 1). In some embodiments, the request includes the time. In other embodiments, the request is a direct read operation from the 5G-USIM/UICC memory. The 5G-USIM/UICC then chooses the privacy key (e.g., based on time, if provided in the request) (step 2). The 5G-USIM/UICC returns the privacy key to the ME (step 3). At this point, the ME may, in some embodiments (but not necessarily all embodiments) store the privacy key and/or the SUPI to a non-volatile memory of the ME (step 4). The ME then generates the SUCI based on the SUPI and the privacy key (step 5).

[0036] Figure 9 illustrates an example in which the ME gets notified if the privacy key is updated in the 5G-USIM/UICC. In this scenario, the ME subscribes to changes in the privacy keys, and gets notifications when updates are available. This scenario assumes that the ME stores the privacy key or asks the 5G-USIM/UICC for the privacy key as needed to obtain the latest privacy key.

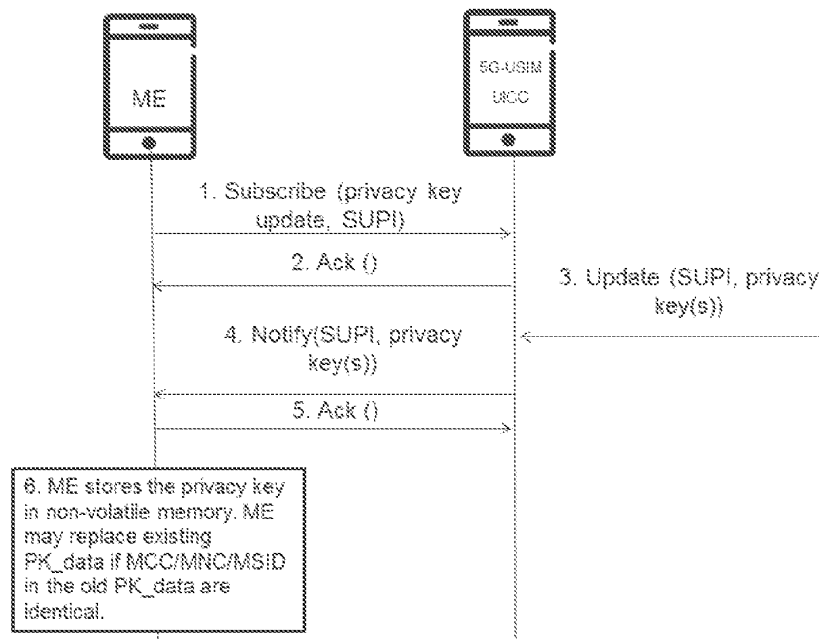


FIG. 9

[0037] According to the example of Figure 9, the ME sends a request to the 5G-USIM/UICC requesting to subscribe to privacy key updates (step 1). The request may, in some embodiments, include a SUPI. The 5G-USIM/UICC accepts the subscription and transmits an acknowledgement to the ME in response (step 2). When the home network updates the privacy key(s) or delivers one or more new ones to the 5G-USIM/UICC (step 3), the 5G-USIM/UICC notifies the ME that one or more new privacy keys are available (step 4). Although Figure 9 depicts the notification message including the privacy key, according to other embodiments, the ME may alternatively read the key from the 5G-USIM/UICC based on the notification. The ME

acknowledges the notification (step 5). The ME then stores the new privacy key(s) to the non-volatile memory of the ME (step 6).

[0038] Figure 10 illustrates an example in which the UE is powered on, and the ME detects that the 5G-USIM/UICC has been replaced (e.g., with a different 5G-USIM/UICC, or simply removed and reinserted, according to various embodiments). Although particular embodiments may treat replacement with a different 5G-USIM/UICC the same as a removal and reinsertion (e.g., for security reasons), other embodiments may respond differently based on which of these two scenarios is detected.

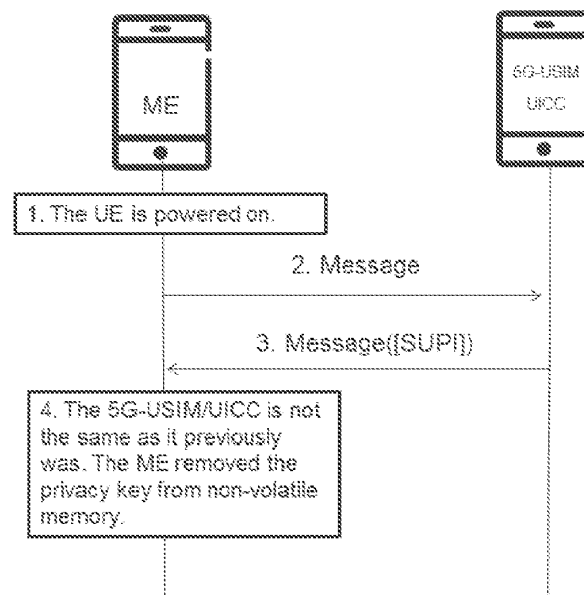


FIG. 10

[0039] According to the example of Figure 10, the UE is powered on (step 1). The ME sends a message to the 5G-USIM/UICC (step 2) and the 5G-USIM/UICC responds in a manner that is inconsistent with when the UE was previously powered on (step 3). For example, the response message may include a different SUPI than any previously seen by the ME.

[0040] The ME determines that the 5G-USIM/UICC has been replaced (step 4). For example, the 5G-USIM/UICC may be different in some way from the previous time when the

UE was powered on, indicating that the 5G-USIM/UICC has been replaced with a different one. Alternatively, the ME may detect that the 5G-USIM/UICC has been replaced using non-volatile memory that is updated by a mechanical, electrical, or software mechanism, such as an optical sensor, switch, weight sensor, pressure sensor, and/or electrical circuitry that is triggered when 5G-USIM/UICC is removed and/or inserted, e.g., regardless of whether the same 5G-USIM/UICC or a different one has been removed and reinserted.

[0041] The ME removes the privacy key it had previously stored from the non-volatile memory (if there is one). Additionally or alternatively, if the ME stored the SUPI of the old 5G-USIM/UICC with the privacy key to its memory, the ME may decide to remove the privacy key from the non-volatile memory based on a comparison of the SUPI returned by the new 5G-USIM/UICC with the SUPI stored with the old privacy key.

[0042] Particular embodiments described above describe ways in which the devices within a wireless communication system may securely exchange a subscription identifier, including the generation and use of particular data structures and corresponding encryption/decryption schemes. In particular, embodiments described above allow for this secure exchange to be performed as part of registering the UE with the wireless communication network. Many such embodiments presume that the UE is provisioned with a valid privacy key.

[0043] To ensure that the UE does, in fact, have a valid privacy key, further embodiments of the present disclosure describe ways in which to provision the UE. Particular embodiments relating to provisioning may include Privacy Key Verification Data (MAC-P). As shown in the example of Figure 11, a MAC-P includes a message authentication code (MAC). The MAC is calculated based on the privacy key and a provisioning key (which will be explained in greater detail below). For example, the MAC may be calculated over the various fields of the privacy key, including but not limited to the home network public key and its related parameters as described above, in combination with the provisioning key.

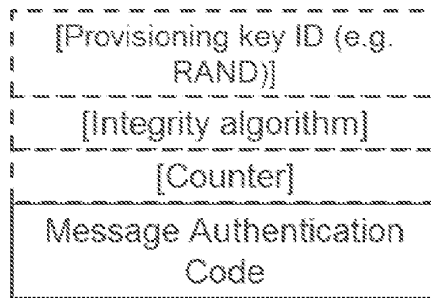


FIG. 11

[0044] The MAC-P may, according to some embodiments, also include a provisioning key identifier (e.g. a RAND) and/or an integrity protection algorithm identifier. According to some embodiments in which the MAC-P does not include the integrity protection algorithm identifier, the integrity protection algorithm to be used may be identified separately from the MAC-P, or a predefined Key Derivation Function (KDF) KDF such as, e.g., HMAC-SHA-256 may be used. The MAC-P may additionally or alternatively include a counter field, which may be used to identify the MAC-P from a plurality of MAC-Ps (e.g., in cases where more than one MAC-P is calculated using the same provisioning key). The relationship between the privacy key (e.g., as shown in Figure 3) and the MAC-P (e.g., as shown in Figure 11) is further explained below with respect to Figure 14.

[0045] The provisioning key is a secret shared between the UE and a PKPF, which is described in further detail below. The provisioning key is UE-specific. In some embodiments, the provisioning key may be derived from the home network master key that is created when the UE authenticates with the network. In some such embodiments, the AUSF may have the home network master key. Further, a new home network master key may be created when the UE re-authenticates.

[0046] According to one example, the provisioning key may be created from a CK (Confidentiality Key), IK (Integrity Key) (e.g., by applying a KDF such as HMAC-SHA-256 or other secure one-way hash function, such as SHA-256). As the same home network master

key may be used to derive numerous keys, embodiments of the present disclosure use at least one further standard parameter in combination with the home network master key as input for deriving the provisioning key. For example, when standard KDF is used, the FC (Function Code) may be used as an input (e.g., as specified in TS 33.220) to produce a provisioning key that is distinguishable from other keys produced using the home network master key.

[0047] According to another example, the provisioning key may be a key which is same as, or derived from, an ephemeral shared key that is shared between the SIDF and the UE, particularly when the encryption scheme used is a hybrid public key scheme such as ECIES. For example, ECIES uses a public key mechanism (e.g., Diffie–Hellman) for key agreement that results in a shared key, which is ephemeral, between the SIDF and the UE. That ephemeral shared key, for security purposes, is generally processed further through a key derivation function (e.g., SHA-256) to derive yet other derived shared keys between the SIDF and the UE (e.g., encryption key and MAC key in ECIES). One of these other derived shared keys is generally used for encryption and is called the ephemeral encryption key. As applied to embodiments of the present disclosure, one of these other derived shared keys may be used, e.g., to generate a SUCI from a SUPI. Further, in some embodiments, another of the derived shared keys (e.g., MAC key in ECIES), a new one further derived from one of the derived shared keys, or yet another key derived from the ephemeral shared key, may be used as the provisioning key. In some embodiments in which the SIDF has, or is able to obtain/derive the provisioning key, the SIDF may also calculate the MAC or MAC-P.

[0048] A PKPF is a function located in the home network that is responsible for provisioning the privacy key. According to particular embodiments, the PKPF may be co-located with the AUSF, and particularly in at least some embodiments in which the provisioning key is derived from the home network master key that is created based on primary authentication between UE and the network. In other embodiments, the PKPF may be collocated with other 5GC entities, such as UDM. According to yet other embodiments, the

PKPF is its own separate entity. In some embodiments, the SIDF and PKPF are implemented together as a single function, and there is no need to transfer the provisioning key. In some other embodiments, the PKPF may obtain the provisioning key from the SIDF. The PKPF may also obtain the MAC/MAC-P from the SIDF.

[0049] Figure 12 illustrates an example UE Registration process in which the UE has no valid privacy key. For example, the end-user may have inserted a new USIM/UICC into the UE, and this new USIM/UICC does not contain a privacy key.

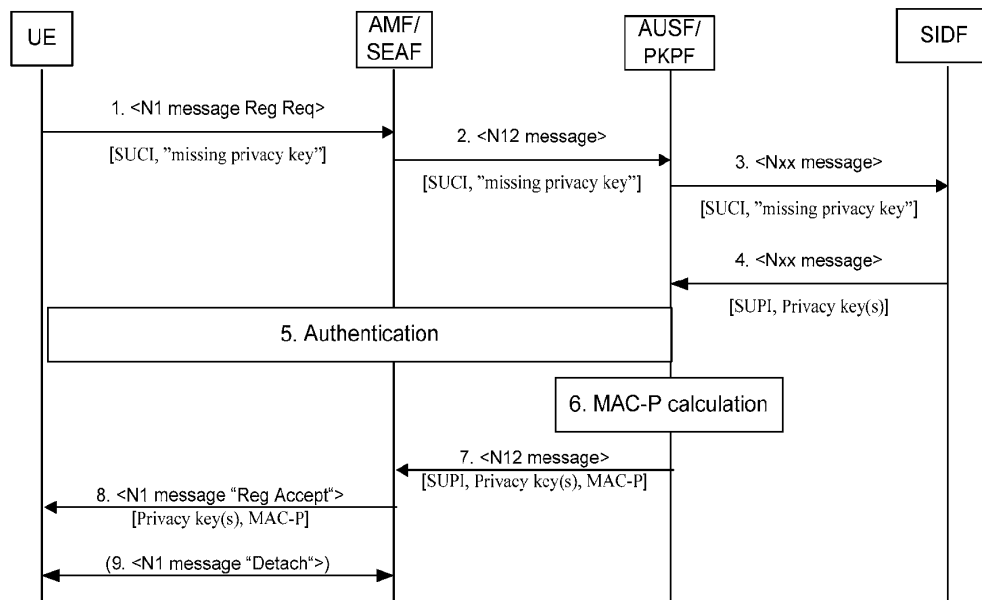


FIG 12

[0050] According to the example illustrated in Figure 12, the UE sends a Registration request to an AMF/SEAF, including a SUCI in the request (step 1). Because the UE initially has no privacy key in this scenario, the UE uses a null-scheme or null-encryption method to create the SUCI. Further, because the UE has no privacy key that would indicate the null-scheme or null-encryption method (which the home network may be free to choose, according to embodiments), an explicit or implicit indicator that the actual privacy key is missing from the

UE may be used, according to particular embodiments. For example, as discussed above, the SUCI may use a null encryption scheme for the encrypted part, which may implicitly signal that the privacy key is missing. Alternatively, a "missing privacy key" indicator may be, e.g., a standardized or well-known public key identifier value, a flag and/or a message type indicator (e.g., a registration request of type "privacy provisioning" or "pre initial registration").

[0051] The AMF/SEAF, having received the registration request, requests UE authentication from the AUSF/PKPF (step 2). The AUSF sends the SUCI (and the "missing privacy key" indicator, if one was included in the authentication request) to an SIDF (step 3). According to embodiments in which the SIDF is co-located in UDM (e.g., the Nxx message is a N13 message), then the same message may be used to request an authentication vector/credentials from the UDM.

[0052] The SIDF sees that the SUCI is in cleartext, and that the UE is missing a privacy key. According to this example, the SIDF has a local policy that all SUCIs must be protected using ECIES. Accordingly, the SIDF returns a SUPI to the AUSF, together with a request to provision the ECIES privacy key to the UE (step 4). In some embodiments, the response includes multiple privacy keys to be provisioned to the UE. According to embodiments in which the SIDF is co-located in UDM, then the same message may be used to return the authentication vector/credentials to the AUSF.

[0053] According to embodiments in which the AUSF has not received the authentication vector/credentials from UDM already, the AUSF may request said authentication vector/credentials from UDM before initiating the authentication with the UE (not shown). Alternatively, according to embodiments in which the AUSF has received the authentication vector/credentials from UDM already, the AUSF and UE exchange authentication messages using said authentication vectors/credentials (step 5). Alternatively, the AUSF may have delegated the authentication to the AMF/SEAF.

[0054] According to this example, a PKPF is co-located with the AUSF. Consequently, upon successful authentication, the AUSF/PKPF creates a provisioning key that may be used to protect the privacy key provisioning message to the UE, i.e., without the need to exchange signaling to transfer the provisioning key. According to other embodiments in which the AUSF and PKPF are not co-located, the AUSF may request that the provisioning key be generated by the PKPF and the PKPF may transfer the provisioning key to the AUSF in response (not shown).

[0055] The AUSF/PKPF protects the privacy key(s) (received from SIDF in step 4) with the provisioning key by calculating a MAC (e.g., as described above with respect to Figure 11) and constructing MAC-P (step 6). In some embodiments, the privacy key may also be encrypted. In some embodiments, the AUSF/PKPF may receive the MAC and/or MAC-P from the SIDF, as described above, particularly in at least some embodiments in which the provisioning key is based on the ephemeral shared key of, e.g., an EICES scheme. In particular, as discussed above, the SIDF may have generated the MAC and/or MAC-P.

[0056] The AUSF then returns the SUPI, the privacy key(s), and the MAC-P to AMF/SEAF (step 7). In some embodiments, the SUPI, the privacy key(s), and/or the MAC-P are transmitted to the AMF/SEAF in the same registration related message flow for registering the UE with the wireless communication network. In some embodiments, the SUPI, the privacy key(s), and/or the MAC-P are transmitted to the AMF/SEAF in a separate message flow (not shown).

[0057] According to embodiments in which the AUSF delegated authentication of the UE to the AMF/SEAF, the AMF/SEAF may authenticate the UE at this point (not shown). In such embodiments, the AMF/SEAF may have received the SUPI, the privacy key(s), and the MAC-P previously, e.g., directly from the SIDF in step 4.

[0058] The AMF/SEAF accepts the registration of the UE, and forwards the privacy key(s) and the MAC-P to the UE, e.g., in a registration acceptance message (step 8). The UE then

attempts to verify the MAC, and if successful, stores the privacy key(s). To verify the MAC, the UE creates the same provisioning key as the AUSF/PKPF previously did.

[0059] In some embodiments, the UE then detaches from the network (step 9), e.g., to start a new registration procedure using a provisioned privacy key to conceal its subscriber identity, according to one or more embodiments described above (not shown in Figure 12). For example, detaching and reregistering in this way may prevent an attacker from linking the SUPI to a temporary identifier of the UE.

[0060] The UE may, in some embodiments, need to be provisioned with a privacy key due to the expiration or invalidation of a privacy key that was previously provisioned to the UE.

Figure 13 illustrates an example UE Registration process in which the UE's privacy key needs to be updated, e.g., for some security or operational reason. Some reasons that the previously provisioned privacy key may need to be updated, according to various embodiments, may be that the previously provisioned privacy key may have reached (or is reaching) its expiry date, security in the wireless communication network has been compromised in some way, and/or the privacy key is subject to regular updates.

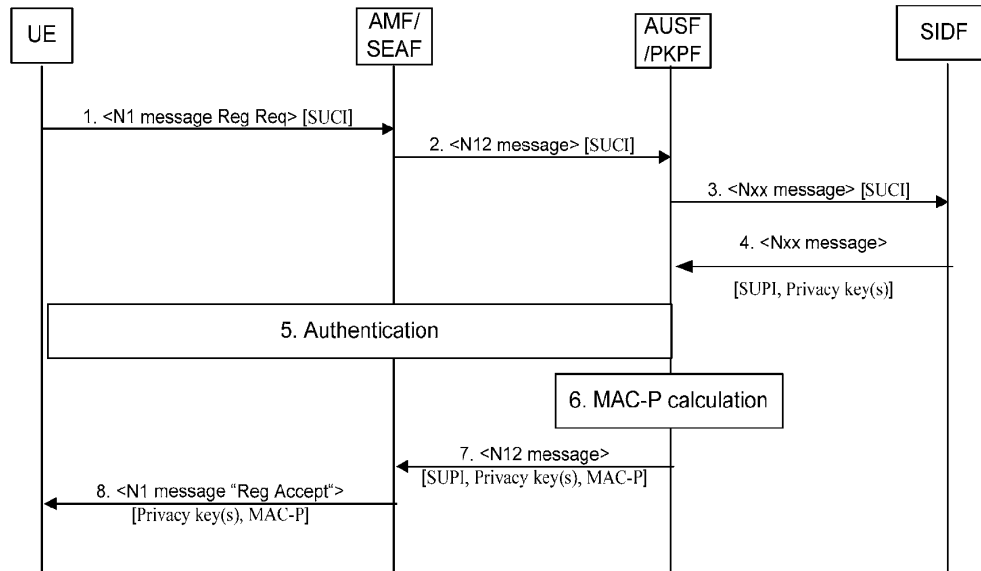


FIG. 13

[0061] According to the example of Figure 13, the UE sends a registration request to an AMF/SEAF (step 1). The registration request includes a SUCI. In this example, since the UE has a privacy key, the UE uses an encryption scheme or method (e.g., ECIES) to create the SUCI, e.g., according to one or more of the embodiments described above.

[0062] The AMF/SEAF requests UE authentication from a AUSF/PKPF (step 2). The AUSF sends the SUCI to an SIDF (step 3). As in the previous example, according to some embodiments in which the SIDF is co-located with UDM, then the same message may be used to request an authentication vector/credentials from the UDM.

[0063] The SIDF sees that the SUCI is encrypted with a privacy key that needs to be updated. For example, the SIDF may detect that the privacy key is expired or is about to expire, or that the privacy key is invalid for any other reason as previously discussed. The SIDF returns a SUPI to the AUSF together with a request to provision the updated ECIES privacy key to the UE (step 4). According to some embodiments, the response may include several privacy keys.

Further, as previously discussed, according to some embodiments in which the SIDF is co-located in UDM, the same message may be used to return the authentication vector/credentials to the AUSF.

[0064] The AUSF and UE exchange authentication messages using authentication vectors/credentials received from UDM (step 5). As discussed in previous examples, the AUSF may have received the required authentication vector/credentials from UDM already in step 4 (e.g., in some embodiments in which the SIDF is co-located in UDM), or the AUSF may request such authentication vector/credentials from UDM before initiating the authentication with the UE.

[0065] According to embodiments in which the PKPF is co-located with the AUSF, the AUSF/PKPF may create a provisioning key used to protect the privacy key provisioning message to the UE as a result of successful authentication. For example, the authentication procedure may include producing a home network master key that may be used to derive the provisioning key. Alternatively, in embodiments in which the PKPF and AUSF are not co-located, the AUSF and PKPF may exchange the provision key through appropriate messaging (not shown).

[0066] The AUSF/PKPF protects the privacy key(s) (received from SIDF in step 4) with the provisioning key by calculating a MAC and constructing MAC-P, e.g., according to the example process illustrated in Figure 7 (step 6). As discussed above, in some embodiments, the AUSF/PKPF may receive the MAC and/or MAC-P from the SIDF, as described above, particularly in at least some embodiments in which the provisioning key is based on the ephemeral shared key of, e.g., an EICES scheme. In particular, as discussed above, the SIDF may have generated the MAC and/or MAC-P.

[0067] After successful authentication, the AUSF sends the SUPI, the privacy key(s) and the MAC-P to the AMF/SEAF (step 7), e.g., in the same registration-related message flow. Other embodiments may use separate message flows for one or more of the SUPI, privacy key(s) or MAC-P. Also, as previously discussed, the AUSF may have delegated

authentication of the UE to the SEAF, in which case the SUPI, the privacy key(s), and the MAC-P may have been returned to SEAF already in step 4, and the AUSF performs the authentication as previously described.

[0068] The AMF/SEAF accepts the registration of the UE, and forwards the privacy key(s) and the MAC-P to the UE, e.g., in a registration acceptance message (step 8). The UE creates the same provisioning key from the primary authentication as AUSF/PKPF did, and verifies the MAC in the message. If verification is successful, the UE stores the privacy key(s). The old privacy key may also be removed.

[0069] As previously discussed, the MAC may be calculated based on a privacy key (e.g., as illustrated in Figure 3) and a provisioning key to generate a MAC-P (e.g., as illustrated in Figure 11). In some embodiments in which multiple privacy keys are being provisioned to the UE, the same MAC may be calculated over all of the privacy keys sent in the same message.

[0070] Figure 14 illustrates an example of how the privacy key and MAC-P are related to each other, and what parameters are used as input to the MAC calculation (or expected MAC (XMAC), as appropriate). As shown in Figure 14, the provisioning key and privacy key are both used to generate a MAC, which may be then used in combination with another privacy key to update the MAC, and so on until all privacy keys are processed. Once all privacy keys are processed, the privacy key(s) and MAC may be sent to the UE.

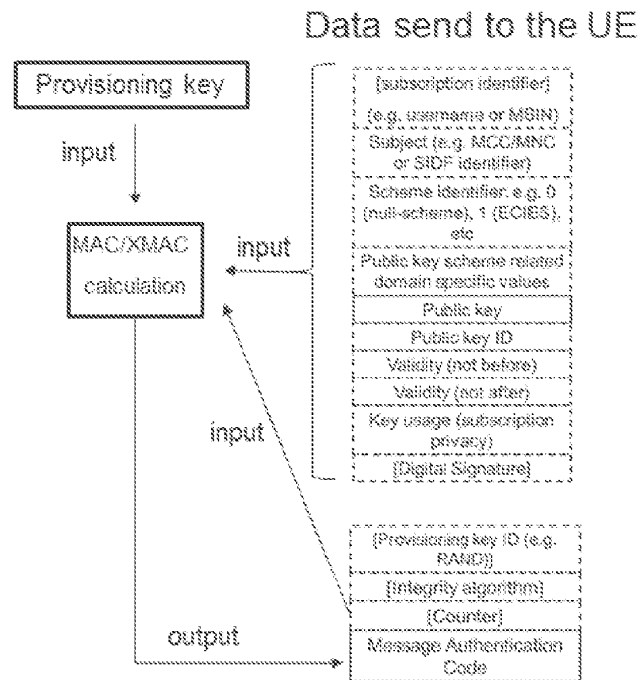


FIG. 14

[0071] In view of all of the above, one or more of the devices or functions described above may be implemented using the example hardware illustrated in Figure 15. The example hardware includes processing circuitry and communication circuitry. The processing circuitry is communicatively coupled to the communication circuitry, e.g., via one or more buses. The processing circuitry may comprise one or more microprocessors, microcontrollers, hardware circuits, discrete logic circuits, hardware registers, digital signal processors (DSPs), field-programmable gate arrays (FPGAs), application-specific integrated circuits (ASICs), or a combination thereof. For example, the processing circuitry may be programmable hardware capable of executing software instructions stored, e.g., as a machine-readable computer program in memory circuitry. The memory circuitry of the various embodiments may comprise any non-transitory machine-readable media known in the art or that may be developed, whether volatile or non-volatile, including but not limited to solid state media (e.g., SRAM, DRAM,

DDRAM, ROM, PROM, EPROM, flash memory, solid state drive, etc.), removable storage devices (e.g., Secure Digital (SD) card, miniSD card, microSD card, memory stick, thumb-drive, USB flash drive, ROM cartridge, Universal Media Disc), fixed drive (e.g., magnetic hard disk drive), or the like, wholly or in any combination. According to particular embodiments in which the hardware is used to implement the UE, the memory circuitry may comprise a tamper resistant secure hardware component providing secure storage, such as a 5G-USIM and/or UICC.

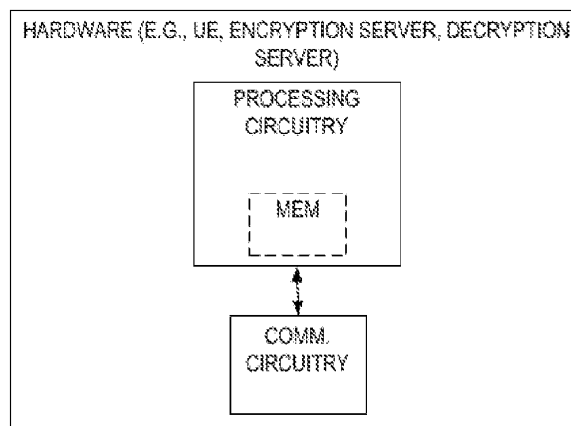


FIG. 15

[0072] The communication circuitry may be a controller hub configured to control the input and output (I/O) data paths of the hardware. Such I/O data paths may include data paths for exchanging signals over a wireless communication network. For example, the communication circuitry may comprise a transceiver configured to send and receive communication signals within and/or between the UE, the serving network, and/or the home network, e.g., over an air, electrical, and/or optical medium.

[0073] The communication circuitry may be implemented as a unitary physical component, or as a plurality of physical components that are contiguously or separately arranged, any of which may be communicatively coupled to any other, or may communicate with any other via

the processing circuitry. For example, the communication circuitry may comprise transmitter circuitry configured to send communication signals, and receiver circuitry configured to receive communication signals (not shown).

[0074] According to particular embodiments, the hardware illustrated in Figure 15 may be configured with a plurality of components. These components may include a plurality of communicatively coupled hardware units and/or software modules. One or more of the hardware units may be, e.g., part of the processing circuitry. One or more of the software units may be, e.g., stored in the memory circuitry and executed by the processing circuitry.

[0075] For example, hardware such as illustrated in Figure 15 may be used to implement an authentication server (e.g., an AMF, SEAF, AUSF) in a home network of a UE and configured with the example components illustrated in Figure 16 to obtain a subscription identifier of a UE. The components of Figure 16 include a determining unit or module and an interfacing unit or module. The determining unit or module is configured to determine, based on information received from the UE, which of a plurality of de-concealing servers to use to decrypt at least part of a subscription concealed identifier (SUCI) in which the subscription identifier is encrypted. The interfacing unit or module is configured to send the SUCI to the determined de-concealing server and receiving the subscription identifier in response.

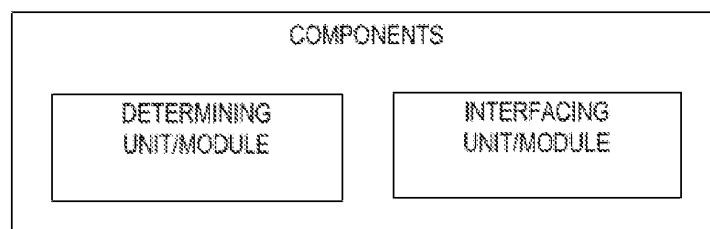


FIG. 16

[0076] Such an authentication server may additionally or alternatively be configured with the example components illustrated in Figure 17 to provision a UE. The components of Figure 17 include an obtaining unit or module, and a transmitting unit or module. The obtaining unit or

module is configured to obtaining a message authentication code (MAC) based on a provisioning key specific to the UE and a privacy key of a home network of the UE. The transmitting unit or module is configured to transmit the privacy key and MAC to the UE.

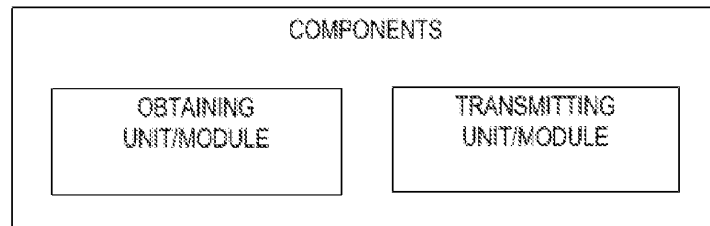


FIG. 17

[0077] Such an authentication server may further be configured to additionally or alternatively perform any of the methods described herein with respect to an authentication server, e.g., using any of the above described authentication server hardware or software components.

[0078] Other hardware consistent with the example illustrated in Figure 15, may be used to implement a de-concealing server (e.g., SIDF) for providing a subscription identifier of a UE to an authentication server, and may be configured with the example components illustrated in Figure 18. The components of Figure 18 include a receiving unit or module, a decrypting unit or module, and a sending unit or module. The receiving unit or module is configured to receive, from the authentication server, a subscription concealed identifier (SUCI) in which the subscription identifier is encrypted. The decrypting unit or module is configured to decrypt at least part of the SUCI, using a decryption key identified from information received from the UE, to obtain the subscription identifier. The sending unit or module is configured to send the subscription identifier to the authentication server.

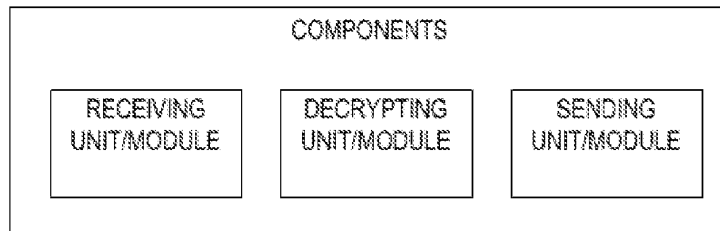


FIG. 18

[0079] Such a de-concealing server may additionally or alternatively be configured with the example components illustrated in Figure 19 to provision a UE. The components of Figure 19 include a generating unit or module, and a transmitting unit or module. The generating unit or module is configured to generate a Subscription Permanent Identifier (SUPI) and privacy key for the UE responsive to receiving, from an authentication server, a Subscription Concealed Identifier (SUCI) of the UE that indicates that the UE lacks a valid privacy key. The transmitting unit or module is configured to transmit the SUPI and privacy key to the authentication server.

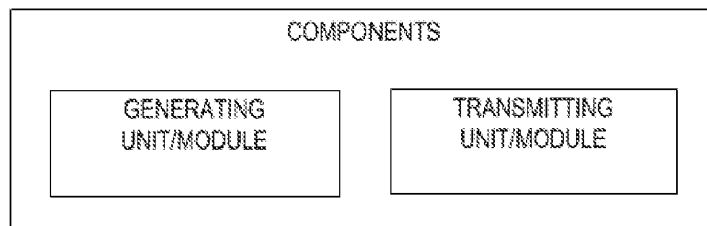


FIG. 19

[0080] Such an de-concealing server may further be configured to additionally or alternatively perform any of the methods described herein with respect to a de-concealing server, e.g., using any of the above described de-concealing server hardware or software components.

[0081] Yet other hardware consistent with the example illustrated in Figure 15, may be used to implement a UE for securely notifying a wireless communication network of a subscription identifier, and may be configured with the example components illustrated in Figure 20. The

components of Figure 20 include a generating unit or module, and a transmitting unit or module. The generating unit or module is configured to generate a subscription concealed identifier (SUCI) in which a subscription identifier of the UE is encrypted. The transmitting unit or module is configured to transmit, to an authentication server, the SUCI and information identifying a de-concealing server capable of decrypting the subscription identifier.

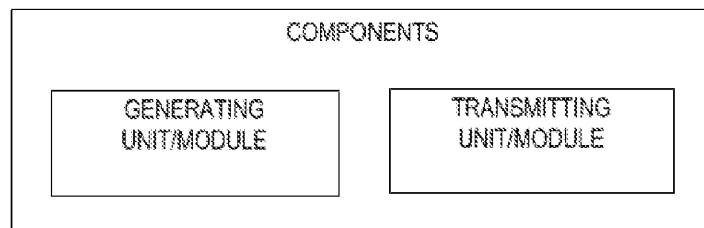


FIG. 20

[0082] Such a UE may additionally or alternatively be configured with the example components illustrated in Figure 21 to obtain a privacy key. The components of Figure 21 include a receiving unit or module, and a verifying unit or module. The receiving unit or module is configured to receiving the privacy key and a message authentication code (MAC) from an authentication server. The verifying unit or module is configured to verify the integrity of the privacy key by generating a provisioning key and using the provisioning key and privacy key to reproduce the MAC received from the authentication server, the provisioning key being a shared secret between the UE and the authentication server.

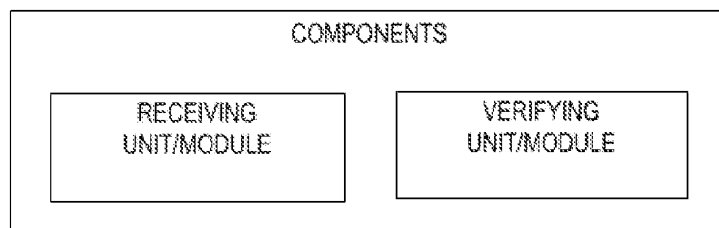


FIG. 21

[0083] Such a UE may further be configured to additionally or alternatively perform any of the methods described herein with respect to a UE, e.g., using any of the above-described UE hardware or software components.

[0084] The various methods and processes described herein may be implemented in ways that vary in certain details from the broad descriptions given above. For example, although steps of various processes or methods described herein may be shown and described as being in a sequence or temporal order, the steps of any such processes or methods are not limited to being carried out in any particular sequence or order, absent an indication otherwise. Indeed, the steps in such processes or methods generally may be carried out in various different sequences and orders while still falling within the scope of the present disclosure. The embodiments described herein are to be considered in all respects as illustrative and not restrictive. In particular, all changes coming within the meaning and equivalency range of the enumerated embodiments appended below are intended to be embraced therein.

ENUMERATED EMBODIMENTS

100. A method, implemented in an authentication server in a home network of a user equipment (UE), for obtaining a subscription identifier of the UE in a wireless communication network, the method comprising:
- determining, based on information received from the UE, which of a plurality of de-concealing servers to use to decrypt at least part of a subscription concealed identifier (SUCI) in which the subscription identifier is encrypted;
 - sending the SUCI to the determined de-concealing server and receiving the subscription identifier in response.
101. The method of embodiment 100, wherein the information comprises a key identifier that identifies one or more of the determined de-concealing server or a decryption key for decryption of the at least part of the SUCI.
102. The method of any of embodiments 100-101, wherein the information comprises a scheme identifier that identifies an encryption scheme used to encrypted the subscription identifier in the SUCI, and the determined de-concealing server supports decryption according to the encryption scheme.
103. The method of any of embodiments 100-102, further comprising receiving the SUCI from the UE as part of a registration procedure for registering the UE with the wireless communication network.
104. The method of any of embodiments 100-103, further comprising receiving the SUCI from the UE via an authentication request from a mobility management function.

105. The method of any of embodiments 100-104, wherein the authentication server is one of the plurality of de-concealing servers.

106. The method of any of embodiment 100-105, further comprising sending the SUCI and a request for an authentication vector for authenticating the UE to the determined de-concealing server in the same message.

107. The method of embodiment 106, further comprising receiving the authentication vector and the subscription identifier from the determined de-concealing server in the same response.

200. A method, implemented in a de-concealing server, for providing a subscription identifier of a user equipment (UE) to an authentication server, the method comprising:

- receiving, from the authentication server, a subscription concealed identifier (SUCI) in which the subscription identifier is encrypted;
- decrypting at least part of the SUCI, using a decryption key identified from information received from the UE, to obtain the subscription identifier;
- sending the subscription identifier to the authentication server.

201. The method of embodiment 200, wherein the information received from the UE is received via the authentication server as part of the SUCI.

202. The method of any of embodiments 200-201, wherein the information received from the UE is a key identifier identifying the de-concealing server and identifying the decryption key.

203. The method of any of embodiments 200-202, wherein the information received from the UE comprises a scheme identifier identifying an encryption scheme supported by the de-concealing server.

204. The method of any of embodiments 200-203, wherein receiving the SUCI comprises receiving the SUCI and a request for an authentication vector for authenticating the UE in the same message.

205. The method of embodiment 204, wherein sending the authentication vector and the subscription identifier to the authentication server in the same message.

300. A method, implemented in a user equipment (UE), for securely notifying a wireless communication network of a subscription identifier, the method comprising:
generating a subscription concealed identifier (SUCI) in which a subscription identifier of the UE is encrypted;
transmitting, to an authentication server, the SUCI and information identifying a de-concealing server capable of decrypting the subscription identifier.

301. The method of embodiment 300, wherein the SUCI and information identifying the de-concealing server are transmitted in a request to register with the wireless communication network.

302. The method of any of embodiments 300-301, wherein generating the SUCI comprises using a tamper resistant secure hardware component of the UE to generate the SUCI.

303. The method of embodiment 302, wherein generating the SUCI comprises generating the SUCI based on a privacy key selected from a plurality of privacy keys stored in the tamper resistant secure hardware component.

304. The method of any of embodiments 302-303, wherein generating the SUCI comprises sending a time to the tamper resistant secure hardware component for use in the generating.

305. The method of any of embodiments 302-304, generating the SUCI comprises generating the SUCI from a privacy key comprising the subscription identifier of the UE.

306. The method of any of embodiments 300-305, wherein transmitting the SUCI to the authentication server comprises transmitting the SUCI to the authentication server in response to an identifier request message received from a mobility management function as part of a procedure for registering the UE with the wireless communication network.

307. The method of embodiment 306, further comprising transmitting a registration request to the mobility management function comprising a 5G Globally Unique Temporary Identifier (5G-GUTI), and receiving the identifier request message in response.

308. The method of any of embodiments 306-307, further comprising successfully authenticating with the authentication server after transmitting the SUCI, and receiving a registration acceptance message in response.

400. A method, implemented in an authentication server for provisioning a user equipment (UE), the method comprising:

obtaining a message authentication code (MAC) based on a provisioning key specific to the UE and a privacy key of a home network of the UE;
transmitting the privacy key and MAC to the UE.

401. The method of embodiment 400, wherein obtaining the MAC comprises generating the MAC.

402. The method of embodiment 400, wherein obtaining the MAC comprises receiving the MAC from a de-concealing server.

403. The method of any of embodiments 400-402, further comprising obtaining the provisioning key responsive to successfully authenticating the UE.

404. The method of embodiment 403, wherein the provisioning key is a shared secret between the authentication server and the UE.

405. The method of any of embodiments 403-404, wherein obtaining the provisioning key comprises generating the provisioning key.

406. The method of any of embodiments 403-404, wherein obtaining the provisioning key comprises receiving the provisioning key from a de-concealing server.

407. The method of embodiment 406, wherein the provisioning key is a shared secret between the de-concealing server and the UE.

408. The method of any of embodiments 400-407, further comprising receiving a request to provision the UE, the request comprising the privacy key.

409. The method of embodiment 408, wherein receiving the request to provision the UE comprises receiving the request to provision the UE and an authentication vector for authenticating the UE in the same message.

410. The method of any of embodiments 408-409, wherein the request to provision the UE further comprises at least one additional privacy key of the home network of the UE, and the method further comprises transmitting the at least one additional privacy key to the UE.

411. The method of any of embodiments 408-410, further comprising transmitting a subscription concealed identifier (SUCI) of the UE indicating that the UE lacks a valid privacy key to a de-concealing server, and receiving the request to provision the UE from the de-concealing server in response.

412. The method of embodiment 411, wherein the privacy key is one of a plurality of privacy keys of the home network managed by the de-concealing server.

413. The method of any of embodiments 408-412, wherein the request further comprises a Subscription Permanent Identifier (SUPI) of the UE.

414. The method of any of embodiments 400-413, wherein transmitting the privacy key and MAC to the UE comprises transmitting the privacy key and MAC to the UE together in the same registration acceptance messaging procedure.

415. The method of any of embodiments 400-414, further comprising receiving a subscription concealed identifier (SUCI) of the UE using a null encryption scheme for a subscription identifier comprised in the SUCI.

500. A method, implemented in a de-concealing server, for provisioning a user equipment (UE), the method comprising:

generating a Subscription Permanent Identifier (SUPI) and privacy key for the UE
responsive to receiving, from an authentication server, a Subscription Concealed Identifier (SUCI) of the UE that indicates that the UE lacks a valid privacy key;
transmitting the SUPI and privacy key to the authentication server.

501. The method of embodiment 500, further comprising detecting that the SUCI indicates that the UE lacks a valid privacy key by detecting that at least part of the SUCI is encrypted using an obsolete privacy key.

502. The method of embodiment 501, wherein the obsolete privacy key is an expired or compromised privacy key.

503. The method of any of embodiments 500-502, further comprising generating the privacy key.

504. The method of embodiment 503, wherein generating the privacy key comprises generating the privacy key in accordance with an encryption scheme policy governing secure communication of a subscriber identifier of the UE in the wireless communication network.

505. The method of embodiment 504, wherein generating the privacy key in accordance with the encryption scheme policy comprises generating the privacy key such that the privacy key is suitable for generating a new SUCI in which the subscriber identifier of the UE is encrypted according to an Elliptic Curve Integrated Encryption scheme.

506. The method of any of embodiments 500-505, further comprising generating at least one additional privacy key responsive to receiving the SUCI, and transmitting the at least one additional privacy key to the authentication server.

507. The method of any of embodiments 500-506, further comprising transmitting a provisioning key that is a shared secret between the de-concealing server and the UE to the authentication server.

508. The method of any of embodiments 500-507, further comprising generating a message authentication code (MAC) based on a provisioning key specific to the UE and the privacy key, and transmitting the MAC to the authentication server.

509. The method of any of embodiments 500-508, wherein the privacy key comprises a public key of a home network of the UE.

510. The method of embodiment 509, wherein the privacy key further comprises an identifier that identifies in which of plurality of encryption schemes the public key is used.

511. The method of embodiment 510, wherein the privacy key further comprises a parameter used in the encryption scheme in which the public key is used.

512. The method of any of embodiments 500-511, wherein the privacy key comprises a subscription identifier of the UE.
513. The method of any of embodiments 500-512, wherein the privacy key comprises an identifier of a home network of the UE.
514. The method of any of embodiments 500-513, wherein the privacy key comprises validity time information indicating a time in which the privacy key is valid.
515. The method of any of embodiments 500-514, wherein the privacy key comprises a digital signature calculated over one or more other parts of the privacy key.
516. The method of any of embodiments 500-515, wherein the privacy key comprises a field explicitly indicating a procedure in which the privacy key may be used.
600. A method, implemented in a user equipment (UE), for obtaining a privacy key, the method comprising:
- receiving the privacy key and a message authentication code (MAC) from an authentication server;
 - verifying the integrity of the privacy key by generating a provisioning key and using the provisioning key and privacy key to reproduce the MAC received from the authentication server, the provisioning key being a shared secret between the UE and the authentication server.

601. The method of embodiment 600, further comprising transmitting a Subscription Concealed Identifier (SUCI) to the authentication server and receiving the privacy key in response.
602. The method of embodiment 601, wherein the SUCI indicates that the UE lacks a valid privacy key.
603. The method of any of embodiments 601-602, wherein transmitting the SUCI comprises transmitting the SUCI in a request to register with a wireless communication network.
604. The method of embodiment 603, further comprising receiving the privacy key and MAC from the authentication server via an mobility management Function and in a registration acceptance message.
605. The method of embodiment 604, further comprising, responsive to verifying the privacy key:
detaching from the wireless communication network;
generating a different SUCI in which a subscription identifier of the UE is encrypted by at least part of the privacy key;
re-registering with the wireless communication network using the different SUCI.
606. The method of any of embodiments 601-605, further comprising using a tamper resistant secure hardware component of the UE to obtain the SUCI.
607. The method of embodiment 606, further comprising storing the privacy key in the tamper resistant secure hardware component.

608. The method of any of embodiments 606-607, further comprising detecting that the UE lacks the valid privacy key responsive to insertion of the tamper resistant secure hardware component into the UE.

609. The method of any of embodiments 606-608, wherein using the tamper resistant secure hardware component to obtain the SUCI comprises using the tamper resistant secure hardware component to generate the SUCI.

610. The method of any of embodiments 606-609, wherein using the tamper resistant secure hardware component to obtain the SUCI comprises performing a read operation on the tamper resistant secure hardware component to obtain the SUCI.

611. The method of any of embodiments 606-610, wherein using the tamper resistant secure hardware component to obtain the SUCI comprises sending a time to the tamper resistant secure hardware component and receiving the SUCI from the tamper resistant secure hardware component in response.

612. The method of any of embodiments 606-611, wherein using the tamper resistant secure hardware component to obtain the SUCI comprises using a different privacy key obtained from the tamper resistant hardware component to generate the SUCI.

613. The method of embodiment 612, wherein the different privacy key is expired, and method further comprises replacing the different privacy key with the privacy key.

700. An authentication server in an home network of a user equipment (UE), for obtaining a subscription identifier of the UE in a wireless communication network, the authentication server comprising:

a processor and a memory, the memory containing instructions executable by the processor whereby the authentication server is operative to:
determine, based on information received from the UE, which of a plurality of de-concealing servers to use to decrypt at least part of a subscription concealed identifier (SUCI) in which the subscription identifier is encrypted;
send the SUCI to the determined de-concealing server and receiving the subscription identifier in response.

701. An authentication server in an home network of a user equipment (UE), for obtaining a subscription identifier of the UE in a wireless communication network, the authentication server configured to:

determine, based on information received from the UE, which of a plurality of de-concealing servers to use to decrypt at least part of a subscription concealed identifier (SUCI) in which the subscription identifier is encrypted;
send the SUCI to the determined de-concealing server and receiving the subscription identifier in response.

702. An authentication server in an home network of a user equipment (UE), for obtaining a subscription identifier of the UE in a wireless communication network, the authentication server comprising:

a determining module configured to determine, based on information received from the UE, which of a plurality of de-concealing servers to use to decrypt at least part of a

subscription concealed identifier (SUCI) in which the subscription identifier is encrypted;
an interfacing module configured to send the SUCI to the determined de-concealing server and receiving the subscription identifier in response.

703. The authentication server of any one of embodiments 700-702, configured to perform the method of any one of embodiments 101-199.

800. A de-concealing server for providing a subscription identifier of a user equipment (UE) to an authentication server, the de-concealing server comprising:

a processor and a memory, the memory containing instructions executable by the processor whereby the de-concealing server is operative to:

receive, from the authentication server, a subscription concealed identifier (SUCI) in which the subscription identifier is encrypted;
decrypt at least part of the SUCI, using a decryption key identified from information received from the UE, to obtain the subscription identifier
send the subscription identifier to the authentication server.

801. A de-concealing server for providing a subscription identifier of a user equipment (UE) to an authentication server, the de-concealing server configured to:

receive, from the authentication server, a subscription concealed identifier (SUCI) in which the subscription identifier is encrypted;
decrypt at least part of the SUCI, using a decryption key identified from information received from the UE, to obtain the subscription identifier;
send the subscription identifier to the authentication server.

802. A de-concealing server for providing a subscription identifier of a user equipment (UE) to an authentication server, the de-concealing server comprising:

- a receiving module configured to receive, from the authentication server, a subscription concealed identifier (SUCI) in which the subscription identifier is encrypted;
- a decrypting module configured to decrypt at least part of the SUCI, using a decryption key identified from information received from the UE, to obtain the subscription identifier;
- a sending module configured to send the subscription identifier to the authentication server.

803. The de-concealing server of any of embodiments 800-802, configured to perform the method of any one of embodiments 201-299.

900. A user equipment (UE) for securely notifying a wireless communication network of a subscription identifier, the UE comprising:

- a processor and a memory, the memory containing instructions executable by the processor whereby the UE is operative to:
 - generate a subscription concealed identifier (SUCI) in which a subscription identifier of the UE is encrypted;
 - transmit, to an authentication server, the SUCI and information identifying a de-concealing server capable of decrypting the subscription identifier.

901. A user equipment (UE) for securely notifying a wireless communication network of a subscription identifier, the UE configured to:

- generate a subscription concealed identifier (SUCI) in which a subscription identifier of the UE is encrypted;

transmit, to an authentication server, the SUCI and information identifying a de-concealing server capable of decrypting the subscription identifier.

902. A user equipment (UE) for securely notifying a wireless communication network of a subscription identifier, the UE comprising:

a generating module configured to generate a subscription concealed identifier (SUCI) in which a subscription identifier of the UE is encrypted;

a transmitting module configured to transmit, to an authentication server, the SUCI and information identifying a de-concealing server capable of decrypting the subscription identifier.

903. The UE of any of embodiments 900-902, configured to perform the method of any one of embodiments 301-399.

1000. An authentication server for provisioning a user equipment (UE), the authentication server comprising:

a processor and a memory, the memory containing instructions executable by the processor whereby the authentication server is operative to:

obtain a message authentication code (MAC) based on a provisioning key specific to the UE and a privacy key of a home network of the UE;

transmit the privacy key and MAC to the UE.

1001. An authentication server for provisioning a user equipment (UE), the authentication server configured to:

obtain a message authentication code (MAC) based on a provisioning key specific to the UE and a privacy key of a home network of the UE;

transmit the privacy key and MAC to the UE.

1002. An authentication server for provisioning a user equipment (UE), the authentication server comprising:

an obtaining module configured to obtain a message authentication code (MAC) based on a provisioning key specific to the UE and a privacy key of a home network of the UE;

a transmitting module configured to transmit the privacy key and MAC to the UE.

1003. The authentication server of any of embodiments 1000-1002, configured to perform the method of any one of embodiments 401-499.

1100. A de-concealing server, for provisioning a user equipment (UE), the de-concealing server comprising:

a processor and a memory, the memory containing instructions executable by the processor whereby the de-concealing server is operative to:

responsive to receiving, from an authentication server, a Subscription Concealed Identifier (SUCI) of the UE that indicates that the UE lacks a valid privacy key, generate a Subscription Permanent Identifier (SUPI) and privacy key for the UE;

transmit the SUPI and privacy key to the authentication server.

1101. A de-concealing server, for provisioning a user equipment (UE), the de-concealing server configured to:

responsive to receiving, from an authentication server, a Subscription Concealed Identifier (SUCI) of the UE that indicates that the UE lacks a valid privacy key, generate a Subscription Permanent Identifier (SUPI) and privacy key for the UE; transmit the SUPI and privacy key to the authentication server.

1102. A de-concealing server, for provisioning a user equipment (UE), the de-concealing server comprising:

a generating module configured to responsive to receiving, from an authentication server, a Subscription Concealed Identifier (SUCI) of the UE that indicates that the UE lacks a valid privacy key, generate a Subscription Permanent Identifier (SUPI) and privacy key for the UE;

a transmitting module configured to transmit the SUPI and privacy key to the authentication server.

1103. The de-concealing server of any of embodiments 1100-1102, configured to perform the method of any one of embodiments 501-599.

1200. A user equipment (UE) for obtaining a privacy key, the UE comprising:

a processor and a memory, the memory containing instructions executable by the processor whereby the device is operative to:

receive the privacy key and a message authentication code (MAC) from an authentication server;

verify the integrity of the privacy key by generating a provisioning key and using the provisioning key and privacy key to reproduce the MAC received from the

authentication server, the provisioning key being a shared secret between the UE and the authentication server.

1201. A user equipment (UE) for obtaining a privacy key, the UE configured to:
receive the privacy key and a message authentication code (MAC) from an authentication server;
verify the integrity of the privacy key by generating a provisioning key and using the provisioning key and privacy key to reproduce the MAC received from the authentication server, the provisioning key being a shared secret between the UE and the authentication server.
1202. A user equipment (UE) for obtaining a privacy key, the UE comprising:
a receiving module configured to receive the privacy key and a message authentication code (MAC) from an authentication server;
a verifying module configured to verify the integrity of the privacy key by generating a provisioning key and using the provisioning key and privacy key to reproduce the MAC received from the authentication server, the provisioning key being a shared secret between the UE and the authentication server.
1203. The user equipment of any of embodiments 1200-1202, configured to perform the method of any one of embodiments 601-699.
1300. A computer program, comprising instructions which, when executed on at least one processor of a server device, cause the at least one processor to carry out the method according to any one of claims 100-699.

1301. A carrier containing the computer program of claim 1300, wherein the carrier is one of an electronic signal, optical signal, radio signal, or computer readable storage medium.

Application Data Sheet 37 CFR 1.76		Attorney Docket Number	4015-10071 / P72588-US1
		Application Number	
Title of Invention	ENABLING SUBSCRIPTION IDENTIFIER PRIVACY		
The application data sheet is part of the provisional or nonprovisional application for which it is being submitted. The following form contains the bibliographic data arranged in a format specified by the United States Patent and Trademark Office as outlined in 37 CFR 1.76. This document may be completed electronically and submitted to the Office in electronic format using the Electronic Filing System (EFS) or the document may be printed and included in a paper filed application.			

Secrecy Order 37 CFR 5.2:

☐ Portions or all of the application associated with this Application Data Sheet may fall under a Secrecy Order pursuant to 37 CFR 5.2 (Paper filers only. Applications that fall under Secrecy Order may not be filed electronically.)

Inventor Information:

Inventor	1				Remove
Legal Name					
Prefix	Given Name	Middle Name	Family Name	Suffix	
	Vesa		Torvinen		
Residence Information (Select One) US Residency • Non US Residency Active US Military Service					
City	Sauvo		Country of Residenceⁱ	FI	
Mailing Address of Inventor:					
Address 1	Sauvontie 42				
Address 2					
City	Sauvo		State/Province		
Postal Code	21570		Countryⁱ	FI	
Inventor	2				Remove
Legal Name					
Prefix	Given Name	Middle Name	Family Name	Suffix	
	Noamen		Ben Henda		
Residence Information (Select One) US Residency • Non US Residency Active US Military Service					
City	Stockholm		Country of Residenceⁱ	SE	
Mailing Address of Inventor:					
Address 1	Tumultgränd 228				
Address 2					
City	Stockholm		State/Province		
Postal Code	SE-162 47		Countryⁱ	SE	
Inventor	3				Remove
Legal Name					

Application Data Sheet 37 CFR 1.76		Attorney Docket Number		4015-10071 / P72588-US1	
		Application Number			
Title of Invention		ENABLING SUBSCRIPTION IDENTIFIER PRIVACY			

Prefix	Given Name	Middle Name	Family Name	Suffix
	David		Castellanos Zamora	
Residence Information (Select One) US Residency ☒ Non US Residency Active US Military Service				
City	Madrid		Country of Residence ⁱ	ES

Mailing Address of Inventor:				
Address 1		C/ Embajadores 256, 1ºB		
Address 2				
City	Madrid	State/Province		
Postal Code	28045	Country ⁱ	ES	
Inventor	4			Remove
Legal Name				
Prefix	Given Name	Middle Name	Family Name	Suffix
	Prajwol	Kumar	Nakarmi	
Residence Information (Select One) US Residency ☒ Non US Residency Active US Military Service				
City	Sollentuna		Country of Residence ⁱ	SE

Mailing Address of Inventor:				
Address 1		Stupvägen 17		
Address 2				
City	Sollentuna	State/Province		
Postal Code	SE-191 42	Country ⁱ	SE	
Inventor	5			Remove
Legal Name				
Prefix	Given Name	Middle Name	Family Name	Suffix
	Pasi		Saarinen	
Residence Information (Select One) US Residency ☒ Non US Residency Active US Military Service				
City	Stockholm		Country of Residence ⁱ	SE

Mailing Address of Inventor:				
Address 1		Slipgatan 7		
Address 2				
City	Stockholm	State/Province		
Postal Code	SE-117 39	Country ⁱ	SE	

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	4015-10071 / P72588-US1
	Application Number	
Title of Invention	ENABLING SUBSCRIPTION IDENTIFIER PRIVACY	

Inventor	6				Remove
Legal Name					
Prefix	Given Name	Middle Name	Family Name	Suffix	
	Monica		Wifvesson		
Residence Information (Select One) US Residency ☒ Non US Residency Active US Military Service					
City	Lund	Country of Residence		SE	
Mailing Address of Inventor:					
Address 1	Kruthornsgränden 3				
Address 2					
City	Lund	State/Province			
Postal Code	226 52	Country	SE		
All Inventors Must Be Listed - Additional Inventor Information blocks may be generated within this form by selecting the Add button.					

Correspondence Information:

Enter either Customer Number or complete the Correspondence Information section below. For further information see 37 CFR 1.33(a).			
☐ An Address is being provided for the correspondence information of this application.			
Customer Number	24112		
Email Address		Add Email	Remove Email

Application Information:

Title of the Invention	ENABLING SUBSCRIPTION IDENTIFIER PRIVACY		
Attorney Docket Number	4015-10071 / P72588-US1	Small Entity Status Claimed	☐
Application Type	Provisional		
Subject Matter	Utility		
Total Number of Drawing Sheets (if any)		Suggested Figure for Publication (if any)	

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	4015-10071 / P72588-US1
	Application Number	
Title of Invention	ENABLING SUBSCRIPTION IDENTIFIER PRIVACY	

Filing By Reference:

Only complete this section when filing an application by reference under 35 U.S.C. 111(c) and 37 CFR 1.57(a). Do not complete this section if application papers including a specification and any drawings are being filed. Any domestic benefit or foreign priority information must be provided in the appropriate section(s) below (i.e., "Domestic Benefit/National Stage Information" and "Foreign Priority Information").

For the purposes of a filing date under 37 CFR 1.53(b), the description and any drawings of the present application are replaced by this reference to the previously filed application, subject to conditions and requirements of 37 CFR 1.57(a).

Application number of the previously filed application	Filing date (YYYY-MM-DD)	Intellectual Property Authority or Country

Publication Information:

☐ Request Early Publication (Fee required at time of Request 37 CFR 1.219)
☐ Request Not to Publish. I hereby request that the attached application not be published under 35 U.S.C. 122(b) and certify that the invention disclosed in the attached application has not and will not be the subject of an application filed in another country, or under a multilateral international agreement, that requires publication at eighteen months after filing.

Representative Information:

Representative information should be provided for all practitioners having a power of attorney in the application. Providing this information in the Application Data Sheet does not constitute a power of attorney in the application (see 37 CFR 1.32). Either enter Customer Number or complete the Representative Name section below. If both sections are completed the customer Number will be used for the Representative Information during processing.			
Please Select One:	☒ Customer Number	☐ US Patent Practitioner	☐ Limited Recognition (37 CFR 11.9)
Customer Number	24112		

Domestic Benefit/National Stage Information:

This section allows for the applicant to either claim benefit under 35 U.S.C. 119(e), 120, 121, 365(c), or 386(c) or indicate National Stage entry from a PCT application. Providing benefit claim information in the Application Data Sheet constitutes the specific reference required by 35 U.S.C. 119(e) or 120, and 37 CFR 1.78.

When referring to the current application, please leave the "Application Number" field blank.

Prior Application Status		Remove	
Application Number	Continuity Type	Prior Application Number	Filing or 371(c) Date (YYYY-MM-DD)
Additional Domestic Benefit/National Stage Data may be generated within this form by selecting the Add button. Add			

Application Data Sheet 37 CFR 1.76		Attorney Docket Number	4015-10071 / P72588-US1
		Application Number	
Title of Invention	ENABLING SUBSCRIPTION IDENTIFIER PRIVACY		

Foreign Priority Information:

This section allows for the applicant to claim priority to a foreign application. Providing this information in the application data sheet constitutes the claim for priority as required by 35 U.S.C. 119(b) and 37 CFR 1.55. When priority is claimed to a foreign application that is eligible for retrieval under the priority document exchange program (PDX)ⁱ the information will be used by the Office to automatically attempt retrieval pursuant to 37 CFR 1.55(i)(1) and (2). Under the PDX program, applicant bears the ultimate responsibility for ensuring that a copy of the foreign application is received by the Office from the participating foreign intellectual property office, or a certified copy of the foreign priority application is filed, within the time period specified in 37 CFR 1.55(g)(1).

Application Number	Country ⁱ	Filing Date (YYYY-MM-DD)	Access Code ⁱ (if applicable)	Remove

Additional Foreign Priority Data may be generated within this form by selecting the Add button.

Statement under 37 CFR 1.55 or 1.78 for AIA (First Inventor to File) Transition Applications

☐ This application (1) claims priority to or the benefit of an application filed before March 16, 2013 and (2) also contains, or contained at any time, a claim to a claimed invention that has an effective filing date on or after March 16, 2013.

NOTE: By providing this statement under 37 CFR 1.55 or 1.78, this application, with a filing date on or after March 16, 2013, will be examined under the first inventor to file provisions of the AIA.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	4015-10071 / P72588-US1
	Application Number	
Title of Invention	ENABLING SUBSCRIPTION IDENTIFIER PRIVACY	

Authorization or Opt-Out of Authorization to Permit Access:

When this Application Data Sheet is properly signed and filed with the application, applicant has provided written authority to permit a participating foreign intellectual property (IP) office access to the instant application-as-filed (see paragraph A in subsection 1 below) and the European Patent Office (EPO) access to any search results from the instant application (see paragraph B in subsection 1 below).

Should applicant choose not to provide an authorization identified in subsection 1 below, applicant **must opt-out** of the authorization by checking the corresponding box A or B or both in subsection 2 below.

NOTE: This section of the Application Data Sheet is **ONLY** reviewed and processed with the **INITIAL** filing of an application. After the initial filing of an application, an Application Data Sheet cannot be used to provide or rescind authorization for access by a foreign IP office(s). Instead, Form PTO/SB/39 or PTO/SB/69 must be used as appropriate.

1. Authorization to Permit Access by a Foreign Intellectual Property Office(s)

A. Priority Document Exchange (PDX) - Unless box A in subsection 2 (opt-out of authorization) is checked, the undersigned hereby **grants the USPTO authority** to provide the European Patent Office (EPO), the Japan Patent Office (JPO), the Korean Intellectual Property Office (KIPO), the State Intellectual Property Office of the People's Republic of China (SIPO), the World Intellectual Property Organization (WIPO), and any other foreign intellectual property office participating with the USPTO in a bilateral or multilateral priority document exchange agreement in which a foreign application claiming priority to the instant patent application is filed, access to: (1) the instant patent application-as-filed and its related bibliographic data, (2) any foreign or domestic application to which priority or benefit is claimed by the instant application and its related bibliographic data, and (3) the date of filing of this Authorization. See 37 CFR 1.14(h)(1).

B. Search Results from U.S. Application to EPO - Unless box B in subsection 2 (opt-out of authorization) is checked, the undersigned hereby **grants the USPTO authority** to provide the EPO access to the bibliographic data and search results from the instant patent application when a European patent application claiming priority to the instant patent application is filed. See 37 CFR 1.14(h)(2).

The applicant is reminded that the EPO's Rule 141(1) EPC (European Patent Convention) requires applicants to submit a copy of search results from the instant application without delay in a European patent application that claims priority to the instant application.

2. Opt-Out of Authorizations to Permit Access by a Foreign Intellectual Property Office(s)

☐ A. Applicant **DOES NOT** authorize the USPTO to permit a participating foreign IP office access to the instant application-as-filed. If this box is checked, the USPTO will not be providing a participating foreign IP office with any documents and information identified in subsection 1A above.

☐ B. Applicant **DOES NOT** authorize the USPTO to transmit to the EPO any search results from the instant patent application. If this box is checked, the USPTO will not be providing the EPO with search results from the instant application.

NOTE: Once the application has published or is otherwise publicly available, the USPTO may provide access to the application in accordance with 37 CFR 1.14.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	4015-10071 / P72588-US1
	Application Number	
Title of Invention	ENABLING SUBSCRIPTION IDENTIFIER PRIVACY	

Applicant Information:

Providing assignment information in this section does not substitute for compliance with any requirement of part 3 of Title 37 of CFR to have an assignment recorded by the Office.			
Applicant	1 Remove		
If the applicant is the inventor (or the remaining joint inventor or inventors under 37 CFR 1.45), this section should not be completed. The information to be provided in this section is the name and address of the legal representative who is the applicant under 37 CFR 1.43; or the name and address of the assignee, person to whom the inventor is under an obligation to assign the invention, or person who otherwise shows sufficient proprietary interest in the matter who is the applicant under 37 CFR 1.46. If the applicant is an applicant under 37 CFR 1.46 (assignee, person to whom the inventor is obligated to assign, or person who otherwise shows sufficient proprietary interest) together with one or more joint inventors, then the joint inventor or inventors who are also the applicant should be identified in this section. Clear			
Assignee	Legal Representative under 35 U.S.C. 117		Joint Inventor
☒ Person to whom the inventor is obligated to assign.		☐ Person who shows sufficient proprietary interest	
If applicant is the legal representative, indicate the authority to file the patent application, the inventor is:			
Name of the Deceased or Legally Incapacitated Inventor:			
If the Applicant is an Organization check here. ☒			
Organization Name	Telefonaktiebolaget LM Ericsson (publ)		
Mailing Address Information For Applicant:			
Address 1	SE-164 83		
Address 2			
City	Stockholm	State/Province	
Country	SE	Postal Code	
Phone Number		Fax Number	
Email Address			
Additional Applicant Data may be generated within this form by selecting the Add button. Add			

Assignee Information including Non-Applicant Assignee Information:

Providing assignment information in this section does not substitute for compliance with any requirement of part 3 of Title 37 of CFR to have an assignment recorded by the Office.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	4015-10071 / P72588-US1
	Application Number	
Title of Invention	ENABLING SUBSCRIPTION IDENTIFIER PRIVACY	

Assignee	1			
Complete this section if assignee information, including non-applicant assignee information, is desired to be included on the patent application publication. An assignee-applicant identified in the "Applicant Information" section will appear on the patent application publication as an applicant. For an assignee-applicant, complete this section only if identification as an assignee is also desired on the patent application publication.				
Remove				
If the Assignee or Non-Applicant Assignee is an Organization check here. ☐				
Prefix	Given Name	Middle Name	Family Name	Suffix
Mailing Address Information For Assignee including Non-Applicant Assignee:				
Address 1				
Address 2				
City		State/Province		
Country i		Postal Code		
Phone Number		Fax Number		
Email Address				
Additional Assignee or Non-Applicant Assignee Data may be generated within this form by selecting the Add button. Add				

Signature:

Remove

NOTE: This Application Data Sheet must be signed in accordance with 37 CFR 1.33(b). **However, if this Application Data Sheet is submitted with the INITIAL filing of the application and either box A or B is not checked in subsection 2 of the "Authorization or Opt-Out of Authorization to Permit Access" section, then this form must also be signed in accordance with 37 CFR 1.14(c).**

This Application Data Sheet must be signed by a patent practitioner if one or more of the applicants is a **juristic entity** (e.g., corporation or association). If the applicant is two or more joint inventors, this form must be signed by a patent practitioner, **all** joint inventors who are the applicant, or one or more joint inventor-applicants who have been given power of attorney (e.g., see USPTO Form PTO/AIA/81) on behalf of **all** joint inventor-applicants.

See 37 CFR 1.4(d) for the manner of making signatures and certifications.

Signature	William G. Pagán/		Date (YYYY-MM-DD)	2017-07-25	
First Name	William G.	Last Name	Pagán	Registration Number	67192
Additional Signature may be generated within this form by selecting the Add button. Add					

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76		Attorney Docket Number	4015-10071 / P72588-US1
		Application Number	
Title of Invention	ENABLING SUBSCRIPTION IDENTIFIER PRIVACY		

This collection of information is required by 37 CFR 1.76. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 23 minutes to complete, including gathering, preparing, and submitting the completed application data sheet form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

- 1 The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these records.
- 2 A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
- 3 A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
- 4 A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
- 5 A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
- 6 A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
- 7 A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
- 8 A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.
- 9 A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Electronic Acknowledgement Receipt	
EFS ID:	29883195
Application Number:	62536632
International Application Number:	
Confirmation Number:	8175
Title of Invention:	ENABLING SUBSCRIPTION IDENTIFIER PRIVACY
First Named Inventor/Applicant Name:	Vesa Torvinen
Customer Number:	24112
Filer:	William G Pagan/Kenyatta Upchurch
Filer Authorized By:	William G Pagan
Attorney Docket Number:	4015-10071 / P72588-US1
Receipt Date:	25-JUL-2017
Filing Date:	
Time Stamp:	14:35:37
Application Type:	Provisional

Payment information:

Submitted with Payment	yes
Payment Type	EFT
Payment was successfully received in RAM	\$ 260
RAM confirmation Number	072617INTEFSW14362300
Deposit Account	
Authorized User	
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:	

File Listing:					
Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		P72588-US1_Provisional_Application.pdf	384553	yes	53
			c01b460611fee1b74e0bc7da003e2a546d311b80		
	Multipart Description/PDF files in .zip description				
	Document Description		Start	End	
	Specification		1	34	
	Claims		35	53	
Warnings:					
Information:					
2	Application Data Sheet	P72588-US1_Application_Data_Sheet.pdf	1823521	no	10
			adedb025cb4fdff4ee5d56d025ce0cbe8976ca521		
Warnings:					
Information:					
3	Fee Worksheet (SB06)	fee-info.pdf	30113	no	2
			dca1b1b81708728b802e4c5e36992521793f15df		
Warnings:					
Information:					
Total Files Size (in bytes):			2238187		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

**DOCUMENT MADE AVAILABLE UNDER THE
PATENT COOPERATION TREATY (PCT)**

International application number:	PCT/EP2018/069432
International filing date:	17 July 2018 (17.07.2018)
Document type:	Certified copy of priority document
Document details:	Country/Office: US
	Number: 62/536632
	Filing date: 25 July 2017 (25.07.2017)
Date of receipt at the International Bureau:	04 August 2018 (04.08.2018)

Remark: Priority document submitted or transmitted to the International Bureau in compliance with Rule 17.1(a),(b) or (b-bis)

34, chemin des Colombettes
1211 Geneva 20, Switzerland
www.wipo.int