Innovation, Sciences et Développement économique Canada
Office de la Propriété Intellectuelle du Canada

Innovation, Science and Economic Development Canada
Canadian Intellectual Property Office

CA 2916527 C 2023/10/10

(11)(21) 2 916 527

(12) BREVET CANADIEN
CANADIAN PATENT

(13) C

(86) Date de dépôt PCT/PCT Filing Date: 2014/06/24
(87) Date publication PCT/PCT Publication Date: 2015/01/22
(45) Date de délivrance/Issue Date: 2023/10/10
(85) Entrée phase nationale/National Entry: 2015/12/21
(86) N° demande PCT/PCT Application No.: IB 2014/002161
(87) N° publication PCT/PCT Publication No.: 2015/008158
(30) Priorité/Priority: 2013/06/24 (US13/925,299)

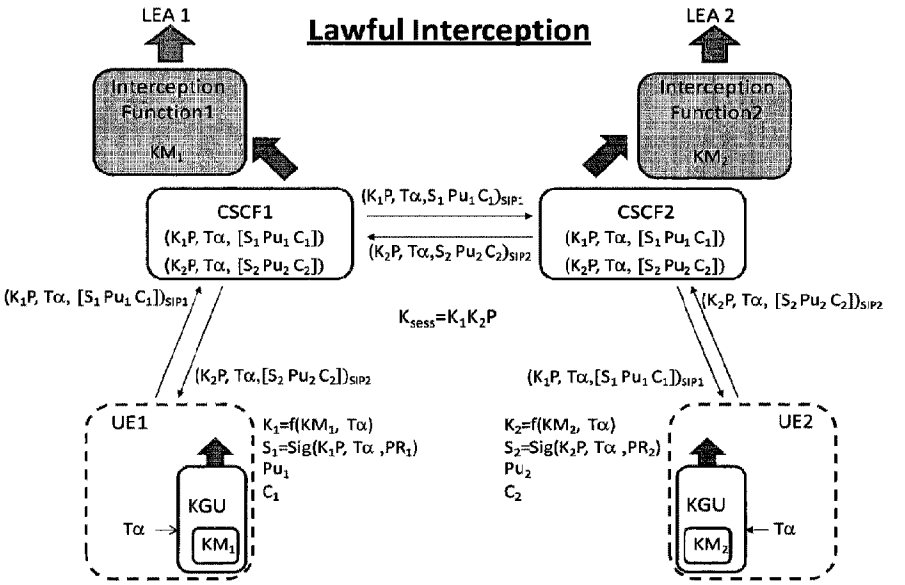
(51) Cl.Int./Int.Cl. *H04L 9/30* (2006.01)

(72) Inventeurs/Inventors:
BUCKLEY, MICHAEL EOIN, US;
HOLLATZ, MICHAEL CHARLES, US;
LAMBERT, ROBERT JOHN, CA;
EBEID, NAVINE MAURICE NASSIF, CA

(73) Propriétaire/Owner:
BLACKBERRY LIMITED, CA

(74) Agent: RIDOUT & MAYBEE LLP

(54) Titre : PROCEDE DE SECURISATION POUR UNE INTERCEPTION LEGALE
(54) Title: SECURING METHOD FOR LAWFUL INTERCEPTION



(57) Abrégé/Abstract:
A method is presented for secure communication, the method including generating a signature using a private key, a nonce, and at least one of an identifier and a key component; and transmitting the signature, the nonce, a security parameter, and the at least one of the identifier and the key component, wherein the security parameter associates a user identity with a public key, the public key being associated with the private key.

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

CORRECTED VERSION

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
22 January 2015 (22.01.2015)

WIPO | PCT

(10) International Publication Number
WO 2015/008158 A8

(51) International Patent Classification:
H04L 9/30 (2006.01) *H04W 12/04* (2009.01)

(21) International Application Number:
PCT/IB2014/002161

(22) International Filing Date:
24 June 2014 (24.06.2014)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
13/925,299 24 June 2013 (24.06.2013) US

(71) Applicants: **BLACKBERRY LIMITED** [CA/CA]; 2200 University Avenue East, Waterloo, ON N2K 0A7 (CA). **CERTICOM CORP** [CA/CA]; 4701 Tahoe Blvd, Building A, Mississauga, ON L4W 0B5 (CA).

(72) Inventors: **BUCKLEY, Michael, Eoin**; 1368 Wild Indigo Road, Grayslake, IL 60030 (US). **HOLLATZ, Michael, Charles**; 10415 Fair Lane, Huntley, IL 60142 (US). **LAMBERT, Robert, John**; 63 Holm Street, Cambridge, ON N3C 3N3 (CA). **EBEID, Navine, Maurice Nassif**; 242 Briarmeadow Drive, Kitchener, ON N2A 4C4 (CA).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ,

[Continued on next page]

(54) Title: SECURING METHOD FOR LAWFUL INTERCEPTION

(57) Abstract: A method is presented for secure communication, the method including generating a signature using a private key, a nonce, and at least one of an identifier and a key component; and transmitting the signature, the nonce, a security parameter, and the at least one of the identifier and the key component, wherein the security parameter associates a user identity with a public key, the public key being associated with the private key.

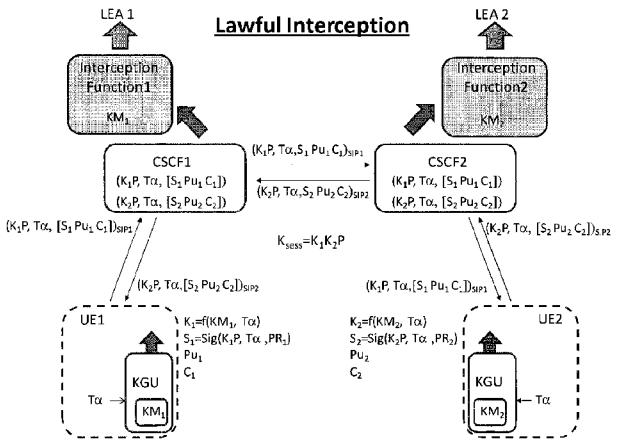


FIG. 4

WO 2015/008158 A8

WO 2015/008158 A8

TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Published:

— *with international search report (Art. 21(3))*

(88) Date of publication of the international search report:
16 July 2015

(48) Date of publication of this corrected version:
3 September 2015

(15) Information about Correction:
see Notice of 3 September 2015

SECURING METHOD FOR LAWFUL INTERCEPTION

FIELD

The present disclosure is directed to a secure method of lawful interception.

BACKGROUND

The 3rd Generation Partnership Project (3GPP) is currently considering several lawful interception and key generation approaches for IP Multimedia Subsystem (IMS) media security. One such key generation approach is Multimedia Internet KEYing – Identity Based Authentication Key Exchange (MIKEY-IBAKE), which is an example of the well-known Diffie-Hellman key exchange. The goal of such a key generation protocol is to establish agreement on a session key K_{sess} between two UEs, where UE stands for user equipment

As shown in Figure 1, the steps in the MIKEY-IBAKE processcan be summarized as follows: (1) UE_1 generates private key information K_1 by using a its key generation unit (KGU); (2) UE_1 computes K_1P using K_1 and a publicly known elliptic curve point P; (3) UE_1 transmits K_1P to UE_2 using Session Initiation Protocol (SIP) signaling via device $CSCF_1$ and device $CSCF_2$, each of which implements a Call Session Control Function (CSCF); (4) UE_2 generates private key information K_2 by using its KGU; (5) UE_2 computes K_2P using K_2 and the publicly known elliptic curve point P; (6) UE_2 transmits K_2P to UE_1 using SIP signaling; and (7) UE_1 and UE_2 each generate $K_{sess}=K_1K_2P$ using $[K_1,K_2P]$ and $[K_1P, K_2]$, respectively.

In Figure 1, the only entities with knowledge of the session key are UE_1 and UE_2. However, in addition to providing secure communications between UEs, government regulations also require that lawful interception be supported.

Figure 2 illustrates a conventional key generation process allowing for lawful interception. As shown in Figure 2, each KGU in a corresponding UE_i produces

corresponding keying information K_i in a defined way from a corresponding master key KM_i and a timestamp $T\alpha$. The master key KM_i is known only to the corresponding UE_i and a corresponding network device that is configured to perform a network intercept function under control of a corresponding law enforcement agency (LEA), as illustrated in Figure 2. For example, $CSCF_1$ and a corresponding intercept device of LEA_1 are part of a first network, while $CSCF_2$ and a corresponding intercept device of LEA_2 are part of a second network, which is in communication with the first network.

Further, the timestamp $T\alpha$ used in generating the corresponding keying information K_i is transmitted along with K_iP in SIP by each corresponding UE_i. Both K_iP and $T\alpha$ can be stored in one or more of the CSCF devices ($CSCF_1$ and $CSCF_2$) in the respective networks, as shown in Figure 2. In particular, note that Figure 2 shows the general case of UEs located in different networks, thus requiring separate CSCF devices. When UEs are located in a single network, only one CSCF device need be used.

The steps taken by the interception device of LEA_2 in generating the session key K_{sess} for the purpose of lawful interception are as follows: (1) retrieve KM_2 (used by UE_2) from internal storage, and retrieve K_1P and $T\alpha$ from device $CSCF_2$; (2) generate keying information $K_2 = f(KM_2,T\alpha)$; and (3) generate $K_{sess} = K_1K_2P$. The interception device of LEA_2 can now decrypt traffic between UE_1 and UE_2 and forward it to LEA_2. The interception process for the interception device of LEA_1 is analogous, but uses KM_1, $T\alpha$, and K_2P.

Further, note that the above lawful interception process can be generalized so that UE_1 and UE_2 use different timestamps for key generation and/or signaling (e.g., $T\alpha_1$, $T\alpha_2$).

BRIEF DESCRIPTION OF THE DRAWINGS

A more complete appreciation of the embodiments described therein, and many of the attendant advantages thereof will be readily obtained as the same becomes better understood by reference to the following detailed description when considered in connection with the accompanying drawings, wherein:

FIG. 1 illustrates the MIKEY-IBAKE process;

FIG. 2 illustrates a conventional lawful interception process;

FIG. 3 illustrates a process that prevents lawful interception;

FIG. 4 illustrates a novel method for secure lawful interception according to one embodiment;

FIG. 5 is a flowchart of the steps in a novel method of secure lawful interception according to one embodiment;

FIG. 6 illustrates a novel method of secure lawful interception using IMEI according to one embodiment;

FIG. 7 illustrates a novel method of secure lawful interception using MAC tags according to one embodiment; and

FIG. 8 illustrates hardware that can be used in the disclosed embodiments.

DETAILED DESCRIPTION

Lawful interception for the MIKEY-IBAKE process relies on network knowledge of the timestamp Tα used to generate keying information. However, a subversive user could change the software running on a UE to avoid lawful interception by using a timestamp in generating key information that is different from the timestamp signaled in SIP, thus generating a different key component ($K_{2\beta}P$), but transmitting a timestamp Tα that was not used to generate the key component $K_{2\beta}P$.

For example, as shown in Figure 3, suppose UE_2's user is malicious and wants to prevent lawful interception in his network. He thus rebuilds the kernel software that runs on his device and modifies the SIP stack such that the timestamp $T\alpha$ used for signaling on SIP is different from the timestamp $T\beta$ used for generating the keying information. As a result, the network is unable to regenerate the necessary keying information $K_{2\beta}$ for UE_2, thus preventing lawful interception.

In this example, the second network stores $K_{2\beta}P$, and thus has the necessary information to determine that UE_2 has not used $T\alpha$ in generating $K_{2\beta}$.

If device $CSCF_2$ in the second network detects the misuse at call set-up, the network could disallow the communication. However, to be effective, the network would be required to verify $K_{2\beta}P$ in at least some percentage of call set-ups, which is highly undesirable from an operator's point of view. Operators strongly prefer any such checking, if necessary, be done at the UE.

Alternatively device $CSCF_2$ in the second network could verify $K_{2\beta}P$ as a part of the lawful interception process. However, any action such as disabling the phone or simply cutting communication, would break an existing requirement that lawful interception be undetectable by any entity except the requesting law enforcement agency and the intercepting network.

An additional consequence of this requirement is that the second network cannot work with the first network for lawful interception. For instance, in the above example, the first network has all the information necessary for lawful interception, i.e., $K_{2\beta}P$, $T\alpha$, and KM_1. However, because LEA_2 may not necessarily wish to reveal that lawful interception is occurring, any final key exchange protocol must enable the second network to carry out lawful interception without the need for contacting any additional entity.

Therefore, while the second network can detect malformed key information in the current MIKEY-IBAKE process, this process requires further modification in order to become a feasible solution meeting all current requirements.

Further, it should be noted that if both UE_1 and UE_2 have the freedom to modify their kernels, they are also free to implement any key agreement scheme, potentially even one different from a standardized key agreement scheme, but with signaling that is compliant. With the arrival of open source operating systems, such as Android, the ability to modify a kernel is, unfortunately, an accepted fact today. In fact, that ability is often touted as being desirable. Since lawful interception becomes highly improbable in such a scenario, the problem addressed herein is that of protecting against one of two UEs maliciously modifying its kernel to prevent lawful interception.

A related problem is SIP signaling of the International Mobile Station Equipment Identity (IMEI), which is an identifier of the mobile equipment (ME), i.e, of the UE not including the Subscriber Identity Module (SIM) card. The IMEI is used in some jurisdictions as the identifier under which lawful interception occurs. However, due to counterfeiting, more than one phone may share the same IMEI. While this is less of a problem in Western regions of the world, it is quite problematic in others. If multiple MEs share the same IMEI, then specifying the targeted ME becomes a more-involved process, making lawful interception more difficult. Additionally, if a UE modifies its kernel, there is a danger the UE may also signal a false IMEI, perhaps preventing lawful interception through IMEI targeting. Thus, a solution for the secure signaling of the IMEI is also needed.

In conventional systems, the subversive user will often be successful since there is insufficient security protection of the timestamp $T\alpha$ used by each KGU. What is needed is a method to guarantee that the timestamp used by the KGU is also signaled in SIP.

Accordingly, there is provided a method for secure communication, comprising: (1) generating a signature using a private key, a nonce, and at least one of an identifier and a key component; and (2) transmitting the signature, the nonce, a security parameter, and the at least one of the identifier and the key component, wherein the security parameter associates a user identity with a public key, the public key being associated with the private key. The identifier is one of an International Mobile Station Equipment Identity (IMEI), a Globally Routable User Agent URI (GRUU), an International Mobile Subscriber Identity (IMSI), and a Temporary International Mobile Subscriber Identity (TIMSI). Further, the nonce is one of a timestamp, a random number, and a sequence number and the security parameter is a certificate.

In another embodiment, there is provided a method for secure communication, the method comprising: (1) receiving a nonce, at least one of an identifier and a key component, a security parameter, and a signature that was generated using a private key, the nonce, and the at least one of the identifier and the key component; and (2) verifying the nonce and the at least one of the identifier and the key component using the received signature and the security parameter, wherein the security parameter associates a user identity with a public key, the public key being associated with the private key. When verification is successful in the verifying step, the method further includes (1) generating a session key using the at least one of the identifier and the key component; (2) generating a second signature using a second private key, a second nonce, and at least one of a second identifier and a second key component; and (3) transmitting the second signature, the second nonce, a second security parameter, and the at least one of the second identifier and the second key component, wherein the second security parameter associates a second user identity with a second public key, the second public key being associated with the second private key.

In another embodiment, there is provided a method for secure communication, the method comprising: (1) generating a MAC tag using a MAC key, a nonce, and at least one of an identifier and a key component; and (2) transmitting the MAC tag, the nonce, and the at least one of the identifier and the key component.

In another embodiment, there is provided a method for secure communication, the method comprising: (1) receiving a nonce, at least one of an identifier and a key component, and a MAC tag that was generated using the nonce, the at least one of the identifier and the key component, and a MAC key; (2) verifying the nonce and the at least one of the identifier and the key component using the received MAC tag.

In particular, in one embodiment, the KGU of a UE_j signs the timestamp $T\alpha$ and the key component K_jP using a private key PR_j obtained at the time of manufacture. The public key Pu_j associated with the private key PR_j is certified by a certificate C_j, which can also be provided to the KGU at the time of manufacture. Note that while the public key is described as being separate from the certificate, in general, the public key can form part of the certificate.

Figure 4 provides an illustration of a method of key component protection according to one embodiment.

As shown in Figure 4, after signing $T\alpha$□□ and K_jP using the function $S_j = Sig(K_jP, T\alpha, PR_j)$□, each KGU passes not only the key component K_jP and the timestamp $T\alpha$ to the software, but also the signature S_j, the public key Pu_j, and the certificate C_j for transmission on SIP. Note that since the KGUs are often implemented in hardware, the KGUs are expected to be significantly more robust to tampering by a malicious user. Further, by passing S_j, Pu_j, and C_j to SIP for signaling, both the receiving UE and the network can be assured of the timestamp $T\alpha$ used in generating K_{sess}.

While it is necessary that the key components and timestamps transmitted by UE_1 and UE_2 are verified during the key generation process, it is preferable that the verification entity be the KGU or some other entity of the UE. Additionally the network CSCF devices can also perform this verification. However, it is likely that operators would prefer not to verify every key exchange, and instead would push such checking to the UE rather than perform this task within the network, other than for lawful interception warrants, in order to lighten the network load. When verification of the timestamp fails, the connection attempt can be terminated by the verification entity in which the failure occurs. If a UE refuses a connection due to failed verification, an alert can be signaled to the network, e.g., as a first step in blacklisting the transgressing UE.

Figure 5 illustrates the steps in the key component protection method according to one embodiment.

In step 501, UE_1's KGU generates the key component K_1 and the signature S_1.

In step 502, UE_1 transmits $(K_1P, T\alpha, [S_1\ Pu_1\ C_1])_{SIP1}$ in the SIP header to device $CSCF_1$.

In step 503, device $CSCF_1$ stores a copy of $(K_1P, T\alpha, [S_1\ Pu_1\ C_1])_{SIP1}$ in addition to forwarding $(K_1P, T\alpha, [S_1\ Pu_1\ C_1])_{SIP1}$ to device $CSCF_2$.

In step 504, device $CSCF_2$ stores a copy of $(K_1P, T\alpha, [S_1\ Pu_1\ C_1])_{SIP1}$ in case it is needed for lawful interception. Device $CSCF_2$ also forwards $(K_1P, T\alpha, [S_1\ Pu_1\ C_1])_{SIP1}$ to UE_2.

In step 505a, UE_2 receives $(K_1P, T\alpha, [S_1\ Pu_1\ C_1])_{SIP1}$ and checks the signature S_1. If the signature is verified, UE_2 computes the session key $K_{sess}=K_1K_2P$ in step 505b. then proceeds to step 506. Otherwise, the connection is refused and the key agreement protocol terminated.

In step 506, UE_2's KGU generates the key component K_2 and the signature S_2.

In step 507, UE_2 transmits $(K_2P, T\alpha, [S_2\ Pu_2\ C_2])_{SIP2}$ in the SIP header to device $CSCF_2$.

In step 508, device $CSCF_2$ stores a copy of $(K_2P, T\alpha, [S_2\ Pu_2\ C_2])_{SIP2}$ in addition to forwarding $(K_2P, T\alpha, [S_2\ Pu_2\ C_2])_{SIP2}$ to device $CSCF_1$.

Step In step 509, device $CSCF_1$ stores a copy of $(K_2P, T\alpha, [S_2\ Pu_2\ C_2])_{SIP2}$ in case it is needed for lawful interception. Device $CSCF_1$ also forwards $(K_2P, T\alpha, [S_2\ Pu_2\ C_2])_{SIP2}$ to UE_1.

In step 510a, UE_1 receives $(K_2P, T\alpha, [S_2\ Pu_2\ C_2])_{SIP2}$ and checks the signature S_2. If the signature is verified, UE_1 computes the session key $K_{sess}=K_1K_2P$ in step 510b and protected communication commences. Otherwise, the connection is refused and the key agreement protocol terminated.

Note that this embodiment includes the signing of parameters used in key generation, and thus need not be limited to the example case of the MIKEY-IBAKE key agreement protocol discussed above. This embodiment can be extended to other key agreement protocols currently under consideration for IMS Media Security, such as MIKEY-TICKET and Session Description protocol security description (SDES).

Similarly, the signed parameter need not be a timestamp and need not be the same in both UEs. For example, each UE could use its own specific nonce value in generating the keying information K_j, which it signs and which is signaled in some fashion to the target UE through the network. A signature on the nonce value will enable it to be verified, similarly to the timestamp discussed above. The nonce can be, e.g., a timestamp, a random number, or a sequence number.

In another embodiment, to protect the integrity of the IMEI, a hardware portion of the UE signs a nonce and the IMEI. The nonce N_i can be, e.g., randomly generated or be the timestamp $T\alpha$ signaled in SIP. As shown in Figure 6, instead of signaling the IMEI alone, a

protocol contains the elements $IMEI_i$, N_i, and $[S_i\ Pu_i\ C_i]$, where the additional information N_i and $[S_i\ Pu_i\ C_i]$ is carried in an extension field.

Similar to the case in key generation, the integrity protection of $IMEI_1$ can be verified by any one of several entities, such as LEA_1, LEA_2, UE_2 or any network (including either CSCF device). As discussed above, it is preferable that such checking be done by UEs, and connections refused in the case of verification failure.

If a UE refuses a connection due to a failed verification, an alert can be signaled to the network, e.g. as a first step in blacklisting a likely counterfeit UE. Since the verification information ($IMEI_i$, N_i, $[S_i, Pu_i\ C_i]$) is stored in the CSCF device, the network also has the means to re-validate any such alert as a further step in determining a counterfeit UE.

In another embodiment, instead of using a signature mechanism, each KGU computes a Message Authentication Code (MAC) tag from a MAC key. As shown in Figure 7, the signature, the public key, and the certificate used in the embodiment of Figure 4 are replaced by the computed MAC tag.

Note that since the use of a MAC tag amounts essentially to a symmetric key signature scheme, the interception device associated with a given UE network and the corresponding KGU of the UE must first agree on a MAC key ($KMAC_i$) with which to compute the MAC tag, as shown in Figure 7. Note that this embodiment has an advantage in complexity over the embodiment shown in Figure 4 since generation of a MAC tag is cheaper than that of a digital signature.

However, one disadvantage of this embodiment is that only the interception function in the UE's current network stores the MAC key $KMAC_i$, which is needed to verify the MAC tag of UE_i. Thus, storage of the MAC tag may only be needed in the CSCF device directly serving the UE. Further, UE_2 can no longer verify the timestamp of UE_1 (or visa versa).

Stated differently, interception device of LEA_1 is the only entity outside of UE_1 that can verify MAC_1 as the MAC tag computed for $[K_1P,T\alpha]$.

The embodiment of Figure 4 achieves the goal of lawful interception by binding the Elliptic curve Diffie–Hellman (ECDH) key component K_iP to the timestamp used in deriving K_i. In other alternative methods, this binding can be achieved in different ways.

For example, in a first alternative method, the session key can be derived using a key derivation function (KDF) that takes as input the ECDH-generated key as well as the two timestamps (nonces).

In a second alternative method, both time stamps are multiplied as scalars by the ECDH-generated key. For example, UE_2 calculates $K_{sess} = T\alpha_1 T\alpha_2 K_2 K_1 P$ after checking that $T\alpha_1 T\alpha_2 K_2 \bmod n \neq 1$, where n is the group order, i.e., the order of P.

A third alternative method is a slightly modified version of Elliptic Curve Menezes-Qu-Vanstone (ECMQV) that incorporates both time stamps, which are here called $T\alpha_1$ and $T\alpha_2$, in the session key calculation. The timestamps are also treated as nonces. This approach is more bandwidth efficient since a signature is not signaled on SIP, and is more calculation efficient compared to the timestamp signature verification method.

In this third alternative method, UE_2 has a long term key (d_2, Pu_2), where Pu_2 is in UE_2's certificate C_2. Here d_2 can be derived from KM_2 through a KDF, since LEA_2 is able to calculate it. Alternatively, d_2 can be another ephemeral derived through KDF along with k_2.

Then, the sequence of calculations in the KGU of UE_2 is:

(1) $k_2 = f(KM_2, T\alpha_2)$; (same as K_2 as calculated in Fig. 2)

(2) $G_2 = k_2P$; (as before, here ECMQV starts)

(3) $s_2 = k_2 + T\alpha_2 \, x(G_2) \, d_2 \pmod n$; (ECMQV with the addition of $T\alpha_2$)

(4) UE_2 sends $[G_2, T\alpha_2, C_2]$ to UE_1 and UE_2 receives $[G_1, T\alpha_1, C_1]$ from UE_1;

(5) $K_{sess} = hs_2(G_1 + [T\alpha_1 \, x(G_1)] \, Pu_1)$; (ECMQV with the addition of $T\alpha_1$)

Note that while calculating s_2, UE_2 checks that $T\alpha_2\ x(G_2) \bmod n \neq 1$, otherwise the process goes back to step 1. Further, while calculating K_{sess}, UE_2 checks that $T\alpha_1\ x(G_1) \bmod n \neq 1$, otherwise the process aborts.

If UE_2 attempts to signal on SIP a $T\alpha_2$' that is different from $T\alpha_2$, the session key will not be established correctly. This assures LEA_2 that $T\alpha_2$ is the one used in the calculation inside KGU_2. An extra check can be performed by LEA_2: (1) $k_2' = f(KM_2, T\alpha_2)$, and (2) check that $G_2' = k_2' P$ is equal to G_2.

Also note the second and third alternative methods described above both require some modification to the key protocol itself, and thus might entail greater changes to prior agreements within 3GPP.

The embodiments described above have several advantages in that they (1) can secure integrity protection of keying information and UE-identifier information using a MAC tag or signature; (2) can be used to refuse connection and/or reporting of malicious UEs by other UEs; (3) can be used by the network as a means of blacklisting counterfeit or compromised UEs; and (4) if the target UE or KGU are verification entities, the embodiments place no significant load on the network, thus reducing network implementation concerns.

Devices $CSCF_1$ and $CSCF_2$, as well as the intercepting devices of LEA_1 and LEA_2, can be implemented by one or more computers and/or one or more specialized circuits. A hardware description of such a computer is described with reference to FIG. 8. Further, each UE includes at least one or more processors (e.g., CPUs) , a memory, a display, and a communication interface. The processor is configured to execute software to perform the functionality of the UEs described above. The KGUs described above can be implemented as a specialized hardware circuit or as software executed on the one or more processors.

As shown in Figure 8, the process data and instructions may be stored in memory 302. These processes and instructions may also be stored on a storage medium disk 304 such as a hard drive (HDD) or portable storage medium or may be stored remotely. Further, the claimed advancements are not limited by the form of the computer-readable media on which the instructions of the inventive process are stored. For example, the instructions may be stored on CDs, DVDs, in FLASH memory, RAM, ROM, PROM, EPROM, EEPROM, hard disk or any other information processing device with which the computer communicates, such as a server.

Further, the claimed embodiments may be provided as a utility application, background daemon, or component of an operating system, or combination thereof, executing in conjunction with CPU 300 and an operating system such as Microsoft Windows 7, UNIX, Solaris, LINUX, Apple MAC-OS and other systems known to those skilled in the art.

CPU 301 may be a Xenon or Core processor from Intel of America or an Opteron processor from AMD of America, or may be other processor types that would be recognized by one of ordinary skill in the art. Alternatively, the CPU 301 may be implemented on an FPGA, ASIC, PLD or using discrete logic circuits, as one of ordinary skill in the art would recognize. Further, CPU 301 may be implemented as multiple processors cooperatively working in parallel to perform the instructions of the inventive processes described above.

The computer in FIG. 8 also includes a network controller 306, such as an Intel Ethernet PRO network interface card from Intel Corporation of America, for interfacing with network 399. As can be appreciated, the network 399 can be a public network, such as the Internet, or a private network such as an LAN or WAN network, or any combination thereof and can also include PSTN or ISDN sub-networks. The network 399 can also be wired, such as an Ethernet network, or can be wireless such as a cellular network including EDGE, 3G and 4G wireless cellular systems. The wireless network can also be WiFi, Bluetooth, or any

other wireless form of communication that is known. The network controller 306 may be used to establish a communication channel between the two parties, possibly through the network 399.

The computer further includes a display controller 308, such as a NVIDIA GeForce GTX or Quadro graphics adaptor from NVIDIA Corporation of America for interfacing with display 310, such as a Hewlett Packard HPL2445w LCD monitor. A general purpose I/O interface 312 interfaces with a keyboard and/or mouse 514 as well as a touch screen panel 316 on or separate from display 310. General purpose I/O interface also connects to a variety of peripherals 318 including printers and scanners, such as an OfficeJet or DeskJet from Hewlett Packard.

A sound controller 320 is also provided in the computer, such as Sound Blaster X-Fi Titanium from Creative, to interface with speakers/microphone 322 thereby providing sounds and/or music. The speakers/microphone 322 can also be used to accept dictated words as commands for controlling the computer or for providing location and/or property information with respect to the target property.

The general purpose storage controller 324 connects the storage medium disk 304 with communication bus 326, which may be an ISA, EISA, VESA, PCI, or similar, for interconnecting all of the components of the computer. A description of the general features and functionality of the display 310, keyboard and/or mouse 314, as well as the display controller 308, storage controller 324, network controller 306, sound controller 320, and general purpose I/O interface 312 is omitted herein for brevity as these features are known.

In the above description, any processes, descriptions or blocks in flowcharts should be understood to represent modules, segments, or portions of code that include one or more executable instructions for implementing specific logical functions or steps in the process, and alternate implementations are included within the scope of the exemplary embodiments

of the present advancements in which functions may be executed out of order from that shown or discussed, including substantially concurrently or in reverse order, depending upon the functionality involved, as would be understood by those skilled in the art.

While certain embodiments have been described, these embodiments have been presented by way of example only, and are not intended to limit the scope of the inventions. Indeed, the novel methods, apparatuses and systems described herein may be embodied in a variety of other forms; furthermore, various omissions, substitutions and changes in the form of the methods, apparatuses and systems described herein may be made without departing from the spirit of the inventions. The accompanying claims and their equivalents are intended to cover such forms or modifications as would fall within the scope and spirit of the inventions.

CLAIMS

1. A method for secure communication by an electronic device with at least one other electronic device, the method comprising:

generating a signature using a private key, a nonce, and at least one of an identifier and a key component;

transmitting the signature, the nonce, a security parameter, and the at least one of the identifier and the key component, wherein the security parameter associates a user identity with a public key, the public key being associated with the private key;

receiving, based on the transmitting, session security data generated by the at least one other electronic device; and

establishing a secure communication session with the at least one other electronic device based on at least the session security data.

2. The method of claim 1, wherein the session security data comprises:

a second nonce, at least one of a second identifier and a second key component, a second security parameter, and a second signature that was generated using a second private key, the second nonce, and the at least one of the second identifier and the second key component; and

wherein establishing the secure communication session comprises:

verifying the second nonce and the at least one of the second identifier and the second key component using the received second signature and the second security parameter, wherein the second security parameter associates a second user identity with a second public key, the second public key being associated with the second private key; and

generating a session key using the at least one of the second identifier and the second key component, when verification is successful in the verifying step.

3. The method of any one of claims 1 or 2, wherein the key component is generated using a master key, the nonce, and a known elliptic curve point.

Date Reçue/Date Received 2022-12-21

4. The method of any one of claims 1 to 3, wherein the transmitting step further comprises transmitting the signature and the public key; and wherein the security parameter is a certificate.

5. A method for secure communication by an electronic device with at least one other electronic device, the method comprising:

receiving a nonce, at least one of an identifier and a key component, a security parameter, and a signature that was generated using a private key, the nonce, and the at least one of the identifier and the key component;

verifying the nonce and the at least one of the identifier and the key component using the received signature and the security parameter, wherein the security parameter associates a user identity with a public key, the public key being associated with the private key;

transmitting, by the electronic device, a session security data to the at least one other electronic device; and

establishing a secure communication session with the at least one other electronic device based on at least the key component that has been verified.

6. The method of claim 5, further comprising:

when verification is successful in the verifying step:

generating a session key using the at least one of the identifier and the key component.

7. The method of claim 5 or claim 6, further comprising:

when verification is successful in the verifying step:

generating a second signature using a second private key, a second nonce, and at least one of a second identifier and a second key component; and

transmitting the second signature, the second nonce, a second security parameter, and the at least one of the second identifier and the second key component, wherein the second security parameter associates a second user identity

with a second public key, the second public key being associated with the second private key.

8. A method for secure communication by an electronic device with at least one other electronic device, comprising:

generating, by the electronic device, a Message Authentication Code (MAC) tag using a MAC key, a nonce, and at least one of an identifier and a key component based on private key information associated with the electronic device and a publically known elliptic curve point;

transmitting the MAC tag, the nonce, and the at least one of the identifier and the key component;

receiving, based on the transmitting, session security data generated by the at least one other electronic device; and

establishing a secure communication session with the at least one other electronic device based on at least the session security data.

9. The method of any one of claims 1 to 8, wherein the identifier is one of an International Mobile Station Equipment Identity (IMEI), a Globally Routable User Agent URI (GRUU), an International Mobile Subscriber Identity (IMSI), and a Temporary International Mobile Subscriber Identity (TIMSI).

10. The method of any one of claims 1 to 9, wherein the nonce is one of a timestamp, a random number, and a sequence number.

11. A method for secure communication by an electronic device with at least one other electronic device, the method comprising:

receiving a nonce, at least one of an identifier and a key component, and a Message Authentication Code (MAC) tag that was generated by the at least one other electronic device using the nonce, the at least one of the identifier and the key component, and a MAC key, wherein the key component was generated by the at least one other electronic device and a publically known elliptic curve point; and

verifying the nonce and the at least one of the identifier and the key component using the received MAC tag; and

establishing a secure communication session with the at least one other electronic device based on at least the key component that has been verified.

12. An apparatus for secure communication, the apparatus being configured to perform the method of any one of claims 1 to 11.

13. A non-transitory machine readable medium having tangibly stored thereon executable instructions that, in response to execution by a processor, cause the processor to perform the method of any one of claims 1 to 11.

14. A method, by an electronic device, for secure communication with at least one other electronic device, the method comprising:

generating, by a processor of the electronic device, a signature using a private key, a nonce, and at least one of an identifier and a key component;

transmitting, by the processor, the signature, the nonce, a security parameter, and the at least one of the identifier and the key component, wherein the security parameter associates a user identity with a public key, the public key being associated with the private key;

receiving, by the processor, based on the transmitting, session security data generated by the at least one other electronic device; and

establishing, by the processor, a secure communication session with the at least one other electronic device based on at least the session security data.

15. The method of claim 14, wherein the identifier is one of an International Mobile Station Equipment Identity (IMEI), a Globally Routable User Agent URI (GRUU), an International Mobile Subscriber Identity (IMSI), and a Temporary International Mobile Subscriber Identity (TIMSI).

16. The method of claim 14, wherein the nonce is one of a timestamp, a random number, and a sequence number.

Date Reçue/Date Received 2022-12-21

17. The method of claim 14, wherein the security parameter is a certificate.

18. The method of claim 14, further comprising:

generating the key component using a master key, the nonce, and a known elliptic curve point.

19. The method of claim 14, wherein the transmitting step further comprises:

transmitting the signature and the public key.

20. The method of claim 14, wherein the session security data comprises a second nonce, at least one of a second identifier and a second key component, a second security parameter, and a second signature that was generated using a second private key, the second nonce, and the at least one of the second identifier and the second key component, and wherein establishing the secure communication session comprises verifying the second nonce and the at least one of the second identifier and the second key component using the received second signature and the second security parameter, wherein the second security parameter associates a second user identity with a second public key, the second public key being associated with the second private key; and generating a session key using the at least one of the second identifier and the second key component, when verification is successful in the verifying step.

21. A method, by an electronic device, for secure communication with at least one other electronic device, the method comprising:

receiving, by a processor of the electronic device, a nonce, at least one of an identifier and a key component, a security parameter, and a signature that was generated using a private key, the nonce, and the at least one of the identifier and the key component;

verifying, by the processor, the nonce and the at least one of the identifier and the key component using the received signature and the security parameter, wherein the security parameter associates a user identity with a public key, the public key being associated with the private key; and

Date Reçue/Date Received 2022-12-21

establishing, by the processor, a secure communication session with the at least one other electronic device based on at the at least one of the identifier and the key component that has been verified.

22. The method of claim 21, further comprising, when verification is successful in the verifying step:

generating a session key using the at least one of the identifier and the key component.

23. The method of claim 21, further comprising, when verification is successful in the verifying step:

generating a second signature using a second private key, a second nonce, and at least one of a second identifier and a second key component; and

transmitting the second signature, the second nonce, a second security parameter, and the at least one of the second identifier and the second key component, wherein the second security parameter associates a second user identity with a second public key, the second public key being associated with the second private key.

24. A method, by an electronic device, for secure communication with at least one other electronic device, the method comprising:

generating, by a processor of the electronic device, a Message Authentication Code (MAC) tag using a MAC key, a nonce, and a key component generated by the electronic device based on private key information associated with the electronic device and a publicly known elliptic curve point; and

transmitting, by the processor, the MAC tag, the nonce, and the key component;

receiving, by the processor, based on to the transmitting, session security data generated by the at least one other electronic device; and

establishing, by the processor, a secure communication session with the at least one other electronic device based on at least the session security data.

25. The method of claim 24, wherein the MAC tag is further generated using an identifier, wherein the identifier is one of an International Mobile Station Equipment Identity (IMEI), a Globally Routable User Agent URI (GRUU), an International Mobile Subscriber Identity (IMSI), and a Temporary International Mobile Subscriber Identity (TIMSI).

26. The method of claim 24, wherein the nonce is one of a timestamp, a random number, and a sequence number.

27. A method, by an electronic device, for secure communication with at least one other electronic device, the method comprising:

receiving, by a processor of the electronic device, a nonce, a key component, and a Message Authentication Code (MAC) tag that was generated by the at least one other electronic device using the nonce, the key component, and a MAC key, wherein the key component was generated by the at least one other electronic device based on private key information associated with the at least one other electronic device and a publicly known elliptic curve point;

verifying, by the processor, the nonce and the key component using the received MAC tag; and

establishing, by the processor, a secure communication session with the at least one other electronic device based on at least the key component that has been verified.

28. An apparatus for secure communication with at least one other apparatus, comprising:

a processing circuit configured to generate a signature using a private key, a nonce, and at least one of an identifier and a key component;

a transmitter configured to transmit the signature, the nonce, a security parameter, and the at least one of the identifier and the key component, wherein the security parameter associates a user identity with a public key, the public key being associated with the private key; and

a receiver configured to receive, based on the transmitting, session security data generated by the at least one other apparatus, wherein the processing circuit is further

Date Reçue/Date Received 2022-12-21

configured to establish, a secure communication session with the at least one other apparatus based on at least the session security data.

29. An apparatus for secure communication with at least one other apparatus, comprising:

a receiver configured to receive a nonce, at least one of an identifier and a key component, a security parameter, and a signature that was generated using a private key, the nonce, and the at least one of the identifier and the key component; and

a processing circuit configured to verify the nonce and the at least one of the identifier and the key component using the received signature and the security parameter, wherein the security parameter associates a user identity with a public key, the public key being associated with the private key, and establish a secure communication session with the at least one other apparatus based on at the at least one of the identifier and the key component that has been verified.

30. An apparatus for secure communication with at least one other apparatus, comprising:

a processing circuit configured to generate a Message Authentication Code (MAC) tag using a MAC key, a nonce, and a key component generated by the apparatus based on private key information associated with the apparatus and a publicly known elliptic curve point; and

a transmitter configured to transmit the MAC tag, the nonce, and the at least one of an identifier and the key component; and

a receiver configured to receive, based on to the transmitting, session security data generated by the at least one other apparatus, wherein the processing circuit is further configured to establish, a secure communication session with the at least one other electronic device based on at least the session security data.

31. An apparatus for secure communication with at least one other apparatus, comprising:

a receiver configured to receive a nonce, a key component, and a Message Authentication Code (MAC) tag that was generated using the nonce, the key component, and a MAC key, wherein the key component was generated by the at least one other apparatus

based on private key information associated with the at least one other electronic device and a publicly known elliptic curve point; and

a processing circuit configured to verify the nonce and the at least one of an identifier and the key component using the received MAC tag; and

establish a secure communication session with the at least one other electronic device based on at least the key component that has been verified.

32. An apparatus for secure communication, the apparatus being configured to perform the method of any one of claims 14 to 27.

33. A non-transitory machine readable medium having tangibly stored thereon executable instructions that, in response to execution by a processor, cause the processor to perform the method of any one of claims 14 to 27.

34. A method, by an electronic device, for secure communication, comprising:

generating, by a processor of the electronic device, a signature using a private key, a nonce, and at least one of an identifier and a key component, at least the signature being destined for reception by at least one other electronic device; and

establishing, by the processor, a secure communication session with the at least one other electronic device based on generating the signature and at least session security data associated with the at least one other electronic device and obtained by the electronic device, the session security data having been verified by at least one remote information processing system that is separate and distinct from the electronic and the least one other electronic device, wherein the session security data is generated, at least in part, by the at least one other electronic device.

35. The method of claim 34, wherein the identifier is one of an International Mobile Station Equipment Identity (IMEI), a Globally Routable User Agent URI (GRUU), an International Mobile Subscriber Identity (IMSI), and a Temporary International Mobile Subscriber Identity (TIMSI).

36. The method of claim 34, wherein the nonce is one of a timestamp, a random number, and a sequence number.

37. The method of claim 34, wherein the secure communication session is further established with the at least one electronic device based on a security parameter, wherein the security parameter is a certificate that associates a user identity with a public key, the public key being associated with the private key.

38. The method of claim 34, further comprising:

generating the key component using a master key, the nonce, and a known elliptic curve point.

39. The method of claim 34, further comprising:

transmitting the signature and a public key associated with the private key.

40. The method of claim 34, further comprising:

receiving the session security data, wherein the session security data comprises a second nonce, at least one of a second identifier and a second key component, a second security parameter, and a second signature that was generated using a second private key, the second nonce, and the at least one of the second identifier and the second key component, and wherein establishing the secure communication session comprises verifying the second nonce and the at least one of the second identifier and the second key component using the received second signature and the second security parameter, wherein the second security parameter associates a second user identity with a second public key, the second public key being associated with the second private key; and

generating a session key using the at least one of the second identifier and the second key component, when verification is successful in the verifying step.

41. A method, by an electronic device, for secure communication, comprising:

establishing, by a processor of the electronic device, a secure communication session with at least one other electronic device based on session security data associated with the at least one other electronic device and obtained by the electronic device, the session security data having been verified by at least one remote information processing system that is separate and distinct from the electronic and the least one other electronic device, wherein the session security data is generated, at least in part, by the at least one other electronic device,

the session security data comprising a nonce, at least one of an identifier and a key component, a security parameter, and a signature that was generated by the at least one other electronic device using a private key, the nonce, and the at least one of the identifier and the key component.

42. The method of claim 41, wherein prior to establishing the secure communication session, the method further comprising:

verifying the nonce and the at least one of the identifier and the key component using the received signature and the security parameter; and

generating a session key using the at least one of the identifier and the key component.

43. The method of claim 41, further comprising, wherein establishing the secure communication session comprises:

generating a second signature using a second private key, a second nonce, and at least one of a second identifier and a second key component; and

transmitting the second signature, the second nonce, a second security parameter, and the at least one of the second identifier and the second key component, wherein the second security parameter associates a second user identity with a second public key, the second public key being associated with the second private key.

44. An apparatus for secure communication, comprising:

a processing circuit configured to generate a signature using a private key, a nonce, and at least one of an identifier and a key component; and

a transmitter configured to transmit session security data comprising the signature, the nonce, a security parameter, and the at least one of the identifier and the key component, where the session security data is destined for reception by at least one electronic device for establishing a secure communication session therewith, and wherein the security parameter associates a user identity with a public key, the public key being associated with the private key.

Date Reçue/Date Received 2022-12-21

45. An apparatus for secure communication, comprising:

a processing circuit configured to establish a secure communication session with at least one other electronic device based on session security data associated with the at least one other electronic device and obtained by the apparatus, the session security data having been verified by at least one remote information processing system that is separate and distinct from the apparatus and the least one other electronic device, the session security data comprising a nonce, at least one of an identifier and a key component, a security parameter, and a signature that was generated by the at least one other electronic device using a private key, the nonce, and the at least one of the identifier and the key component.

46. An apparatus for secure communication, the apparatus being configured to perform the method of any one of claims 34 to 43.

47. A non-transitory machine readable medium having tangibly stored thereon executable instructions that, in response to execution by a processor, cause the processor to perform the method of any one of claims 34 to 43.

48. A method, by an electronic device, for secure communication, comprising:

generating, by a processor of the electronic device, a Message Authentication Code (MAC) tag using a MAC key, a nonce, and at least one of an identifier or a key component generated by the processor based on private key information associated with the electronic device and a publicly known elliptic curve point, wherein the identifier is one of an International Mobile Station Equipment Identity (IMEI), a Globally Routable User Agent URI (GRUU), an International Mobile Subscriber Identity (IMSI), and a Temporary International Mobile Subscriber Identity (TIMSI); and

establishing, by the processor, a secure communication session with the at least one other electronic device based on generating the MAC tag and at least session security data associated with the at least one other electronic device.

49. The method of claim 48, wherein the nonce is one of a timestamp, a random number, and a sequence number.

50. The method of claim 48, further comprising:

generating the key component using a master key, the nonce, and the publically known elliptic curve point.

51. The method of claim 48, further comprising:

transmitting at least the MAC tag, the nonce, and the at least one of the identifier and the key component.

52. The method of claim 51, wherein the MAC tag is received and stored by a remote information processing system.

53. The method of claim 48, further comprising:

receiving the session security data, wherein the session security data comprises a second nonce, at least one of a second identifier and a second key component.

54. A method, by an electronic device, for secure communication, comprising:

establishing, by a processor of the electronic device, a secure communication session with at least one other electronic device based on session security data associated with the at least one other electronic device having been verified by at least one remote information processing system that is separate and distinct from the electronic device and the least one other electronic device, the session security data comprising a nonce, at least one of an identifier and a key component, and a Message Authentication Code (MAC) tag that was generated using the nonce, the at least one of the identifier and the key component, and a MAC key associated with the at least one other electronic device, wherein the identifier is one of an International Mobile Station Equipment Identity (IMEI), a Globally Routable User Agent URI (GRUU), an International Mobile Subscriber Identity (IMSI), and a Temporary International Mobile Subscriber Identity (TIMSI).

55. The method of claim 54, wherein establishing the secure communication session is further based on receiving, from the at least one remote information processing system, at least the key component and the nonce associated with the at least one information processing system.

56. The method of claim 54, wherein the nonce is one of a timestamp, a random number, and a sequence number.

57. The method of claim 54, wherein the key component was generated by the least one electronic device.

58. An apparatus for secure communication, comprising:

a processing circuit configured to generate a Message Authentication Code (MAC) tag using a MAC key, a nonce, and at least one of an identifier or a key component generated by the processing circuit based on private key information associated with the apparatus and a publicly known elliptic curve point, wherein the identifier is one of an International Mobile Station Equipment Identity (IMEI), a Globally Routable User Agent URI (GRUU), an International Mobile Subscriber Identity (IMSI), and a Temporary International Mobile Subscriber Identity (TIMSI); and

establish, a secure communication session with the at least one other electronic device based on generating the MAC tag and at least session security data associated with the at least one other electronic device.

59. The apparatus of claim 58, wherein the nonce is one of a timestamp, a random number, and a sequence number.

60. The apparatus of claim 58, wherein the processing circuit is further configured to generate the key component using a master key, the nonce, and the publicly known elliptic curve point.

61. The apparatus of claim 58, wherein the processing circuit is further configured to transmit at least the MAC tag, the nonce, and the at least one of the identifier and the key component.

62. The apparatus of claim 58, wherein the MAC tag is received and stored by a remote information processing system.

63. The apparatus of claim 58, wherein the processing circuit is further configured to

receive the session security data, wherein the session security data comprises a second nonce and at least one of a second identifier and a second key component.

64. An apparatus for secure communication, comprising:

a processing circuit configured to establish a secure communication session with at least one electronic device based on session security data associated with the at least one electronic device having been verified by at least one remote information processing system that is separate and distinct from the electronic device and the least one other electronic device, the session security data comprising a nonce, at least one of an identifier and a key component, and a Message Authentication Code (MAC) tag that was generated using the nonce, the at least one of the identifier and the key component, and a MAC key associated with the at least one electronic device, wherein the key component was generated by the least one electronic device based on private key information associated with the at least one electronic device and a publicly known elliptic curve point, wherein the identifier is one of an International Mobile Station Equipment Identity (IMEI), a Globally Routable User Agent URI (GRUU), an International Mobile Subscriber Identity (IMSI), and a Temporary International Mobile Subscriber Identity (TIMSI).

65. The apparatus of claim 64, wherein the processing circuit is further configured to establish the secure communication session based on receiving, from the at least one remote information processing system, at least the key component and the nonce associated with the at least one information processing system.

66. The apparatus of claim 64, wherein the nonce is one of a timestamp, a random number, and a sequence number.

67. An apparatus for secure communication, the apparatus being configured to perform the method of any one of claims 48 to 56.

68. A non-transitory machine readable medium having tangibly stored thereon executable instructions that, in response to execution by a processor, cause the processor to perform the method of any one of claims 48 to 56.

Date Reçue/Date Received 2022-12-21

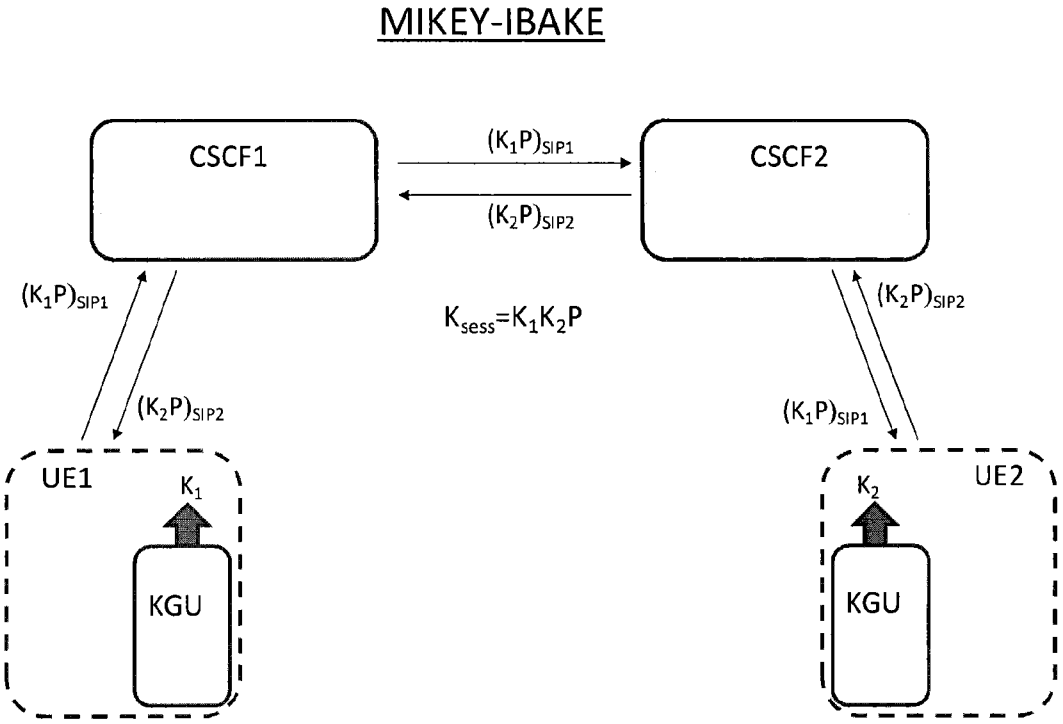

MIKEY-IBAKE
CSCF1
CSCF2
$(K_1P)_{SIP1}$
$(K_2P)_{SIP2}$
$K_{sess}=K_1K_2P$
UE1
UE2
K_1
K_2
KGU
KGU

FIG. 1

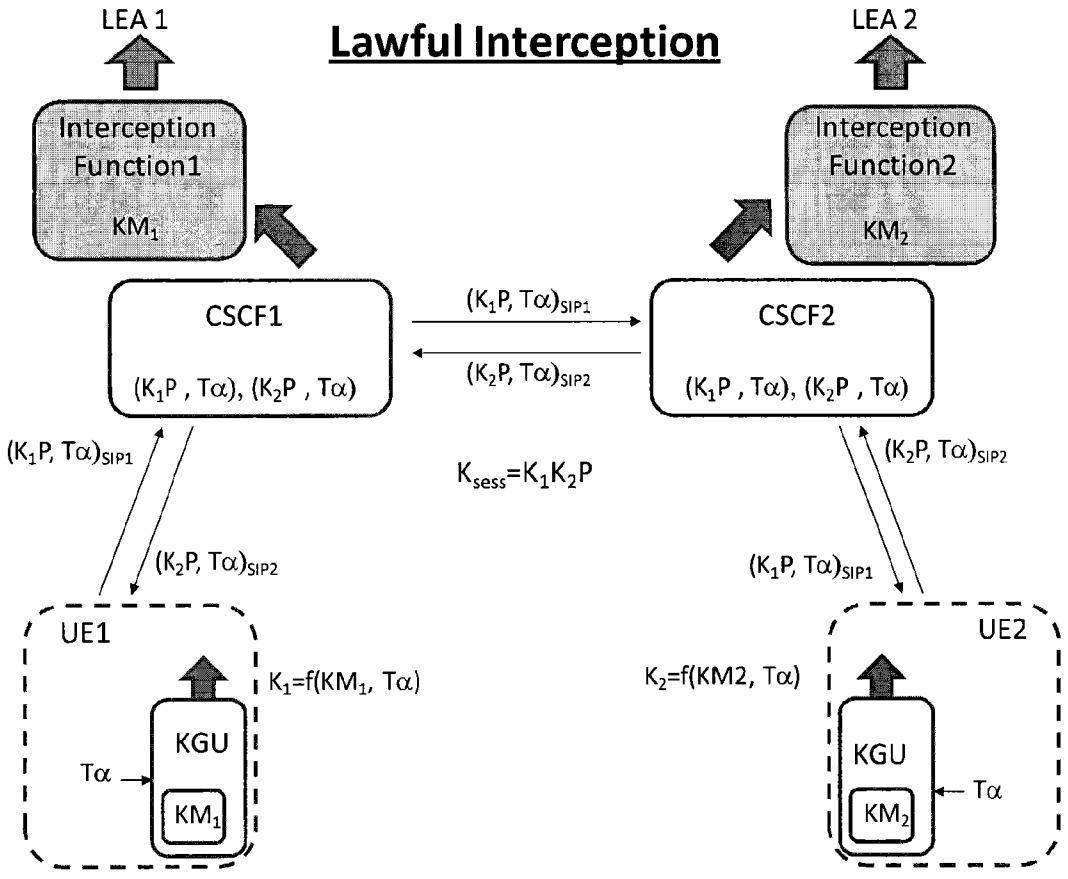

LEA 1
Lawful Interception
LEA 2
Interception Function1
KM1
Interception Function2
KM2
CSCF1
(K1P , Tα), (K2P , Tα)
(K1P, Tα)SIP1
(K2P, Tα)SIP2
CSCF2
(K1P , Tα), (K2P , Tα)
(K1P, Tα)SIP1
(K2P, Tα)SIP2
Ksess=K1K2P
(K2P, Tα)SIP2
(K1P, Tα)SIP1
UE1
K1=f(KM1, Tα)
Tα
KGU
KM1
K2=f(KM2, Tα)
UE2
KGU
KM2
Tα

FIG. 2

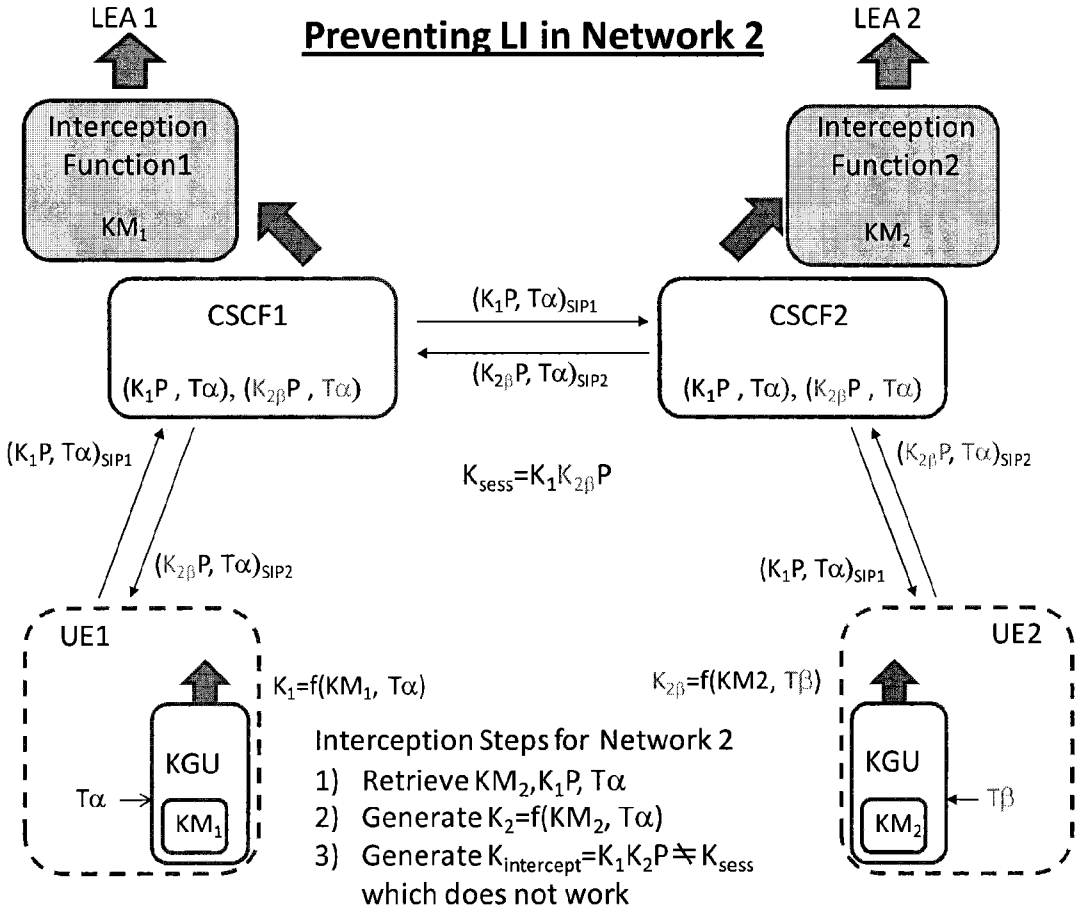

Preventing LI in Network 2
LEA 1
LEA 2
Interception Function1
KM1
Interception Function2
KM2
CSCF1
(K1P , Tα), (K2βP , Tα)
CSCF2
(K1P , Tα), (K2βP , Tα)
(K1P, Tα)SIP1
(K2βP, Tα)SIP2
Ksess=K1K2βP
UE1
UE2
K1=f(KM1, Tα)
K2β=f(KM2, Tβ)
KGU
KM1
Tα
KGU
KM2
Tβ
Interception Steps for Network 2
1) Retrieve KM2,K1P, Tα
2) Generate K2=f(KM2, Tα)
3) Generate Kintercept=K1K2P≠Ksess
which does not work

FIG. 3

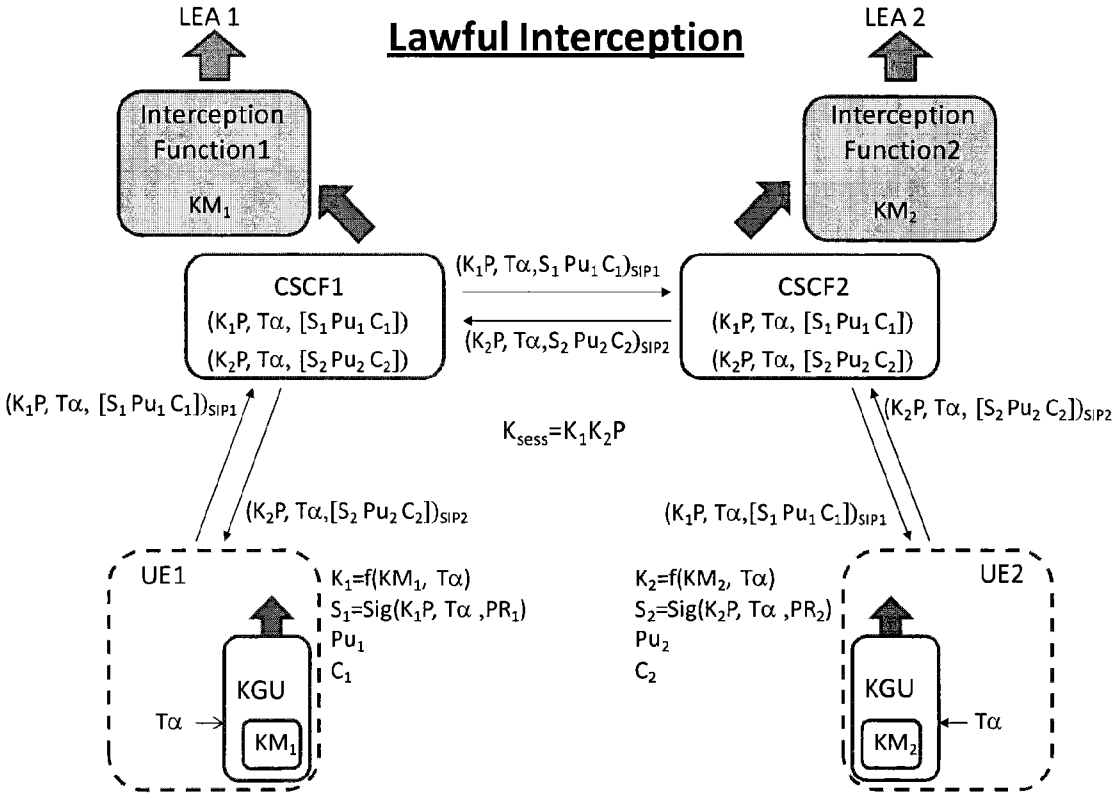

LEA 1
Lawful Interception
LEA 2
Interception Function1
KM1
Interception Function2
KM2
CSCF1
(K1P, Tα, [S1 Pu1 C1])
(K2P, Tα, [S2 Pu2 C2])
(K1P, Tα,S1 Pu1 C1)SIP1
(K2P, Tα,S2 Pu2 C2)SIP2
CSCF2
(K1P, Tα, [S1 Pu1 C1])
(K2P, Tα, [S2 Pu2 C2])
(K1P, Tα, [S1 Pu1 C1])SIP1
(K2P, Tα,[S2 Pu2 C2])SIP2
Ksess=K1K2P
(K2P, Tα, [S2 Pu2 C2])SIP2
(K1P, Tα,[S1 Pu1 C1])SIP1
UE1
K1=f(KM1, Tα)
S1=Sig(K1P, Tα ,PR1)
Pu1
C1
KGU
Tα
KM1
K2=f(KM2, Tα)
S2=Sig(K2P, Tα ,PR2)
Pu2
C2
UE2
KGU
KM2
Tα

FIG. 4

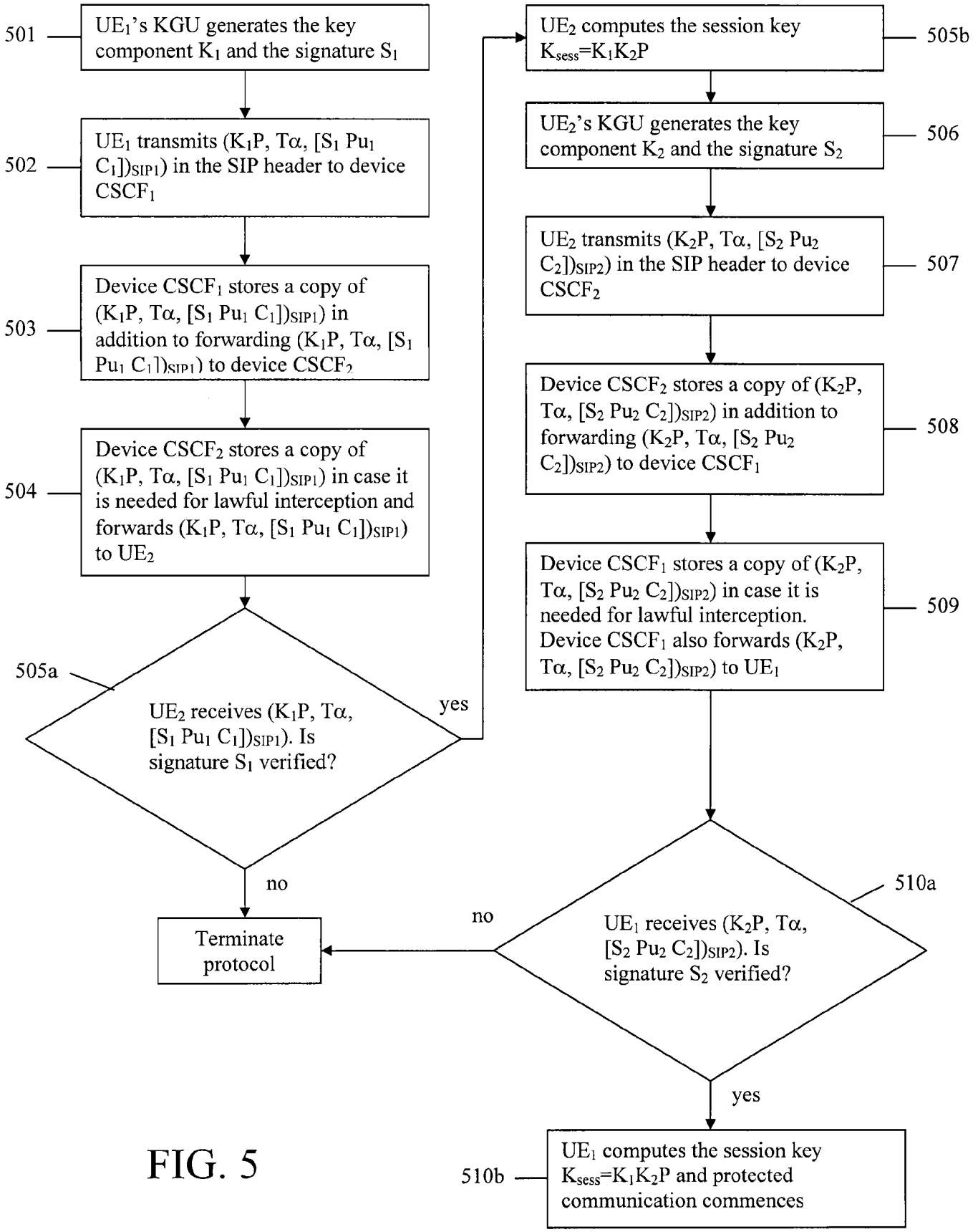

501
UE1's KGU generates the key component K1 and the signature S1
502
UE1 transmits (K1P, Tα, [S1 Pu1 C1])SIP1) in the SIP header to device CSCF1
503
Device CSCF1 stores a copy of (K1P, Tα, [S1 Pu1 C1])SIP1) in addition to forwarding (K1P, Tα, [S1 Pu1 C1])SIP1) to device CSCF2
504
Device CSCF2 stores a copy of (K1P, Tα, [S1 Pu1 C1])SIP1) in case it is needed for lawful interception and forwards (K1P, Tα, [S1 Pu1 C1])SIP1) to UE2
505a
UE2 receives (K1P, Tα, [S1 Pu1 C1])SIP1). Is signature S1 verified?
yes
no
Terminate protocol
505b
UE2 computes the session key Ksess=K1K2P
506
UE2's KGU generates the key component K2 and the signature S2
507
UE2 transmits (K2P, Tα, [S2 Pu2 C2])SIP2) in the SIP header to device CSCF2
508
Device CSCF2 stores a copy of (K2P, Tα, [S2 Pu2 C2])SIP2) in addition to forwarding (K2P, Tα, [S2 Pu2 C2])SIP2) to device CSCF1
509
Device CSCF1 stores a copy of (K2P, Tα, [S2 Pu2 C2])SIP2) in case it is needed for lawful interception. Device CSCF1 also forwards (K2P, Tα, [S2 Pu2 C2])SIP2) to UE1
510a
UE1 receives (K2P, Tα, [S2 Pu2 C2])SIP2). Is signature S2 verified?
no
yes
510b
UE1 computes the session key Ksess=K1K2P and protected communication commences

FIG. 5

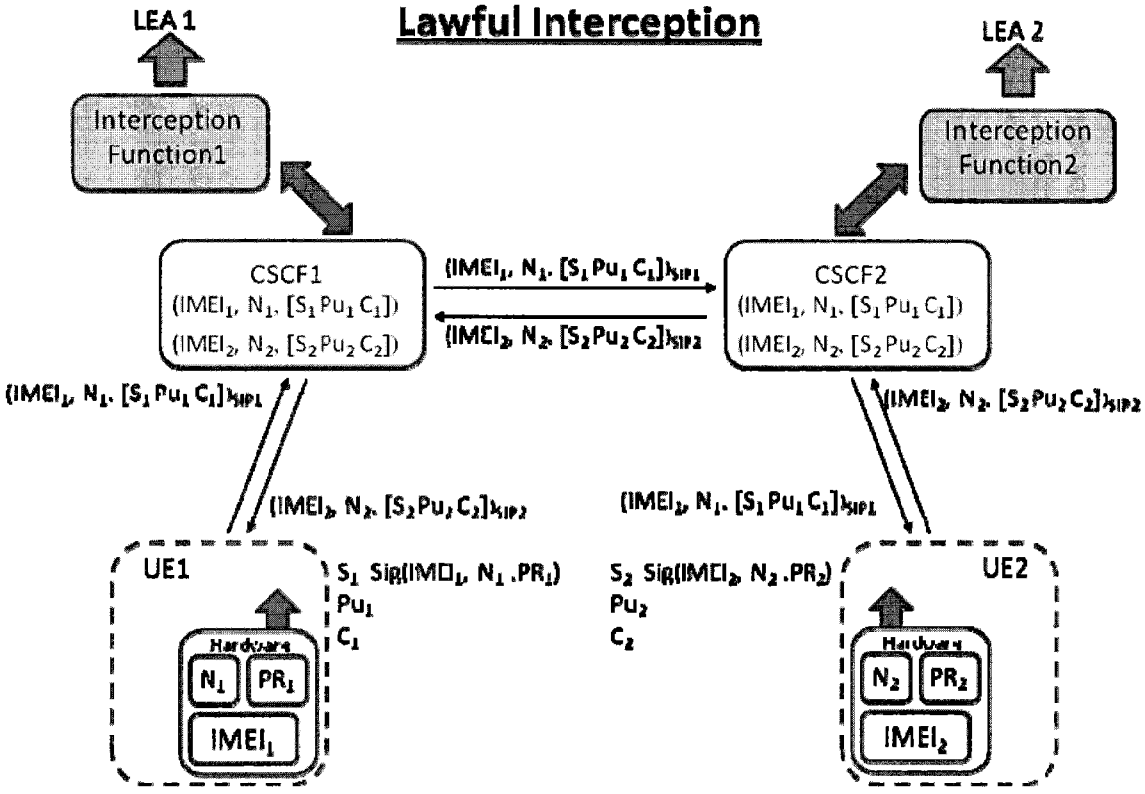

Lawful Interception
LEA 1
LEA 2
Interception Function1
Interception Function2
CSCF1
(IMEI1, N1, [S1 Pu1 C1])
(IMEI2, N2, [S2 Pu2 C2])
CSCF2
(IMEI1, N1, [S1 Pu1 C1])
(IMEI2, N2, [S2 Pu2 C2])
(IMEI1, N1, [S1 Pu1 C1])kSIP1
(IMEI2, N2, [S2 Pu2 C2])kSIP2
UE1
UE2
Hardware
N1
PR1
IMEI1
N2
PR2
IMEI2
S1 Sig(IMEI1, N1 .PR1)
Pu1
C1
S2 Sig(IMEI2, N2 .PR2)
Pu2
C2

FIG. 6

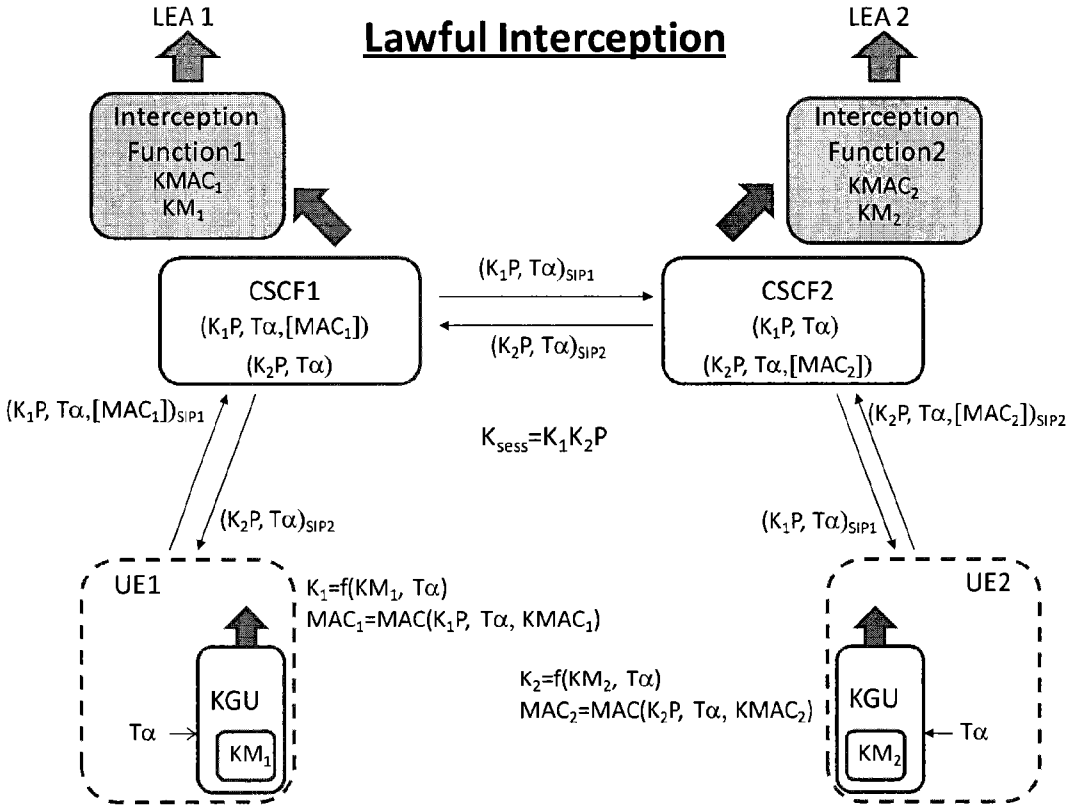

LEA 1
Lawful Interception
LEA 2
Interception Function1
KMAC1
KM1
Interception Function2
KMAC2
KM2
CSCF1
(K1P, Tα,[MAC1])
(K2P, Tα)
(K1P, Tα)SIP1
(K2P, Tα)SIP2
CSCF2
(K1P, Tα)
(K2P, Tα,[MAC2])
(K1P, Tα,[MAC1])SIP1
(K2P, Tα)SIP2
Ksess=K1K2P
(K2P, Tα,[MAC2])SIP2
(K1P, Tα)SIP1
UE1
K1=f(KM1, Tα)
MAC1=MAC(K1P, Tα, KMAC1)
K2=f(KM2, Tα)
MAC2=MAC(K2P, Tα, KMAC2)
UE2
KGU
Tα
KM1
KGU
KM2
Tα

FIG. 7

8/8

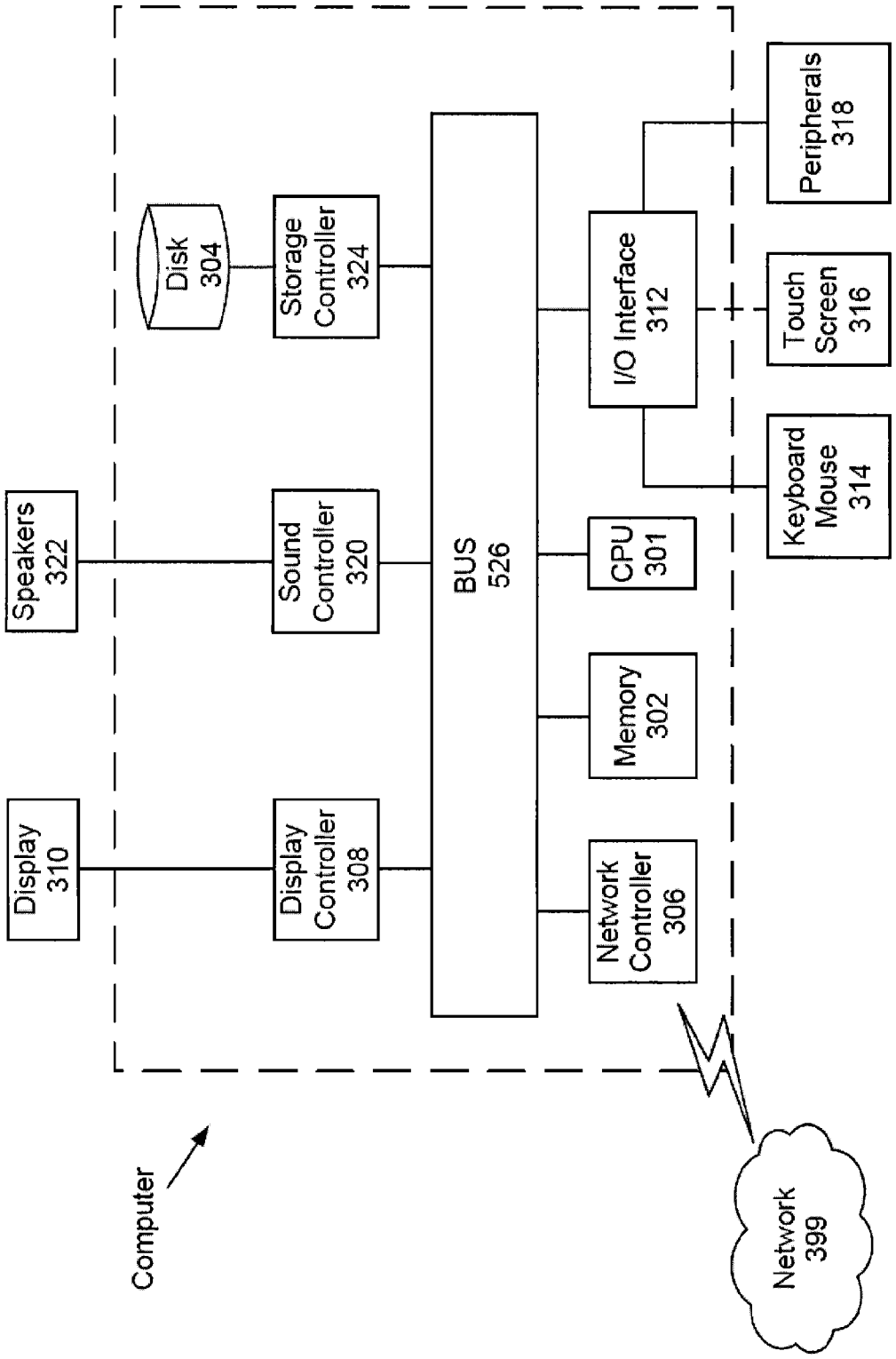
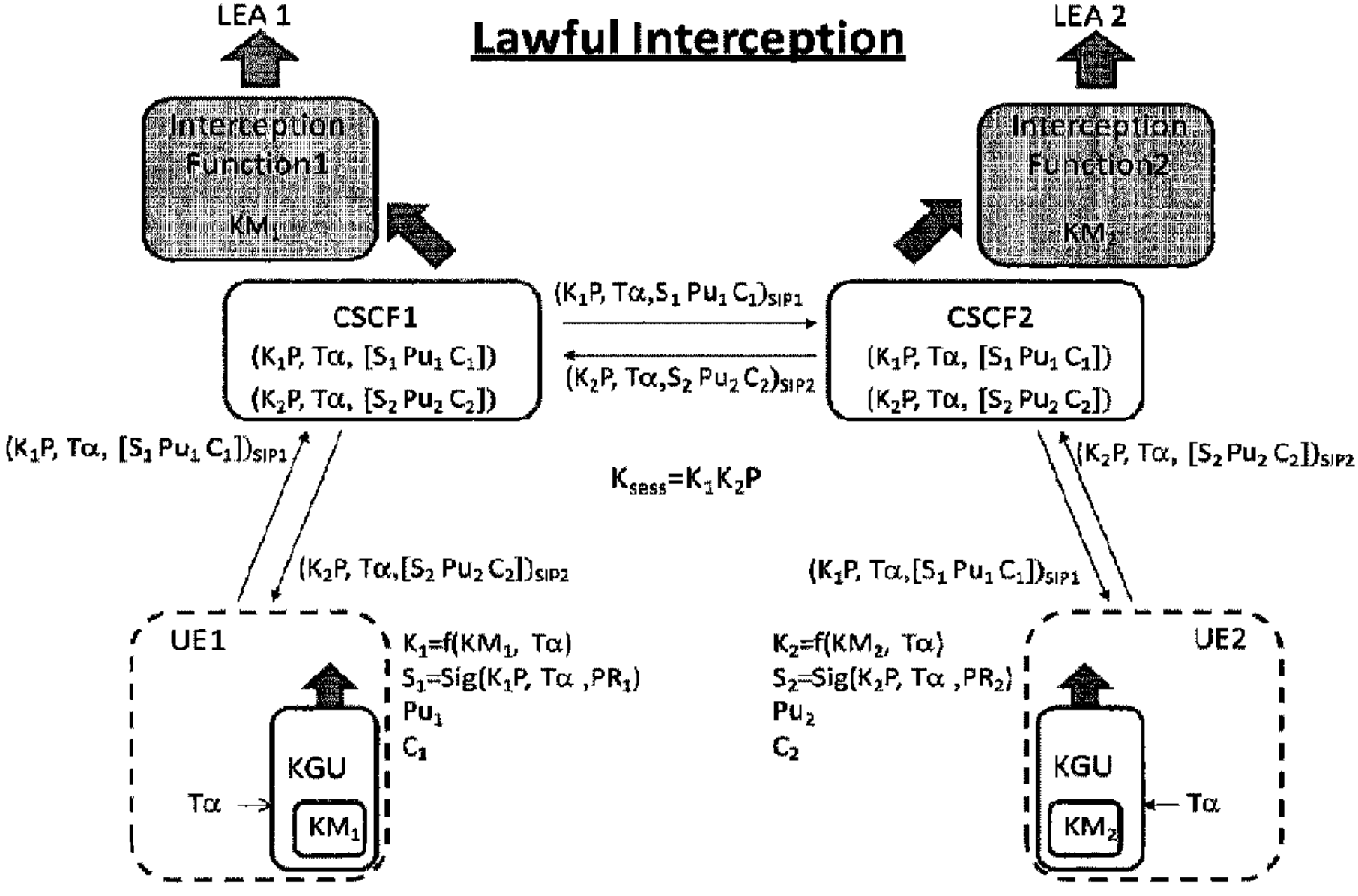

Computer
Network 399
Display 310
Display Controller 308
Speakers 322
Sound Controller 320
Disk 304
Storage Controller 324
Network Controller 306
Memory 302
CPU 301
BUS 526
I/O Interface 312
Keyboard Mouse 314
Touch Screen 316
Peripherals 318

FIG. 8


Lawful Interception
LEA 1
LEA 2
Interception Function1
KM1
Interception Function2
KM2
CSCF1
(K1P, Tα, [S1 Pu1 C1])
(K2P, Tα, [S2 Pu2 C2])
CSCF2
(K1P, Tα, [S1 Pu1 C1])
(K2P, Tα, [S2 Pu2 C2])
(K1P, Tα,S1 Pu1 C1)SIP1
(K2P, Tα,S2 Pu2 C2)SIP2
(K1P, Tα, [S1 Pu1 C1])SIP1
(K2P, Tα,[S2 Pu2 C2])SIP2
Ksess=K1K2P
(K2P, Tα, [S2 Pu2 C2])SIP2
(K1P, Tα,[S1 Pu1 C1])SIP1
UE1
K1=f(KM1, Tα)
S1=Sig(K1P, Tα ,PR1)
Pu1
C1
KGU
Tα
KM1
K2=f(KM2, Tα)
S2=Sig(K2P, Tα ,PR2)
Pu2
C2
UE2
KGU
KM2
Tα