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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
15 October 2009 (15.10.2009)

PCT

(10) International Publication Number
WO 2009/124587 A1

(51) International Patent Classification:
H04W 4/26 (2009.01) *H04W 12/06* (2009.01)
H04L 29/08 (2006.01)

(21) International Application Number:
PCT/EP2008/054255

(22) International Filing Date:
9 April 2008 (09.04.2008)

(25) Filing Language: English

(26) Publication Language: English

(71) Applicant *(for all designated States except US)*: **NOKIA SIEMENS NETWORKS OY** [FI/FI]; Karaportti 3, FI-02610 Espoo (FI).

(72) Inventor; and

(75) Inventor/Applicant *(for US only)*: **TUOMINEN, Hannu** [FI/FI]; Forsellesintie 1-3 C2, FI-02700 Kauniainen (FI).

(74) Common Representative: **NOKIA SIEMENS NETWORKS OY**; COO RTP IPR/Patent administration, 80240 Munich (DE).

(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, BR, BW, BY, BZ, CA, CH, 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, IS, JP, KE, KG, KM, 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, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, SV, SY, 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, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV,

[Continued on next page]

(54) Title: SERVICE REPORTING

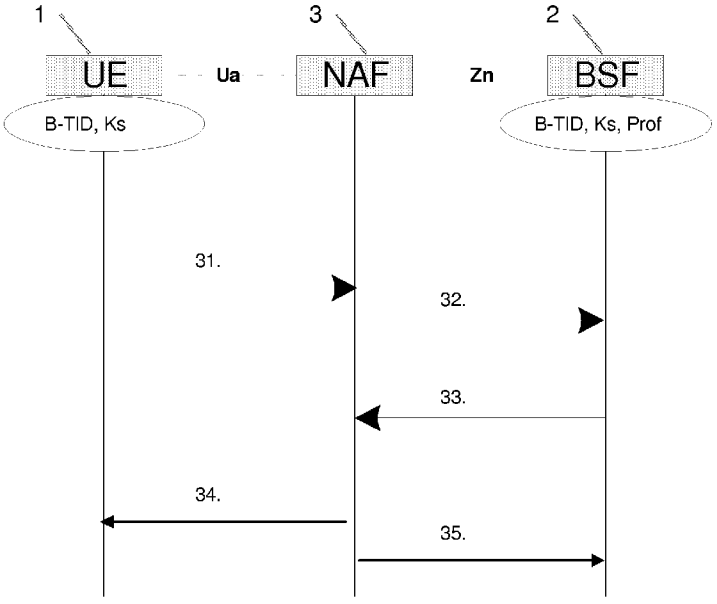

Fig 3

Soc Classification level
3 © Nokia Siemens Networks Presentation / Author / Date

[Continued on next page]

WO 2009/124587 A1

MC, MT, NL, NO, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:

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

(57) Abstract: An application server (3) is receiving a request for a service associated with a user (1), requesting security parameters from a security server (2) to authenticate the user, and sending information about use of the service to the security server. The security server can send instruction to the application server relating to the information about the use of the service the application server is to report to the security server.

Description

Title

Service reporting

Technical field of the invention

The invention relates to a method, an application server, a security server and a computer program product for reporting information about use of services.

Background of the invention

Generic Authentication Architecture (GAA) and Generic Bootstrapping Architecture (GBA) as specified by 3rd generation partnership project (3GPP) define a framework how smartcards can be used for service authentication, e.g for mobile television (Mobile TV) or internet services (web services). The GBA defines how to establish a shared secret between a service provider and a mobile terminal with help of a trusted authenticating party. The authentication is possible if a user owns a valid identity in a Home Location Register (HLR) or a Home Subscriber Server (HSS). The shared secret can be given by the authenticating party to the service provider so that the terminal and the service provider have a common shared secret that can be used for user authentication or message confidentiality.

Although GAA/GBA specifies a mechanism how a user is authenticated and authorized with help of an authenticating party to access services provided by service providers, the authenticating party, such as a

mobile network operator, lacks the mechanism to manage the total service portfolio offered by the service providers.

The object of the invention is to overcome the above drawbacks.

Summary of the invention

Embodiments of the invention solve the problem of prior art by providing an application server, method and computer program product comprising, receiving a request for a service associated with a user, requesting security parameters from a security server to authenticate the user, and sending information about use of the service to the security server. The application server, method and computer program product can comprise receiving instruction relating to sending the information about the use of the service to the security server. The instruction can comprises at least one of

- time interval for sending the information to the security server,
- list of sub-services which use is to be reported to the security server.

The information about the use of the service may comprise at least one of

- information relating to identification of at least one sub service,
- transferred data volume relating to the service and/or the at least one sub service
- information relating to when and/or how long the service or the at least one sub service has been used.

The service may comprise a mobile television service and the sub service may comprise a television channel the user has selected. The information about the use of the service can comprise at least one of

- information relating to identification of a type of a content file downloaded by the user,
- information relating to a name of a content file downloaded by the user,
- information relating to a type of a device of the user to which a content file has been downloaded,
- information relating to a model of a device of the user to which a content file has been downloaded.

The content may comprise one of audio, video, ring tone, software application. The information about the use of the service may comprise an identification of an electronic service.

The authentication may comprise authenticating according to generic authentication architecture of 3rd generation partnership project. The application server can be a network application function of the generic authentication architecture of 3rd generation partnership project. The application server can provide the service to the user. The application server can be hosted by a service provider and the requesting security parameters from the security server can comprise contacting the security server of a network operator, other than the service provider, whose subscriber the user is.

Also a security server, method and computer program product are provided, comprising obtaining security parameters associated with a subscriber of a network

operator, sending the security parameters to an application server controlled by a service provider other than the network operator, and receiving information about use of a service provided to the subscriber by the application server controlled by the service provider.

The security server, method and computer program product can comprise charging the subscriber on behalf of the service provider, and/or collecting statistics about use of services provided to subscribers of the network operator wherein the services are provided by a service providers other than the network operator, and statistics is collected based on the information received.

The security server can be a bootstrapping function and/or obtaining the security parameters can include obtaining the security parameters according to a generic bootstrapping architecture of 3rd generation partnership project.

The security server, method and computer program product can comprise sending instruction to the application server relating to the information about the use of the service the application server is to report to the security server. The security server can be hosted by the network operator.

A system is provided, the system comprises the security and the application server described above.

In certain embodiments, the present invention can provide one or more of advantages below:

- a network operator can have better focus on the services that end-users are interested to use.
- a network operator may advertise other services that are similar than users are currently using.
- a network operator can decide to drop those services from the service portfolio that are not used by end-users. This is beneficial if there are many service providers wishing to provide services by means of GBA/GAA authenticating users with the network operator.
- Add average revenue per user (ARPU) and reduce churn by being able better monitor the behaviour of the end-users.

Description of drawings

Figure 1 presents an overview of a network architecture relevant for this invention.

Figure 2 presents a signaling flow of a bootstrapping authentication procedure.

Figure 3 presents a signaling flow of an embodiment of the invention.

Figure 4 illustrates process steps of an embodiment of the invention.

Figure 5 illustrates internal structures and functions of an entity providing an application and a security server of an embodiment of the invention.

Figure 6 illustrates process steps of an embodiment of the invention.

Detailed description of the invention

An example of an authenticating party is a bootstrapping server function (BSF) which mutually authenticates with the user equipment (UE) by using the authentication and key agreement (AKA) procedure, and agrees on session keys that are then applied between the UE and a service provider controlled network application function (NAF). Instead of asking the service provider to trust the BSF and relying on it at every authentication request, the BSF establish a shared secret between the SIM card of the UE and the service provider. This shared secret is limited in time and for a domain. The NAF shall be able to locate and communicate securely with the subscriber's BSF. Hence, the GAA/GBA enables a user to authenticate to and communicate in a secure manner with third party service providers (NAFs) using existing trusted relationship to a home mobile network operator (BSF, HSS/HLR) of the user. There can be many service providers (NAFs) providing services this way to users of the mobile network operator. Currently the mobile network operator lacks means for managing the service portfolio and service providers based on actual use of the services.

For providing an application to the user after the bootstrapping has been completed, the UE and a NAF can run some application specific protocol where the authentication and securing of the actual content or messages can be based on those session keys generated during the mutual authentication between the UE and the BSF.

The BSF can be hosted in a network element under the control of a mobile network operator (MNO).

An example of a smart card is a subscriber identity module (SIM) which is a security module that is inserted into a piece of mobile equipment for subscriber identification and other security related information. A SIM card may include for example a phone number of the user, phone book information, and account information. A universal integrated circuit card (UICC) is a smart card that contains a Universal Mobile Telecommunications System (UMTS) subscriber identity module (USIM).

Authentication and key agreement (AKA) is a procedure defined by Internet Engineering Task force (IETF), used for example in third generation (3G) mobile networks and which authenticates the user and establishes a new pair of cipher and integrity keys. During the authentication, the user verifies the freshness of the authentication vector that is used. The AKA is a challenge-response based mechanism that uses symmetric cryptography and is typically run in a UMTS IP Multimedia Subsystem (IMS) Identity Module (ISIM), which resides on a smart card like device that also provides tamper resistant storage of shared secrets. Hypertext transfer protocol (HTTP) digest authentication is an HTTP authentication which verifies with a challenge-response mechanism that both parties to the communication know a shared secret, such as a password.

User Security Setting (USS) is an application and subscriber specific parameter set that defines two parts, an authentication part, which contains the list of identities of the user needed for the application

(e.g. public user identities (IMPU), MSISDN, pseudonyms), and an authorisation part, which contains the user permission flags (e.g. access to application allowed, type of certificates which may be issued). In addition, a USS may contain a key selection indication, which is used in the UICC based GBA (GBA_U) case to mandate the usage of either the mobile equipment (ME) based key or the UICC-based key or both. The USS can be delivered to the BSF as a part of GBA User Security Settings (GUSS) from the HSS, and from the BSF to the NAF if requested by the NAF. GUSS can contain the BSF specific information element and the set of all application-specific USSs.

Reference is now made to figure 1 to explain architecture relevant for the invention. Reference point Ub 11 is between a UE 1 and a BSF 2. Reference point Ub 11 provides mutual authentication between the UE 1 and the BSF 2. It allows the UE 1 to bootstrap session keys based on the 3GPP AKA infrastructure. Reference point Ua 12 between the UE 1 and a NAF 3 carries the application protocol, which is secured using the key material agreed between the UE 1 and the BSF 2 as a result of the run of HTTP Digest AKA over reference point Ub 11. Reference point Zn 13 between the BSF 2 and the NAF 3 is used by the NAF 3 to fetch the key material agreed during the previous HTTP Digest AKA protocol run over the reference point Ub 11 from the UE 1 to the BSF 2. It can also be used to fetch application-specific user security settings from the BSF 2, if requested by the NAF 3. The reference point Zh 14 used between the BSF 2 and a HSS 4 (or the HLR 4) allows the BSF 2 to fetch the required authentication information and all GBA user security settings from the HSS 4 (or from the HLR 4).

In figure 1, a cloud 15 illustrates a network of a mobile network operator. As can be seen, the UE 1, the BSF 2 and the HSS 4 can be associated with the network 15 which means that the UE 1, the BSF 2 and the HSS 4 can communicate with each other in trusted way through the network 15. The UE 1 can be a subscriber to the network 15. However, the NAF 3 is located outside the trusted network 15, and belongs to a network of a service provider 16. Normally there exists no trusted way of communication between the UE 1 and the third party NAF 3. However, the GAA/GBA provides this trusted relationship by means of the BSF 2 and the NAF 3 agreeing security parameters over trusted Zn interface 13.

When a UE wants to interact with a NAF, and it knows that the bootstrapping procedure is needed, it can first perform a bootstrapping authentication presented in figure 2. In step 21 a UE 1 sends an HTTP request towards the BSF 2. The request contains a user identity, such as a private user identity (IMPI). In step 22, based on the user identity the BSF 2 can retrieve a set of GBA user security settings and an Authentication Vector (AV, AV = RAND||AUTN||XRES||CK||IK) of the user over the reference point Zh 14 from a HSS 4 (or a HLR 4). RAND is a non-predictable number which is used as challenge in a challenge response protocol.

AUTN is an authentication token that can be used to authenticate its sender containing the claimant identity and a ticket, as well as signed and encrypted secret key exchange messages conveying a secret key to be used in future cryptographic operations. Cipher key (CK) is a

sequence of symbols that can control the operation of encipherment and decipherment. Integrity key (IK) is a data protection key that can be used for protecting the integrity of data items. The integrity key (IK) is generated, together with the ciphering key (CK). Expected user response (XRES) is a part of the authentication quintuplet which is used as a reference value for the response to the challenge during the authentication and key agreement (AKA).

In step 23, the BSF 2 forwards the RAND and AUTN to the UE 1 in the 401 "Unauthorized WWW -Authenticate" message (without the CK, IK and XRES). This is to demand the UE 1 to authenticate itself.

In step 24 the UE 1 checks the AUTN to verify that the challenge is from an authorised network. The UE 1 can also calculate CK, IK and response (RES). This will result in the session keys IK and CK in both the BSF 2 and the UE 1. In step 25, the UE 1 can send another HTTP request, containing the Digest AKA response (calculated using the RES), to the BSF 2 and in step 26, the BSF 2 can authenticate the UE 1 by verifying the Digest AKA response.

In step 27, the BSF 2 can generate key material (Ks) by concatenating the CK and the IK. Also a Bootstrapping Transaction Identifier (B-TID) value is generated. B-TID is used to bind the subscriber identity to the keying material in reference points Ua 12, Ub 11 and Zn 13. In step 28, the BSF 2 can send a 200 OK message, including the B-TID, to the UE 1 to indicate the success of the authentication. In addition, in the 200 OK message, the BSF 2 can supply the lifetime of the key Ks. The key

material Ks can be generated in the UE 1 by concatenating CK and IK is step 29.

Figure 3 presents an embodiment of the invention. Before communication between a UE 1 and a NAF 3 can start, the UE 1 and the NAF 3 can first agree whether to use shared keys obtained by means of the GBA. In step 31 the UE 1 can start communication over reference point Ua 12 with the NAF 3 by sending an application request. The UE 1 may supply the B-TID to the NAF 3, to allow the NAF 3 to retrieve the corresponding keys from the BSF 2. In step 32 the NAF 3 starts communication over reference point Zn 13 with the BSF 2 by sending an authentication request to request key material corresponding to the B-TID supplied by the UE 1 to the NAF 3 over reference point Ua 12. The NAF 3 may also request one or more application-specific USSs for applications which the UE 1 may access over reference point Ua 12.

In step 33 the BSF 2 can derive the keys required to protect the protocol used over reference point Ua 12 from the key Ks and the key derivation parameters, and can supply to the NAF 3 in an authentication answer the requested key Ks_NAF, as well as the bootstrapping time and the lifetime of that key, and the requested application-specific and potentially NAF group specific USSs if they are available in subscriber's GUSS and if the NAF 3 is authorized to receive the requested USSs. The BSF 2 may also send the private user identity (IMPI) and requested USSs to the NAF 3 according to the policy of the BSF 2. According to one aspect of the invention the BSF 2 may request in the authentication answer the NAF 3 to report to the BSF 2 information relating to use of the application the NAF 3 provides to the UE 1.

In step 34, the NAF 3 can continue with the protocol used over the reference point Ua 12 with the UE 1 and responds with application answer to the UE 1. The NAF 3 can then provide the requested application, for example mobile TV, to the UE 1. According to an aspect of the invention, in step 35, the NAF 3 can report to the BSF 2 information relating to use of the application. The NAF 3 may do the reporting according to instructions received from the BSF 2, for example, in an Authentication Answer 33. Alternatively, the NAF 3 may do the reporting based on other logic, for example based on its internal policy or configuration, or based on some other trigger.

An embodiment of this invention modifies a message, for example Authentication Answer, by adding a new information element in the message that allows a BSF 2 to request information about the service usage. In an example of the invention, a new message called Application Report 35 can send by the NAF 3 to the BSF 2 containing information about the service usage. The Application Report 35 may contain parameters relating to at least one of service usage time (when, how long) and data volumes transferred. In one aspect of the invention, a new information element is added, for example to Authentication Answer 33 signaling message, from the BSF 2 to the NAF 3 for instructing which details and/or how often the NSF 3 should report to the BSF 2. The BSF 2 can instruct the NAF 3 also using other signaling message than Authentication Answer, for example a completely new signaling message.

For example, a user is authenticated to use Mobile TV service via a NAF 3, and can be authorized according a USS for the service to watch following TV channels: YLE, MTV, Eurosport and Disney Channel. An Application Report 35 may contain information about the channels the user watched, and when. For example the Application Report 35 may contain 'start time' and 'stop time' of watching certain channel(s):

YLE news: 11:00-11:15,
Disney Channel: 11:15-12.30,
Eurosport: 13:40-15:35.

A BSF 2 can instruct the NAF 3 to send reports in certain intervals (e.g. every 30 minutes) or based on other criteria. If the BSF 2 is not giving any instructions to the NAF 3 about how often the reporting should be done, the NAF 3 may report to the BSF 2 after the user stops using or disconnects the service, or based on other criteria configured to the NAF 3. A NAF 3 can be an application server which provides the service to a user.

A NAF can interface one or more further (trusted) application servers for providing parts of a service to the user. These other application servers can belong to the same service provider which hosts also the NAF, thereby having trusted interfaces between each other.

Figure 5 shows an example of the internal structure of an application server 3, such as NAF. The NAF 3 can include a receiving unit 501 configured to receive a request for a service from a user 1. The request can be an application request over Ua reference point of 3GPP GBA. The NAF 3 may include security unit 502 which can

request security parameters from a security server 2, such as BSF 2, for the user 1, for example to authenticate the user 1. The security unit 502 can send an authentication request over Zn reference point to request key material corresponding to the B-TID supplied by the UE 1 to the receiving unit 501. The NAF 3 can include sending unit 504 to send information about use of the service or application to the security server 2. The information may be sent in an application report signaling message over Zn reference point. The NAF 3 can comprise an instruction unit 505 configured to receive instruction relating to sending the information about the use of the service to the security server 2. The instruction can define, for example, what information and/or when (for example how often) the sending unit 504 should report to BSF 2. Alternatively or in addition, the NAF 3 can have a rules unit 506 to store rules and policy relating to sending information about use of services. The rules can define, for example, what information and/or when (for example how often) the sending unit 504 should report to BSF 2. The NAF 3 can include service unit 503 configured to provide a service or application to the user 1. The service unit 503 can apply the security parameters obtained from the security unit 502 to protect content or messages relating to providing the service or application to the user 1. The service unit 503 can provide the service or application with help of a further trusted application server (not shown in Fig 5).

Figure 5 also shows an example structure of a security server 2, such as BSF. The BSF 2 can include a security unit 516 to obtain security parameters for a subscriber 1 of a network operator. The security unit 516 can

communicate with a HLR or HSS 4 over Zh reference point of 3GPP to retrieve at least part of the security parameters, for example, as described in the explanation of step 22 of Fig 2 earlier in this document. The security unit 516 can comprise an internal database for storing security parameters of subscribers of the network operator. The BSF 2 can comprise sending unit 511 to send the security parameters to an application server 3, such as NAF, which can be controlled by a service provider other than the network operator. The BSF 2 may have a receiving unit 513 configured to receive information about use of a service provided to the subscriber 1 by the application server 3. The BSF 2 can comprise a charging unit 514 which may be configured to collect and/or process charging and/or billing related data relating to providing the service or application to the subscriber 1. The charging unit 514 can manage the data for subscriber charging and billing which the network operator can take care of on behalf of service provider(s) providing the actual services. The BSF 2 can comprise a statistics unit 515 to collect statistics about use of services provided to subscribers 1 of the network operator. The services can be provided by service providers other than the network operator. The statistics unit 515 can be configured to collect statistics based on information received by the receiving unit 513. The collected can be used for preparing charging/billing of the user. The BSF 2 can include instruction unit 512 to send instruction to the application server 3 relating to the information about the use of the service the application server 3 should report to the receiving unit 513. The instruction unit 512 can for example send instruction about what information and/or when (for example how often) the

application server 3 should report to the receiving unit 513.

All units described above may be implemented for example using microprocessors and/or other electrical components and/or by software.

In the following some non-limiting examples of services provided by the NAF 3 and items which can be reported by the sending unit 504 of the NAF 3 and received by the receiving unit 513 of the BSF 2 are given:

1.) Streaming services, such as mobile TV. Items reported to a BSF can include identification of a used sub-service (e.g. watched TV channel), a time (when and/or how long a (sub-)service has been used, for example by indicating start/stop times of watching a channel), transferred data volume (per service or sub-service).

2.) Content services (music, games, file download, ring tones). Items reported to a BSF can include a name and/or a type (audio, video, ring tone, software application etc) of downloaded file. A type of a device or a model of a mobile device of the user 1 to which the content was downloaded can be reported to the BSF.

3.) Other electronic services for which the type of service (such as e-ticket, train ticket) can be reported to the BSF.

Figure 4 presents a process according to an embodiment of the invention. The process can be implemented for example by an application server, such as NAF 3. In step

41 a request for providing a service is received. The request can be received from a UE 1, and/or can be associated with a user 1. The request can include a B-TID. In step 42, security parameters are retrieved. The security parameters can be retrieved based on the B-TID received in step 41, and thereby the security parameters can be linked to the user 1. The security parameters may include at least one security key and/or at least one USS. The USS can be linked to the service requested in step 41. Optionally, in step 43, a reporting instruction can be received on reporting service use related parameters. The instruction can be received from a security entity, such as BSF, and may treat reporting to the security entity. In step 44, the service is provided to the user 1. In step 45, information relating to the service is reported. The reporting in step 45 and instruction in step 43 can include details described above in connection with 1.) streaming services, 2.) content services and 3.) electronic services. Providing the service in step 44 can continue over time as indicated by arrow 46 and reporting information relating to the service in step 45 may take place several times. Alternatively the reporting step 45 can be done once after the service has been provided in step 44. The reporting step 45 can be done based on pre-configured rules and policy.

Figure 6 presents another process according to an embodiment of the invention. The process can be implemented, for example, by a security server, such as BSF 2. Is step 61, security parameters of a user 1 can be obtained. This may include retrieving from a HLR 4 or HSS 4 a set of GBA user security settings and/or authentication vector based on the identity of user 1,

for example, IMPI. The obtaining may include generating security keys (CK, IK, Ks) based on the retrieved security parameters. Also a B-TID can be generated. In step 62, security parameters are transmitted to an application server. The security parameters may include security keys, and the security parameters to be transmitted can be identified and/or associated with the user 1 based on the B-TID which can be received from the application server. Optionally, in step 63, a reporting instruction can be sent on reporting service use related parameters. In step 64, a report is received. The report comprises information relating to providing a service to the user 1. The reporting in step 64 and instruction in step 63 can include details described above in connection with 1.) streaming services, 2.) content services and 3.) electronic services. As shown with arrow 66, several reports can be received during providing the service. Alternatively the reporting 64 can be done once after the service has been provided. In step 65, information for charging and/or billing of the user can be prepared based on the reported information relating to services provided to the user 1. In step 67, statistics on use of services can be prepared based on reported information relating to services provided to users. As shown, one, both or none of the steps 65 and 67 can belong to the process.

Without this invention either an authenticating party (mobile network operator, BSF) can not receive information about use of services provided by third party application servers or proprietary methods must be mutually agreed between the authenticating party and the third party (internet service provider ISP, NAF). With aspects of the invention, mobile network operators can

receive information from service providers how subscribers of the mobile network operators use services relying on GAA/GBA authentication. Embodiments of the invention can allow mobile networks operators to take care of charging and billing of end users on behalf of service providers by collecting relevant charging and billing related data through a BSF.

An application server and a security server may be physically implemented in a switch, router, server or other hardware platform or electronic equipment which can support data transmission and processing tasks, or can be implemented as a component of other existing device.

The invention is not limited to mobile networks, but can also be applied in other type of networks having similar type of authentication logic as the GAA/GBA, similar type of security entity role as the BSF and similar type of application server role as the NAF. Therefore, the BSF is only used here as an example of a security entity, and NAF only as an example of an application serving entity. Functions of the security entity (BSF) and the application entity (NAF) described above may be implemented by code means, as software, and loaded into memory of a computer.

Claims

1. An application server (3) comprising,

receiving means (501) for receiving a request for a service associated with a user (1),

requesting means (502) for requesting security parameters from a security server (2) to authenticate the user (1), and

sending means (504) for sending information about use of the service to the security server (2).

2. The application server (3) of claim 1 further comprising

instruction means (505) for receiving instruction relating to sending the information about the use of the service to the security server (2).

3. The application server (3) of claim 2 wherein the instruction comprises at least one of

- time interval for sending the information to the security server (2),

- list of sub services which use is to be reported to the security server (2).

4. The application server (3) of any of claims 1 - 3, wherein the information about the use of the service comprises at least one of

- information relating to identification of at least one sub service,

- transferred data volume relating to the service and/or the at least one sub service

- information relating to when and/or how long the service or the at least one sub service has been used.

5. The application server (3) of claim 4, wherein the service comprises a mobile television service and the sub service comprises a television channel the user (1) has selected.

6. The application server (3) of any of claims 1 - 3, wherein the information about the use of the service comprises at least one of

- information relating to identification of a type of a content file downloaded by the user (1),
- information relating to a name of a content file downloaded by the user (1),
- information relating to a type of a device of the user (1) to which a content file has been downloaded,
- information relating to a model of a device of the user (1) to which a content file has been downloaded.

7. The application server (3) of claim 6, wherein the content comprises one of audio, video, ring tone or software application.

8. The application server (3) of any of claims 1 - 3, wherein the information about the use of the service comprises an identification of an electronic service.

9. The application server (3) of any of preceding claims, wherein the authentication comprises authenticating according to generic authentication architecture of 3rd generation partnership project.

10. The application server (3) of any of preceding claims, wherein the application server (3) comprises a

network application function of generic authentication architecture of 3rd generation partnership project.

11. The application server (3) of any of preceding claims, further comprising service means (503) for providing the service to the user (1).

12. The application server (3) of any of preceding claims, wherein the application server (3) is hosted by a service provider (16) and wherein the requesting security parameters from the security server (2) comprises contacting the security server (2) of a network operator (15), other than the service provider (16), whose subscriber the user (1) is.

13. A security server (2) in a communication system, comprising

security means (516) for obtaining security parameters associated with a subscriber (1) of a network operator (15),

sending means (511) for sending the security parameters to an application server (3) controlled by a service provider (16) other than the network operator (15),

receiving means (513) for receiving information about use of a service provided to the subscriber (1) by the application server (3) controlled by the service provider (16).

14. The security server (2) of claim 13 further comprising charging means (514) for preparing charging related data for billing the subscriber (1) on behalf of the service provider (16).

15. The security server (2) of claim 13 or 14 further comprising statistics means (515) for collecting statistics about use of services provided to subscribers (1) of the network operator (15) and wherein the services are provided by service providers (16) other than the network operator (15), wherein the statistics means (515) is configured to collect statistics based on information received by the receiving means (513).

16. The security server (2) of any of claims 13 or 15 wherein the security server (2) comprises a bootstrapping function and the security means (516) is configured to obtain the security parameters according to a generic bootstrapping architecture of 3rd generation partnership project.

17. The security server (2) of any of claims 13 or 16 further comprising instruction means (512) for sending instruction to the application server (3) relating to the information about the use of the service the application server (3) is to report to the security server (2).

18. The security server (2) of any of claims 13 or 17 wherein the security server (2) is hosted by the network operator (15).

19. A system comprising a security server of any of claims 13-18 and an application server of any of claims 1-12.

20. A method for sending service reports comprising steps of,

receiving a request (31, 41) for a service associated with a user (1),

requesting (32, 42) security parameters from a security server (2) to authenticate the user (1), and

sending (35, 45) information about use of the service to the security server (2).

21. The method according to claim 20 further comprising receiving (33, 43) instruction relating to sending the information about the use of the service to the security server (2).

22. The method according to claim 21 wherein the instruction comprises at least one of

- time interval for sending the information to the security server (2),

- list of sub-services which use is to be reported to the security server (2).

23. The method according to any of claims 20 - 22, wherein the information about the use of the service comprises at least one of

- information relating to identification of at least one sub service,

- transferred data volume relating to the service and/or the at least one sub service

- information relating to when and/or how long the service or the at least one sub service has been used.

24. The method according to claim 23, wherein the service comprises a mobile television service and the sub service comprises a television channel the user (1) has selected.

25. The method according to any of claims 20 - 22, wherein the information about the use of the service comprises at least one of

- information relating to identification of a type of a content file downloaded by the user (1),
- information relating to a name of a content file downloaded by the user (1),
- information relating to a type of a device of the user (1) to which a content file has been downloaded,
- information relating to a model of a device of the user (1) to which a content file has been downloaded.

26. The method according to claim 25, wherein the content comprises one of audio, video, ring tone, software application.

27. The method according to any of claims 20 - 22, wherein the information about the use of the service comprises an identification of an electronic service.

28. The method according to any of claims 20 - 27, wherein the authentication comprises authenticating according to generic authentication architecture of 3rd generation partnership project.

29. The method according to any of claims 20 - 28, wherein the method steps are implemented by an application server (3) comprising a network application function of generic authentication architecture of 3rd generation partnership project.

30. The method according to any of claims 20 - 29, further comprising providing (34, 44) the service to the user (1).

31. The method according to any of claims 20 or 30, wherein the method steps are implemented by an application server (3) hosted by a service provider (16) and wherein the requesting security parameters from the security server (2) comprises contacting the security server (2) of a network operator (15), other than the service provider (16), whose subscriber the user (1) is.

32. A method for receiving information on use of services in a communications system comprising steps of

obtaining (22, 61) security parameters associated with a subscriber (1) of a network operator (15),

sending (33, 62) the security parameters to an application server (3) controlled by a service provider (16) other than the network operator (15),

receiving (35, 64) information about use of a service provided to the subscriber (1) by the application server (3) controlled by the service provider (16).

33. The method of claim 32, further comprising preparing charging related data (65) for billing the subscriber (1) on behalf of the service provider (16).

34. The method of claim 32 or 33, further comprising collecting statistics (67) about use of services provided to subscribers (1) of the network operator (15), wherein the services are provided by service providers (16) other than the network operator (15) and

the collecting statistics (67) is based on the received information about the use of the service.

35. The method of any of claims 32 or 34 wherein the method steps are implemented by a security server (2) comprising a bootstrapping function and wherein the obtaining the security parameters comprises obtaining the security parameters according to a generic bootstrapping architecture of 3rd generation partnership project.

36. The method of any of claims 32 or 35, further comprising sending (33, 63) instruction to the application server (3) relating to the information about the use of the service the application server (3) is to report to the security server (2).

37. The method of any of claims 32 or 36 wherein the security server (2) is hosted by the network operator (15).

38. A computer program product comprising code means adapted to produce the steps of any one of claims 20 - 37 when loaded into the memory of a computer.

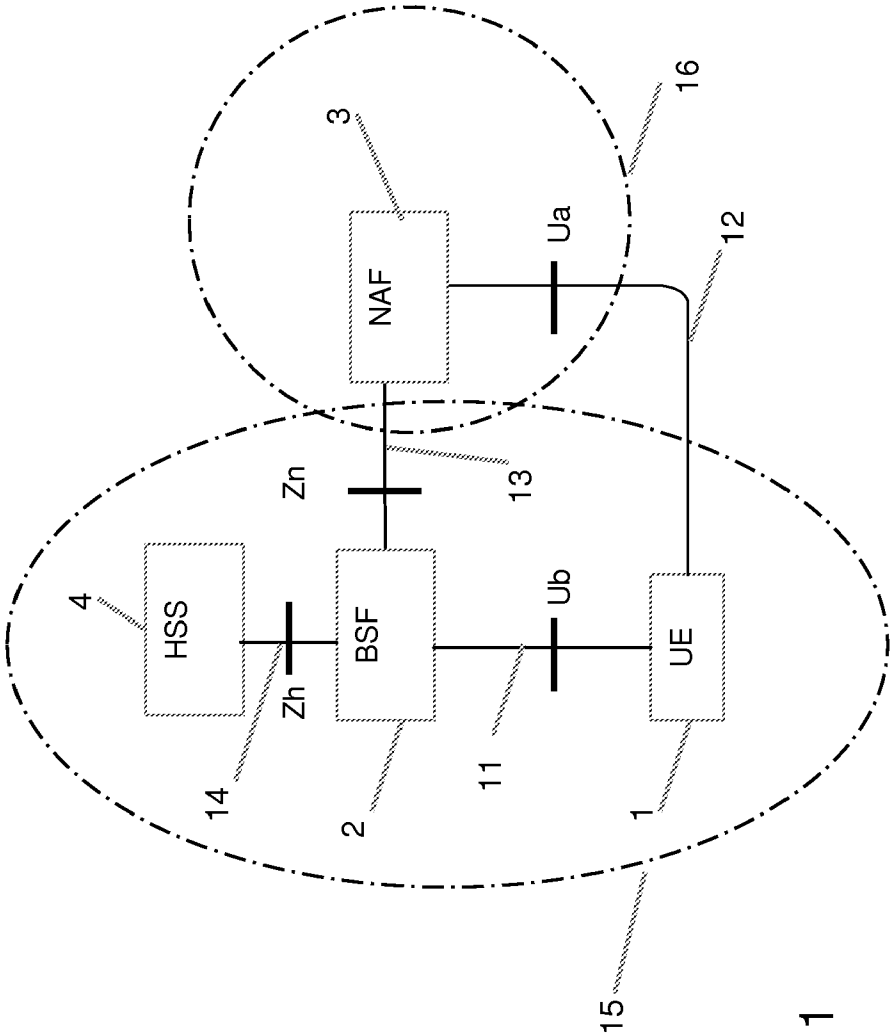

Fig 1

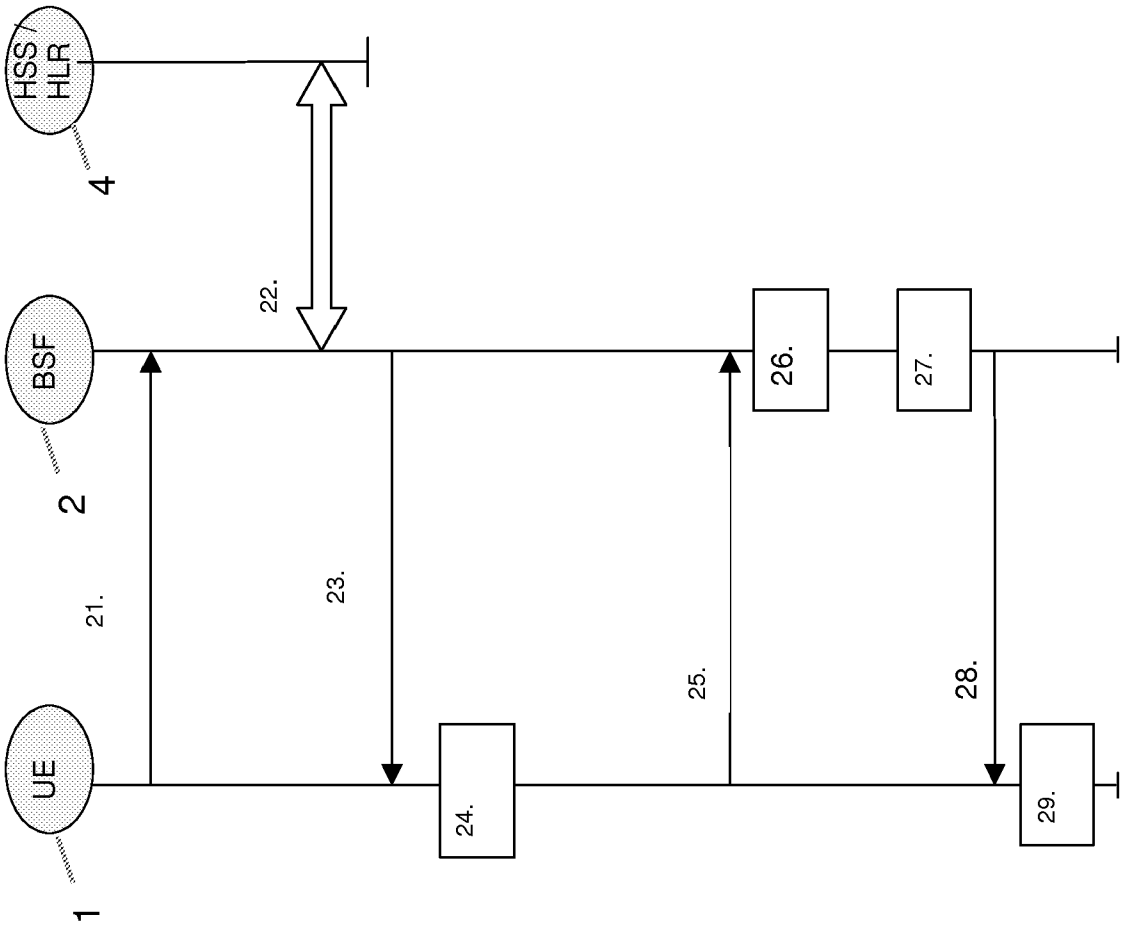

Fig 2

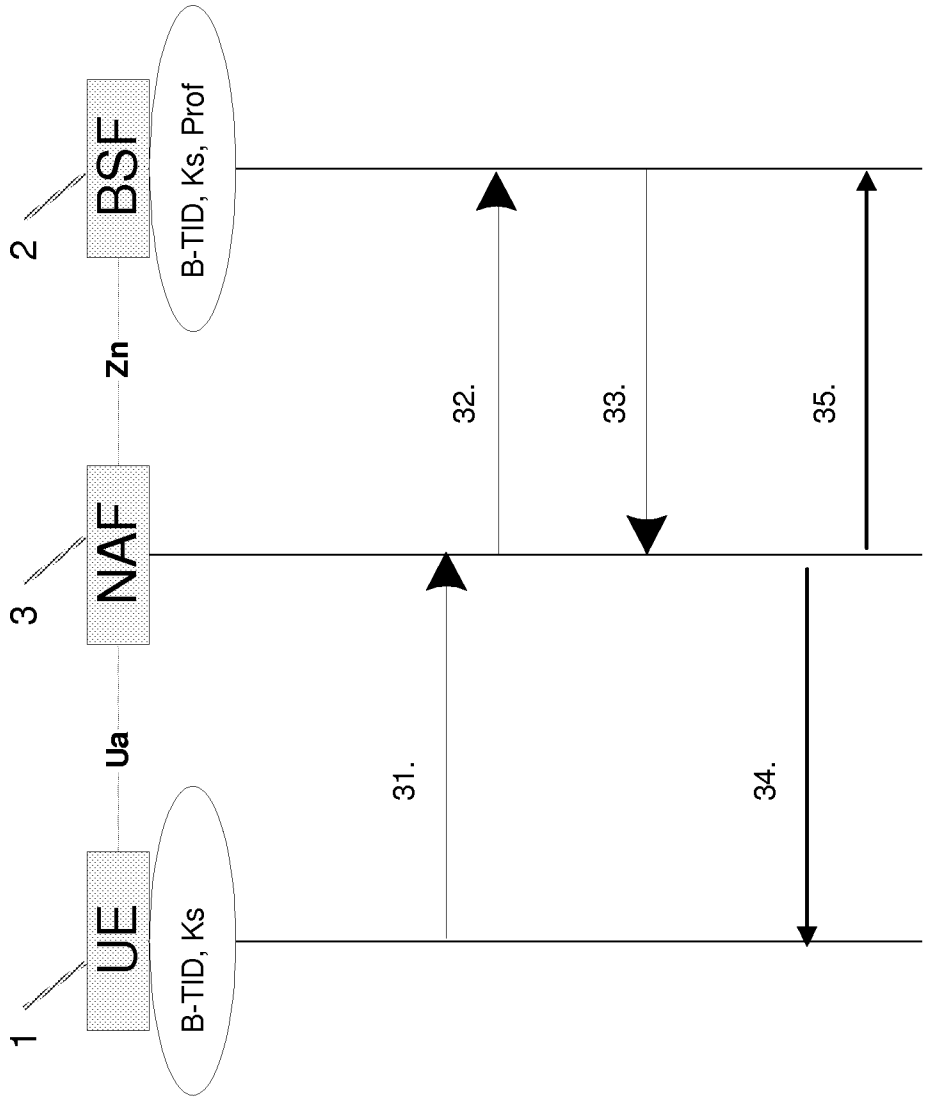

Fig 3

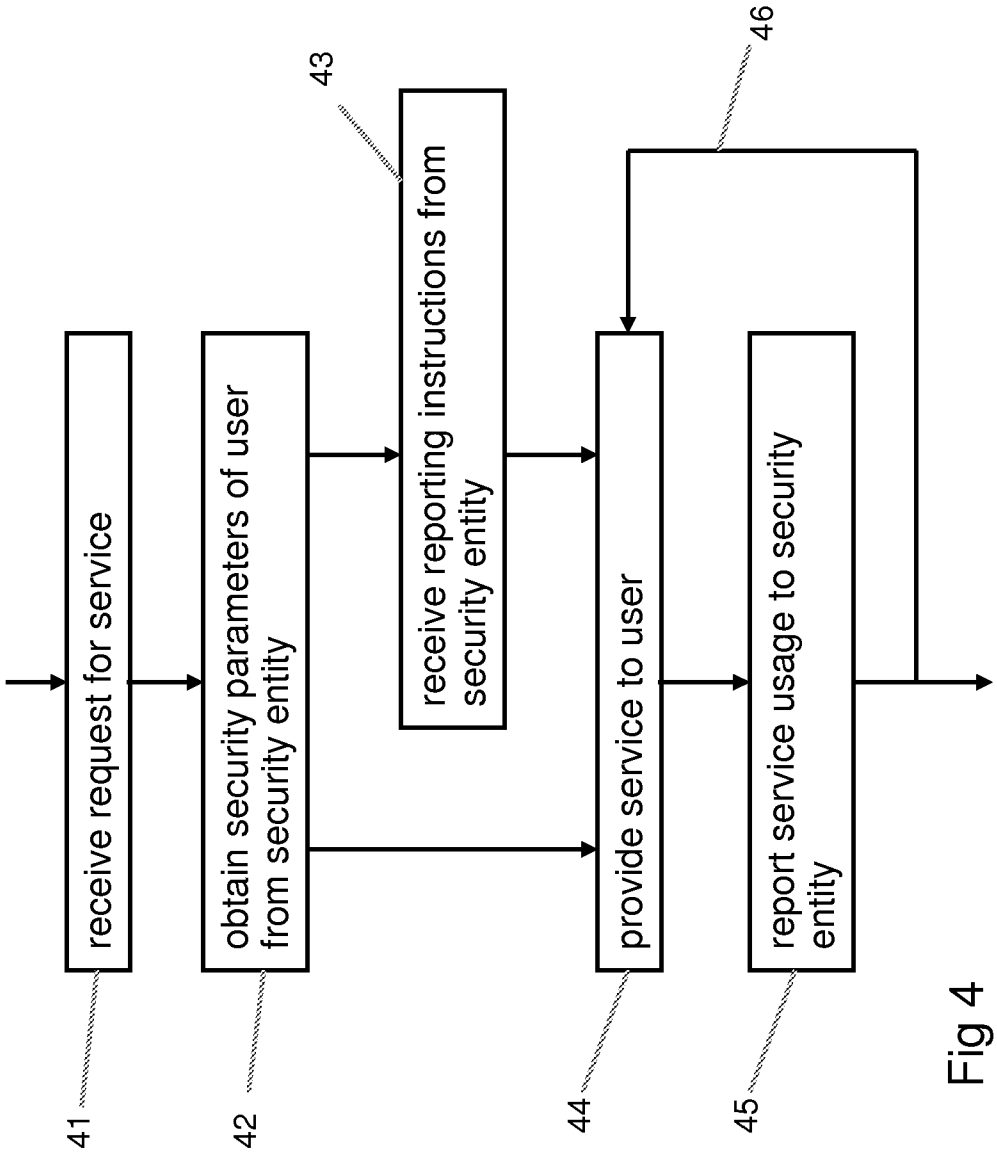
receive request for service
obtain security parameters of user from security entity
receive reporting instructions from security entity
provide service to user
report service usage to security entity
41
42
43
44
45
46

Fig 4

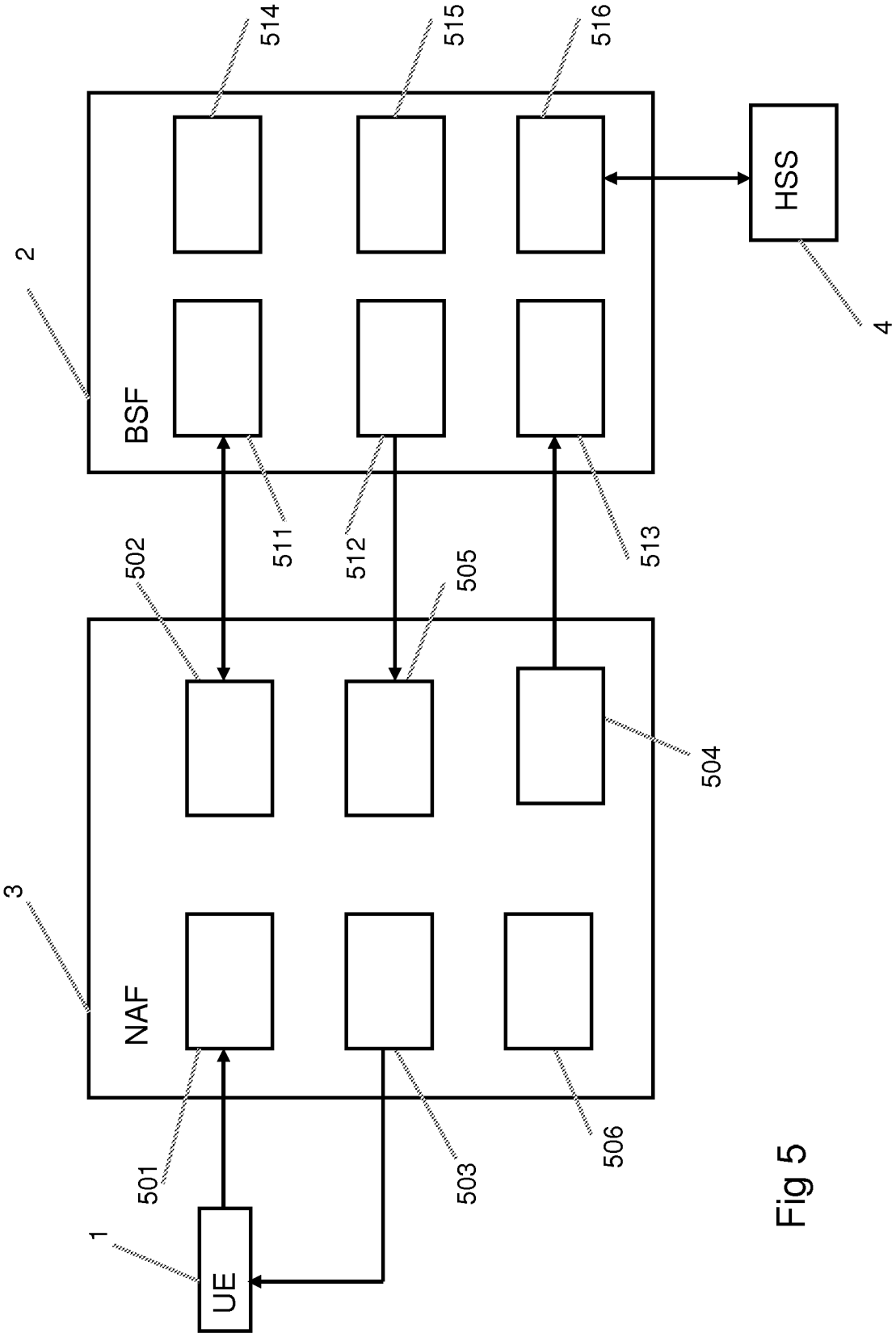
514
515
516
HSS
4
2
BSF
511
512
513
502
505
504
3
NAF
501
503
506
1
UE

Fig 5

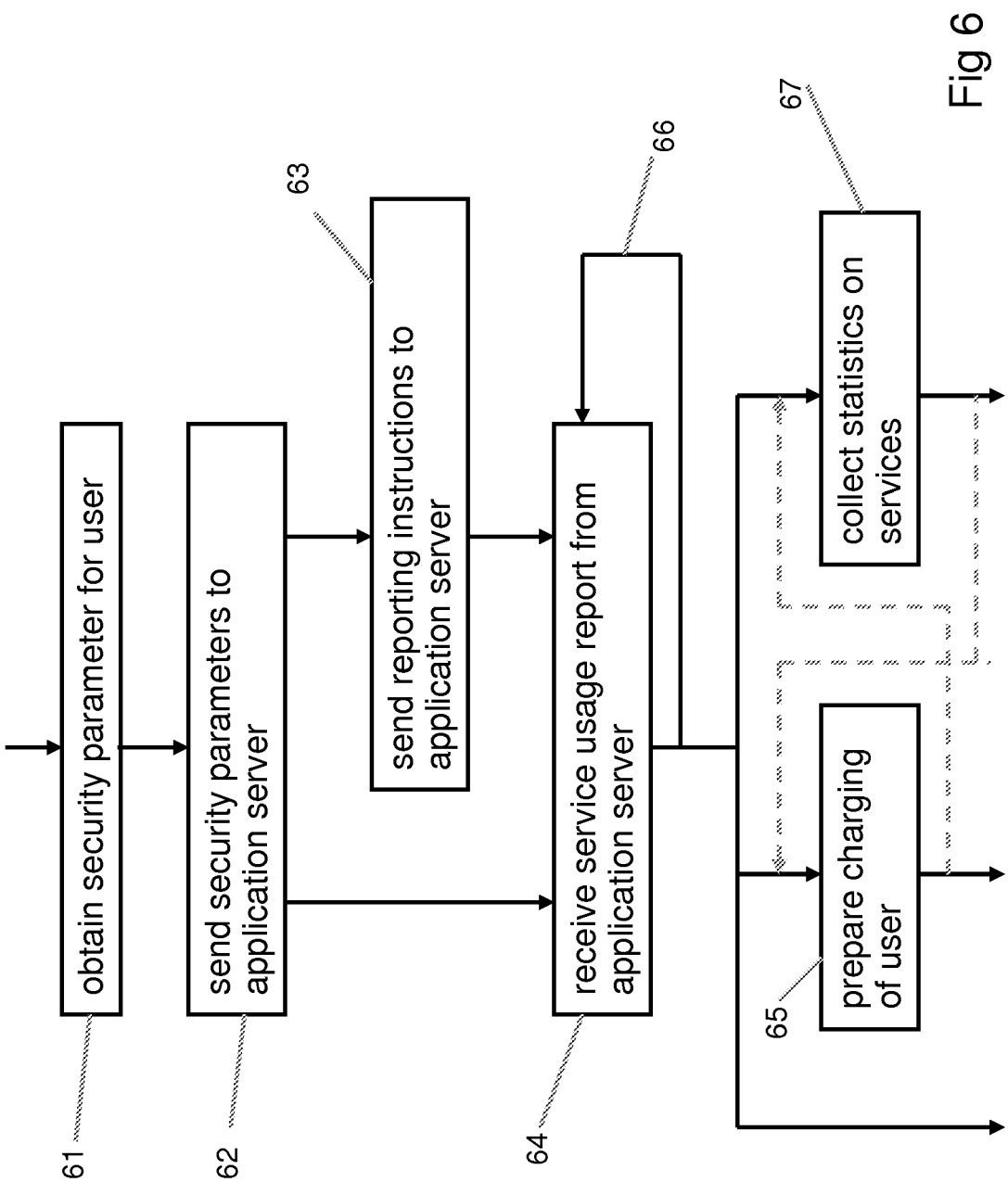
obtain security parameter for user
send security parameters to application server
send reporting instructions to application server
receive service usage report from application server
prepare charging of user
collect statistics on services
61
62
63
64
65
66
67

Fig 6

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2008/054255

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04W4/26 H04L29/08
ADD. H04W12/06

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
H04W H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, WPI Data, COMPENDEX, INSPEC

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 2004/071012 A (KT FREETEL CO LTD [KR]; CHOI WOO-HYUNG [KR]; OH MI-NA [KR]; JOE EUN-YE) 19 August 2004 (2004-08-19) paragraphs [0051], [0060] paragraphs [0068] - [0074] paragraphs [0088] - [0090] paragraphs [0102] - [0116] figures 1-4	1-38
X	WO 03/032618 A (SERVICE FACTORY SF AB [SE]; PIHLSGAARD JOHAN [SE]; MELLSTRAND MATS [SE]) 17 April 2003 (2003-04-17) page 7, line 12 - page 8, line 14 page 10, line 1 - page 11, line 22 figures 4-6	1-38

-/--

[X] Further documents are listed in the continuation of Box C.

[X] See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
16 March 2009	25/03/2009

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Bengi, Kemal

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2008/054255

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2005/177515 A1 (KALAVADE ASAWAREE [US] ET AL) 11 August 2005 (2005-08-11) paragraphs [0102], [0103] paragraphs [0122], [0123], [0143] paragraphs [0255] - [0298] figures 13,15-18	1-38
X	EP 1 898 349 A (SIEMENS AG [DE]) 12 March 2008 (2008-03-12) paragraphs [0021], [0022] paragraphs [0052] - [0056] claim 14; figure 3	1-38
A	WO 2005/109938 A (ERICSSON TELEFON AB L M [SE]; BOMAN KRISTER [SE]; RYDNELL GUNNAR [SE]) 17 November 2005 (2005-11-17) abstract page 8, line 25 - page 11, line 31 figures 3,4	1-38

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/EP2008/054255

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 2004071012 A	19-08-2004	CN 1745539 A	08-03-2006
		KR 20040072210 A	18-08-2004
WO 03032618 A	17-04-2003	EP 1440560 A1	28-07-2004
		US 2004248547 A1	09-12-2004
US 2005177515 A1	11-08-2005	CA 2555767 A1	25-08-2005
		EP 1782576 A2	09-05-2007
		WO 2005076884 A2	25-08-2005
EP 1898349 A	12-03-2008	NONE	
WO 2005109938 A	17-11-2005	AT 405123 T	15-08-2008
		EP 1745667 A1	24-01-2007
		ES 2311821 T3	16-02-2009
		US 2007274522 A1	29-11-2007