

(19) **DANMARK**

(10) **DK/EP 3459278 T3**



(12)

Oversættelse af europæisk patentskrift

Patent- og
Varemærkestyrelsen

-
- (51) Int.Cl.: **H 04 W 12/06 (2009.01)** **H 04 L 29/06 (2006.01)**
- (45) Oversættelsen bekendtgjort den: **2020-06-15**
- (80) Dato for Den Europæiske Patentmyndigheds bekendtgørelse om meddelelse af patentet: **2020-04-22**
- (86) Europæisk ansøgning nr.: **17797092.8**
- (86) Europæisk indleveringsdag: **2017-10-25**
- (87) Den europæiske ansøgnings publiceringsdag: **2019-03-27**
- (86) International ansøgning nr.: **EP2017077330**
- (87) Internationalt publikationsnr.: **WO2018077960**
- (30) Prioritet: **2016-10-31 US 201662415006 P**
- (84) Designerede stater: **AL AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HR HU IE IS IT LI LT LU LV MC MK MT NL NO PL PT RO RS SE SI SK SM TR**
- (73) Patenthaver: **Telefonaktiebolaget LM Ericsson (PUBL), , 164 83 Stockholm, Sverige**
- (72) Opfinder: **BEN HENDA, Noamen, Tumultgränd 228, 162 47 Stockholm, Sverige**
LEHTOVIRTA, Vesa, Veininmäki 10B, 02620 Espoo, Finland
CASTELLANOS ZAMORA, David, c/ Embajadores 256, 1ºB, 28045 Madrid, Spanien
- (74) Fuldmægtig i Danmark: **Zacco Denmark A/S, Arne Jacobsens Allé 15, 2300 København S, Danmark**
- (54) Benævnelse: **Autentifikation til næstegenerationssystemer**
- (56) Fremdragne publikationer:
Qualcomm Inc., LG Electronics: "Way forward on support of non-3GPP access and update to solution 8.6 for support of untrusted non-3GPP access", 3RD GENERATION PARTNERSHIP PROJECT (3GPP), SA WG2 Meeting #117, S2-166283 , 24 October 2016 (2016-10-24), XP051170203, Retrieved from the Internet: URL: http://www.3gpp.org/ftp/tsg_sa/WG2_Arch/TSGS2_117_Kaohsiung_City/Docs/ [retrieved on 2016-10-24]
3RD GENERATION PARTNERSHIP PROJECT: "Study on Architecture for Next Generation System (Release 14)", 3RD GENERATION PARTNERSHIP PROJECT (3GPP), TECHNICAL SPECIFICATION GROUP SERVICES AND SYSTEM ASPECTS, TR 23.799 V0.4.0, 27 April 2016 (2016-04-27), XP051123441, [retrieved on 2016-04-27] cited in the application
3RD GENERATION PARTNERSHIP PROJECT: "Study on control and user plane separation of EPC nodes (Release 14)", 3RD GENERATION PARTNERSHIP PROJECT (3GPP), TECHNICAL SPECIFICATION GROUP SERVICES AND SYSTEM ASPECTS, TR 23.714 V14.0.0, 22 June 2016 (2016-06-22), XP051295181, [retrieved on 2016-06-22] cited in the application

DESCRIPTION

TECHNICAL FIELD

[0001] The present disclosure relates to a method and apparatus for secondary authentication in a network

BACKGROUND

[0002] 3rd Generation Partnership Project (3GPP) is currently developing the standards for 5G, also known as next generation (NG) systems. It is expected that 5G will support many new scenarios and use cases and will be an enabler for Internet of things (IoT). It is expected that NG systems will provide connectivity to a wide range of new devices such as sensors, smart wearables, vehicles, machines, etc. Flexibility is thus a key property in NG Systems. This is reflected in security requirement for network access that are mandating the support of alternative authentication methods and different types of credentials, compared to the usual authentication and key agreement (AKA) credentials pre-provisioned by an operator and securely stored in a universal integrated circuit card (UICC). This would allow factory owners or enterprises to leverage their own identity and credential management systems for authentication and access network security.

[0003] Among the new features in NG Systems is the concept of network slicing. A network slice (NS) is basically an instance of a core network dedicated to provide a particular service. This will allow operators to handle a wide variety of new use cases, each with different service requirements in terms of Quality of Service (QoS). For example, an operator could be running a NS for usual mobile broadband (MBB) services, in parallel with a mission critical NS for public safety services (such as Mission-critical push-to-talk (MCPTT)) requiring very low latency, further in parallel with an IoT NS for electricity meters with very low bandwidth.

[0004] Among topics being studied in relation to Network Slicing is the decoupling of authentication and authorization procedures for accessing different NSs.

[0005] Qualcomm Inc., LG Electronics: "Way forward on support of non-3GPP access and update o solution 8.6 for support of untrusted non-3GPP access", 3rd Generation Partnership Project (3GPP), SA WG2 Meeting #117, S2-166283, discloses a method for authentication via untrusted non-3GPP access. After obtaining IP connectivity over untrusted non-3GPP access, a UE discovers a gateway (called an ngPDG) using a mechanism similar to ePDG discovery in the EPC. The UE then performs a network attach in two steps. Firstly, the UE establishes an IPSec tunnel with the ngPDG using the same procedures defined for the ePDG in EPC. Secondly, once the tunnel is established, and the UE is therefore authenticated, the UE sends NAS signalling containing an Attach Request. The network, upon receiving the NAS attach

request from the UE, verifies that the UE is already authenticated and processes the attach procedure without re-authenticating the UE.

SUMMARY

[0006] An object of embodiments presented herein is to enable decoupling of authentication in next generation systems.

[0007] According to a first aspect a method for secondary authentication in a network is presented. The method is performed by a user equipment (UE) and comprises establishing a primary authentication with a security anchor function (SEAF), establishing a user plane (UP) session or connection with or via a UP function (UPF), receiving an extensible authentication protocol (EAP) based authentication request from the UPF, sending an EAP based authentication response to the UPF and receiving an EAP based authentication result from the UPF, the EAP based authentication result based on a verification response from an external authentication, authorization, and accounting (AAA) server.

[0008] The UE may further be a next generation (NG) UE. The UPF may further be a NG UPF.

[0009] According to a second aspect a method for secondary authentication in a network is presented. The method is performed by a user plane (UP) function (UPF), and comprises establishing a user plane (UP) session or connection with a user equipment (UE), sending an extensible authentication protocol (EAP) based authentication request to the UE, receiving an EAP based authentication response from the UE, sending a verification request of the received EAP based authentication response to an external authentication, authorization, and accounting (AAA) server, receiving a verification response from the external AAA server, and sending an authentication result to the UE, wherein the authentication result is based on the verification response from the external AAA server.

[0010] The UE may further be a next generation (NG) UE. The UPF may further be a NG UPF.

[0011] According to a third aspect a user equipment (UE) for operation in a network is presented. The UE comprises a processor, and a computer program product. The computer program product stores instructions that, when executed by the processor, causes the UE to establish a primary authentication with a security anchor function (SEAF), establish a user plane (UP) session or connection with a UP function (UPF), receive an extensible authentication protocol (EAP) based authentication request from the UPF, send an EAP based authentication response to the UPF, and receive an EAP based authentication result via the UPF, the EAP based authentication result based on a verification response from an external authentication, authorization, and accounting (AAA) server.

[0012] The UE may further be a next generation (NG) UE. The UPF may further be a NG UPF.

[0013] According to a fourth aspect a user plane (UP) function (UPF) operative in a network is presented. The UPF comprises a processor, and a computer program product. The computer program product stores instructions that, when executed by the processor, causes the UPF to establish a user plane (UP) session or connection with a user equipment (UE), send an extensible authentication protocol (EAP) based authentication request to the UE, receive an EAP based authentication response from the UE, send a verification request of the received EAP based authentication response to an external authentication, authorization, and accounting, (AAA,) server, receive a verification response from the external AAA server, and to send an authentication result to the UE, wherein the authentication result is based on the verification response from the external AAA server.

[0014] The UE may further be a next generation (NG) UE. The UPF may further be a NG UPF.

[0015] According to an example of the present disclosure, a user equipment (UE) for operation in a network is presented. The UE comprises means for establishing a user plane (UP) session or connection with a UP function (UPF), means receiving an extensible authentication protocol (EAP) based authentication request from the UPF, and means for sending an EAP based authentication response to the UPF.

[0016] The UE may further comprise means for establishing a primary authentication with a security anchor function (SEAF).

[0017] The UE may further comprise means for receiving an EAP based authentication result from the UPF.

[0018] The UE may further be a next generation (NG) UE. The UPF may further be a NG UPF.

[0019] According to another example of the present disclosure, a user plane (UP) function (UPF) operative in a network is presented. The UPF comprises means for establishing a user plane (UP) session or connection with a user equipment (UE), means for sending an extensible authentication protocol (EAP) based authentication request to the UE, and means for receiving an EAP based authentication response from the UE.

[0020] The UPF may further comprise means for sending a verification request of the received EAP based authentication response to an authentication, authorization, and accounting (AAA) server; and means for receiving a verification response from the AAA server.

[0021] The UPF may further comprise means for sending an authentication result to the UE, wherein the authentication is based on the verification response from the AAA server.

[0022] The UE may further be a next generation (NG) UE. The UPF may further be a NG UPF.

[0023] According to a seventh aspect a computer program for secondary authentication in a network is presented. The computer program comprises computer program code which, when

run on user equipment (UE), causes the UE to perform the steps of the first aspect.

[0024] The UE may further be a next generation (NG) UE. The UPF may further be a NG UPF.

[0025] According to an eighth aspect a computer program for secondary authentication in a network is presented. The computer program comprising computer program code which, when run on a user plane (UP) function (UPF), causes the UPF to perform the steps of the second aspect.

[0026] The UE may further be a next generation (NG) UE. The UPF may further be a NG UPF.

[0027] According to a ninth aspect a computer program product is presented. The computer program product comprises a computer program and a computer readable storage means on which the computer program is stored. Generally, all terms used in the claims are to be interpreted according to their ordinary meaning in the technical field, unless explicitly defined otherwise herein. All references to "a/an/the element, apparatus, component, means, step, etc." are to be interpreted openly as referring to at least one instance of the element, apparatus, component, means, step, etc., unless explicitly stated otherwise. The steps of any method disclosed herein do not have to be performed in the exact order disclosed, unless explicitly stated.

BRIEF DESCRIPTION OF THE DRAWINGS

[0028] The inventive concept is now described, by way of example, with reference to the accompanying drawings, in which:

Fig. 1 is a schematic diagram illustrating an environment where embodiments presented herein can be applied;

Fig. 2 schematically shows a flow for secondary authentication in LTE;

Fig. 3 schematically shows a flow for EAP-based secondary authentication in next generation systems;

Figs. 4-5 schematically show protocol architectures for EAP-based secondary authentication for embodiments presented herein;

Figs. 6A-6B are flow charts illustrating methods for embodiments presented herein;

Figs. 7-8 are schematic diagrams illustrating some components of devices presented herein; and

Figs. 9-10 are schematic diagrams showing functional modules of devices presented herein.

DETAILED DESCRIPTION

[0029] The inventive concept will now be described more fully hereinafter with reference to the accompanying drawings, in which certain embodiments of the inventive concept are shown. This inventive concept may, however, be embodied in many different forms and should not be construed as limited to the embodiments set forth herein; rather, these embodiments are provided by way of example so that this disclosure will be thorough and complete, and will fully convey the scope of the inventive concept to those skilled in the art. Like numbers refer to like elements throughout the description.

[0030] One possible scenario for decoupling of authentication and authorization procedures for accessing different network slices (NSs) is the following. In order for an NG-user equipment (UE) to access a particular NS, the operator would first run a primary (usual) authentication for initial network access followed by a secondary NS-specific authentication. The secondary NS-specific authentication may possibly be under the control of a 3rd party. This is assuming trust between the 3rd party service provider and the mobile network operator (MNO) who for example is offering access and transport services to this 3rd party in a dedicated NS instance.

[0031] In long term evolution (LTE), there is a mechanism that could be relevant for the described scenario. This mechanism is described in clause 5.3.2 from TS 23.401. It is based on the so called ciphered option request and uses an information element called the protocol configuration options (PCO).

[0032] The PCO is one of the information elements in non-access stratum (NAS) messages. The PCO may be used in several types of messages such as a packet data network (PDN) connectivity request to send information transparently through an Mobility Management Entity (MME) and a serving gateway (S-GW) to a PDN-GW. For example, the PCO may include an address allocation preference indicating that the UE prefers to obtain an Internet protocol version 4 (IPv4) address only after a default bearer activation by means of dynamic host configuration protocol version four (DHCPv4).

[0033] One use case of the PCO is the transfer of password authentication protocol (PAP) and challenge handshake authentication protocol (CHAP) usernames and passwords to the PDN-GW, which then runs them through an authentication, authorization, and accounting (AAA) server for access authorization. The AAA server may be located in an external domain. Since usernames and passwords are sensitive and needs to be protected, if the UE intends to send PCO which require ciphering (e.g., PAP/CHAP usernames and passwords), the UE shall set a ciphered options transfer flag in an attach request message and send the PCO only after authentication and NAS security setup have been completed.

[0034] Fig. 2 shows the message flow required for running such an additional (i.e. secondary) authentication procedure through the PDN-GW in LTE. In the following, a more detailed

description of the steps therein is provided.

[0035] An UE is within the UE domain. An MME, a S-GW, a home subscriber server (HSS), and a PDN-GW are within the MNO domain. An AAA server is within a third party domain.

[0036] In step 1 the UE sends an attach request message with a ciphered options transfer flag set to the MME.

[0037] In step 2 an authentication and key agreement (AKA) procedure is run between the UE and the HSS. Upon successful authentication the next steps are executed.

[0038] In step 3 a NAS security is set up, using secure mode command (SMC). After the NAS security has been set up, all NAS messages are confidentiality and integrity protected.

[0039] In step 4 the MME sends a ciphered options request message to the UE for the retrieval of the PCO.

[0040] In step 5 the UE replies with a ciphered options response message including the PAP/CHAP username and password in the PCO information element. In case the UE has subscriptions to multiple PDNs, then the UE includes an access point name (APN) in the message as well.

[0041] In step 6 the MME deciphers the received data, uses possible provided APN to identify a PDN-GW, and forwards the PCO through the S-GW to the target PDN-GW in a create session request message.

[0042] In step 7 the PDN-GW sends the received PAP/CHAP information in a diameter/radius access request message to an external AAA server. Upon success, the session creation procedure proceeds as usual.

[0043] The above steps 4-7 thus represent a secondary authentication, performed after the first authentication in step 2 has been completed. However, to use this mechanism in or extension into NG systems would provide some drawbacks.

[0044] Firstly, the mechanism is very limited in terms of possible authentication methods. Currently there is only support for PAP and CHAP. But since PAP today is obsolete from a security point of view, only CHAP is essentially possible to use.

[0045] Secondly, in order to support other methods and use the PCO information element for the transport of authentication information, the mechanism would be required to specify special messages between the MME and the S-GW and the S-GW and PDN-GW dedicated to this purpose. I.e. to handle authentication methods that require more than just one round-trip.

[0046] Furthermore, it is difficult to see how this mechanism would fit in the NG architecture,

which is going to be broken further down. In fact, taking into consideration the new architectural features (TR 23.799), there will probably be more hops in the path between the UE and the PDN-GW, for example in relation to ongoing work on the split of the MME into a mobility management function (MMF) and a session management function SMF (TR 23.799) and control and user plane separation (CUPS) work for the control and user plane split (TR 23.714). This implies more overload and signaling in the core network (CN).

[0047] Finally, this mechanism is a workaround because there is no direct protocol between the UE and the PDN-GW. Making it generic enough to support other authentication methods would be technically challenging, especially since many methods have strict recommendations and requirements on the transport layer.

[0048] Running the secondary authentication on the user plane (UP), once it is set up is presented. A limited UP session may be run for the secondary authentication procedure, rather than allowing full access to the PDN. Once the secondary authentication is completed, a limited UP session may be upgraded to one having full access to a data network. The use of an extensible authentication protocol (EAP), as defined in RFC3748, is also presented. The EAP is used for authentication between the UE and a potentially external AAA server, where an NG-UP function (UPF), playing a similar role to that of the PDN-GW in LTE, endorses the role of an EAP authenticator. EAP payloads would be carried by a protocol for carrying authentication for network access (PANA), as defined in RFC5191, which protocol is IP-based. Another alternative is that the NG-UPF endorses the role of the EAP server.

[0049] The presented solution uses EAP which is widely used and provides support for many authentication methods such as EAP-transport layer security (TLS), EAP-authentication and key agreement (AKA), EAP-tunneled TLS (TTLS) and EAP-protected extensible authentication protocol (PEAP). The presented solution is IP-based and thus agnostic to the type of access network (AN). Further, since it is UP based, the secondary authentication can be performed independently on NS specific basis even for scenarios where the NG-UE supports multiple possibly simultaneous NS connectivity. By using EAP, the solution also supports different types of credentials and authentication methods. The EAP exchange may benefit from the protection over an air interface.

[0050] The secondary authentication is thus run of the UP bearers once the NG-UE is allocated an IP address. EAP is then used for authentication between the NG-UE and the (potentially external) AAA server where the NG-UPF endorses the role of the EAP authenticator.

[0051] An embodiment wherein the NG-UPF acts as an EAP authenticator is presented with reference to Fig. 3.

[0052] Fig. 3 shows a flow where an UP-based secondary authentication is run with an external AAA server. The NG-UE is in the UE domain. The NG mobility management function (MMF), the NG session management function (SMF), NG security anchor function (SEAF) and

NG-UPF are in the MNO domain. The NG-UPF is an UPF corresponding to a PDN-GW in LTE. The AAA server is in a third party domain. The requirements on the NG-UPF is to include support of PANA and EAP, possibly in addition to the support of all needed UP features of the PDN-GW in LTE such as the support of an SGi interface. In general, a NG-prefix is used for NG system function corresponding to LTE concepts.

[0053] In step 1 the NG-UE sends an attach request initiating the attach procedure. The solution presented herein is not dependent on how network slicing is supported, e.g. how the NS instances are selected and how the NG-UE is directed to the proper ones.

[0054] In step 2 the NG-UE runs a primary authentication with the NG SEAF. The NG SEAF may further be connected to a NG authentication server function (AUSF). A later, secondary authentication is not dependent on how the NG SEAF and NG MMF are deployed (i.e. collocated or split) nor on the location of the NG SEAF (home or visited public land mobile network (PLMN)).

[0055] In step 3 a control plane security is established between the NG-UE and the end point of the NG NAS. The end point of the NG NAS may e.g. be the NG MMF or the NG SMF.

[0056] In step 4 a protocol data unit (PDU) session is thereafter established for the transport of UP data between the NG-UE and a data network via the NG-UPF. Step 4 may be a limited session allowing only for running the secondary authentication procedure. The later, secondary authentication depends on the UP being set up, since it establishes IP connectivity between the NG-UE and the NG-UPF.

[0057] In step 5 a secondary EAP-based authentication is run between the NG-UE and the NG-UPF, here endorsing the role of an EAP authenticator and relying on a backend external AAA server. The NG-UE is thereafter granted access in the data network based on the outcome of this authentication procedure.

[0058] This presented solution is agnostic on how non-3GPP access will be integrated and whether steps 1 to 3 are executed exactly as depicted here or differently. As long as an IP connectivity is established between the NG-UE and the NG-UPF, which is achieved in step 4, the EAP-based authentication can be run in step 5. In case radio access network (RAN) security has been established before step 5, then the EAP exchange would be protected also on the air interface.

[0059] Fig. 4 shows a protocol architecture for the EAP-based secondary authentication, between the NG-UPF and the NG-UE with NG-UPF as EAP authenticator, as described with reference to Fig. 3. The architecture shown in Fig. 4 is similar to the architecture of LTE regarding the transport of the UP traffic between the UE and the PDN-GW. The greyed boxes highlight the required additional protocol layers to provide the above described EAP-based secondary authentication.

[0060] An embodiment with a protocol architecture for EAP-based secondary authentication with NG-UPF as EAP server is presented with reference to Fig. 5.

[0061] In this embodiment the NG-UPF terminates the EAP exchange and endorses the role of a complete EAP server. The message flow for this embodiment is thus similar to that of Fig. 3, except that in step 5 an external AAA server is not contacted.

[0062] A mechanism for additional or secondary authentication in NG systems between the NG-UE and the NG-UPF terminating the UP traffic within the core network and possibly interacting with an external AAA-server has been presented. The NG-UPF corresponds to the PDN-GW in LTE. The mechanism is based on EAP over IP over UP traffic such that the NG-UPF endorses the EAP authenticator role or the EAP server role.

[0063] A communication network 4, wherein embodiments described herein can be implemented is presented in Fig. 1. A user equipment (UE) 1 is wirelessly connectable to a base station (BS) 2. The BS 2 is connected to a core network (CN) 3.

[0064] A method, according to an embodiment, for secondary authentication in a network is presented with reference to Fig. 6A. The method is performed by a next generation (NG) user equipment (UE), and comprises establishing 110 a user plane (UP) session or connection with a NG-UP function (UPF), receiving 130 an extensible authentication protocol (EAP) based authentication request from the NG-UPF, and sending 140 an EAP based authentication response to the NG-UPF.

[0065] The method may further comprise establishing 100 a primary authentication with a NG SEAF.

[0066] The method may further comprise receiving an EAP based authentication result from the UPF.

[0067] A method, according to an embodiment, for secondary authentication in a core network is presented with reference to Fig. 6B. The method is performed by a next generation (NG)-user plane (UP) function (UPF), and comprises establishing 110 a user plane (UP) session or connection with a NG user equipment (UE), sending 120 an extensible authentication protocol (EAP) based authentication request to the NG UE, and receiving 150 an EAP based authentication response from the NG UE.

[0068] The method may further comprise sending 160 a verification request of the received EAP based authentication response to an authentication, authorization, and accounting (AAA) server, and receiving 170 a verification response from the AAA server.

[0069] The method may further comprise sending an authentication result to the UE, wherein the authentication is based on the verification response from the AAA server.

[0070] A NG UE, according to an embodiment, for operation in a network is presented with reference to Fig. 7. The NG UE 1 comprises a processor 10, and a computer program product 12, 13. The computer program product stores instructions that, when executed by the processor, causes the NG UE to establish 110 a UP session or connection with a NG-UPF, receive 130 an EAP based authentication request from the NG-UPF, and to send 140 an EAP based authentication response to the NG-UPF.

[0071] A NG-UPF according to an embodiment, operative in a core network is presented with reference to Fig. 8. The NG-UPF comprises a processor 10, and a computer program product 12, 13 storing instructions that, when executed by the processor, causes the NG-UPF to establish 110 a UP session or connection to a NG UE, send 120 an EAP based authentication request to the NG UE, and to receive 150 an EAP based authentication response from the NG UE.

[0072] A NG UE, according to an embodiment, for operation in a network, is presented with reference to Fig. 9. The NG UE comprises a communication manager 61 for establishing 110 a UP session or connection with a NG-UPF, receiving 130 an EAP based authentication request from the NG-UPF, and for sending 140 an EAP based authentication response to the NG-UPF.

[0073] A NG-UPF, according to an embodiment, operative in a network is presented with reference to Fig. 10. The NG-UPF comprises a communication manager 71 for establishing 110 a UP session or connection with a NG UE, sending 120 an EAP based authentication request to the NG UE, and for receiving 150 an EAP based authentication response from the NG UE.

[0074] A computer program 14, 15, according to an embodiment, for secondary authentication in a network is presented. The computer program comprises computer program code which, when run on a NG UE, causes the NG UE to establish 110 a UP session or connection with a NG-UPF, receive 130 an EAP based authentication request from the NG-UPF, and to send 140 an EAP based authentication response to the NG-UPF.

[0075] A computer program 14, 15, according to an embodiment, for secondary authentication in a network is presented. The computer program comprises computer program code which, when run on a NG-UPF, causes the NG-UPF to establish 110 a UP session or connection with a NG UE, send 120 an EAP based authentication request to the NG UE, and to receive 150 an EAP based authentication response from the NG UE.

[0076] A computer program product 12, 13, according to an embodiment, is presented. The computer program product comprises a computer program 14, 15 as presented above and a computer readable storage means on which the computer program 14, 15 is stored.

[0077] Fig. 7 is a schematic diagram showing some components of the NG UE 1. A processor 10 may be provided using any combination of one or more of a suitable central processing unit, CPU, multiprocessor, microcontroller, digital signal processor, DSP, application specific

integrated circuit etc., capable of executing software instructions of a computer program 14 stored in a memory. The memory can thus be considered to be or form part of the computer program product 12. The processor 10 may be configured to execute methods described herein with reference to Figs. 12 and 13.

[0078] The memory may be any combination of read and write memory and read only memory, ROM. The memory may also comprise persistent storage, which, for example, can be any single one or combination of magnetic memory, optical memory, solid state memory or even remotely mounted memory.

[0079] A second computer program product 13 in the form of a data memory may also be provided, e.g. for reading and/or storing data during execution of software instructions in the processor 10. The data memory can be any combination of read and write memory and read only memory, ROM, and may also comprise persistent storage, which, for example, can be any single one or combination of magnetic memory, optical memory, solid state memory or even remotely mounted memory. The data memory may e.g. hold other software instructions 15, to improve functionality for the NG UE 1.

[0080] The NG UE 1 may further comprise an input/output, I/O, interface 11 including e.g. a user interface. The NG UE 1 may further comprise a receiver configured to receive signalling from other nodes, and a transmitter configured to transmit signalling to other nodes (not illustrated). Other components of the NG UE 1 are omitted in order not to obscure the concepts presented herein.

[0081] Fig. 9 is a schematic diagram showing functional blocks of the NG UE 1. The modules may be implemented as only software instructions such as a computer program executing in the cache server or only hardware, such as application specific integrated circuits, field programmable gate arrays, discrete logical components, transceivers, etc. or as a combination thereof. In an alternative embodiment, some of the functional blocks may be implemented by software and other by hardware. The modules correspond to the steps in the method illustrated in Fig. 6A, comprising a communication manager unit 61 and a determination module unit 60. In the embodiments where one or more of the modules are implemented by a computer program, it shall be understood that these modules do not necessarily correspond to process modules, but can be written as instructions according to a programming language in which they would be implemented, since some programming languages do not typically contain process modules.

[0082] The communication manager 61 is for operation in a network. This module corresponds to the establish UP step 110, the receive request step 130 and the send response step 140 of Fig. 6A. This module can e.g. be implemented by the processor 10 of Fig. 7, when running the computer program.

[0083] The determination manager 60 is for operation in a network. This module corresponds to the primary authentication step 100 of Fig. 6A. This module can e.g. be implemented by the

processor 10 of Fig. 7, when running the computer program.

[0084] Fig. 8 is a schematic diagram showing some components of the NG-UPF 3. A processor 10 may be provided using any combination of one or more of a suitable central processing unit, CPU, multiprocessor, microcontroller, digital signal processor, DSP, application specific integrated circuit etc., capable of executing software instructions of a computer program 14 stored in a memory. The memory can thus be considered to be or form part of the computer program product 12. The processor 10 may be configured to execute methods described herein with reference to Fig. 6B.

[0085] The memory may be any combination of read and write memory, RAM, and read only memory, ROM. The memory may also comprise persistent storage, which, for example, can be any single one or combination of magnetic memory, optical memory, solid state memory or even remotely mounted memory.

[0086] A second computer program product 13 in the form of a data memory may also be provided, e.g. for reading and/or storing data during execution of software instructions in the processor 10. The data memory can be any combination of read and write memory, RAM, and read only memory, ROM, and may also comprise persistent storage, which, for example, can be any single one or combination of magnetic memory, optical memory, solid state memory or even remotely mounted memory. The data memory may e.g. hold other software instructions 15, to improve functionality for the NG-UPF 3.

[0087] The NG-UPF 3 may further comprise an input/output, I/O, interface 11 including e.g. a user interface. The NG-UPF 3 may further comprise a receiver configured to receive signalling from other nodes, and a transmitter configured to transmit signalling to other nodes (not illustrated). Other components of the NG-UPF 3 are omitted in order not to obscure the concepts presented herein.

[0088] Fig. 10 is a schematic diagram showing functional blocks of the NG-UPF 3. The modules may be implemented as only software instructions such as a computer program executing in the cache server or only hardware, such as application specific integrated circuits, field programmable gate arrays, discrete logical components, transceivers, etc. or as a combination thereof. In an alternative embodiment, some of the functional blocks may be implemented by software and other by hardware. The modules correspond to the steps in the methods illustrated in Fig. 6B, comprising a communication manager unit 71 and a determination manager unit 70. In the embodiments where one or more of the modules are implemented by a computer program, it shall be understood that these modules do not necessarily correspond to process modules, but can be written as instructions according to a programming language in which they would be implemented, since some programming languages do not typically contain process modules.

[0089] The communication manger 71 is for operation in a core network. This module corresponds to the establish UP step 110, the send request step 120, and the receive

response step 150 of Fig. 6B. This module can e.g. be implemented by the processor 10 of Fig. 8, when running the computer program.

[0090] The determination manager unit 70 is for operation in a core network. This module corresponds to the verification request step 160 and the verification response step 170 of Fig. 6B. This module can e.g. be implemented by the processor 10 of Fig. 8, when running the computer program.

[0091] The inventive concept has mainly been described above with reference to a few embodiments. However, as is readily appreciated by a person skilled in the art, other embodiments than the ones disclosed above are equally possible within the scope of the appended patent claims.

REFERENCES CITED IN THE DESCRIPTION

This list of references cited by the applicant is for the reader's convenience only. It does not form part of the European patent document. Even though great care has been taken in compiling the references, errors or omissions cannot be excluded and the EPO disclaims all liability in this regard.

Non-patent literature cited in the description

- Way forward on support of non-3GPP access and update o solution 8.6 for support of untrusted non-3GPP access3rd Generation Partnership Project (3GPP), SA WG2 Meeting #1172-166283 **[0005]**

P a t e n t k r a v

1. Fremgangsmåde til sekundær autentifikation i et netværk, hvilken fremgangsmåde udføres af en brugerindretning, UE, hvilken fremgangsmåde omfatter:

at etablere (100) en primær autentifikation med en SEAF, security anchor function;

at etablere (110) en brugerplan, UP, -session eller -forbindelse med eller via en UP-funktion, UPF;

at modtage (130) en EAP, extensible authentication protocol, -baseret autentifikationsanmodning via UPF'en;

at sende (140) et EAP-baseret autentifikationssvar til UPF'en; og

at modtage et EAP-baseret autentifikationsresultat via UPF'en, hvor det EAP-baserede autentifikationsresultat er baseret på et verifikationssvar fra en ekstern AAA, authentication, authorization and accounting, -server.

2. Fremgangsmåde ifølge krav 1, hvor brugerindretningen, UE, er en næstegenerations, NG, -UE.

3. Fremgangsmåde ifølge krav 1, hvor brugerplanfunktionen, UPF, er en næstegenerations, NG, -UPF.

4. Fremgangsmåde ifølge krav 1, hvor SEAF'en endvidere er forbundet med en autentifikationsserverfunktion, AUSF.

5. Fremgangsmåde til sekundær autentifikation i et netværk, udført gennem en brugerplan, UP, -funktion, UPF, hvilken fremgangsmåde omfatter:

at etablere (110) en UP-session eller -forbindelse til en brugerindretning, UE;

at sende (120) en EAP, extensible authentication protocol, -baseret autentifikationsanmodning til UE'en;

at modtage (150) et EAP-baseret autentifikationssvar fra UE'en;

at sende (160) en verifikationsanmodning af det modtagne EAP-baserede autentifikationssvar til en ekstern AAA, authentication, authorization and accounting, -server;

at modtage (170) et verifikationssvar fra den eksterne AAA-server; og

at sende et autentifikationsresultat til UE'en, hvor autentifikationsresultatet er baseret på verifikationssvaret fra den eksterne AAA-server.

10 **6.** Fremgangsmåde ifølge krav 5, hvor brugerindretningen, UE, er en næstegenerations, NG-, brugerindretning, -UE.

7. Fremgangsmåde ifølge krav 5, hvor brugerplanfunktionen, UPF, er en næstegenerations, NG, -UPF.

15 **8.** Brugerindretning, UE, til anvendelse i et netværk, hvilken UE omfatter:

en processor (10); og

et computerprogramprodukt (12, 12), der lagrer instruktioner, som, når de eksekveres af processoren, får UE'en til:

20 at etablere (100) en primær autentifikation med en SEAF, security anchor function;

at etablere (110) en brugerplan, UP, -session eller -forbindelse med eller via en UP-funktion, UPF;

25 at modtage (130) en EAP, extensible authentication protocol, -baseret autentifikationsanmodning via UPF'en;

at sende (140) et EAP-baseret autentifikationssvar til UPF'en; og

30 at modtage et EAP-baseret autentifikationsresultat via UPF'en, hvor det EAP-baserede autentifikationsresultat er baseret på et verifikationssvar fra en ekstern AAA, authentication, authorization and accounting, -server.

9. Brugerindretning, UE, ifølge krav 8, hvor UE'en er en næstegenerations, NG, -UE.

5 **10.** Brugerindretning, UE, ifølge krav 8, hvor UPF'en er en næstegenerations, NG, -UPF.

11. Brugerindretning, UE, ifølge krav 8, hvor SEAF'en endvidere er forbundet med en autentifikationsserverfunktion, AUSF.

10 **12.** Brugerplan, UP, -funktion, UPF, der kan anvendes i et netværk, hvilken UPF omfatter:
en processor (10); og

et computerprogramprodukt (12, 13), der lagrer instruktioner, som, når de eksekveres af processoren, får UPF'en til:

15 at etablere (110) en UP-session eller -forbindelse med en brugerindretning, UE;

at sende (120) en EAP, extensible authentication protocol, -baseret autentifikationsanmodning til UE'en;

at modtage (150) et EAP-baseret autentifikationssvar fra UE'en;

20 at sende (160) en verifikationsanmodning af det modtagne EAP-baserede autentifikationssvar til en ekstern AAA, authentication, authorization and accounting, -server;

at modtage (170) et verifikationssvar fra den eksterne AAA-server;
og

25 at sende et autentifikationsresultat til UE'en, hvor autentifikationsresultatet er baseret på verifikationssvaret fra den eksterne AAA-server.

30 **13.** Brugerplan, UP, -funktion, UPF, ifølge krav 12, hvor UPF'en er en næstegenerations, NG, -UPF.

14. Brugerplan, UP, -funktion, UPF, ifølge krav 12, hvor UE'en er en næstegenerations, NG, -UE.

15. Computerprogram (14, 15) til sekundær autentifikation i et netværk, hvilket computerprogram omfatter en computerprogramkode, som, når den køres på en brugerindretning, UE, får UE'en til:

5 at etablere (100) en primær autentifikation med en SEAF, security anchor function;

at etablere (110) en brugerplan, UP, -session eller -forbindelse med eller via en UP-funktion, UPF;

10 at modtage (130) en EAP, extensible authentication protocol, -baseret autentifikationsanmodning via UPF'en;

at sende (140) et EAP-baseret autentifikationssvar til UPF'en;

og at modtage et EAP-baseret autentifikationsresultat via UPF'en, hvor det EAP-baserede autentifikationsresultat er baseret på et verifikationssvar fra en ekstern AAA, authentication, authorization and accounting, -server.

15

16. Computerprogram (14, 15) til sekundær autentifikation i et netværk, hvilket computerprogram omfatter en computerprogramkode, som, når den køres på en brugerplan, UP, -funktion, UPF, får UPF'en til:

20

at etablere (110) en brugerplan, UP, -session eller -forbindelse til en brugerindretning, UE;

at sende (120) en EAP, extensible authentication protocol, -baseret autentifikationsanmodning til UE'en;

25

at modtage (150) et EAP-baseret autentifikationssvar fra UE'en;

at sende (160) en verifikationsanmodning af det modtagne EAP-baserede autentifikationssvar til en ekstern AAA, authentication, authorization and accounting, -server;

at modtage (170) et verifikationssvar fra den eksterne AAA-server;

30

og

at sende et autentifikationsresultat til UE'en, hvor autentifikationen er baseret på verifikationssvaret fra den eksterne AAA-server.

17. Computerprogramprodukt (12, 13) omfattende et computerlæsbart lagringsmedium, på hvilket et computerprogram (14, 15) ifølge et hvilket som helst af kravene 15 eller 16 er lagret.

DRAWINGS

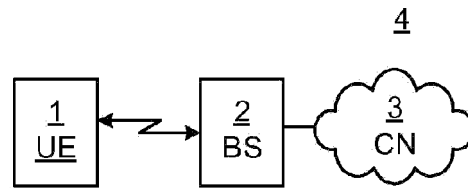


Fig. 1

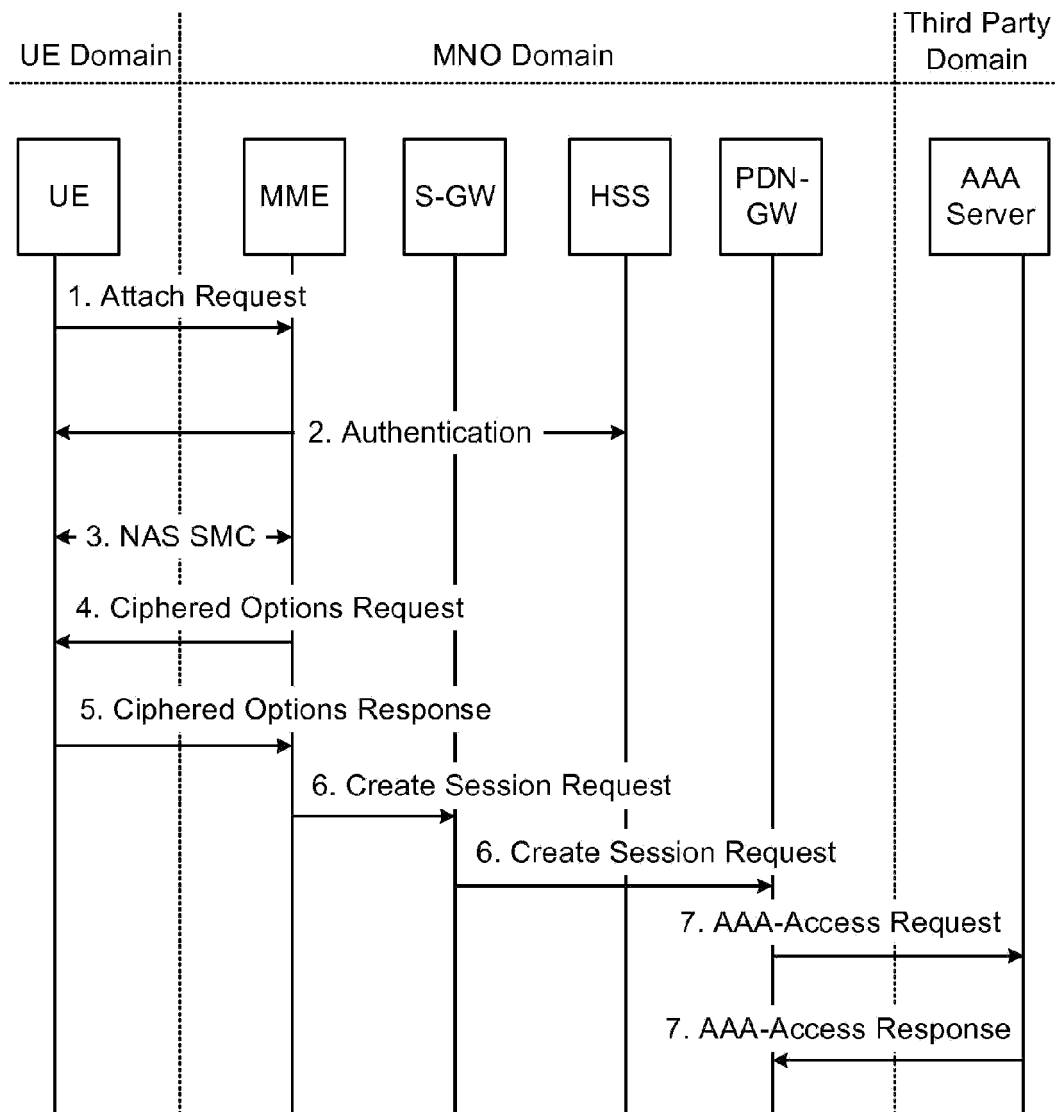


Fig. 2

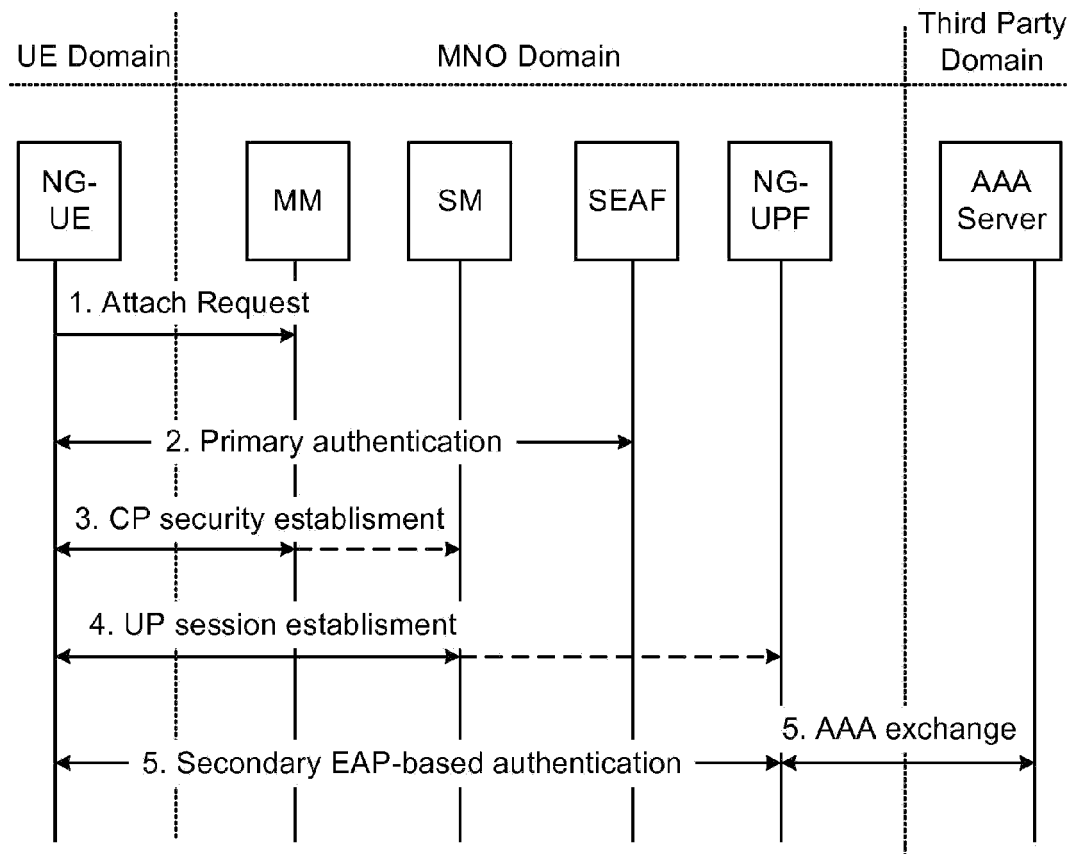


Fig. 3

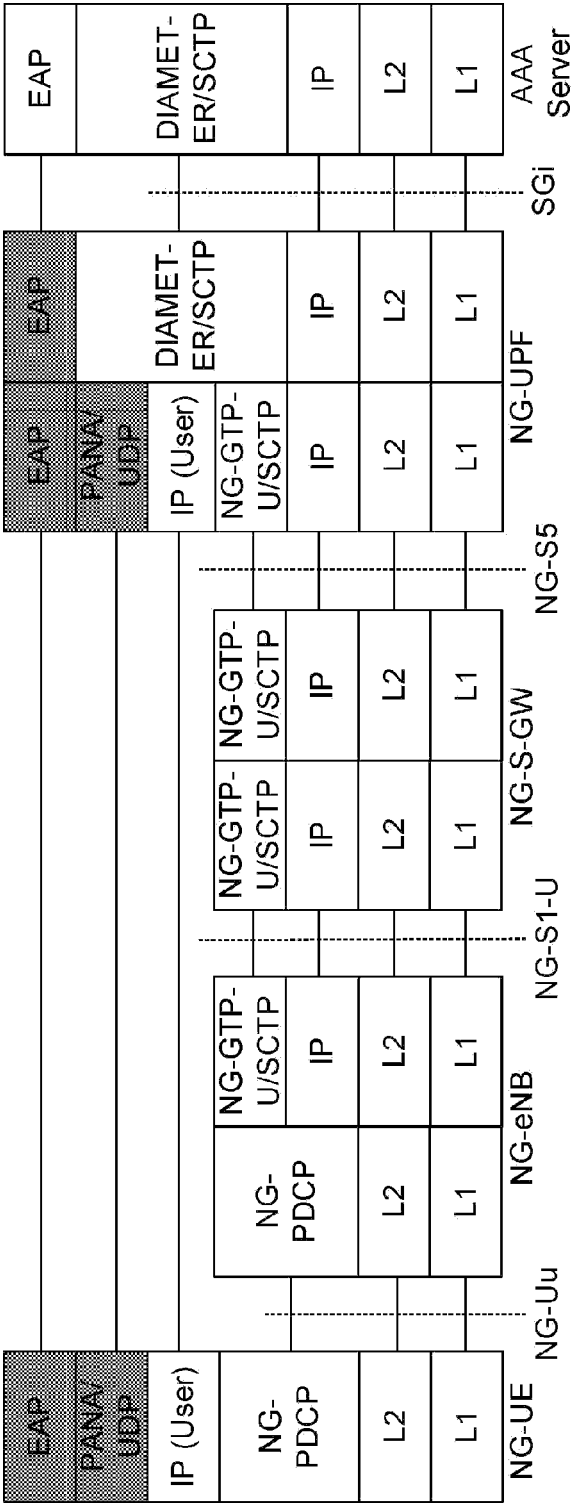


Fig. 4

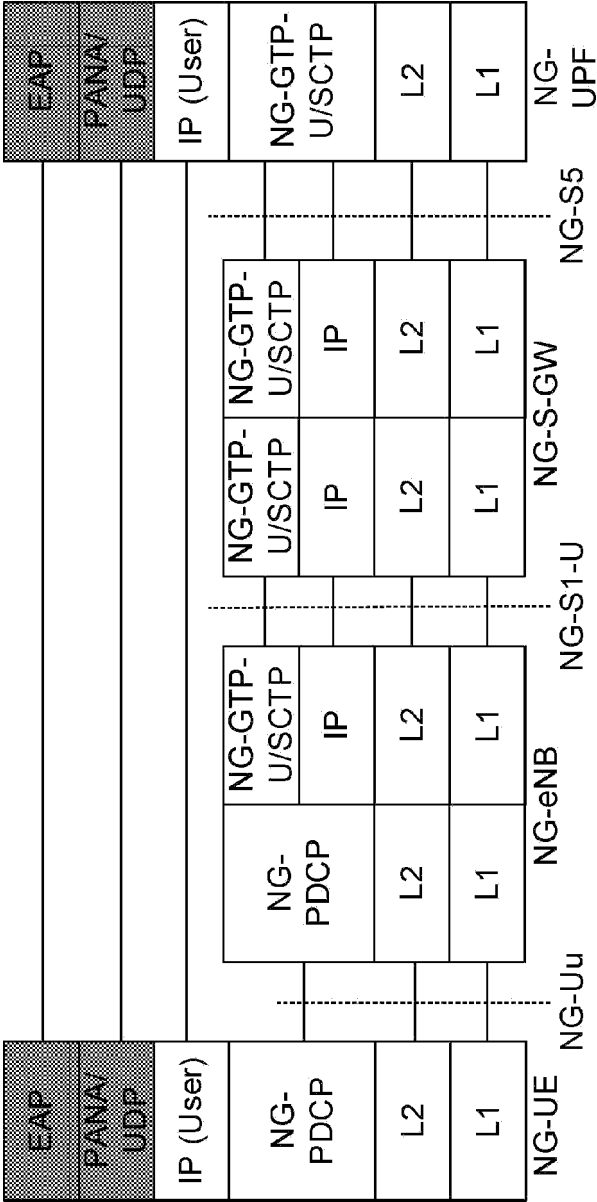


Fig. 5

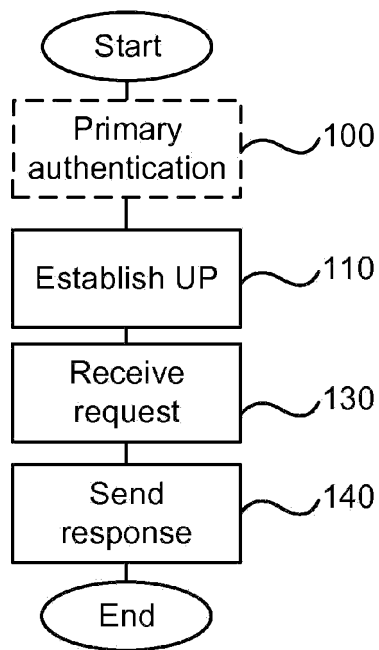


Fig. 6A

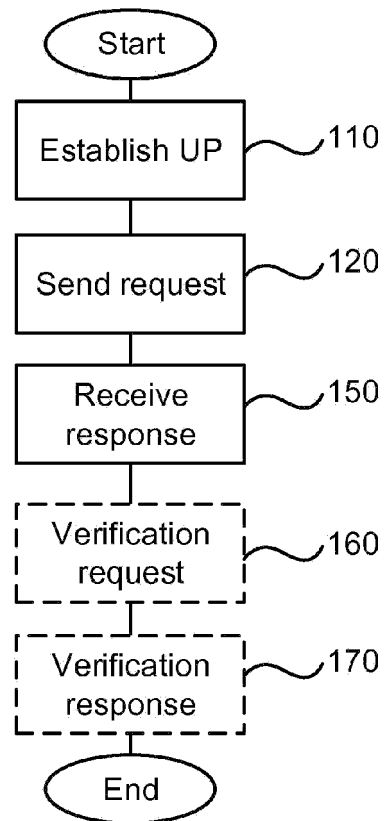


Fig. 6B

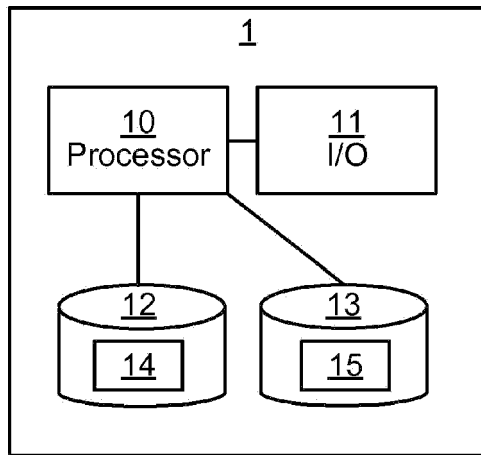


Fig. 7

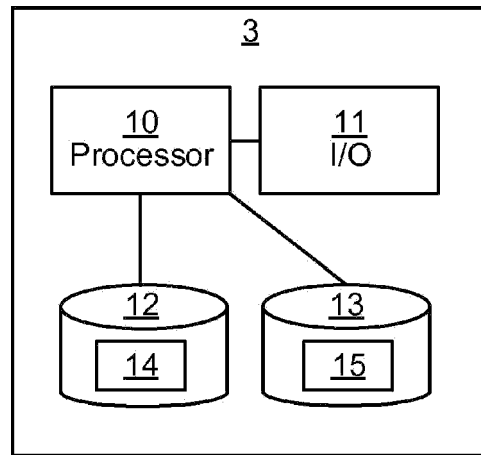


Fig. 8

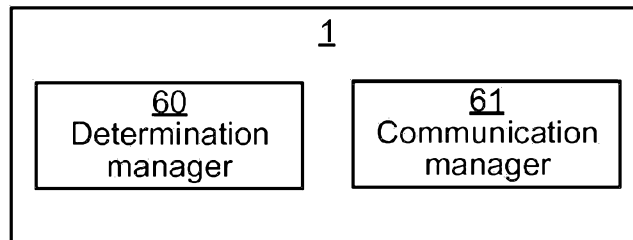


Fig. 9

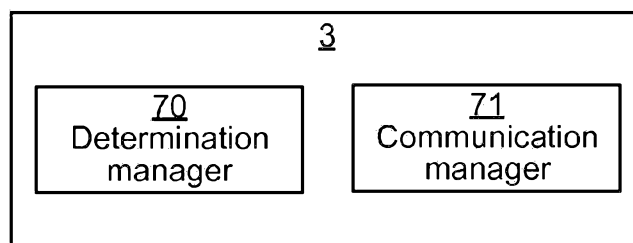


Fig. 10