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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
24 December 2020 (24.12.2020)

WIPO | PCT

(10) International Publication Number
WO 2020/256366 A1

(51) International Patent Classification:
H04L 29/08 (2006.01) *H04L 29/06* (2006.01)

(21) International Application Number:
PCT/KR2020/007706

(22) International Filing Date:
15 June 2020 (15.06.2020)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
201941023952 17 June 2019 (17.06.2019) IN
201941023952 03 June 2020 (03.06.2020) IN

(71) Applicant: **SAMSUNG ELECTRONICS CO., LTD.** [KR/KR]; 129, Samsung-ro, Yeongtong-gu, Suwon-si, Gyeonggi-do 16677 (KR).

(72) Inventors: **GUPTA, Nishant**; 74, Rampa Cinema Road, Thompsonganj, Sitapur, Uttar Pradesh, 261001 (IN). **RAJADURAI, Rajavelsamy**; D-2183, 3rd Main, Sahakara Nagar, Bangalore, Karnataka, 560092 (IN). **TANGUDU, Narendranath Durga**; J304, Vijetha Elysium Apartments, Opp Prestige Ozone, Hagadur Road, Whitefield, Bangalore, Karnataka, 560066 (IN).

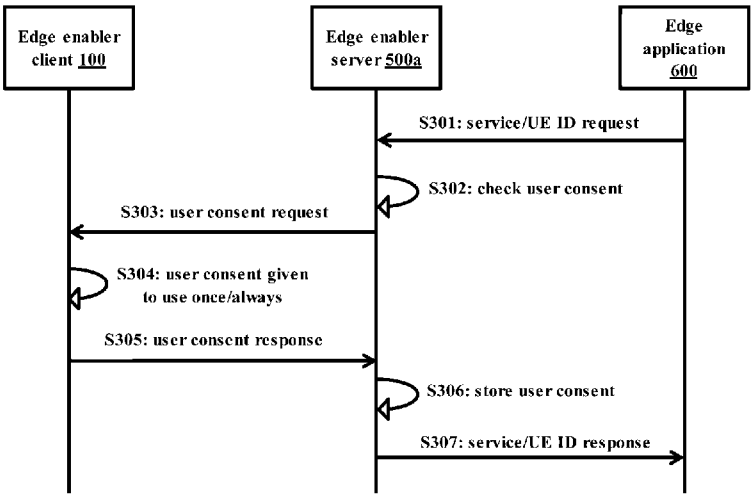
(74) Agent: **Y.P.LEE,MOCK & PARTNERS**; 12F Daelim Acrotel, 13 Eonju-ro 30-gil, Gangnam-gu, Seoul 06292 (KR).

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

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

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

(54) **Title:** METHOD AND SERVER FOR PROVIDING USER CONSENT TO EDGE APPLICATION



(57) **Abstract:** Embodiments herein provide a method for providing a service to an edge application (600). The method includes receiving, by a server (500), at least one of a request for accessing the service associated with a User Equipment (300) from the edge application (600), and a request for a user consent associated with the UE (300) from the edge application (600). The method includes retrieving, by the server (500), the user consent from the edge enabler client (100), where the user consent indicates a consent of a user of the edge enabler client (100) to provide at least one of the service and the user consent with the edge application (600). The method includes sending, by the server (500), at least one of the service and the user consent to the edge application (600).

WO 2020/256366 A1

Description

Title of Invention: METHOD AND SERVER FOR PROVIDING USER CONSENT TO EDGE APPLICATION

Technical Field

[1] Present disclosure relates to edge computing systems, and more specifically to a method and a system for providing a service to an edge application based on a user consent.

Background Art

[2] To meet the demand for wireless data traffic having increased since deployment of 4th generation (4G) communication systems, efforts have been made to develop an improved 5th generation (5G) or pre-5G communication system. The 5G or pre-5G communication system is also called a 'beyond 4G network' or a 'post long term evolution (LTE) system'. The 5G communication system is considered to be implemented in higher frequency (mmWave) bands, e.g., 60 GHz bands, so as to accomplish higher data rates. To decrease propagation loss of the radio waves and increase the transmission distance, beamforming, massive multiple-input multiple-output (MIMO), full dimensional MIMO (FD-MIMO), array antenna, analog beamforming, and large scale antenna techniques are discussed with respect to 5G communication systems. In addition, in 5G communication systems, development for system network improvement is under way based on advanced small cells, cloud radio access networks (RANs), ultra-dense networks, device-to-device (D2D) communication, wireless backhaul, moving network, cooperative communication, coordinated multi-points (CoMP), reception-end interference cancellation and the like. In the 5G system, hybrid frequency shift keying (FSK) and Feher's quadrature amplitude modulation (FQAM) and sliding window superposition coding (SWSC) as an advanced coding modulation (ACM), and filter bank multi carrier (FBMC), non-orthogonal multiple access (NOMA), and sparse code multiple access (SCMA) as an advanced access technology have been developed.

[3] The Internet, which is a human centered connectivity network where humans generate and consume information, is now evolving to the Internet of things (IoT) where distributed entities, such as things, exchange and process information without human intervention. The Internet of everything (IoE), which is a combination of the IoT technology and the big data processing technology through connection with a cloud server, has emerged. As technology elements, such as as As technonologyed connectivity network where humans generate and consume information, is now evolving to the Internet of things (IoT) where ud server, has emeIoT implementation, a

sensor network, a machine-to-machine (M2M) communication, machine type communication (MTC), and so forth have been recently researched. Such an IoT environment may provide intelligent Internet technology services that create a new value to human life by collecting and analyzing data generated among connected things. IoT may be applied to a variety of fields including smart home, smart building, smart city, smart car or connected cars, smart grid, health care, smart appliances and advanced medical services through convergence and combination between existing information technology (IT) and various industrial applications.

[4] In line with this, various attempts have been made to apply 5G communication systems to IoT networks. For example, technologies such as a sensor network, MTC, and M2M communication may be implemented by beamforming, MIMO, and array antennas. Application of a cloud RAN as the above-described big data processing technology may also be considered to be as an example of convergence between the 5G technology and the IoT technology.

[5] As described above, various services can be provided according to the development of a wireless communication system, and thus a method for easily providing such services is required.

Disclosure of Invention

Solution to Problem

[6] e principal object of the embodiments herein is to provide a method and a server for obtaining a user consent for providing a service to an edge application, where the service includes a network service, user specific information and device specific information.

[7] Another object of the embodiments herein is to obtain a grant of the user consent from an authorized user for providing the service to the edge application, in response to receiving a request for accessing the service associated with a UE for a first time.

[8] Another object of the embodiments herein is to store the user consent at a server user for a future usage of the user consent, in response to receiving the user consent.

[9] Another object of the embodiments herein is to use the user consent stored at the server for providing the service to the edge application, in response to receiving the request for the service associated with the UE for a second time.

[10] Another object of the embodiments herein is to allow the authorized user to modify the user consent stored at the server for controlling an exposure of the service with the edge application.

[11] Another object of the embodiments herein is to provide private and sensitive information of the authorized user to only a legitimate edge application trusted by the authorized user.

Brief Description of Drawings

[12] This method and apparatus are illustrated in the accompanying drawings, throughout which like reference letters indicate corresponding parts in the various figures. The embodiments herein will be better understood from the following description with reference to the drawings, in which:

[13] FIG. 1 is a block diagram of a system for providing a service to an edge application of an edge data network, according to an embodiment as disclosed herein;

[14] FIG. 2A-2H illustrates a block diagram of devices in the system for providing the service to the edge application, according to an embodiment as disclosed herein;

[15] FIG. 3 is a sequential diagram illustrating signaling between the devices in the system for providing the service to the edge application in response to receiving a request for the service, according to an embodiment as disclosed herein;

[16] FIG. 4 is a sequential diagram illustrating signaling between the devices in the system for providing the user consent to the edge application in response to receiving a request for a user consent, according to an embodiment as disclosed herein;

[17] FIG. 5 is a sequential diagram illustrating signaling between the devices in the system for providing a User Equipment Identifier (UE ID) to the edge application in response to receiving a request for the UE ID, according to an embodiment as disclosed herein;

[18] FIG. 6 is a sequential diagram illustrating signaling between the devices in the system for providing a user consent to the edge application in response to receiving the user consent voluntarily provided by a user, according to an embodiment as disclosed herein;

[19] FIG. 7 is a sequential diagram illustrating signaling between the devices in the system for storing the user consent at an edge enabler server in response to receiving the user consent voluntarily provided by the user and verifying the user consent, according to an embodiment as disclosed herein;

[20] FIG. 8 is a sequential diagram illustrating signaling between the devices in the system for storing the user consent at the edge enabler server in response to receiving the user consent voluntarily provided by the user, according to an embodiment as disclosed herein;

[21] FIG. 9 is a sequential diagram illustrating signaling between the devices in the system for providing the UE ID to the edge application in response to receiving the user consent voluntarily provided by the user and verifying an application specific user information, according to an embodiment as disclosed herein;

[22] FIG. 10 is a sequential diagram illustrating signaling between the devices in the system for providing the service to the edge application in response to initiating a user

consent grant by an application client and verifying a OTP, according to an embodiment as disclosed herein;

[23] FIG. 11 is a sequential diagram illustrating signaling between the devices in the system for providing the service to the edge application in response to initiating the user consent grant by an edge enabler client and verifying the OTP, according to an embodiment as disclosed herein;

[24] FIG. 12 is a sequential diagram illustrating signaling between the devices in the system for providing the service to the edge application based on an authorization from a CAPIF core function device, according to an embodiment as disclosed herein;

[25] FIG. 13 is a sequential diagram illustrating signaling between the devices in the system for providing authorizing credentials to the edge application based on the user consent, according to an embodiment as disclosed herein;

[26] FIG. 14 is a sequential diagram illustrating signaling between the devices in the system for providing the authorization credentials to the edge application based on the user consent obtained through the edge enabler server, according to an embodiment as disclosed herein;

[27] FIG. 15 is a sequential diagram illustrating signaling between the devices in the system for providing the service to an edge application server in response to obtaining the user consent from the edge enabler client through a Policy Control Function (PCF), according to an embodiment as disclosed herein;

[28] FIG. 16 is a sequential diagram illustrating signaling between the devices in the system for providing the service to the edge application server in response to obtaining the user consent from the edge enabler client through a Unified Data Management/ Unified Data Repository (UDM/ UDR), according to an embodiment as disclosed herein;

[29] FIG. 17 is a sequential diagram illustrating signaling between the devices in the system for providing the service to the edge application server in response to obtaining the user consent from a non-access stratum layer through the PCF, according to an embodiment as disclosed herein;

[30] FIG. 18 is a sequential diagram illustrating signaling between the devices in the system for providing the service to the edge application server in response to obtaining the user consent from the non-access stratum layer through the UDM/UDR, according to an embodiment as disclosed herein;

[31] FIG. 19 is a sequential diagram illustrating signaling between the devices in the system for providing the service to the edge application server in response to receiving the request for the service from the edge application server and the user consent through the PCF, according to an embodiment as disclosed herein; and

[32] FIG. 20 is a sequential diagram illustrating signaling between the devices in the

system for providing the service to the edge application server in response to receiving the request for the service from the edge application server and the user consent through the UDM/UDR, according to an embodiment as disclosed herein.

[33] FIG. 21 schematically illustrates the server according to embodiments of the present disclosure.

[34] FIG. 22 illustrates a user equipment (UE) according to embodiments of the present disclosure.

Best Mode for Carrying out the Invention

[35] The present disclosure provides a method and a server (or system) for providing a service to an edge application (600). The method for providing a service to an edge application (600) includes following steps of: receiving, by a server (500), a request for accessing at least one service associated with a UE (300) from the edge application (600); determining, by the server (500), availability of a user consent for accessing the at least one service requested by the edge application (600); and authorizing, by the server (500), access of the at least one service to the edge application (600) when the user consent is available.

[36] In an embodiment, the method further comprising: sending, by the server (500), a user consent request to the UE (300) when the user consent for accessing the at least one service is not available at the server (500), wherein the user consent request indicates a request for the user consent; receiving, by the server (500), a user consent response comprising the user consent from the UE (300) for authorizing the access of the at least one service; and storing, by the server (500), the user consent, in response to receiving the user consent.

[37] In an embodiment, the service associated with the UE (300) is a service associated with a user.

[38] In an embodiment, the server (500) is one of an edge enabler server (500a) and a Common Application Program Interface Framework (CAPIF) core function device (500b).

[39] In an embodiment, the method further comprising: receiving, by the server (500), a user consent update request from the edge enabler client (100), wherein the user consent update request comprises information about at least one parameter of the user consent to be updated; updating, by the server (500), the at least one parameter of the user consent stored at the server (500); and sending, by the server (500), a user consent update response to the edge enabler client (100).

[40] In an embodiment, the method comprising: receiving, by the server (500), a user consent update request from an application client (200) through an edge application server (700), wherein the user consent update request comprises information about at

least one parameter of the user consent to be updated; generating, by the server (500), an OTP for the user consent; sending, by the server (500), the OTP to the UE (300); receiving, by the server (500), a user consent update notification comprising the user consent and the OTP from one of the application client (200) through the edge application server (700) and the edge enabler client (100); verifying, by the server (500), the user consent based on the OTP; updating, by the server (500), the at least one parameter of the user consent stored at the server (500); and sending, by the server (500), a user consent response to the application client (200) through the edge application server (700).

[41] Also, the method for providing a service to an edge application (600) includes following steps of: receiving, by a server (500), at least one of a request for accessing the service associated with a User Equipment (UE) (300) from the edge application (600), and a request for a user consent associated with the UE (300) from the edge application (600); retrieving, by the server (500), the user consent from the edge enabler client (100), wherein the user consent indicates a consent of a user of the edge enabler client (100) to provide at least one of the service and the user consent with the edge application (600); and sending, by the server (500), at least one of the service associated with the UE (300) and the user consent to the edge application (600).

[42] In an embodiment, wherein the user consent sent to the edge application (600) is an authorization response.

[43] In an embodiment, wherein retrieving, by the server (500), the user consent from the edge enabler client (100), comprising: determining, by the server (500), an availability of the user consent for accessing the requested service associated with the UE (300) by the edge application (600); and performing, by the server (500), one of: authorizing an access of the service to the edge application (600) when the user consent is available at the server (500), and sending a user consent request to the UE (300) when the user consent is not available at the server (500), and storing the user consent in response to receiving a user consent response comprising the user consent from the UE (300).

[44] In an embodiment, wherein retrieving, by the server (500), the user consent from the edge enabler client (100), comprising: receiving, by the server (500), the request for the user consent associated with the UE (300) from an application client (200) through an edge application server (700); generating, by the server (500), a One Time Password (OTP) for the user consent; sending, by the server (500), the OTP to the UE (300); receiving, by the server (500), a user consent grant notification comprising the user consent and the OTP from one of the application client (200) through the edge application server (700) and the edge enabler client (100); verifying, by the server (500), the user consent based on the OTP; storing, by the server (500), the user consent; and sending, by the server (500), a user consent response to the application client (200)

through the edge application server (700).

[45] Also, the method for providing a service to an edge application (600) includes following steps of: receiving, by an edge enabler server (500a), a user consent grant notification from an application client (200), wherein the user consent grant notification comprises a user consent to provide the service associated with a User Equipment (UE) (300) with the edge application (600); and storing, by the edge enabler server (500a), the user consent for providing at least one of the service and the user consent to the edge application (600);

[46] In an embodiment, wherein receiving, by the edge enabler server (500a), the user consent grant notification from the application client (200), comprising: receiving, by the application client (200), the user consent from a user; sending, by the application client (200), a request for a nonce to the edge enabler client (100); receiving, by the application client (200), the nonce from the edge enabler client (100); sending, by the application client (200), the user consent grant notification to the edge enabler server (500a) through the edge application (600), wherein the user consent grant notification includes the user consent and the nonce; and verifying, by the edge enabler server (500a), the user consent with the edge enabler client (100) based on the nonce.

[47] In an embodiment, the method further comprising: receiving, by the edge enabler server (500a), a user consent update request from the application client (200), wherein the user consent update request comprises information about at least one parameter of the user consent to be updated; updating, by the edge enabler server (500a), the at least one parameter of the user consent stored at the edge enabler server (500a); and sending, by the edge enabler server (500a), a user consent update response to the application client (200).

[48] Also, the method for providing a service to an edge application (600) includes following steps of: receiving, by an application client (200), an application specific user information for providing the service associated with a User Equipment (UE) (300) to the edge application (600); sending, by the application client (200), the application specific user information to the edge application (600) and the edge enabler client (100); receiving, by the edge enabler client (100), a user consent to provide the service associated with the UE (300) to the edge application (600), in response to receiving the application specific user information; sending, by the edge enabler client (100), the application specific user information with the user consent to the edge enabler server (500a); storing, by the edge enabler server (500a), the application specific user information and the user consent; receiving, by the edge enabler server (500a), a request for the service comprising the application specific user information from the edge application (600); verifying, by the edge enabler server (500a), the user consent based on the application specific user information; and sending, by the edge

enabler server (500a), the service associated with the UE (300) to the edge application (600).

[49] Also, the method for providing a service to an edge application (600) includes following steps of: sending, by the edge application (600), an authorization request to a Common Application Program Interface Framework (CAPIF) core function device (500b) for receiving the service associated with a User Equipment (UE) (300); sending, by the edge application (600), a request for the service associated with the UE (300) to an edge enabler server (500a), in response to successfully authorized by the CAPIF core function device (500b); sending, by the edge enabler server (500a), a request for credentials to the CAPIF core function device (500b); sending, by the CAPIF core function device (500b), a user consent request to the edge enabler client (100) for receiving a user consent to provide the service to the edge application (600); receiving, by the CAPIF core function device (500b), the user consent from the edge enabler client (100); sending, by the CAPIF core function device (500b), credentials to the edge enabler server (500a) based on the user consent; and sending, by the edge enabler server (500a), the service to the edge application (600).

[50] Also, the method for providing a service to an edge application (600) includes following steps of: receiving, by a User Equipment (UE) (300) a user consent to provide the service associated with the UE (300) to the edge application (600); sending, by the UE (300), a user consent grant notification to a core network (400), wherein the user consent grant notification comprises the user consent to provide the service with the edge application (600); storing, by the core network (400), the user consent in response to receiving the user consent grant notification from the UE (300); notifying, by the core network (400), an availability of the user consent to an edge enabler server (500a); receiving, by the edge enabler server (500a), a request for the service from an edge application server (700); retrieving, by the edge enabler server (500a), the user consent from the core network (400); storing, by the edge enabler server (500a); the user consent; and sending, by the edge enabler server (500a); a response for the service associated with the UE (300) to the edge application server (700) based on the user consent.

[51] Also, the method for providing a service to an edge application (600) includes following steps of: receiving, by an edge enabler server (500a), a request for the service associated with a User Equipment (UE) (300) from an edge application server (700); sending, by the edge enabler server (500a), a user consent request to a core network (400) wherein the user consent request indicates a request for the user consent; sending, by the core network (400), the user consent request to the UE (300); receiving, by the UE (300), the user consent to provide the service with the edge application (600); sending, by the UE (300), a user consent response to the core network

(400), wherein the user consent response comprises the user consent to provide the service with the edge application (600); storing, by the core network (400), the user consent in response to receiving the user consent response from the UE (300); sending, by the core network (400), the user consent response to the edge enabler server (500a); storing, by the edge enabler server (500a); the user consent in response to receiving the user consent response from the core network (400); and sending, by the edge enabler server (500a) a response for the service associated with the UE (300) to the edge application server (700) based on the user consent.

[52] Also, the system (1000) for providing a service to an edge application (600) in a network, comprising: an edge enabler client (100); an application client (200); a User Equipment (UE) (300); a server (500); the edge application (600); and an edge application server (700), wherein the server (500) is configured to: receive a request for accessing at least one service associated with a UE (300) from the edge application (600); determine availability of a user consent for accessing the at least one service requested by the edge application (600); and authorize access of the at least one service to the edge application (600) when the user consent is available.

[53] Also, the system (1000) for providing a service to an edge application (600), comprising: an edge enabler client (100); an application client (200); a User Equipment UE (300); a server (500); the edge application (600); and an edge application server (700), wherein the server (500) is configured to: receive at least one of a request for accessing the service associated with the UE (300) from the edge application (600), and a request for a user consent associated with the UE (300) from the edge application (600), retrieve the user consent from the edge enabler client (100), wherein the user consent indicates a consent of a user of the edge enabler client (100) to provide at least one of the service and the user consent with the edge application (600), and send at least one of the service associated with the UE (300) and the user consent to the edge application (600).

[54] Also, the system (1000) for providing a service to an edge application (600), comprising: an edge enabler client (100); an application client (200); a User Equipment (UE) (300); an edge enabler server (500a); and

[55] the edge application (600), wherein the edge enabler server (500a) is configured to: receive a user consent grant notification from the application client (200), wherein the user consent grant notification comprises a user consent to provide the service associated with the UE (300) with the edge application (600), store the user consent for providing at least one of the service and the user consent to the edge application (600).

[56] Also, the system (1000) for providing a service to an edge application (600), comprising: an edge enabler client (100); an application client (200); a User Equipment (UE) (300); an edge enabler server (500a); and the edge application (600), wherein the

application client (200) is configured to: receive an application specific user information for providing the service associated with the UE (300) to the edge application (600), and send the application specific user information to the edge application (600) and the edge enabler client (100), wherein the edge enabler client (100) is configured to: receive a user consent to provide the service associated with the UE (300) to the edge application (600), in response to receiving the application specific user information from the application client (200), and send the application specific user information and the user consent to the edge enabler server (500a), wherein the edge enabler server (500a) is configured to: store the application specific user information and the user consent, receive a request for the service comprising the application specific user information from the edge application (600), verify the user consent based on the application specific user information, and send the service associated with the UE (300) to the edge application (600).

[57] Also, the system (1000) for providing a service to an edge application (600), comprising: an edge enabler client (100); a User Equipment (UE) (300); an edge enabler server (500a); a Common Application Program Interface Framework (CAPIF) core function device (500b); and the edge application (600), wherein the edge application (600) is configured to: send an authorization request to the CAPIF core function device (500b) for receiving the service associated with the UE (300), and send a request for the service associated with the UE (300) to the edge enabler server (500a) in response to successfully authorized by the CAPIF core function device (500b), wherein the edge enabler server (500a) is configured to: send a request for credentials to the CAPIF core function device (500b) in response to receiving the request for the service from the edge application (600), and send the service to the edge application (600) in response to receiving the credentials from the CAPIF core function device (500b), wherein the CAPIF core function device (500b) configured to: send a user consent request to the edge enabler client (100) for receiving a user consent to provide the service to the edge application (600) in response to receiving the request for the credentials from the edge enabler server (500a), receive the user consent from the edge enabler client (100), and send the credentials to the edge enabler server (500a) based on the user consent.

[58] Also, the system (1000) for providing a service to an edge application (600), comprising: a User Equipment (UE) (300); a core network (400); an edge enabler server (500a); the edge application (600); and an edge application server (700), wherein the UE (300) is configured to: receive a user consent to provide the service associated with the UE (300) to the edge application (600), and send a user consent grant notification to the core network (400), wherein the user consent grant notification comprises the user consent to provide the service with the edge application (600),

wherein the core network (400) is configured to: store the user consent in response to receiving the user consent grant notification from the UE (300), and notify an availability of the user consent to the edge enabler server (500a), wherein the edge enabler server (500a) is configured to: receive a request for the service from the edge application server (700), retrieve the user consent from the core network (400), store the user consent, and send a response for the service associated with the UE (300) to the edge application server (700) based on the user consent.

[59] Also, the system (1000) for providing a service to an edge application (600), comprising: a User Equipment (UE) (300); a core network (400); an edge enabler server (500a); the edge application (600); and an edge application server (700), wherein the edge enabler server (500a) is configured to: receive a request for the service associated with the UE (300) from the edge application server (700), send a user consent request to the core network (400) wherein the user consent request indicates a request for the user consent, store the user consent in response to receiving the user consent response from the core network (400), and send a response for the service associated with the UE (300) to the edge application server (700) based on the user consent, wherein the core network (400) is configured to: send the user consent request to the UE (300) in response to receiving the user consent request from the edge enabler server (500a), store the user consent in response to receiving the user consent response from the UE (300), and send the user consent response to the edge enabler server (500a), wherein the UE (300) is configured to: receive the user consent to provide the service with the edge application (600) in response to receiving the user consent request from the core network (400), and send a user consent response to the core network (400), wherein the user consent response comprises the user consent to provide the service with the edge application (600).

[60] These and other aspects of the embodiments herein will be better appreciated and understood when considered in conjunction with the following description and the accompanying drawings. It should be understood, however, that the following descriptions, while indicating preferred embodiments and numerous specific details thereof, are given by way of illustration and not of limitation. Many changes and modifications may be made within the scope of the embodiments herein without departing from the spirit thereof, and the embodiments herein include all such modifications.

Mode for the Invention

[61] The embodiments herein and the various features and advantageous details thereof are explained more fully with reference to the non-limiting embodiments that are illustrated in the accompanying drawings and detailed in the following description. Descriptions of well-known components and processing techniques are omitted so as to

not unnecessarily obscure the embodiments herein. Also, the various embodiments described herein are not necessarily mutually exclusive, as some embodiments can be combined with one or more other embodiments to form new embodiments. The term "or" as used herein, refers to a non-exclusive or, unless otherwise indicated. The examples used herein are intended merely to facilitate an understanding of ways in which the embodiments herein can be practiced and to further enable those skilled in the art to practice the embodiments herein. Accordingly, the examples should not be construed as limiting the scope of the embodiments herein.

[62] As is traditional in the field, embodiments may be described and illustrated in terms of blocks which carry out a described function or functions. These blocks, which may be referred to herein as managers, units, modules, hardware components or the like, are physically implemented by analog and/or digital circuits such as logic gates, integrated circuits, microprocessors, microcontrollers, memory circuits, passive electronic components, active electronic components, optical components, hardwired circuits and the like, and may optionally be driven by firmware and software. The circuits may, for example, be embodied in one or more semiconductor chips, or on substrate supports such as printed circuit boards and the like. The circuits constituting a block may be implemented by dedicated hardware, or by a processor (e.g., one or more programmed microprocessors and associated circuitry), or by a combination of dedicated hardware to perform some functions of the block and a processor to perform other functions of the block. Each block of the embodiments may be physically separated into two or more interacting and discrete blocks without departing from the scope of the disclosure. Likewise, the blocks of the embodiments may be physically combined into more complex blocks without departing from the scope of the disclosure.

[63] Prior to describing the embodiments in detail, the following definitions are described for better understanding of the embodiments of the present disclosure.

[64] An edge computing system includes edge data network connected to a User Equipment (UE) as per the 3rd Generation Partnership Project (3GPP) specifications. An edge enabler server of the edge data network caters to the edge applications running at an edge data network and edge enabler clients running at the UE. The edge enabler server is configured to provide a network service (e.g. location service), user specific information (e.g. name, age, contact number, etc. of a user) and device specific information (e.g. UE identifier) to the edge applications by exposing corresponding 3GPP network service Application Program Interfaces (APIs) of the network service to the edge applications. Capabilities of the edge systems allow the edge applications to request the edge enabler server for invoking the network service. In response to receiving the request, the edge enabler server invokes a relevant service APIs and shares invocation results such as a location information of the UE back to the edge ap-

plications.

[65] However, the edge enabler server does not obtain consent of the user to provide the network service and the information to the edge applications. Therefore, private and sensitive information of the user reaches to even an untrusted edge application in the edge data network without knowing by the user, which is a potential threat for a data security and privacy of the user. Hence, an approval of the user is desired for providing the network service, particular device specific information and a user specific information to the edge applications. Further, the approval of the user is also desired to modify and update whenever necessary to revoke privileges of the edge applications. Thus, it is desired to address the above-mentioned shortcomings or at least provide a useful alternative.

[66] Accordingly, the embodiments herein provide a method for providing a service to an edge application. The method includes receiving, by a server, at least one of a request for accessing the service associated with a UE from the edge application, and a request for a user consent associated with the UE from the edge application. Further, the method includes retrieving, by the server, the user consent from the edge enabler client, where the user consent indicates a consent of a user of the edge enabler client to provide at least one of the service and the user consent with the edge application. Further, the method includes providing, by the server, at least one of the service associated with the UE and the user consent to the edge application.

[67] Unlike existing methods and systems, the proposed system is configured to request the user to grant the consent for providing the service such as a geolocation service, a device specific information (e.g. UE ID), user specific information (e.g. a contact number of the user) etc. to the edge application. Therefore, private and sensitive information of the user and the UE are not exposing to the edge application without a permission of the user. Alternatively, the proposed system allows the user to voluntarily provide the consent for providing the service to the edge application. Additionally, the proposed system allows the user to update the consent and set limits for restricting privileges of the edge application to access the service. Thus, the proposed system enhances a user experience, data security and a privacy of the user.

[68] Referring now to the drawings, and more particularly to FIGS. 1 through 20, there are shown preferred embodiments.

[69] FIG. 1 is a block diagram of a system 1000 for providing a service to an edge application 600 of an edge data network, according to an embodiment as disclosed herein. Examples for the service includes at least one of a location information of the UE 300, a device specific information (e.g. a UE identifier), a service identifier, user information (i.e. a user specific information), authorization credentials, etc. Example for the user information is a user profile ID in an application, personal details of the

user, etc. In an embodiment, the system 1000 includes an edge enabler client 100, an application client 200, a UE 300, a core network 400, a server 500, the edge application 600 and an edge application server 700. In an embodiment, the server 500 is an edge enabler server 500a (shown in FIG. 2E) or a CAPIF core function device 500b (shown in FIG. 2F). In an embodiment, the edge enabler client 100 and the application client 200 are components of the UE 300. In an embodiment, the edge application 600 is operating in a device.

[70] The server 500 is configured to receive a request for the service associated with the UE 300 from the edge application 600 or a request for obtaining a user consent associated with the UE 300 from the edge application 600. In an embodiment, the service associated with the UE is a service associated with a user. In an embodiment, the request for the service associated with the UE 300 is a request for accessing the service associated with the UE 300. In an embodiment, the request for obtaining the user consent includes the service requested by the edge application 600 and information about the edge application 600, such as an application ID. In an embodiment, the request for obtaining the user consent includes details of the services needed for the edge application 600. In an embodiment, the request for obtaining the user consent is clubbed with a registration request of the edge application 600 to register on the edge enabler server 500a. In an embodiment, the request for the service includes the application specific user information and the service that required for the edge enabler server 500a. In an embodiment, the user consent indicates a consent of the user of the edge enabler client 100 to share at least the service or the user consent with the edge application 600.

[71] In response to receiving the request for the service or the request for the user consent, the server 500 is configured to check whether the user consent is available at the server 500. When the user consent is available at the server 500, the server 500 is configured to provide at least the service associated with the UE 300 or the user consent to the edge application 600. In an embodiment, the server 500 is configured to send the service to the edge application 600 for providing the service to the edge application 600. In an embodiment, the server 500 is configured to send the user consent to the edge application 600 for providing the user consent to the edge application 600. In an embodiment, when the user consent is available at the server 500, the server 500 is configured to perform authorization to send an authorization response as the user consent to the edge application 600.

[72] When the user consent is not available at the server 500, the server 500 is configured to retrieve the user consent from the edge enabler client 100. In an embodiment, the server 500 is configured to send a user consent request to the edge enabler client 100 of the UE (300) for retrieving the user consent, where the user consent request indicates

the request for the user consent. In an embodiment, the user consent request includes the information about the edge application 600 such as the application ID, and the service for which the user consent is requested by the edge application 600. Further, the server 500 is configured to receive a user consent response includes the user consent from the edge enabler client 100 by authorizing the access of the service. In an embodiment, the edge enabler client 100 is configured to request the user to provide the consent for providing the service to the edge application 600, in response to receiving the user consent request.

[73] The edge enabler client 100 is configured to share the user consent to the server 500, in response to receiving the consent from the user for providing the service to the edge application 600. In an embodiment, the edge enabler client 100 is configured to authorize the user using the any of, but not limited to biometrics, passwords, Personal Identification Number (PIN), pattern lock, etc. for accepting a grant/update of the user consent. In an embodiment, the user provides the consent to the edge application 600 to avail the service to the edge application 600 for once or always or a limited number of times or a time-bound or a location (such as geo-location) bound. The server 500 is configured to store the user consent, in response to receiving the user consent from the UE 300. Further, the server 500 is configured to provide at least the service associated with the UE 300 or the user consent to the edge application 600. In an embodiment, the user consent sent to the edge application 600 is an authorization response.

[74] In another embodiment, the server 500 is configured to determine availability of the user consent for accessing the service requested by the edge application 600, in response to receiving the request for the serv ice or the user consent from the edge application 600. The server 500 is configured to authorize access of the service to the edge application 600 when the user consent is available. The server 500 is configured to authorize access of the service to the edge application 600 when the user consent is available. The server 500 is configured to send the user consent request to the UE 300 when the user consent for accessing the at least one service is not available at the server 500. The server 500 is configured to receive a user consent response including the user consent from the UE 300 for authorizing the access of the at least one service. The server 500 is configured to store the user consent, in response to receiving the user consent.

[75] In an embodiment, the server 500 is configured to receive a user consent update request from the edge enabler client 100 after storing the user consent. The user voluntarily provides an updated user consent to the edge enabler client 100 for sending the user consent update request to the server 500. The user consent update request includes information about at least one parameter of the user consent to be updated. Examples for the parameter of the user consent are the number of times the user consent is

allowed to use, a time-bound or a location (such as geo-location) bound, etc. Further, the server 500 is configured update the at least one parameter of the user consent stored at the server 500. The server 500 is configured send a user consent update response to the edge enabler client 100, in response to updating the at least one parameter of the user consent.

[76] In another embodiment, the server 500 is configured to receive the request for the user consent associated with the UE 300 from the application client 200 through the edge application server 700. Further, the server 500 is configured to generate an OTP for the user consent. Further, the server 500 is configured to send the OTP to the UE 300. In an embodiment, the server 500 choose a channel of sharing the OTP to the UE 300 based on user contact information such as a mobile number, email address, etc. available at the server 500. In an embodiment, the application client 200 configured to request the user to input the OTP in the consent. The server 500 is configured to receive a user consent grant notification includes the user consent and the OTP from the application client 200 through the edge application server 700 or the edge enabler client 100 for retrieving the user consent from the edge enabler client 100. Further, the server 500 is configured to verify the user consent based on the OTP. Further, the server 500 is configured to store the user consent. Further, the server 500 is configured to send a user consent response to the application client 200 through the edge application server 700.

[77] In an embodiment, the server 500 is configured to receive the user consent update request from the application client 200 through the edge application server 700 after storing the user consent. The user consent update request includes information about at least one parameter of the user consent to be updated. Further, the server 500 is configured to generate an OTP for the user consent. Further, the server 500 is configured to send the OTP to the UE 300. Further, the server 500 is configured to receive a user consent update notification includes the user consent and the OTP from one of the application client 200 through the edge application server 700 and the edge enabler client 100. Further, the server 500 is configured to verify the user consent based on the OTP. Further, the server 500 is configured to update the at least one parameter of the user consent stored at the server 500. Further, the server 500 is configured to send the user consent update response to the application client 200 through the edge application server 700.

[78] In another embodiment, the edge enabler server 500a is configured to receive the user consent grant notification from the application client 200. In an embodiment, the user consent grant notification includes the user consent to provide the service associated with the UE 300 with the edge application 600. The edge enabler server 500a is configured to store the user consent for a future usage purpose. The edge enabler

server 500a is configured to use the user consent for providing at least one of the service and the user consent to the edge application 600 whenever the edge enabler server 500a receives the request for the service or the user consent from the edge application 600.

[79] In an embodiment, the edge enabler server 500a is configured to receive the user consent update request from the application client 200 after storing the user consent. The user voluntarily provides the updated user consent to the application client 200 for sending the user consent update request to the edge enabler server 500a. Further, the edge enabler server 500a is configured to update the at least one parameter of the user consent stored at the edge enabler server 500a. Further, the edge enabler server 500a is configured to send the user consent update response to the application client 200.

[80] In another embodiment, the application client 200 is configured to receive the user consent from the user, where the user voluntarily provides the user consent to the application client 200. Further, the application client 200 is configured to send a request for a nonce to the edge enabler client 100. In an embodiment, the request for the nonce can be the request for a voucher or a request for a token. Further, the edge enabler client 100 is configured to send the nonce/voucher/token to the application client 200. The application client 200 is configured to send the user consent grant notification to the edge enabler server 500a through the edge application 600 in response to receiving the nonce/voucher/token from the edge enabler client 100. In an embodiment, the user consent grant notification includes the user consent and the nonce/voucher/token. Further, the edge enabler server 500a is configured to verify the user consent with the edge enabler client 100 based on the nonce. Further, the edge enabler server 500a is configured to store the user consent for the future usage purpose. The edge enabler server 500a is configured to use the user consent for providing at least one of the service and the user consent to the edge application 600 whenever the edge enabler server 500a receives the request for the service or the user consent from the edge application 600.

[81] In another embodiment, the application client 200 is configured to receive an application specific user information for providing the service to the edge application 600. Further, the application client 200 is configured to send the application specific user information to the edge application 600 and the edge enabler client 100. Further, the edge enabler client 100 is configured to receive the user consent to provide the service associated with the UE 300 to the edge application 600, in response to receiving the application specific user information from the application client 200. Further, the edge enabler client 100 is configured to send the application specific user information and the user consent to the edge enabler server 500a. Further, the edge enabler server 500a is configured to store the application specific user information and

the user consent. Further, the edge enabler server 500a is configured to receive the request for the service including the application specific user information from the edge application 600. Further, the edge enabler server 500a is configured to verify the user consent based on the application specific user information. Further, the edge enabler server 500a is configured to provide the service associated with the UE 300 to the edge application 600.

[82] The CAPIF core function device 500b operates as an authority to generate authorization for the edge application 600. In an embodiment, the edge application 600 operates as an API invoker and the edge enabler server 500a operates as an API exposing function. In an embodiment, when the edge application 600 has direct access to the network services, then network entities providing the service operates as the API exposing function. In an embodiment, the CAPIF core function device 500b is directly interfaced with the edge enabler client 100 to obtain the user consent or via the edge enabler server 500a.

[83] In another embodiment, the edge application 600 is configured to send a request for performing authorization to the CAPIF core function device 500b for receiving the service associated with the UE 300. Further, the CAPIF core function device 500b is configured to perform authorization and generate a Pre-shared Key (PSK). Further, the CAPIF core function device 500b is configured to send the PSK to the edge application 600. The edge application 600 is configured to send the request for the service associated with the UE 300 to the edge enabler server 500a in response to successfully authorized by the CAPIF core function device 500b. Further, the edge enabler server 500a is configured to send a request for the credentials to the CAPIF core function device 500b in response to receiving the request for the service from the edge application 600. Further, the CAPIF core function device 500b is configured to send the user consent request to the edge enabler client 100 for receiving the user consent to provide the service. Further, the edge enabler client 100 is configured to obtain the user consent. Further, the edge enabler client 100 is configured to send the user consent to the CAPIF core function device 500b. The CAPIF core function device 500b is configured to send the credentials to the edge enabler server 500a based on the user consent, in response to receiving the user consent. The edge enabler server 500a is configured to provide the service to the edge application 600 in response to receiving the credentials from the CAPIF core function device 500b.

[84] In another embodiment, the UE 300 is configured to receive the user consent voluntarily from the user to provide the service associated with the UE 300 to the edge application 600. The UE 300 is configured to send the user consent grant notification to the core network 400. Further, the core network 400 is configured to store the user consent in response to receiving the user consent grant notification from the UE 300.

Further, the core network 400 is configured to notify an availability of the user consent to the edge enabler server 500a. Further, the edge enabler server 500a is configured to receive the request for the service from the edge application server 700. The edge enabler server 500a is configured to retrieve the user consent from the core network 400, in response to receiving the request for the service. Further, the edge enabler server 500a is configured to store the user consent. Further, the edge enabler server 500a is configured to send the response for the service associated with the UE 300 to the edge application server 700 based on the user consent.

[85] In another embodiment, the edge enabler server 500a is configured to receive the request for the service associated with the UE 300 from the edge application server 700. Further, the edge enabler server 500a is configured to send the user consent request to the core network 400 where the user consent request indicates the request for the user consent. Further, the core network 400 is configured to. send the user consent request to the UE 300 in response to receiving the user consent request from the edge enabler server 500a. Further, the UE 300 is configured to receive the user consent from the user to provide the service with the edge application 600, in response to receiving the user consent request from the core network 400. The UE 300 is configured to send a user consent response to the core network 400, where the user consent response includes the user consent to provide the service with the edge application 600. The core network 400 is configured to store the user consent in response to receiving the user consent response from the UE 300. Further, the core network 400 is configured to send the user consent response to the edge enabler server 500a. The edge enabler server 500a is configured to store the user consent in response to receiving the user consent response from the core network 400. Further, the edge enabler server 500a is configured to send the response for the service associated with the UE 300 to the edge application server 700 based on the user consent.

[86] In an embodiment, the edge enabler client 100, or an entity in the system 1000 requests for consolidated user consents for similar services to the user for optimize a number of consents taken from the user. For example, while taking the user consent for an on-device or device generated user location, the entity clubs the user consent for the location service of the edge.

[87] Although figure in the FIG.1 shows the components in the system 1000 but it is to be understood that other embodiments are not limited thereon. In other embodiments, the system 1000 may include less or more number of components. Further, the labels or names of the components are used only for illustrative purpose and does not limit the scope of the invention. One or more components can be combined together to perform same or substantially similar function for providing the service to the edge application 600.

[88] FIG. 2A-2H illustrates a block diagram of devices in the system 1000 for providing the service to the edge application 600, according to an embodiment as disclosed herein.

[89] The block diagram of the edge enabler client 100 is shown in the FIG. 2A. In an embodiment, the edge enabler client 100 includes a user consent controller 101, a nonce generator 102, a memory 103, a processor 104, and a communicator 105, where the processor 104 is coupled to the memory 103. The user consent controller 101 requests the user to provide the consent for providing the service to the edge application 600, in response to receiving the user consent request. The user consent controller 101 authorizes the user using the any of, but not limited to biometrics, passwords, PIN, pattern lock, etc. for accepting a grant/update of the user consent. The user consent controller 101 receives the user consent to provide the service associated with the UE 300 to the edge application 600, in response to receiving the application specific user information from the application client 200. The user consent controller 101 sends the application specific user information and the user consent to the edge enabler server 500a. In an embodiment, the user consent controller 101 obtains the user consent and sends the user consent to the CAPIF core function device 500b.The nonce generator 102 sends the nonce/voucher/token to the application client 200.

[90] The processor 104 is configured to execute instructions stored in the memory 103. The memory 103 may include non-volatile storage elements. Examples of such non-volatile storage elements may include magnetic hard discs, optical discs, floppy discs, flash memories, or forms of an Electrically Programmable Memory (EPROM) or an Electrically Erasable and Programmable Memory (EEPROM). In addition, the memory 103 may, in some examples, be considered a non-transitory storage medium. The term "non-transitory" may indicate that the storage medium is not embodied in a carrier wave or a propagated signal. However, the term "non-transitory" should not be interpreted that the memory 103 is non-movable. In some examples, the memory 103 can be configured to store larger amounts of information than the memory 103. In certain examples, a non-transitory storage medium may store data that can, over time, change (e.g., in Random Access Memory (RAM) or cache). The communicator 105 is configured to communicate internally between hardware components in the edge enabler client 100. Further, the communicator 105 is configured to facilitate the communication between the edge enabler client 100 and other devices in the system 1000.

[91] The block diagram of the application client 200, is shown in the FIG. 2B. In an embodiment, the application client 200 includes a user consent controller 201, a service engine 202, a memory 203, a processor 204, and a communicator 205, where the processor 204 is coupled to the memory 203. The user consent controller 201 receives the user consent from the user, where the user voluntarily provides the user consent to

the application client 200. The user consent controller 201 sends the request for the nonce to the edge enabler client 100. The user consent controller 201 sends the user consent grant notification to the edge enabler server 500a through the edge application 600 in response to receiving the nonce/voucher/token from the edge enabler client 100. The service engine 202 receives the application specific user information for providing the service to the edge application 600. The service engine 202 sends the application specific user information to the edge application 600 and the edge enabler client 100. The user consent controller 201 requests the user to input the OTP in the consent. The memory 203, the processor 204, and the communicator 205 operates similar as the memory 103, the processor 104, and the communicator 105 respectively for reliable functioning of the application client 200.

[92] The block diagram of the UE 300, is shown in the FIG. 2C. In an embodiment, the UE 300 includes the Edge Enabler Client (EEC) 100, the Application Client (AC) 200, a Non-Access Stratum layer (NAS) 301, a memory 302, a processor 303, and a communicator 304, where the processor 303 is coupled to the memory 302. The edge enabler client 100 or the NAS 301 obtains the user consent voluntarily from the user to provide the service associated with the UE 300 to the edge application 600. The NAS 303 sends the user consent grant notification to the core network 400. The NAS 303 obtains the user consent from the user to provide the service with the edge application 600, in response to receiving the user consent request from the core network 400. The memory 302, the processor 303, and the communicator 304 operates similar as the memory 103, the processor 104, and the communicator 105 respectively for reliable functioning of the UE 300.

[93] In an embodiment, the NAS 303 updates the use consent to the core network 400 (e.g. 5G core network) based on the request from the edge application server 700 or the application client 200. Therefore, the edge enabler server 500a obtains the user consent in an authorized way. In an embodiment, the edge application server 700 triggers the application client 200 to initiate steps for obtaining the user consent. Therefore, an updated user consent is fetched from the edge enabler server 500a.

[94] The block diagram of the core network 400, is shown in the FIG. 2D. In an embodiment, the core network 400 includes an AMF 401, a PCF 402, a UDM/UDR 403, a memory 404, a processor 405, and a communicator 406, where the processor 405 is coupled to the memory 404. The AMF 401 receives the user consent form the UE 300. The PCF 402 or the UDM/UDR 403 notifies the availability of the user consent to the edge enabler server 500a, in response to storing the user consent to the memory 404. The PCF 402 or the UDM/UDR sends the user consent request to the UE 300 in response to receiving the user consent request from the edge enabler server 500a. The PCF 402 or the UDM/UDR sends the user consent response to the edge enabler server

500a, in response to storing the user consent to the memory 404. In an embodiment, the memory 404 stores the user consent, in response to receiving the user consent at the PCF 402 or the UDM/UDR 403. The memory 404 the processor 405, and the communicator 406 operates similar as the memory 103, the processor 104, and the communicator 105 respectively for reliable functioning of the core network 400.

[95] The block diagram of the edge enabler server 500a, is shown in the FIG. 2E. In an embodiment, the edge enabler server 500a includes a user consent controller 501a, a service engine 502a, a memory 503a, a processor 504a, and a communicator 505a, where the processor 504a is coupled to the memory 503a.

[96] The user consent controller 501a receives the request for obtaining a user consent associated with the UE 300 from the edge application 600. In response to receiving the request for the service or the request for the user consent, the user consent controller 501a is checks whether the user consent is available at the edge enabler server 500a. When the user consent is available at the edge enabler server 500a, the user consent controller 501a sends the user consent to the edge application 600. When the user consent is not available at the edge enabler server 500a, the user consent controller 501a retrieves the user consent from the edge enabler client 100. In an embodiment, the user consent controller 501a sends the user consent request to the edge enabler client 100 for retrieving the user consent.

[97] The user consent controller 501a receives a user consent response includes the user consent from the edge enabler client 100. The user consent controller 501a sends the user consent to the edge application 600, in response to receiving or storing the user consent at the edge enabler server 500a. The user consent controller 501a receives a user consent update request from the edge enabler client 100 after storing the user consent. The user consent controller 501a updates the at least one parameter of the user consent stored at the server 500, in response to receiving an updated user consent. The user consent controller 501a sends the user consent update response to the edge enabler client 100, in response to updating the at least one parameter of the user consent.

[98] In an embodiment, the user consent controller 501a receives the request for the user consent associated with the UE 300 from the application client 200 through the edge application server 700. Further, the user consent controller 501a generates the OTP for the user consent. Further, the user consent controller 501a sends the OTP to the UE 300. In an embodiment, the user consent controller 501a chooses the channel of sharing the OTP to the UE 300 based on the user contact information such as the mobile number, the email address, etc. available at the edge enabler server 500a. The user consent controller 501a receives the user consent grant notification includes the user consent and the OTP from the application client 200 through the edge application server 700 or the edge enabler client 100 for retrieving the user consent from the edge

enabler client 100. The user consent controller 501a verifies the user consent based on the OTP. The user consent controller 501a sends the user consent response to the application client 200 through the edge application server 700.

[99] In an embodiment, the user consent controller 501a receives the user consent update request from the application client 200 through the edge application server 700 after storing the user consent. Further, the user consent controller 501a generates the OTP for the user consent. Further, the user consent controller 501a sends the OTP to the UE 300. Further, the user consent controller 501a receives the user consent update notification includes the user consent and the OTP from one of the application client 200 through the edge application server 700 and the edge enabler client 100. Further, the user consent controller 501a verifies the user consent based on the OTP. Further, the user consent controller 501a updates the at least one parameter of the user consent stored at the server 500. Further, the user consent controller 501a sends the user consent update response to the application client 200 through the edge application server 700.

[100] In another embodiment, the user consent controller 501a receives the user consent grant notification from the application client 200. The user consent controller 501a stores the user consent in the memory 503a for a future usage purpose, when the edge enabler server 500a receives the user consent for first time.

[101] In an embodiment, the user consent controller 501a receives the user consent update request from the application client 200 after storing the user consent. Further, the user consent controller 501a updates the at least one parameter of the user consent stored at the edge enabler server 500a. In an embodiment, the user consent controller 501a updates the former user consent stored at the edge enabler server 500a using the user consent received from the edge enabler client 100, when the edge enabler server 500a contains the former user consent. Further, the user consent controller 501a sends the user consent update response to the application client 200.

[102] In an embodiment, the user consent controller 501a verifies the user consent with the edge enabler client 100 based on the nonce. In an embodiment, the user consent controller 501a stores the application specific user information and the user consent in the memory 503a. The user consent controller 501a verifies the user consent based on the application specific user information.

[103] In an embodiment, the user consent controller 501a sends the request for the credentials to the CAPIF core function device 500b in response to receiving the request for the service from the edge application 600. The user consent controller 501a provides the service to the edge application 600 in response to receiving the credentials from the CAPIF core function device 500b. In an embodiment, the user consent controller 501a retrieves the user consent from the core network 400, in response to

receiving the request for the service. In an embodiment, the user consent controller 501a sends the user consent request to the core network 400 where the user consent request indicates the request for the user consent. In an embodiment, the user consent controller 501a stores the user consent to the memory 503a in response to receiving the user consent response from the core network 400.

[104] The service engine 502a receives the request for the service associated with the UE 300 from the edge application 600. When the user consent is available at the edge enabler server 500a, the service engine 502a provides the service associated with the UE 300 to the edge application 600. The service engine 502a provides the service associated with the UE 300 to the edge application 600, in response to receiving or storing the user consent at the edge enabler server 500a. The service engine 502a receives the request for the service including the application specific user information from the edge application 600. In an embodiment, the service engine 502a receives the request for the service from the edge application server 700. The service engine 502a sends the response for the service associated with the UE 300 to the edge application server 700 based on the user consent.

[105] The memory 503a, the processor 504a, and the communicator 505a operates similar as the memory 103, the processor 104, and the communicator 105 respectively for reliable functioning of the edge enabler server 500a.

[106] The block diagram of the CAPIF core function device 500b, is shown in the FIG.F. In an embodiment, the CAPIF core function device 500b includes a user consent controller 501b, an authorization engine 502b, a memory 503b, a processor 504b, and a communicator 505b, where the processor 504b is coupled to the memory 503b. The user consent controller 501b receives the request to perform authorization from the edge application 600. Further, the user consent controller 501b sends the request for the user consent to the edge enabler server 500a or the edge enabler client 100. The memory 503b stores the user consent in response to receiving the user consent from the edge enabler client 100. Further, the authorization engine 502b performs the authorization and the user consent controller 501b sends the authorization response to the edge application 600. In an embodiment, when the user consent is available at the CAPIF core function device 500b and the CAPIF core function device 500b receives the request for the authorization, the authorization engine 502b performs the authorization and the user consent controller 501b sends the authorization response to the edge application 600.

[107] In response to receiving the user consent from the edge enabler server 500a, the authorization engine 502b performs the authorization and the user consent controller 501b sends the authorization response to the edge application 600. In an embodiment, the authorization engine 502b performs the authorization and generate the PSK, in

response to receiving the request to perform the authorization from the edge application 600. Further, the user consent controller 501b sends the PSK to the edge application 600. In an embodiment, the user consent controller 501b sends the user consent request to the edge enabler client 100 for receiving the user consent. The authorization engine 502b sends the credentials to the edge enabler server 500a based on the user consent, in response to receiving the user consent. The memory 503b, the processor 504b, and the communicator 505b operates similar as the memory 103, the processor 104, and the communicator 105 respectively for reliable functioning of the CAPIF core function device 500b.

[108] The block diagram of the edge application 600, is shown in the FIG. 2G. In an embodiment, the edge application 600 includes a user consent controller 601, a service engine 602, a memory 603, a processor 604, and a communicator 605, where the processor 604 is coupled to the memory 603. The user consent controller 601 requests to the edge enabler server 500a for obtaining the user consent. In an embodiment, the user consent controller 601 requests the CAPIF core function device 500b for performing the authorization. In an embodiment, the user consent controller 601 send the authorization request to the CAPIF core function device 500b for performing the authorization or obtaining the authorization credentials. The user consent controller 601 notifies the user consent grant to the Edge enabler server 500a in response to receiving the user consent grant includes the nonce/voucher/token form the application client 200. The service engine 602 requests to the edge enabler server 500a for the service. The memory 603, the processor 604, and the communicator 605 operates similar as the memory 103, the processor 104, and the communicator 105 respectively for reliable functioning of the edge application 600.

[109] The block diagram of the edge application server 700, is shown in the FIG. 2H. In an embodiment, the edge application server 700 includes a user consent controller 701, a service engine 702, a memory 703, a processor 704, and a communicator 705, where the processor 704 is coupled to the memory 703. The user consent controller 701 shares the request for the user consent with the edge enabler server 500a in response to receiving the request for the user consent from the application client 200. The service engine 702 sends the request for the service associated with the UE 300 to the edge enabler server 500a. The memory 703, the processor 704, and the communicator 705 operates similar as the memory 103, the processor 104, and the communicator 105 respectively for reliable functioning of the edge application server 700.

[110] Although each figure in the FIG. 2A-2H shows the hardware components of the devices in the system 1000 but it is to be understood that other embodiments are not limited thereon. In other embodiments, the devices in the system 1000 may include less or more number of components. Further, the labels or names of the components

are used only for illustrative purpose and does not limit the scope of the invention. One or more components can be combined together to perform same or substantially similar function for providing the service to the edge application 600.

[111] FIG. 3 is a sequential diagram illustrating signaling between the devices in the system for providing the service to the edge application 600 in response to receiving the request for the service, according to an embodiment as disclosed herein. At step S301, the edge application 600 sends the request for the service (e.g. a location service) or the UE ID to edge enabler server 500a. At step S302, the edge enabler server 500a checks whether the user consent is stored at the edge enabler server 500a.

[112] At step S303, in response to detecting that the user consent for the service or the UE ID requested by the edge application 600 is not available with the edge enabler server 500a, the edge enabler server 500a sends the request for obtaining the user consent to the edge enabler client 100. The request for obtaining the user consent includes the service requested by the edge application 600 and information about the edge application 600, such as an application ID.

[113] At step S304, the edge enabler client 100 requests to the user to provide the consent of the user for the service requested by the edge application 600. The edge enabler client 100 authorizes the user for accepting the grant/update of the user consent. In an embodiment, the user provides the consent to the edge application 600 to avail the service or the UE ID for once or always or a limited number of times or a time-bound or a location (such as geo-location) bound. At step S305, the edge enabler client 100 responds to the edge enabler server 500a with the user consent, in response to obtaining the consent from the user. At step S306, the edge enabler server 500a stores the received user consent for the future reference. At step S307, the edge enabler server 500a provides the service or the UE ID to the edge application 600 based on the received user consent. The edge enabler server 500a interacts with other devices in the system 1000 to provide the service or the UE ID to the edge application 600.

[114] The various actions, acts, blocks, steps, or the like in the sequential diagram in FIG. 3 may be performed in the order presented, in a different order or simultaneously. Further, in some embodiments, some of the actions, acts, blocks, steps, or the like may be omitted, added, modified, skipped, or the like without departing from the scope of the invention.

[115] FIG. 4 is a sequential diagram illustrating signaling between the devices in the system 1000 for providing the user consent to the edge application 600 in response to receiving the request for the user consent, according to an embodiment as disclosed herein. At step S401, the edge application 600 sends the request to the edge enabler server 500a for obtaining the user consent. The request for obtaining the user consent includes the details of the services needed for the edge application 600. In an em-

bodiment, the request for obtaining the user consent is clubbed with a registration request of the edge application 600 to register on the edge enabler server 500a. At step S402, the edge enabler server 500a sends the request to the edge enabler client 100 to obtain the user consent. The request to obtain the user consent includes the information about the edge application 600 such as the application ID, and the service for which the user consent is requested by the edge application 600.

[116] At step S403, the edge enabler client 100 requests the user to provide the consent for the service requested by the edge application 600. The edge enabler client 100 authorizes the user for accepting the grant/update of the user consent. In an embodiment, the user provides the consent to the edge application 600 to avail the service or the UE ID for once or always or a limited number of times or a time-bound or a location (such as geo-location) bound. At step S404, the edge enabler client 100 responds to the edge enabler server 500a with the user consent obtained from the user. At step S405, the edge enabler server 500a stores the received user consent for the future reference. At step S406, the edge enabler server 500a provides the response to the edge application 600 indicating that the edge enabler server 500a contains the user consent to avail the service or the UE ID.

[117] The various actions, acts, blocks, steps, or the like in the sequential diagram in FIG. 4 may be performed in the order presented, in a different order or simultaneously. Further, in some embodiments, some of the actions, acts, blocks, steps, or the like may be omitted, added, modified, skipped, or the like without departing from the scope of the invention.

[118] FIG. 5 is a sequential diagram illustrating signaling between the devices in the system 1000 for providing the UE ID to the edge application 600 in response to receiving the request for the UE ID, according to an embodiment as disclosed herein. The application client 200 does not provide a list of services to the edge application 600 until the application client 200 receives the user consent to provide the list of services to the edge application 600. In such a scenario, the edge enabler server 500a requests to the edge enabler client 100 to obtain the user consent upon receiving the request for UE ID or the service from the edge application 600 for which the edge application 600 does not have the user consent. At step S501, the edge application 600 send the request to the edge enabler server 500a with the application specific user information and the service that required for the edge enabler server 500a. In an embodiment, the request is for UE ID or for the service itself. At step S502, upon receiving the request, the edge enabler server 500a check for the stored user consents. If the user consent is not available, the edge enabler server 500a sends the user consent request to the edge enabler client 100. The request for the user consent includes the application ID and the service required for the edge application 600.

[119] In an embodiment, the request for the user consent includes the application specific user information. At step S503, the edge enabler client 100 requests to the user for the user consent. The edge enabler client 100 authorizes the user for accepting the grant/ update of the user consent. In an embodiment, the user provides the consent to the edge application 600 to avail the service or the UE ID for once or always or a limited number of times or a time-bound or a location (such as geo-location) bound. At step S504, the edge enabler client 100 shares the user consent with the edge enabler server 500a. At step S505, the edge enabler server 500a stores the user consent for the future reference. At step S506, the edge enabler server 500a responds to the edge application 600 accordingly either with the UE ID or the service which requested by the edge application 600.

[120] The various actions, acts, blocks, steps, or the like in the sequential diagram in FIG. 5 may be performed in the order presented, in a different order or simultaneously. Further, in some embodiments, some of the actions, acts, blocks, steps, or the like may be omitted, added, modified, skipped, or the like without departing from the scope of the invention.

[121] FIG. 6 is a sequential diagram illustrating signaling between the devices in the system 1000 for providing the user consent to the edge application 600 in response to receiving the user consent voluntarily provided by the user, according to an embodiment as disclosed herein. At step S601, the user voluntarily grands or updates the user consent on the UE 300 using the edge enabler client 100 for providing the service to the edge application 600. The edge enabler client 100 authorizes the user for accepting the grant/update of the user consent. In an embodiment, the user provides the consent to the edge application 600 to avail the service or the UE ID for once or always or a limited number of times or a time-bound or a location (such as geo-location) bound.

[122] At step S602, the edge enabler client 100 requests the edge enabler server 500a to grant/update the user consent. At step S603, the edge enabler server 500a sends a user consent grant/update response to the edge enabler client 100, in response to receiving the request for granting or updating the user consent. At step S604, the edge enabler server 500a stores the user consent for the future reference, when the edge enabler server 500a receives the user consent for first time. The edge enabler server 500a updates the former user consent stored at the edge enabler server 500a using the user consent received from the edge enabler client 100, when the edge enabler server 500a contains the former user consent. At step S605, the edge enabler server 500a shares the user consent with the edge application 600 by sending the user consent grant/update notification.

[123] The various actions, acts, blocks, steps, or the like in the sequential diagram in FIG. 6

may be performed in the order presented, in a different order or simultaneously. Further, in some embodiments, some of the actions, acts, blocks, steps, or the like may be omitted, added, modified, skipped, or the like without departing from the scope of the invention.

[124] FIG. 7 is a sequential diagram illustrating signaling between the devices in the system 1000 for storing the user consent at the edge enabler server 500a in response to receiving the user consent voluntarily provided by the user and verifying the user consent, according to an embodiment as disclosed herein. At step S701, the user voluntarily grands the user consent on the UE 300 using the application client 200 for providing the service to the edge application 600. At step S702, the application client 200 requests to the edge enabler client 100 for the voucher/token/nonce. In another embodiment, the edge enabler client 100 requests to a server such as an OAuth authorization server or the CAPIF core function device 500b for the voucher/token/nonce. At step S703, the edge enabler client 100 generates the voucher/token/nonce and send a response including the voucher/token/nonce with the application client 200. At step S704, the application client 200 includes the voucher/token/nonce with the user consent and shares the user consent with the edge application 600 corresponds to the application client 200.

[125] At step S705, the edge application 600 acknowledges the response with the application client 200 upon receiving the user consent. At step S706, the edge application 600 provides the user consent to the edge enabler server 500a as the user consent grant notification. Further, the edge enabler server 500a tries to verify the user consent using the voucher/token/nonce. At step S707, the edge enabler server 500a request to the edge enabler client 100 to verify the user consent, when the edge enabler server 500a is unable to verify the user consent. The edge enabler client 100 verifies the user consent by matching the voucher/token/nonce in the user consent with the voucher/token/nonce generated by the edge enabler client 100. At step S708, the edge enabler client 100 responds to the edge enabler server 500a with the verification response, in response to verifying the user consent. At step S709, the edge enabler server 500a stores the user consent, in response to verifying the user consent or receiving the verification response.

[126] The various actions, acts, blocks, steps, or the like in the sequential diagram in FIG. 7 may be performed in the order presented, in a different order or simultaneously. Further, in some embodiments, some of the actions, acts, blocks, steps, or the like may be omitted, added, modified, skipped, or the like without departing from the scope of the invention.

[127] FIG. 8 is a sequential diagram illustrating signaling between the devices in the system 1000 for storing the user consent at the edge enabler server 500a in response to

receiving the user consent voluntarily provided by the user, according to an embodiment as disclosed herein. At step S801, the user voluntarily grands the user consent on the UE 300 using the application client 200 for providing the service to the edge application 600. At step S802, the application client 200 notifies the edge application 600 with the user consent grant notification includes the user consent. At step S803, the application client 200 notifies the edge application 600 with the user consent grant notification. The edge enabler client 100 being part of a system kernel has a capability to determine whether the user consent received from the application client 200 is legitimate. At step S804, in response to determining that the notification is legitimate, the edge enabler client 100 sends the user consent grant request to the edge enabler server 500a. At step S805, the edge enabler server 500a acknowledges to the edge enabler client 100 by sending the user consent grant response, in response to receiving the user consent. At step S806, the edge enabler server 500a stores the user consent.

[128] The various actions, acts, blocks, steps, or the like in the sequential diagram in FIG. 8 may be performed in the order presented, in a different order or simultaneously. Further, in some embodiments, some of the actions, acts, blocks, steps, or the like may be omitted, added, modified, skipped, or the like without departing from the scope of the invention.

[129] FIG. 9 is a sequential diagram illustrating signaling between the devices in the system 1000 for providing the UE ID to the edge application 600 in response to receiving the user consent voluntarily provided by the user and verifying the application specific user information, according to an embodiment as disclosed herein. At step S901, the application client 200 gathers all the application specific user information which are used to uniquely identify the user within a domain of the edge application 600. In an embodiment, edge application 600 determines the edge related services which requires the user consent while determining the application specific user information. At step S902, the application client 200 notifies the application specific user information to the edge application 600. At step S903, the application client 200 notifies the application specific user information to the edge enabler client 100. In an embodiment, the application client 200 notifies the application specific user information to an operating system of the edge enabler client 100 in a form of the manifest.

[130] At step S904, the edge enabler client 100 notifies the user the details of the services for which the user consent is needed and request for the user consent. The edge enabler client 100 authorizes the user for accepting the grant of the user consent. In an embodiment, the user provides the consent to the edge application 600 to avail the service or the UE ID for once or always or a limited number of times or a time-bound or a

location (such as geo-location) bound. At step S905, in response to obtaining the user consent from the user, the edge enabler client 100 shares the application specific user information with the edge enabler server 500a along with the user consent. At step S906, the edge enabler server 500a stores the application specific user information and the user consent along with a reference to the edge enabler client 100 for a future use. The edge enabler client 100 uses this reference to map the application specific user information to the UE 300 uniquely.

[131] At step S907, the edge application 600 requests the edge enabler server 500a for the UE ID by sending the UE ID request along with the application specific user information to the edge enabler server 500a. The UE ID request indicates the edge enabler server 500a the service required for the edge application 600. At step S908, the edge enabler server 500a verifies the user consent for the services requested by the edge application 600 using the application specific user information stored at the edge enabler server 500a. In an embodiment, the edge enabler server 500a verifies the application-specific user information stored at the edge enabler server 500a to by mapping the application-specific user information in the UE ID request. At step S909, the edge enabler server 500a shares the UE ID with the edge application 600 anonymously.

[132] According to existing 3GPP standards, the edge application 600 shares the application specific user information with the edge enabler server 500a to obtain the UE ID. Further, the edge enabler server 500a provides the UE ID directly to the edge application 600 by invoking corresponding service APIs on the edge enabler server 500a or the 3GPP core network 400 based on the application specific user information. Unlike the existing 3GPP standards, the proposed method allows an application client 200 to share the application specific user information with the edge enabler server 500a for correlating the application specific user information with the UE 300. In an embodiment, the edge application 600 generates the manifest detailing all the services for which the user consent is needed.

[133] The various actions, acts, blocks, steps, or the like in the sequential diagram in FIG. 9 may be performed in the order presented, in a different order or simultaneously. Further, in some embodiments, some of the actions, acts, blocks, steps, or the like may be omitted, added, modified, skipped, or the like without departing from the scope of the invention.

[134] FIG. 10 is a sequential diagram illustrating signaling between the devices in the system 1000 for providing the service to the edge application 600 in response to initiating the user consent grant by the application client 200 and verifying the OTP, according to an embodiment as disclosed herein. At step S1001, the application client 200 sends the request for the user consent to the edge application server 700, when the

application client 200 needs the user consent. At step S1002, upon receiving the request for the user consent from the application client 200, the edge application server 700 shares the request for the user consent to the edge enabler server 500a. At step S1003, the edge enabler server 500a generates the OTP for obtaining the user consent. At step S1004, the edge enabler server 500a shares the OTP with the UE 300. A channel of sharing the OTP by the edge enabler server 500a to the UE 300 is determined based on the user contact information such as a mobile number, email address, etc. available at the edge enabler server 500a. At step S1005, upon requesting the user consent with the edge application server 700, the application client 200 initiates steps to obtain the user consent grant from the user.

[135] At step S1006, the application client 200 requests the user using the UE 300 to input the OTP in the consent for providing the consent to the application client 200. At step S1007, in response to receiving the input for the OTP and the grant of user consent from the user, the UE 300 shares the OTP and the user consent given by the user with the application client 200. At step S1008, the application client 200 notifies the user consent and the OTP to the edge application server 700 using the user consent grant notification. At step S1009, the edge application server 700 notifies the user consent and the OTP to the edge enabler server 500a, in response to receiving the user consent grant notification from the edge application server 700. At step S1010, upon receiving the user consent and the OTP, the edge enabler server 500a verifies the received OTP with the OTP generated by the edge enabler server 500a. At step S1011, upon matching both the OTPs, the edge enabler server 500a responds with the user consent to the edge application server 700. At step S1012, the edge enabler server 500a stores the user consent. At step S1013, the edge application server 700 responds the user consent with the application client 200, in response to receiving the user consent.

[136] The various actions, acts, blocks, steps, or the like in the sequential diagram in FIG. 10 may be performed in the order presented, in a different order or simultaneously. Further, in some embodiments, some of the actions, acts, blocks, steps, or the like may be omitted, added, modified, skipped, or the like without departing from the scope of the invention.

[137] FIG. 11 is a sequential diagram illustrating signaling between the devices in the system 1000 for providing the service to the edge application 600 in response to initiating the user consent grant by the edge enabler client 100 and verifying the OTP, according to an embodiment as disclosed herein. At step S1101, the application client 200 sends the request for the user consent to the edge application server 700, when the application client 200 needs the user consent. At step S1102, upon receiving the request for the user consent from the application client 200, the edge application server 700 shares the request for the user consent to the edge enabler server 500a. At step

S1103, the edge enabler server 500a generates the OTP for obtaining the user consent. At step S1104, the edge enabler server 500a shares the OTP with the UE 300. A channel of sharing the OTP by the edge enabler server 500a to the UE 300 are based on the user contact information such as a mobile number, email address, etc. available at the edge enabler server 500a. At step S1105, upon sending the OTP to the UE 300, edge enabler server 500a requests for granting the user consent to the edge enabler client 100. At step S1106, upon receiving the request for granting the user consent, the edge enabler client 100 initiates steps to obtain the user consent grant from the user.

[138] At step S1107, the edge enabler client 100 requests the user using the UE 300 to input the OTP in the consent for providing the consent to the application client 200. At step S1108, in response to receiving the input for the OTP and the grant of user consent from the user, the UE 300 shares the OTP and the user consent given by the user with the edge enabler client 100. At step S1109, the edge enabler client 100 notifies the user consent and the OTP to the edge enabler server 500a using the user consent grant notification. At step S1110, upon receiving the user consent and the OTP, the edge enabler server 500a verifies the received OTP with the OTP generated by the edge enabler server 500a. At step S1111, upon matching both the OTPs, the edge enabler server 500a responds with the user consent to the edge application server 700. At step S1112, the edge enabler server 500a stores the user consent. At step S1113, the edge application server 700 responds the user consent with the application client 200, in response to receiving the user consent.

[139] The various actions, acts, blocks, steps, or the like in the sequential diagram in FIG. 11 may be performed in the order presented, in a different order or simultaneously. Further, in some embodiments, some of the actions, acts, blocks, steps, or the like may be omitted, added, modified, skipped, or the like without departing from the scope of the invention.

[140] FIG. 12 is a sequential diagram illustrating signaling between the devices in the system 1000 for providing the service to the edge application 600 based on the authorization from the CAPIF core function device 500b, according to an embodiment as disclosed herein. At step S1201, the edge application 600 requests to the CAPIF core function device 500b for authorization. At step S1202, the CAPIF core function device 500b grants the authorization and shares the PSK to the edge application 600. At step S1203, the edge application 600 requests for the service or the UE ID to the edge enabler server 500a in response to receiving the PSK. At step S1204, the edge enabler server 500a requests for the credentials for authorizing the edge application 600 to the CAPIF core function device 500b. In an embodiment, the edge enabler server 500a sends the information about the edge enabler client 100 and the edge application 600 to the CAPIF core function device 500b along with the request for the credentials.

[141] In an embodiment, the edge enabler server 500a sends the details about the authorization request to the CAPIF core function device 500b along with the request. At step S1205, upon receiving the request from the edge enabler server 500a, the CAPIF core function device 500b requests the edge enabler client 100 to obtain the user consent. In an embodiment, the CAPIF core function device 500b shares the details received in the information about the edge enabler client 100, the edge application 600 and details about the authorization request with the edge enabler client 100.At step S1206, the edge enabler client 100 requests to the user for the user consent. The edge enabler client 100 authorizes the user for accepting the grant of the user consent. In an embodiment, the user provides the consent to the edge application 600 to avail the service or the UE ID for once or always or a limited number of times or a time-bound or a location (such as geo-location) bound.

[142] At step S1207, the edge enabler client 100 shares the user consent with the CAPIF core function device 500b, in response to obtaining the user consent from the user. At step S1208, the CAPIF core function device 500b shares the credentials with the edge enabler server 500a based on the user consent received from the edge enabler client 100. At step S1209, upon receiving the credentials from the CAPIF core function device 500b, the edge enabler server 500a authorizes the edge application 600 and provides the requested service or the UE ID to the edge application 600.

[143] The various actions, acts, blocks, steps, or the like in the sequential diagram in FIG. 12 may be performed in the order presented, in a different order or simultaneously. Further, in some embodiments, some of the actions, acts, blocks, steps, or the like may be omitted, added, modified, skipped, or the like without departing from the scope of the invention.

[144] FIG. 13 is a sequential diagram illustrating signaling between the devices in the system 1000 for providing the authorizing credentials to the edge application 600 based on the user consent, according to an embodiment as disclosed herein. At step S1301, the edge application 600 sends the request to the CAPIF core function device 500b for the authorization credentials. The edge application 600 provides the details of the relevant edge enabler client 100 to the CAPIF core function device 500b along with the request for the authorization credentials. In an embodiment, the details of the relevant edge enabler client 100 is provides based on the information received from the application client 200.

[145] At step S1302, the CAPIF core function device 500b sends the request to the edge enabler client 100 to obtain the user consent for performing the authorization and providing the authorization credentials. At step S1303, the edge enabler client 100 requests the user to provide the consent for providing the authorization credentials to the edge application 600. The edge enabler client 100 authorizes the user for accepting

the grant of the user consent. At step S1304, the edge enabler client 100 responds to the CAPIF core function device 500b with the user consent obtained from the user. At step S1305, the CAPIF core function device 500b and stores the received user consent for the future reference. Further, the CAPIF core function device 500b performs the authorization and generates the authorization credentials. At step S1306, the CAPIF core function device 500b provides the authorization response includes the authorization credentials to the edge application 600.

[146] In an embodiment, the CAPIF core function device 500b implements the OAuth authorization server of a mobile network operator. In an embodiment, the CAPIF core function device 500b implements an OpenID connect protocol to provide the authorization to the edge application 600 in form of an anonymous identity token.

[147] In an alternate embodiment, the CAPIF core function device 500b is replaced with a standalone OAuth authorization server also implementing the OpenID connect protocol for providing the authorization to the edge application 600 in form of the anonymous identity token or OAuth tokens.

[148] The various actions, acts, blocks, steps, or the like in the sequential diagram in FIG. 13 may be performed in the order presented, in a different order or simultaneously. Further, in some embodiments, some of the actions, acts, blocks, steps, or the like may be omitted, added, modified, skipped, or the like without departing from the scope of the invention.

[149] FIG. 14 is a sequential diagram illustrating signaling between the devices in the system 1000 for providing the authorization credentials to the edge application 600 based on the user consent obtained through the edge enabler server 500a, according to an embodiment as disclosed herein. At step S1401, the edge application 600 sends the request to the CAPIF core function device 500b for the authorization credentials. At step S1402, upon receiving the request for the authorization credentials from the edge application 600, the CAPIF core function device 500b requests to the edge enabler server 500a for the user consent.

[150] At step S1403, the edge enabler server 500a requests the relevant edge enabler client 100 to obtain the user consent from the user. At step S1404, the edge enabler client 100 obtains the user consent after due authentication of the user. At step S1405, the edge enabler client 100 shares the user consent to the edge enabler server 500a. At step S1406, the edge enabler server 500a shares the user consent to the CAPIF core function device 500b. At step S1407, the edge enabler server 500a stores the user consent for the future reference. Further, the CAPIF core function device 500b performs authorization based on the user consent and generates the authorization credentials. At step S1408, the CAPIF core function device 500b shares the authorization response includes the authorization credentials to the edge application 600.

[151] The various actions, acts, blocks, steps, or the like in the sequential diagram in FIG. 14 may be performed in the order presented, in a different order or simultaneously. Further, in some embodiments, some of the actions, acts, blocks, steps, or the like may be omitted, added, modified, skipped, or the like without departing from the scope of the invention.

[152] FIG. 15 is a sequential diagram illustrating signaling between the devices in the system 1000 for providing the service to the edge application server 700 in response to obtaining the user consent from the edge enabler client 100 through the PCF 402, according to an embodiment as disclosed herein. At step S1501, the application client 200 triggers the edge enabler client 100 to initiate the steps to obtain the user consent based on the request received from the edge application server 700 or the edge application 600. In an embodiment, the edge application server 700 triggers the application client 200 to initiate steps for obtaining the user consent. At step S1502, the edge enabler client 100 requests the user to provide the user consent. The user grants/updates the user consent on the UE 300 for providing the service to the edge application 600.

[153] At step S1503, the edge enabler client 100 authorizes the user for accepting the grant of the user consent. At step S1504, the edge enabler client 100 request the NAS 301 to send the user consent to the core network 400 in response to obtaining the user consent, where the request includes the user consent. At step S1505, the NAS 301 sends the user consent as a NAS user data payload or alternatively as part of a control plane payload to the AMF 401 by securing the user consent using a NAS security key. At step S1506, the AMF 401 acknowledges the reception of the user consent to the NAS 301. At step S1507, the AMF 401 sends the user consent to the PCF 402. At step S1508, the PCF 402 stores the user consent as part of a subscription profile. At step S1509, the PCF 402 acknowledges the reception of the user consent to the AMF 401. At step S1510, the PCF 402 notifies the edge enabler server 500a that the user consent is available at the PCF 402.

[154] At step S1511, the edge enabler server 500a receives the request for a sensitive information such as the UE specific parameter (e.g. UE ID) from the edge application server 700 or any request from the edge application server 700. Further, the edge enabler server 500a checks for the user consent is available for providing the UE specific parameter to the edge application server 700. Upon detecting that the user consent is available at the edge enabler server 500a and not verified, the edge enabler server 500a verifies the user consent by checking whether the user provides the permission to expose the UE specific parameter out of the core network 400. At step S1512, upon detecting that the user consent is not available at the edge enabler server 500a and notification about the availability of the user consent at the PCF 402 is

received, the edge enabler server 500a fetches the user consent from the PCF 402. In an embodiment, the edge enabler server 500a identifies the user consent stored at the PCF 402 for fetching the user consent based on a subscription ID of the UE 300 or an application ID (e.g. application layer client ID). At step S1513, the edge enabler server 500a stores the user consent and deletes the notification. Further, the edge enabler server 500a verifies the user consent. At step S1514, edge enabler server 500a responses with the UE specific parameter to the edge application server 700, in response to verifying the user consent.

[155] The various actions, acts, blocks, steps, or the like in the sequential diagram in FIG. 15 may be performed in the order presented, in a different order or simultaneously. Further, in some embodiments, some of the actions, acts, blocks, steps, or the like may be omitted, added, modified, skipped, or the like without departing from the scope of the invention.

[156] FIG. 16 is a sequential diagram illustrating signaling between the devices in the system 1000 for providing the service to the edge application server 700 in response to obtaining the user consent from the edge enabler client 100 through the UDM/UDR 403, according to an embodiment as disclosed herein. At step S1601, the application client 200 triggers the edge enabler client 100 to initiate the steps to obtain the user consent based on the request received from the edge application server 700 or the edge application 600. In an embodiment, the edge application server 700 triggers the application client 200 to initiate steps for obtaining the user consent. At step S1602, the edge enabler client 100 requests the user to provide the user consent. The user grants/updates the user consent on the UE 300 for providing the service to the edge application 600.

[157] At step S1603, the edge enabler client 100 authorizes the user for accepting the grant of the user consent. At step S1604, the edge enabler client 100 request the NAS 301 to send the user consent to the core network 400 in response to obtaining the user consent, where the request includes the user consent. At step S1605, the NAS 301 sends the user consent as the NAS user data payload or alternatively as part of the control plane payload to the AMF 401 by securing the user consent using the NAS security key. At step S1606, the AMF 401 acknowledges the reception of the user consent to the NAS 301. At step S1607, the AMF 401 sends the user consent to the UDM/UDR 403. At step S1608, the UDM/UDR 403 stores the user consent as part of the subscription profile. At step S1609, the UDM/UDR 403 acknowledges the reception of the user consent to the AMF 401. At step S1610, the UDM/UDR 403 notifies the edge enabler server 500a that the user consent is available at the UDM/UDR 403.

[158] At step S1611, the edge enabler server 500a receives the request for the UE specific

parameter from the edge application server 700 or any request from the edge application server 700. Further, the edge enabler server 500a checks for the user consent is available for providing the UE specific parameter to the edge application server 700. Upon detecting that the user consent is available at the edge enabler server 500a and not verified, the edge enabler server 500a verifies the user consent by checking whether the user provides the permission to expose the UE specific parameter out of the core network 400. At step S1612, upon detecting that the user consent is not available at the edge enabler server 500a and notification about the availability of the user consent at the UDM/UDR 403 is received, the edge enabler server 500a fetches the user consent from the UDM/UDR 403. In an embodiment, the edge enabler server 500a identifies the user consent stored at the UDM/UDR 403 for fetching the user consent based on the subscription ID of the UE 300 or the application ID. At step S1613, the edge enabler server 500a stores the user consent and deletes the notification. Further, the edge enabler server 500a verifies the user consent. At step S1614, edge enabler server 500a responses with the UE specific parameter to the edge application server 700, in response to verifying the user consent.

[159] The various actions, acts, blocks, steps, or the like in the sequential diagram in FIG. 16 may be performed in the order presented, in a different order or simultaneously. Further, in some embodiments, some of the actions, acts, blocks, steps, or the like may be omitted, added, modified, skipped, or the like without departing from the scope of the invention.

[160] FIG. 17 is a sequential diagram illustrating signaling between the devices in the system 1000 for providing the response for the service to the edge application server 700 in response to obtaining the user consent from the NAS 301 through the PCF 402, according to an embodiment as disclosed herein. At step S1701, the application client 200 triggers the edge enabler client 100 to initiate the steps to obtain the user consent based on the request received from the edge application server 700 or the edge application 600. In an embodiment, the edge application server 700 triggers the application client 200 to initiate steps for obtaining the user consent. At step S1702, the edge enabler client 100 requests the NAS 301 to obtain the user consent. At step S1703, the NAS 301 request the user for the user consent. The user grants/updates the user consent on the UE 300 for providing the service to the edge application 600. At step S1704, the NAS 301 authorizes the user for accepting the grant of the user consent. At step S1705, the NAS 301 sends the user consent as the NAS user data payload or alternatively as part of the control plane payload to the AMF 401 by securing the user consent using the NAS security key. At step S1706, the AMF 401 acknowledges the reception of the user consent to the NAS 301. At step S1707, the AMF 401 sends the user consent to the PCF 402. At step S1708, the PCF 402 stores the user

consent as part of the subscription profile. At step S1709, the PCF 402 acknowledges the reception of the user consent to the AMF 401. At step S1710, the PCF 402 notifies the edge enabler server 500a that the user consent is available at the PCF 402.

[161] At step S1711, the edge enabler server 500a receives the request for the UE specific parameter (e.g. UE ID) from the edge application server 700 or any request from the edge application server 700. Further, the edge enabler server 500a checks for the user consent is available for providing the UE specific parameter to the edge application server 700. Upon detecting that the user consent is available at the edge enabler server 500a and not verified, the edge enabler server 500a verifies the user consent by checking whether the user provides the permission to expose the UE specific parameter out of the core network 400. At step S1712, upon detecting that the user consent is not available at the edge enabler server 500a and notification about the availability of the user consent at the PCF 402 is received, the edge enabler server 500a fetches the user consent from the PCF 402. In an embodiment, the edge enabler server 500a identifies the user consent stored at the PCF 402 for fetching the user consent based on the subscription ID of the UE 300 or the application ID. At step S1713, the edge enabler server 500a stores the user consent and deletes the notification. Further, the edge enabler server 500a verifies the user consent. At step S1714, edge enabler server 500a responses with the UE specific parameter to the edge application server 700, in response to verifying the user consent.

[162] The various actions, acts, blocks, steps, or the like in the sequential diagram in FIG. 17 may be performed in the order presented, in a different order or simultaneously. Further, in some embodiments, some of the actions, acts, blocks, steps, or the like may be omitted, added, modified, skipped, or the like without departing from the scope of the invention.

[163] FIG. 18 is a sequential diagram illustrating signaling between the devices in the system 1000 for providing the service to the edge application server 700 in response to obtaining the user consent by the NAS 301 through the UDM/UDR 403, according to an embodiment as disclosed herein. At step S1801, the application client 200 triggers the edge enabler client 100 to initiate the steps to obtain the user consent based on the request received from the edge application server 700 or the edge application 600. In an embodiment, the edge application server 700 triggers the application client 200 to initiate steps for obtaining the user consent. At step S1802, the edge enabler client 100 requests the NAS 301 to obtain the user consent. At step S1803, the NAS 301 request the user for the user consent. The user grants/updates the user consent on the UE 300 for providing the service to the edge application 600. At step S1804, the NAS 301 authorizes the user for accepting the grant of the user consent. At step S1805, the NAS 301 sends the user consent as the NAS user data payload or alternatively as part of the

control plane payload to the AMF 401 by securing the user consent using the NAS security key. At step S1806, the AMF 401 acknowledges the reception of the user consent to the NAS 301. At step S1807, the AMF 401 sends the user consent to the UDM/UDR 403. At step S1808, the UDM/UDR 403 stores the user consent as part of the subscription profile. At step S1809, the UDM/UDR 403 acknowledges the reception of the user consent to the AMF 401. At step S1810, the UDM/UDR 403 notifies the edge enabler server 500a that the user consent is available at the UDM/UDR 403.

[164] At step S1811, the edge enabler server 500a receives the request for the UE specific parameter (e.g. UE ID) from the edge application server 700 or any request from the edge application server 700. Further, the edge enabler server 500a checks for the user consent is available for providing the UE specific parameter to the edge application server 700. Upon detecting that the user consent is available at the edge enabler server 500a and not verified, the edge enabler server 500a verifies the user consent by checking whether the user provides the permission to expose the UE specific parameter out of the core network 400. At step S1812, upon detecting that the user consent is not available at the edge enabler server 500a and notification about the availability of the user consent at the UDM/UDR 403 is received, the edge enabler server 500a fetches the user consent from the UDM/UDR 403. In an embodiment, the edge enabler server 500a identifies the user consent stored at the UDM/UDR 403 for fetching the user consent based on the subscription ID of the UE 300 or the application ID. At step S1813, the edge enabler server 500a stores the user consent and deletes the notification. Further, the edge enabler server 500a verifies the user consent. At step S1814, edge enabler server 500a responses with the UE specific parameter to the edge application server 700, in response to verifying the user consent.

[165] The various actions, acts, blocks, steps, or the like in the sequential diagram in FIG. 18 may be performed in the order presented, in a different order or simultaneously. Further, in some embodiments, some of the actions, acts, blocks, steps, or the like may be omitted, added, modified, skipped, or the like without departing from the scope of the invention.

[166] FIG. 19 is a sequential diagram illustrating signaling between the devices in the system 1000 for providing the service to the edge application server 700 in response to receiving the request for the service from the edge application server 700 and the user consent through the PCF 402, according to an embodiment as disclosed herein. At step S1901, the edge application server 700 requests for the UE specific parameter to the edge enabler server 500a for rendering the edge service for the edge application 600 subscribed by the user. In response to detecting that the user consent is not available at the edge enabler server 500a, the edge enabler server 500a triggers the steps to obtain

the user consent from the user via the core network 400. At step S1902, the edge enabler server 500a request the PCF 402 for obtaining the user consent.

[167] The edge enabler server 500a provides the subscription ID of the UE 300 or the application ID to the PCF 402 while requesting to obtain the user consent. The PCF 402 checks whether the user consent is available at the PCF 402, in response to receiving the request from the edge enabler server 500a. In an embodiment, the PCF 402 retrieves the user consent based on the subscription ID of the UE 300 or the application ID, and sends the user consent to the edge enabler server 500a when the user consent is available at the PCF 402. At step S1903, the PCF 402 requests the AMF 401 to obtain the user consent, when the user consent is not available at the PCF 402. At step S1904, the AMF 401 requests the NAS 301 to obtain the user consent. At step S1905, the NAS 301 requests the user to provide the user consent. The user grants/updates the user consent on the UE 300 for providing the service to the edge application 600. At step S1906, the NAS 301 authorizes the user for accepting the grant of the user consent. At step S1907, the NAS 301 sends the user consent as the NAS user data payload or alternatively as part of the control plane payload to the AMF 401 by securing the user consent using the NAS security key.

[168] At step S1908, the AMF 401 sends the user consent to the PCF 402. At step S1909, the PCF 402 stores the user consent as part of the subscription profile. At step S1910, the PCF 402 responses the edge enabler server 500a with the user consent. At step S1911, the edge enabler server 500a stores the user consent. Further, the edge enabler server 500a verifies the user consent by checking whether the user provides the permission to expose the UE specific parameter out of the core network 400. At step S1912, the edge enabler server 500a responses with the UE specific parameter to the edge application server 700, in response to verifying the user consent.

[169] The various actions, acts, blocks, steps, or the like in the sequential diagram in FIG. 19 may be performed in the order presented, in a different order or simultaneously. Further, in some embodiments, some of the actions, acts, blocks, steps, or the like may be omitted, added, modified, skipped, or the like without departing from the scope of the invention.

[170] FIG. 20 is a sequential diagram illustrating signaling between the devices in the system 1000 for providing the service to the edge application server 700 in response to receiving the request for the service from the edge application server 700 and the user consent through the UDM/UDR 403, according to an embodiment as disclosed herein. At step S2001, the edge application server 700 requests for the UE specific parameter to the edge enabler server 500a for rendering the edge service for the edge application 600 subscribed by the user. In response to detecting that the user consent is not available at the edge enabler server 500a, the edge enabler server 500a triggers the

steps to obtain the user consent from the user via the core network 400.

[171] At step S2002, the edge enabler server 500a request the UDM/UDR 403 for obtaining the user consent. The edge enabler server 500a provides the subscription ID of the UE 300 or the application ID to the UDM/UDR 403 while requesting to obtain the user consent. The UDM/UDR 403 checks whether the user consent is available at the UDM/UDR 403, in response to receiving the request from the edge enabler server 500a. In an embodiment, the UDM/UDR 403 retrieves the user consent based on the subscription ID of the UE 300 or the application ID, and sends the user consent to the edge enabler server 500a when the user consent is available at the UDM/UDR 403. At step S2003, the UDM/UDR 403 requests the AMF 401 to obtain the user consent, when the user consent is not available at the UDM/UDR 403. At step S2004, the AMF 401 requests the NAS 301 to obtain the user consent. At step S2005, the NAS 301 requests the user to provide the user consent.

[172] The user grants/updates the user consent on the UE 300 for providing the service to the edge application 600. At step S2006, the NAS 301 authorizes the user for accepting the grant of the user consent. At step S2007, the NAS 301 sends the user consent as the NAS user data payload or alternatively as part of the control plane payload to the AMF 401 by securing the user consent using the NAS security key. At step S2008, the AMF 401 sends the user consent to the UDM/UDR 403. At step S2009, the UDM/UDR 403 stores the user consent as part of the subscription profile. At step S2010, the UDM/ UDR 403 responses the edge enabler server 500a with the user consent. At step S2011, the edge enabler server 500a stores the user consent. Further, the edge enabler server 500a verifies the user consent by checking whether the user provides the permission to expose the UE specific parameter out of the core network 400. At step S2012, the edge enabler server 500a responses with the UE specific parameter to the edge application server 700, in response to verifying the user consent.

[173] The various actions, acts, blocks, steps, or the like in the sequential diagram in FIG. 20 may be performed in the order presented, in a different order or simultaneously. Further, in some embodiments, some of the actions, acts, blocks, steps, or the like may be omitted, added, modified, skipped, or the like without departing from the scope of the invention.

[174] FIG. 21 schematically illustrates the server according to embodiments of the present disclosure.

[175] Referring to the FIG. 21, the server 500 may include a processor 2110, a transceiver 2120 and a memory 2130. However, all of the illustrated components are not essential. The server 500 may be implemented by more or less components than those illustrated in FIG. 21. In addition, the processor 2110 and the transceiver 2120 and the memory 2130 may be implemented as a single chip according to another embodiment.

[176] The server 500 may correspond to edge enabler server 500a and CAPIF core function device 500b described above. For example, the server 500 may correspond to the edge enabler server 500a illustrated in FIG. 2E and FIG. 3.

[177] The aforementioned components will now be described in detail.

[178] The processor 2110 may include one or more processors or other processing devices that control the proposed function, process, and/or method. Operation of the server 500 may be implemented by the processor 2110.

[179] The transceiver 2120 may include a RF transmitter for up-converting and amplifying a transmitted signal, and a RF receiver for down-converting a frequency of a received signal. However, according to another embodiment, the transceiver 2120 may be implemented by more or less components than those illustrated in components.

[180] The transceiver 2120 may be connected to the processor 2110 and transmit and/or receive a signal. The signal may include control information and data. In addition, the transceiver 2120 may receive the signal through a wireless channel and output the signal to the processor 2110. The transceiver 2120 may transmit a signal output from the processor 2110 through the wireless channel.

[181] The memory 2130 may store the control information or the data included in a signal obtained by the server 500. The memory 2130 may be connected to the processor 2110 and store at least one instruction or a protocol or a parameter for the proposed function, process, and/or method. The memory 2130 may include read-only memory (ROM) and/or random access memory (RAM) and/or hard disk and/or CD-ROM and/or DVD and/or other storage devices.

[182] The embodiments disclosed herein can be implemented using at least one software program running on at least one hardware device and performing network management functions to control the elements.

[183] FIG. 22 illustrates a user equipment (UE) according to embodiments of the present disclosure.

[184] Referring to the FIG. 22, the UE 2200 may include a processor 2210, a transceiver 2220 and a memory 2230. However, all of the illustrated components are not essential. The UE 2200 may be implemented by more or less components than those illustrated in FIG. 22. In addition, the processor 2210 and the transceiver 2220 and the memory 2230 may be implemented as a single chip according to another embodiment.

[185] The UE 2200 may correspond to the UE described above. For example, UE 2200 may correspond to UE 300 illustrated in FIG. 2C and FIG.10.

[186] The aforementioned components will now be described in detail.

[187] The processor 2210 may include one or more processors or other processing devices that control the proposed function, process, and/or method. Operation of the UE 2200 may be implemented by the processor 2210.

[188] The transceiver 2220 may include a RF transmitter for up-converting and amplifying a transmitted signal, and a RF receiver for down-converting a frequency of a received signal. However, according to another embodiment, the transceiver 2220 may be implemented by more or less components than those illustrated in components.

[189] The transceiver 2220 may be connected to the processor 2210 and transmit and/or receive a signal. The signal may include control information and data. In addition, the transceiver 2220 may receive the signal through a wireless channel and output the signal to the processor 2210. The transceiver 2220 may transmit a signal output from the processor 2210 through the wireless channel.

[190] The memory 2230 may store the control information or the data included in a signal obtained by the UE 2200. The memory 2230 may be connected to the processor 2210 and store at least one instruction or a protocol or a parameter for the proposed function, process, and/or method. The memory 2230 may include read-only memory (ROM) and/or random access memory (RAM) and/or hard disk and/or CD-ROM and/or DVD and/or other storage devices.

[191] The foregoing description of the specific embodiments will so fully reveal the general nature of the embodiments herein that others can, by applying current knowledge, readily modify and/or adapt for various applications such specific embodiments without departing from the generic concept, and, therefore, such adaptations and modifications should and are intended to be comprehended within the meaning and range of equivalents of the disclosed embodiments. It is to be understood that the phraseology or terminology employed herein is for the purpose of description and not of limitation. Therefore, while the embodiments herein have been described in terms of preferred embodiments, those skilled in the art will recognize that the embodiments herein can be practiced with modification within the scope of the embodiments as described herein.

Claims

[Claim 1] A method for providing a service to an edge application performed by a server, comprising:
receiving a request for accessing at least one service associated with a UE ;
determining, availability of a user consent for accessing the at least one service; and
authorizing, access of the at least one service when the user consent is available.

[Claim 2] The method as claimed in claim 1, the method comprising:
sending, a user consent request when the user consent for accessing the at least one service is not available at the server, wherein the user consent request indicates a request for the user consent;
receiving, a user consent response comprising the user consent for authorizing the access of the at least one service; and
storing, the user consent, in response to receiving the user consent

[Claim 3] The method as claimed in claim 1, the method comprising:
receiving, a user consent update request, wherein the user consent update request comprises information about at least one parameter of the user consent to be updated;
updating, the at least one parameter of the user consent stored at the server; and
sending, a user consent update response.

[Claim 4] The method as claimed in claim 1, the method comprising:
receiving, a user consent update request, wherein the user consent update request comprises information about at least one parameter of the user consent to be updated;
generating, an OTP for the user consent;
sending, the OTP;
receiving, a user consent update notification comprising the user consent and the OTP;
verifying, the user consent based on the OTP;
updating, the at least one parameter of the user consent stored at the server; and
sending, a user consent response.

[Claim 5] The method as claimed in claim 1, the method comprising:
receiving, at least one of a request for accessing the service associated

with a User Equipment (UE), and a request for a user consent associated with the UE;
retrieving, the user consent, wherein the user consent indicates a consent of a user to provide at least one of the service; and
sending, at least one of the service associated with the UE and the user consent.

[Claim 6] The method as claimed in claim 5, wherein retrieving, the user consent, comprising:
determining, an availability of the user consent for accessing the requested service associated with the UE; and
performing, one of:
authorizing an access of the service when the user consent is available at the server, and
sending a user consent request when the user consent is not available at the server, and storing the user consent in response to receiving a user consent response comprising the user consent.

[Claim 7] The method as claimed in claim 5, wherein retrieving, comprising:
generating, a One Time Password (OTP) for the user consent;
sending, the OTP;
receiving, a user consent grant notification comprising the user consent and the OTP;
verifying, the user consent based on the OTP;
storing, the user consent; and
sending, a user consent response.

[Claim 8] A server for providing a service to an edge application, comprising:
transceiver;
a processor coupled with the transceiver and configured to:
receive a request for accessing at least one service associated with a UE,
determine availability of a user consent for accessing the at least one service, and
authorize access of the at least one service when the user consent is available.

[Claim 9] The server as claimed in claim 8, wherein the processor is further configured to:
send a user consent request when the user consent for accessing the at least one service is not available at the server, wherein the user consent request indicates a request for the user consent,

receive a user consent response comprising the user consent for authorizing the access of the at least one service, and
store the user consent, in response to receiving the user consent.

[Claim 10] The server as claimed in claim 8, wherein the processor is further configured to:
receive a user consent update request, wherein the user consent update request comprises information about at least one parameter of the user consent to be updated,
update the at least one parameter of the user consent, and
send a user consent update response.

[Claim 11] The server as claimed in claim 8, wherein the processor is further configured to:
receive a user consent update request, wherein the user consent update request comprises information about at least one parameter of the user consent to be updated,
generate an OTP for the user consent,
send the OTP,
receive a user consent update notification comprising the user consent and the OTP,
verify the user consent based on the OTP,
update the at least one parameter of the user consent, and
send a user consent response.

[Claim 12] The server as claimed in claim 8, wherein the processor is further configured to:
receive at least one of a request for accessing the service associated with a User Equipment (UE), and a request for a user consent associated with the UE,
retrieve the user consent, wherein the user consent indicates a consent of a user to provide at least one of the service, and
send at least one of the service associated with the UE and the user consent.

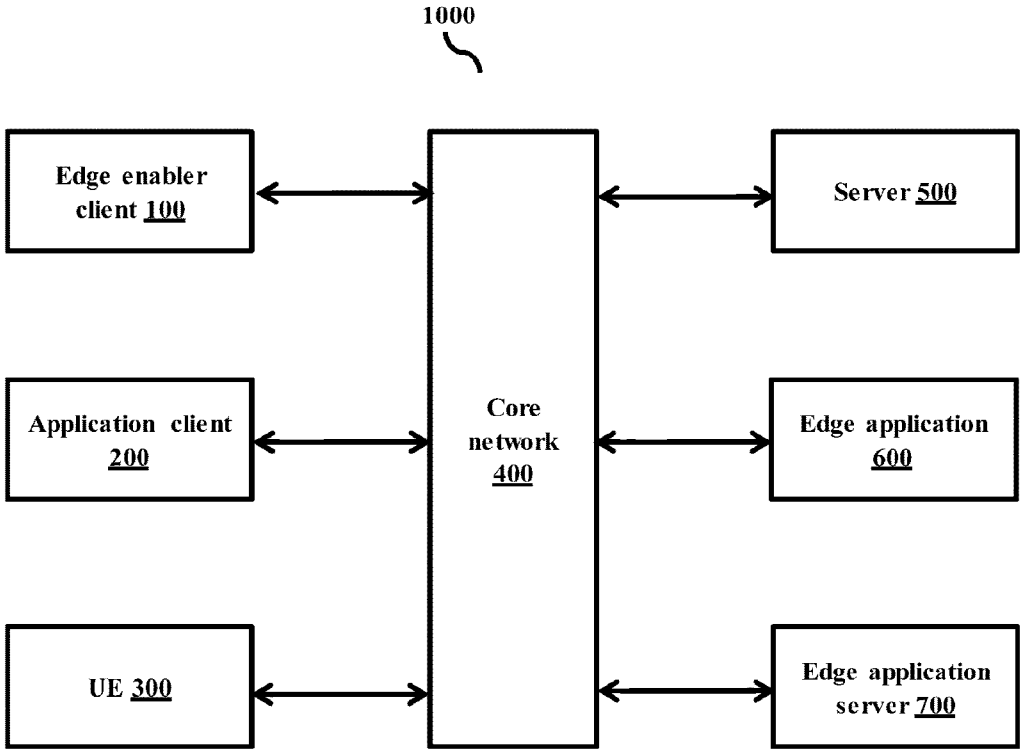
[Claim 13] The server as claimed in claim 12, wherein retrieve the user consent, comprising:
determine an availability of the user consent for accessing the requested service associated with the UE and
perform one of:
authorize an access of the service when the user consent is available at the server, and

send a user consent request when the user consent is not available at the server, and store the user consent in response to receiving a user consent response comprising the user consent.

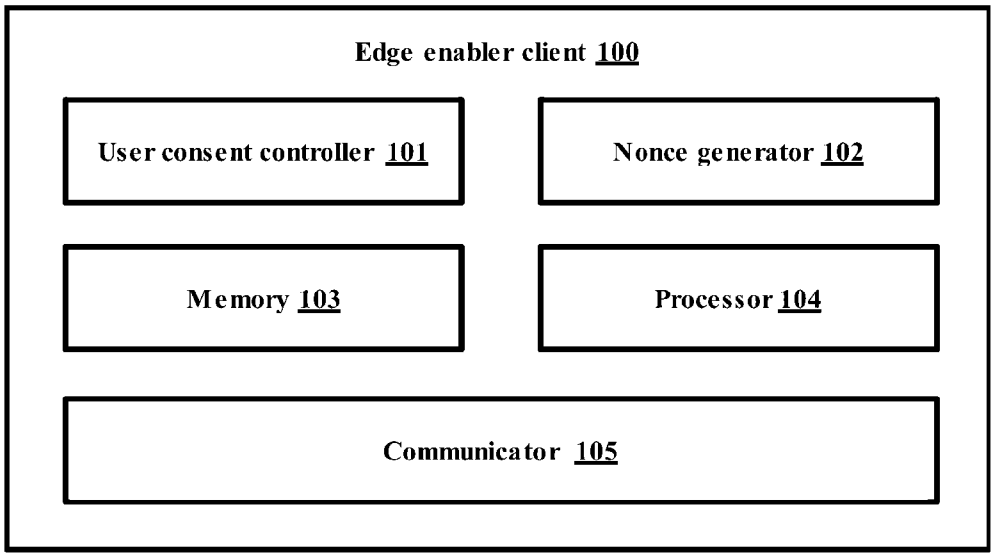
[Claim 14] The server as claimed in claim 12, wherein retrieve the user consent, comprising:
generate a One Time Password (OTP) for the user consent,
send the OTP,
receive a user consent grant notification comprising the user consent and the OTP,
verify the user consent based on the OTP;
store the user consent; and
send a user consent response.

[Claim 15] A method for providing a service to an edge application performed by a UE comprising:
receiving, an application specific user information for providing the service associated with the UE to the edge application;
sending, the application specific user information to the edge application and the edge enabler client;
receiving, a user consent to provide the service associated with the UE to the edge application, in response to receiving the application specific user information;
sending, the application specific user information with the user consent to the edge enabler server.

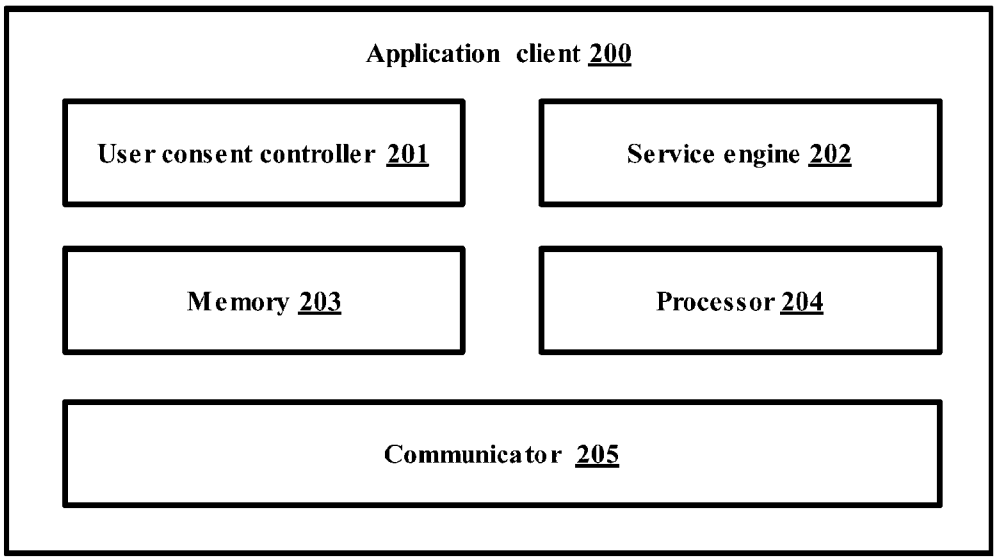
[Fig. 1]


1000
Edge enabler client 100
Server 500
Application client 200
Core network 400
Edge application 600
UE 300
Edge application server 700

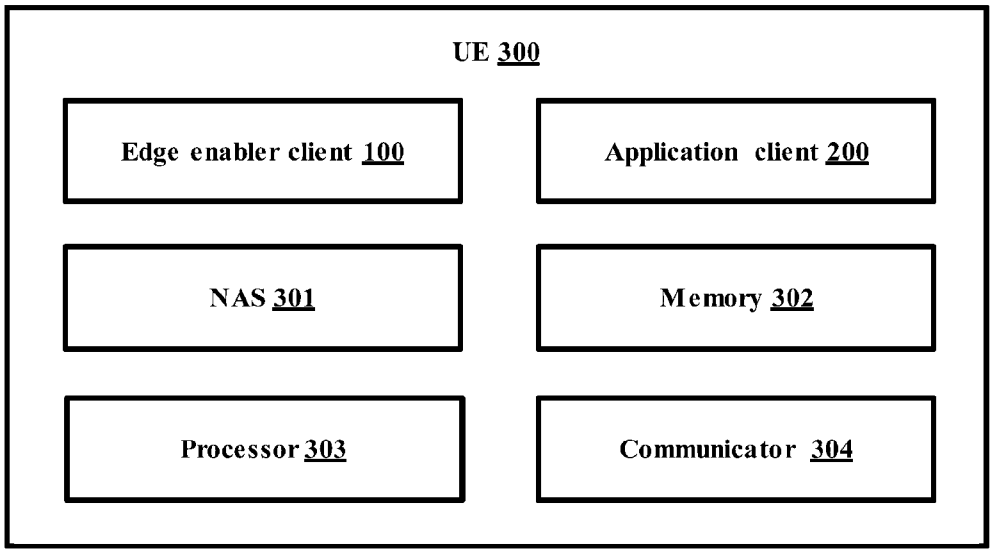
[Fig. 2A]


Edge enabler client 100
User consent controller 101
Nonce generator 102
Memory 103
Processor 104
Communicator 105

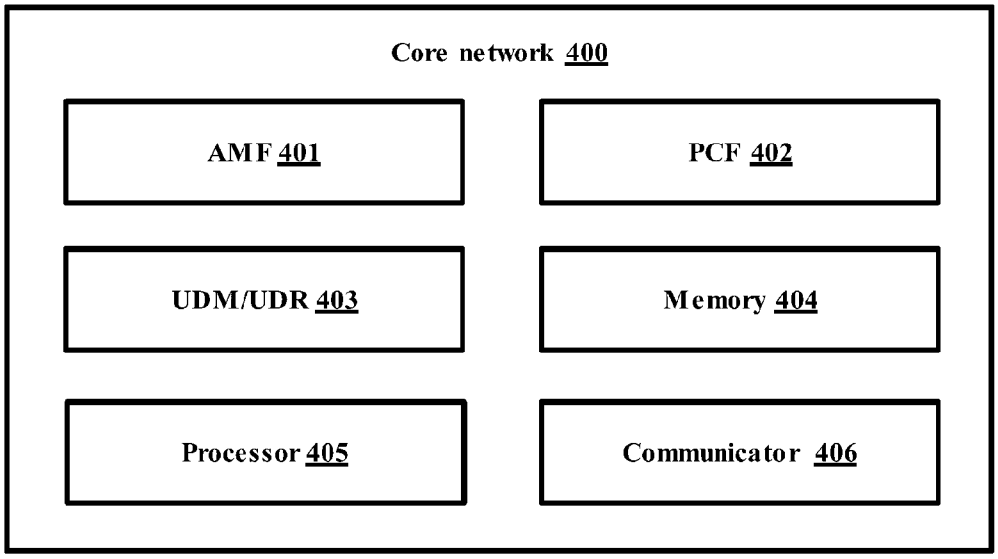
[Fig. 2B]



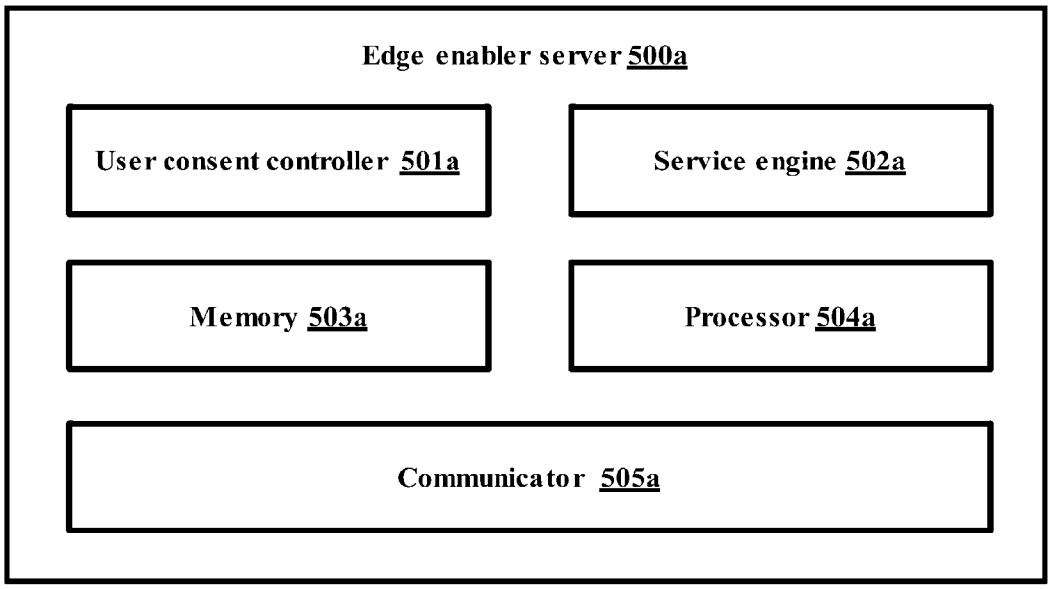
[Fig. 2C]



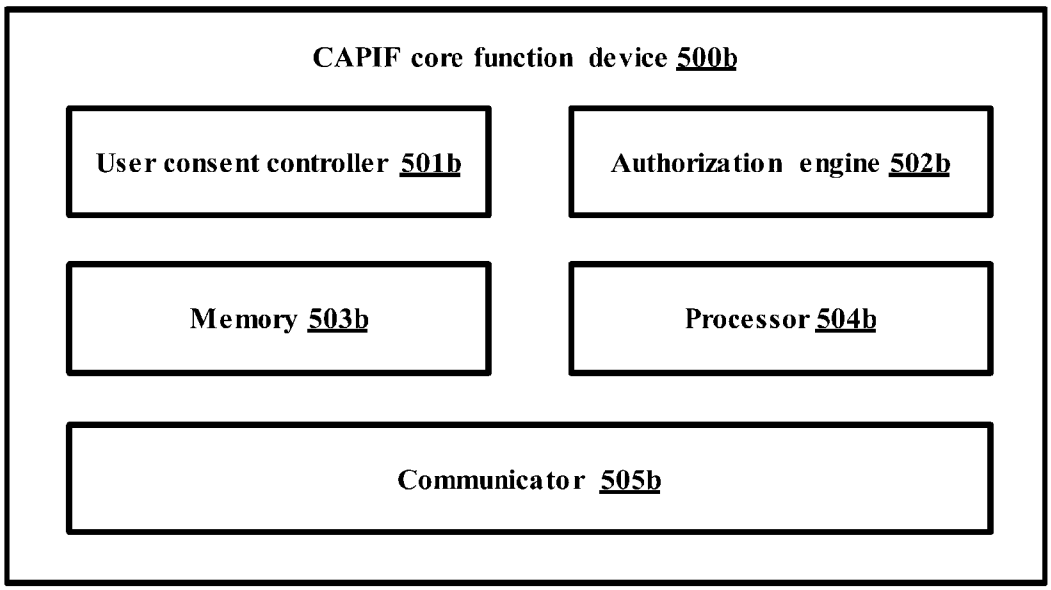
[Fig. 2D]



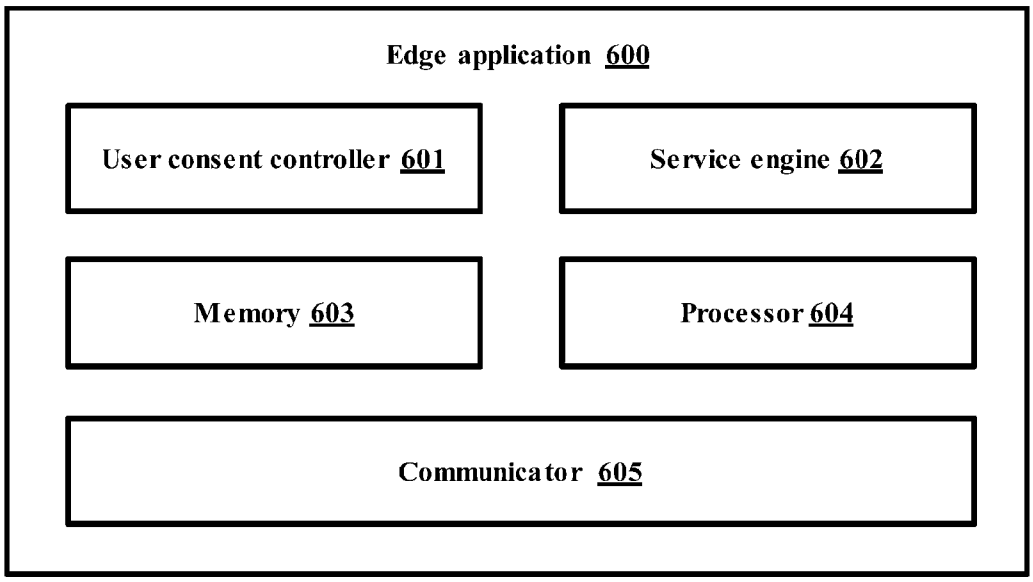
[Fig. 2E]



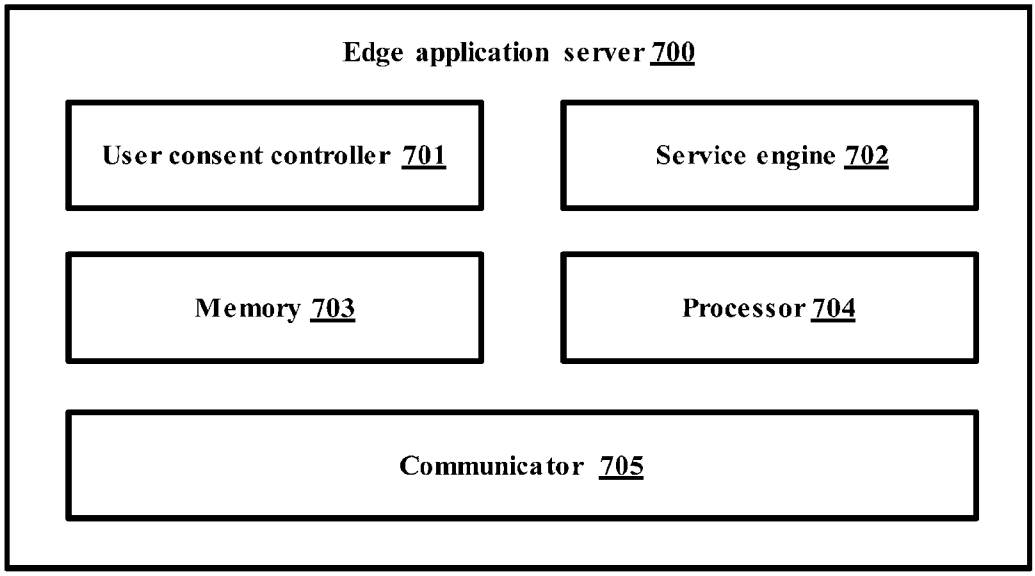
[Fig. 2F]



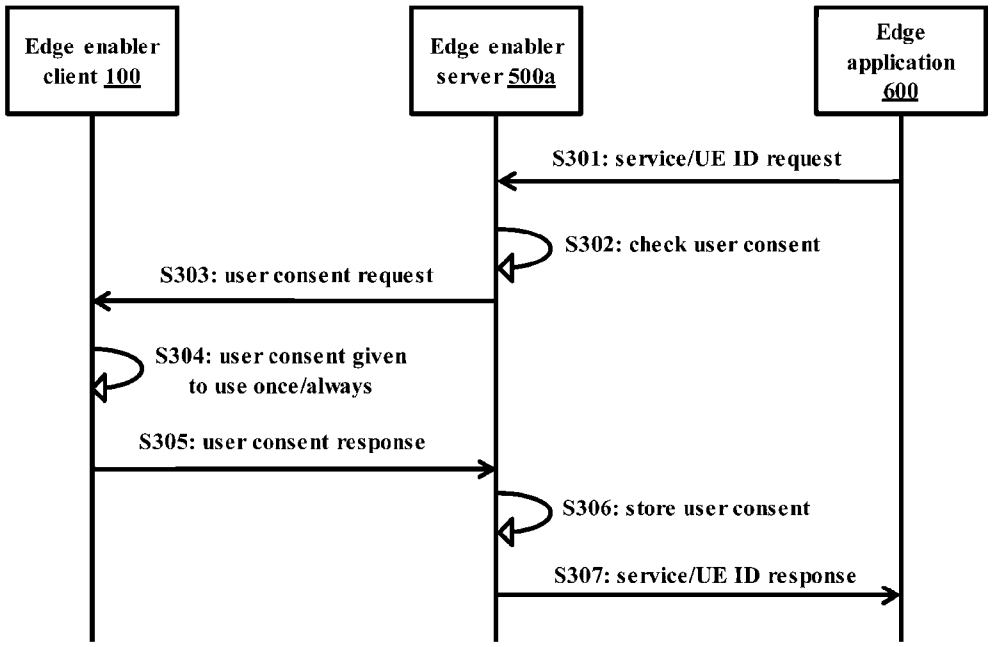
[Fig. 2G]



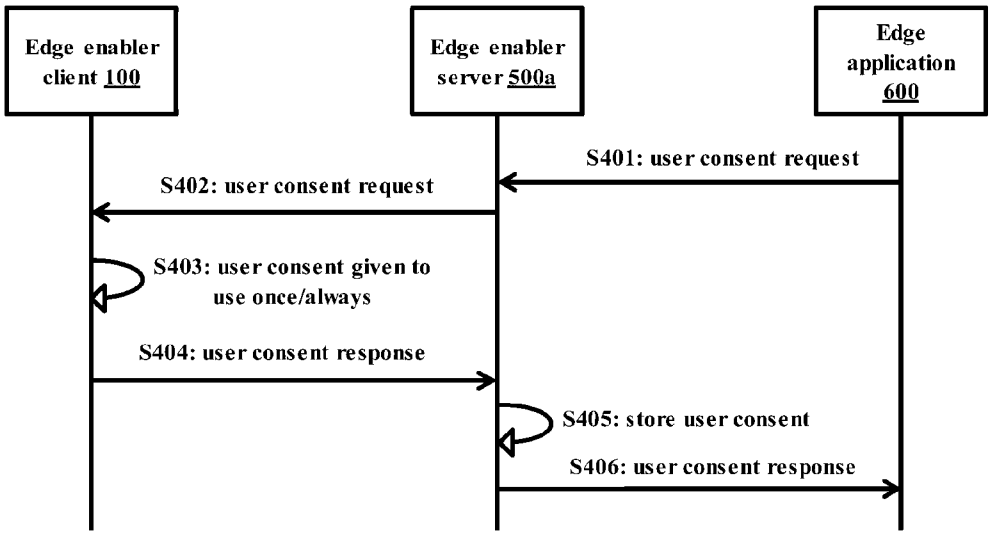
[Fig. 2H]



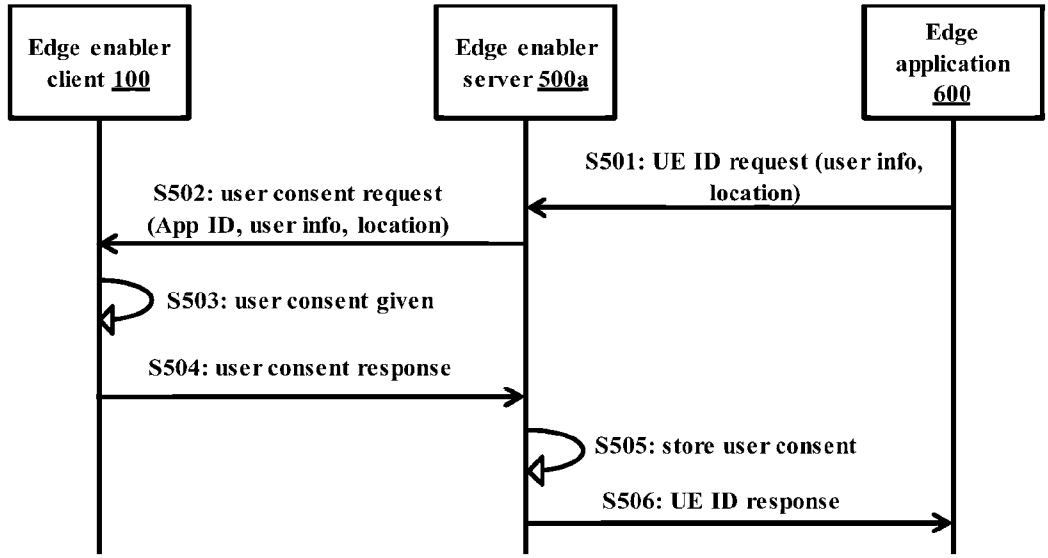
[Fig. 3]



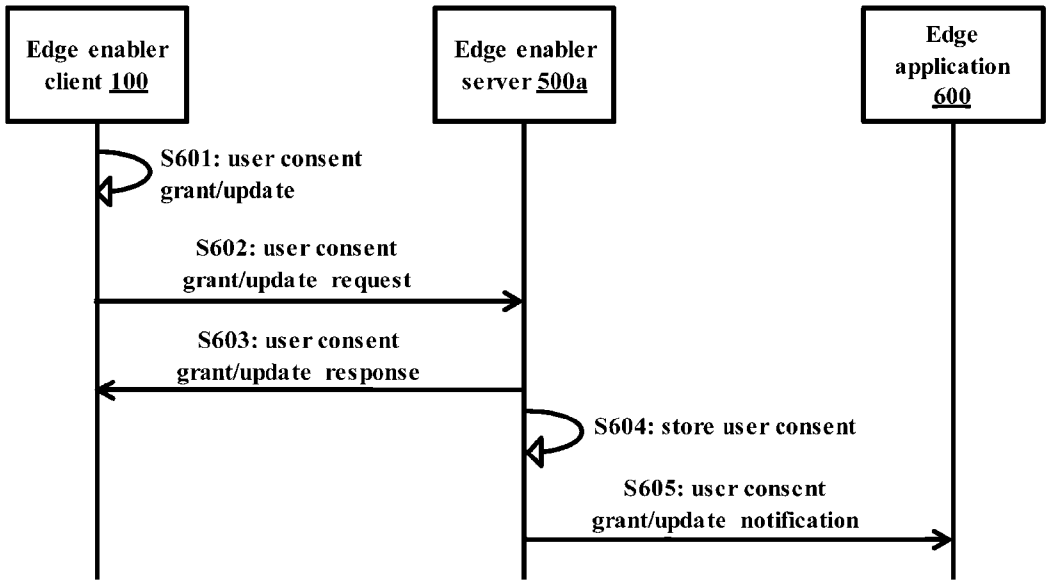
[Fig. 4]



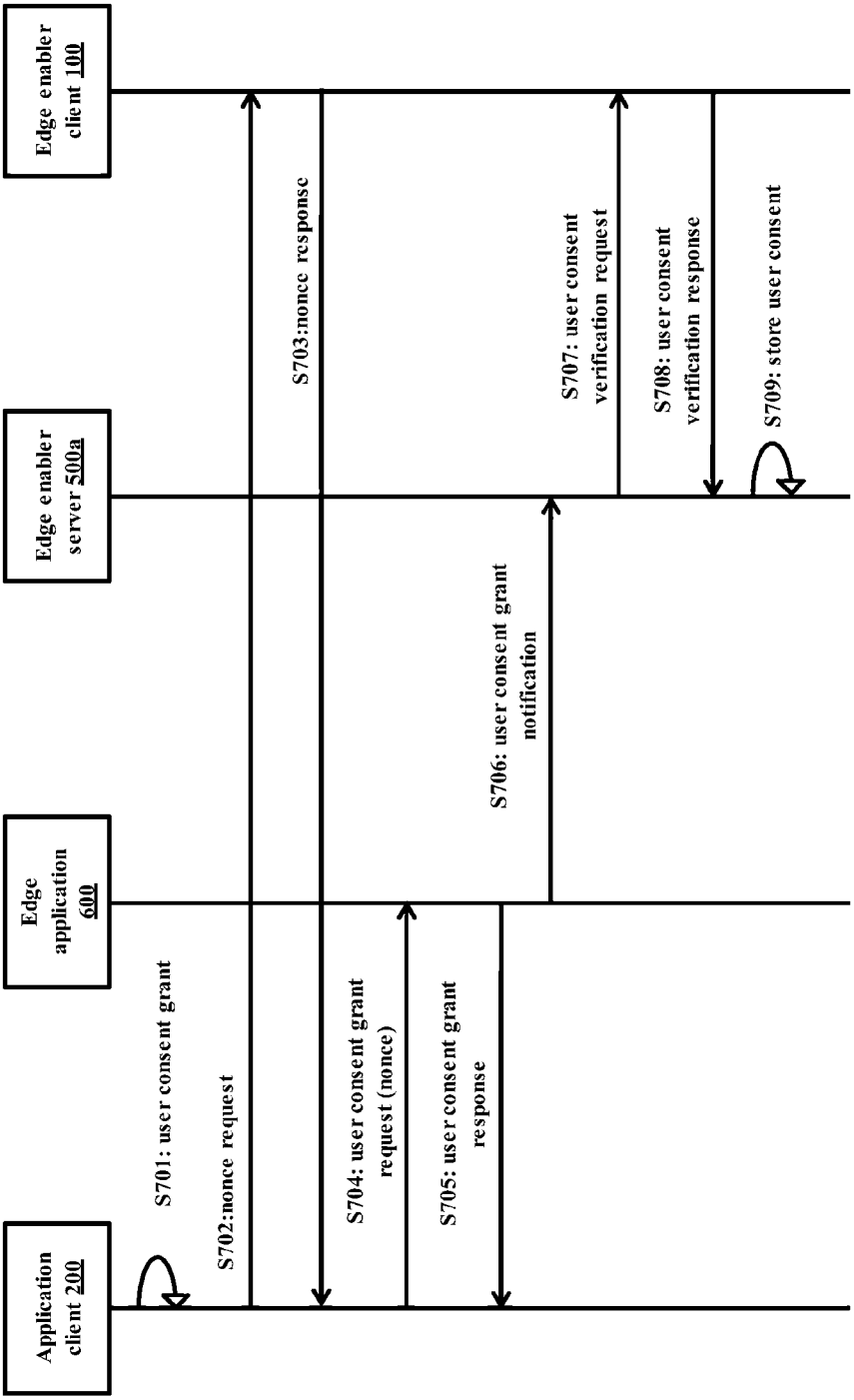
[Fig. 5]


Edge enabler client 100
Edge enabler server 500a
Edge application 600
S501: UE ID request (user info, location)
S502: user consent request (App ID, user info, location)
S503: user consent given
S504: user consent response
S505: store user consent
S506: UE ID response

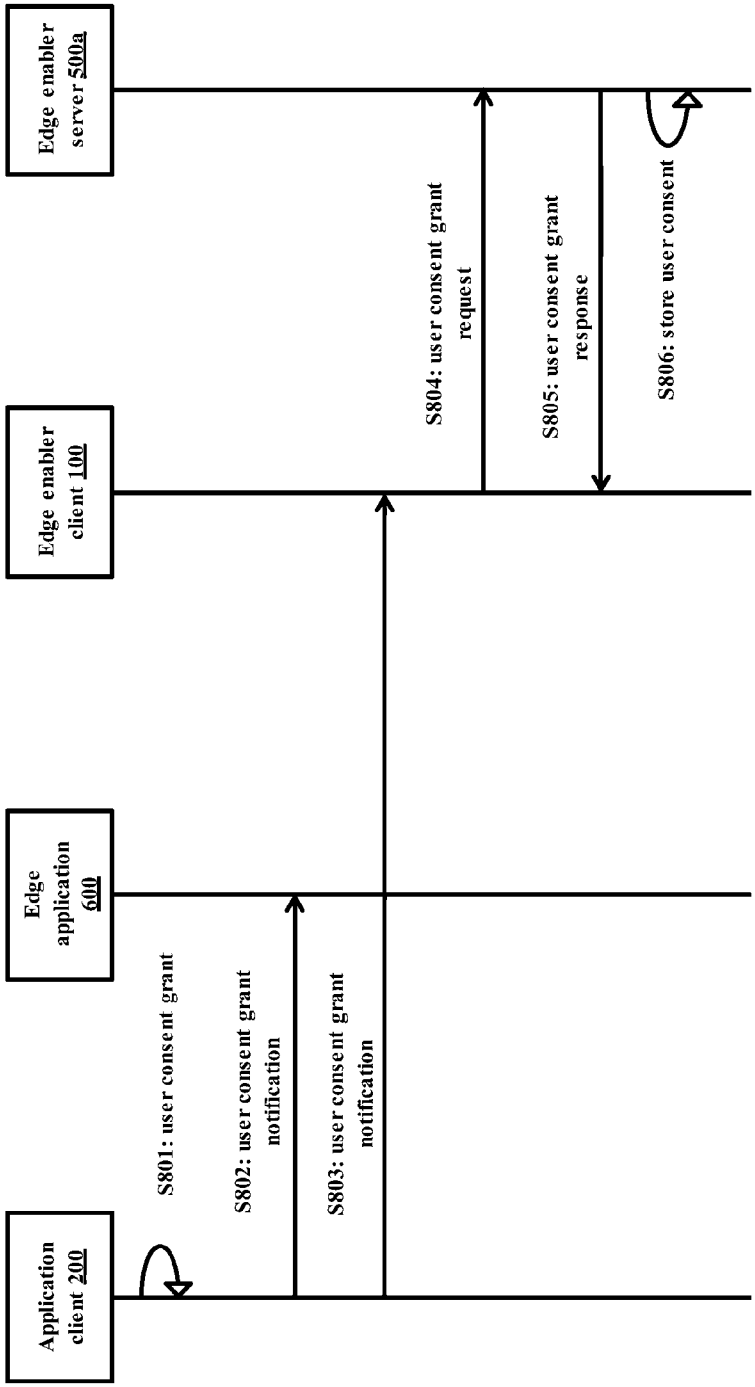
[Fig. 6]


Edge enabler client 100
Edge enabler server 500a
Edge application 600
S601: user consent grant/update
S602: user consent grant/update request
S603: user consent grant/update response
S604: store user consent
S605: user consent grant/update notification

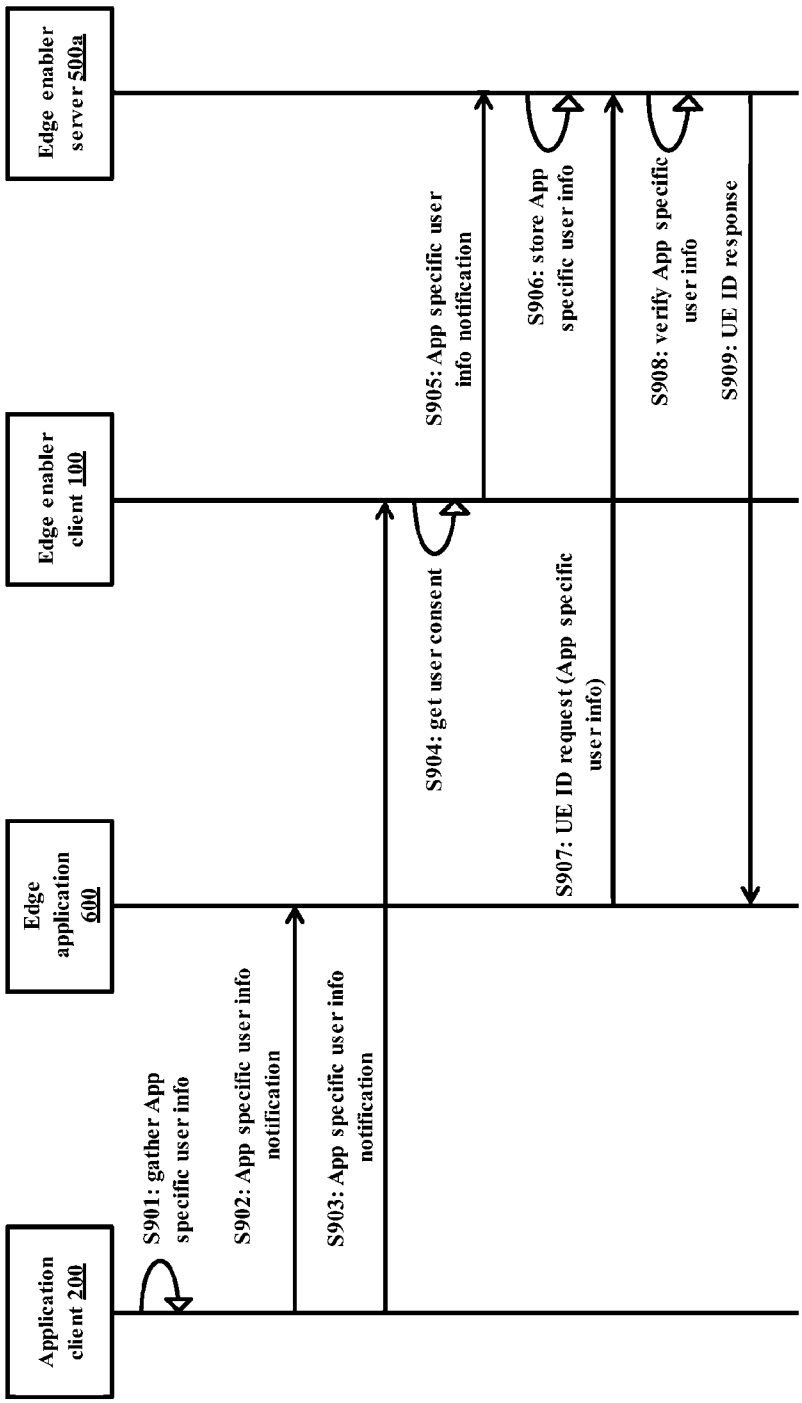
[Fig. 7]


Application client 200
Edge application 600
Edge enabler server 500a
Edge enabler client 100
S701: user consent grant
S702:nonce request
S703:nonce response
S704: user consent grant request (nonce)
S705: user consent grant response
S706: user consent grant notification
S707: user consent verification request
S708: user consent verification response
S709: store user consent

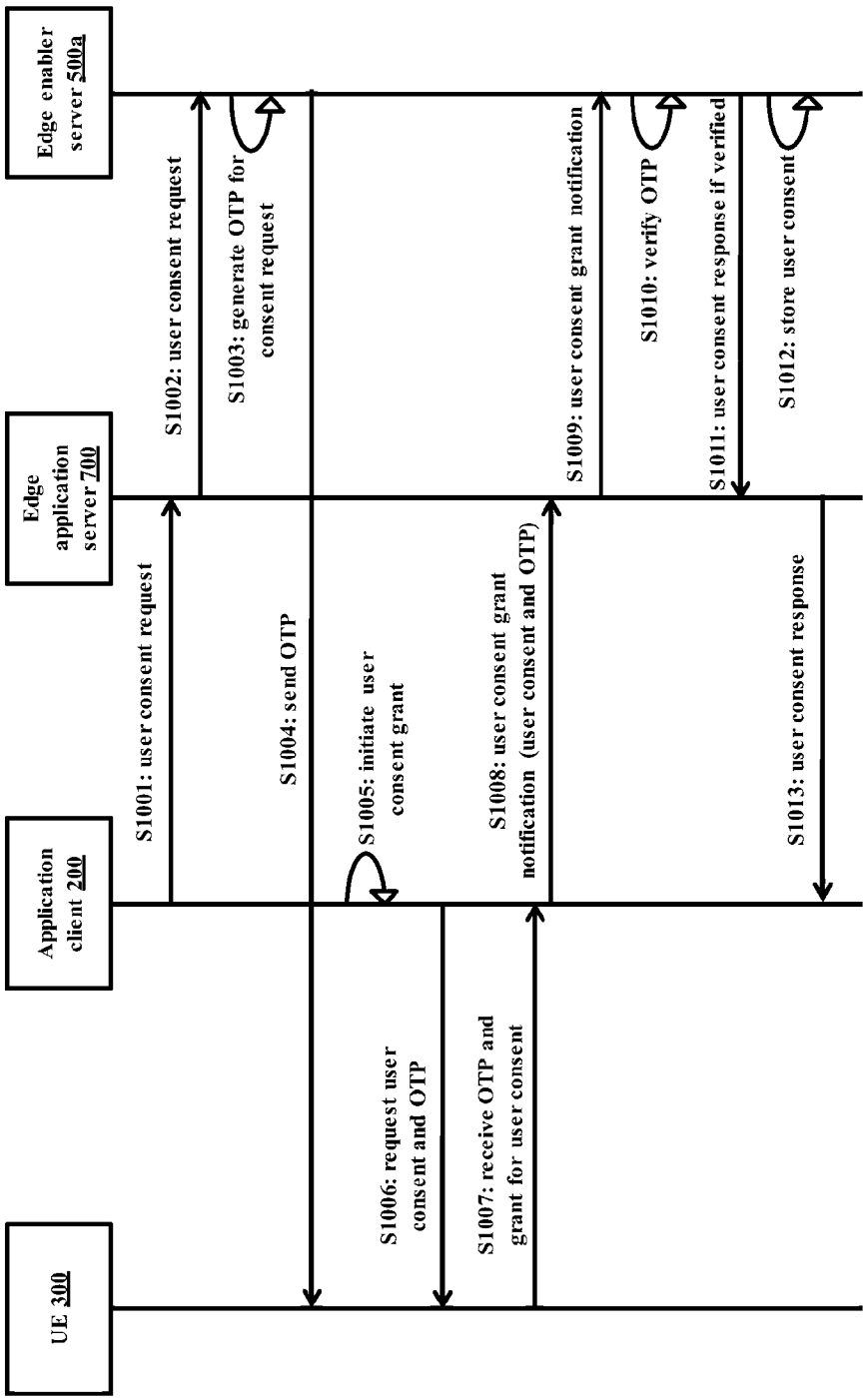
[Fig. 8]


Edge enabler server 500a
Edge enabler client 100
Edge application 600
Application client 200
S801: user consent grant
S802: user consent grant notification
S803: user consent grant notification
S804: user consent grant request
S805: user consent grant response
S806: store user consent

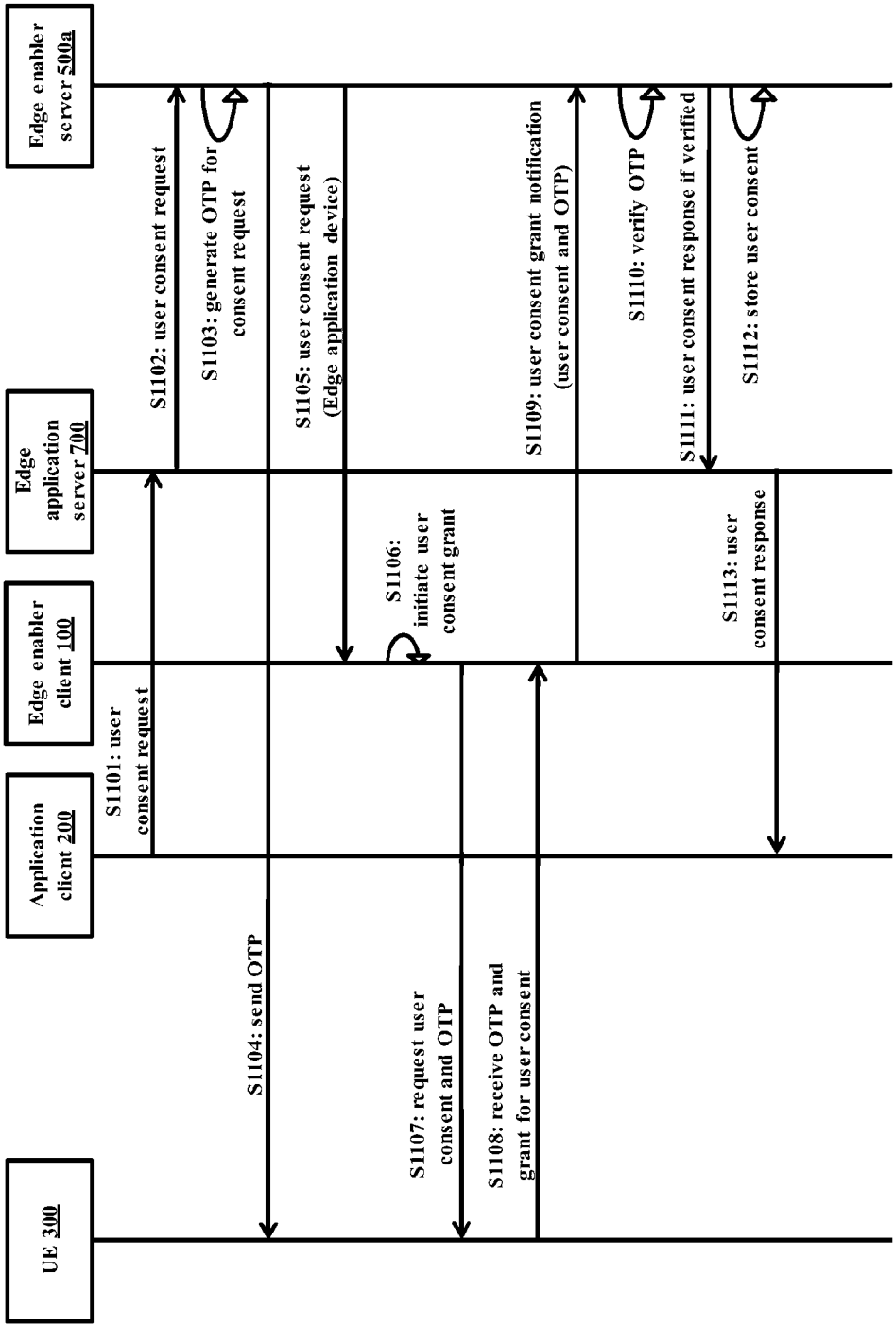
[Fig. 9]


Application client 200
Edge application 600
Edge enabler client 100
Edge enabler server 500a
S901: gather App specific user info
S902: App specific user info notification
S903: App specific user info notification
S904: get user consent
S905: App specific user info notification
S906: store App specific user info
S907: UE ID request (App specific user info)
S908: verify App specific user info
S909: UE ID response

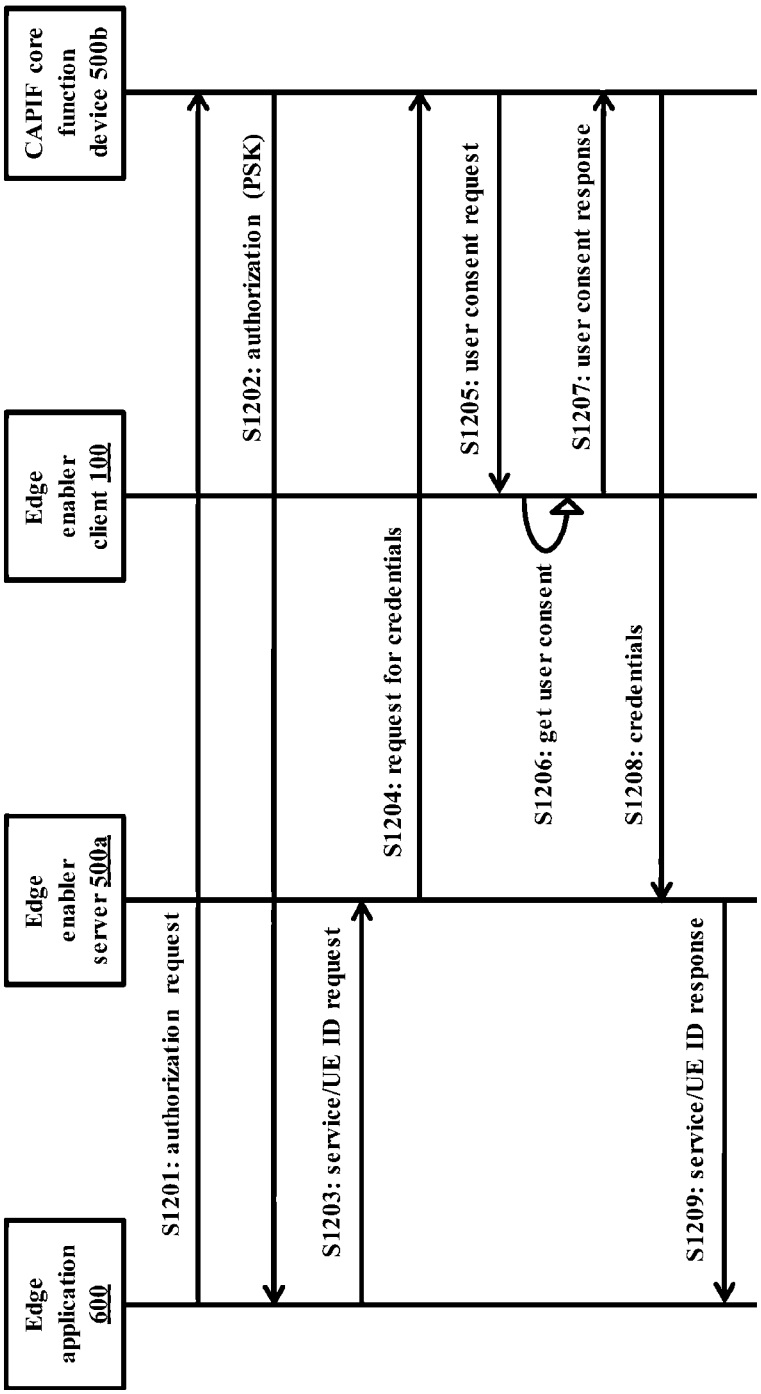
[Fig. 10]


Edge enabler server 500a
Edge application server 700
Application client 200
UE 300
S1001: user consent request
S1002: user consent request
S1003: generate OTP for consent request
S1004: send OTP
S1005: initiate user consent grant
S1006: request user consent and OTP
S1007: receive OTP and grant for user consent
S1008: user consent grant notification (user consent and OTP)
S1009: user consent grant notification
S1010: verify OTP
S1011: user consent response if verified
S1012: store user consent
S1013: user consent response

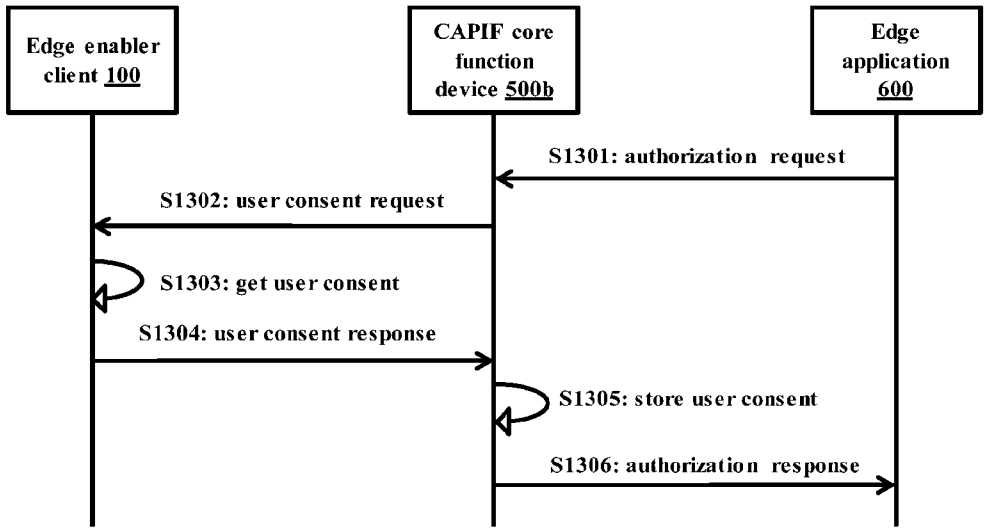
[Fig. 11]


Edge enabler server 500a
Edge application server 700
Edge enabler client 100
Application client 200
UE 300
S1101: user consent request
S1102: user consent request
S1103: generate OTP for consent request
S1104: send OTP
S1105: user consent request (Edge application device)
S1106: initiate user consent grant
S1107: request user consent and OTP
S1108: receive OTP and grant for user consent
S1109: user consent grant notification (user consent and OTP)
S1110: verify OTP
S1111: user consent response if verified
S1112: store user consent
S1113: user consent response

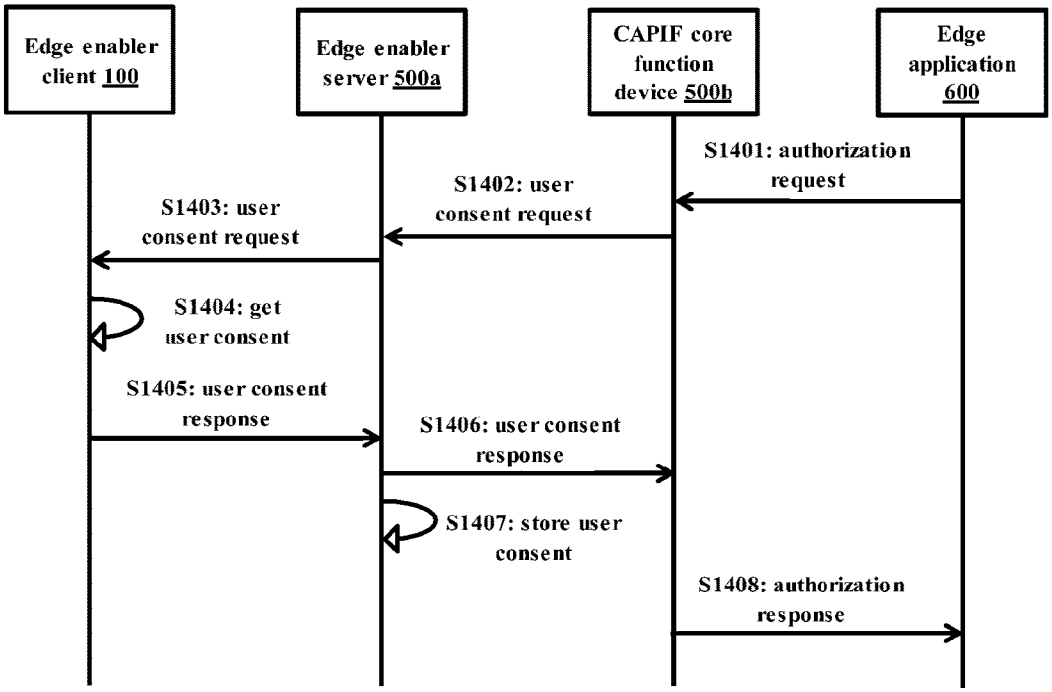
[Fig. 12]


Edge application 600
Edge enabler server 500a
Edge enabler client 100
CAPIF core function device 500b
S1201: authorization request
S1202: authorization (PSK)
S1203: service/UE ID request
S1204: request for credentials
S1205: user consent request
S1206: get user consent
S1207: user consent response
S1208: credentials
S1209: service/UE ID response

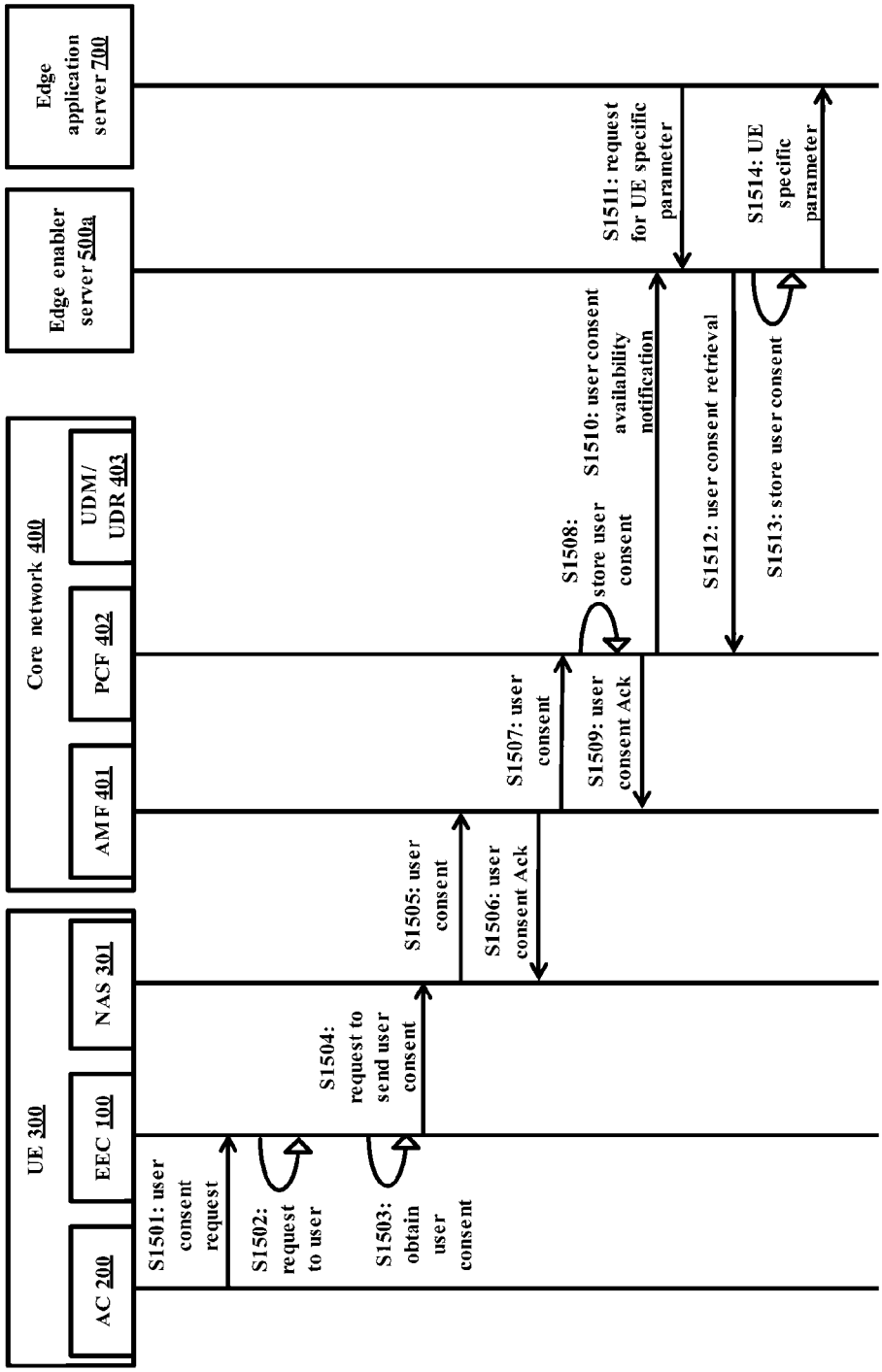
[Fig. 13]


Edge enabler client 100
CAPIF core function device 500b
Edge application 600
S1301: authorization request
S1302: user consent request
S1303: get user consent
S1304: user consent response
S1305: store user consent
S1306: authorization response

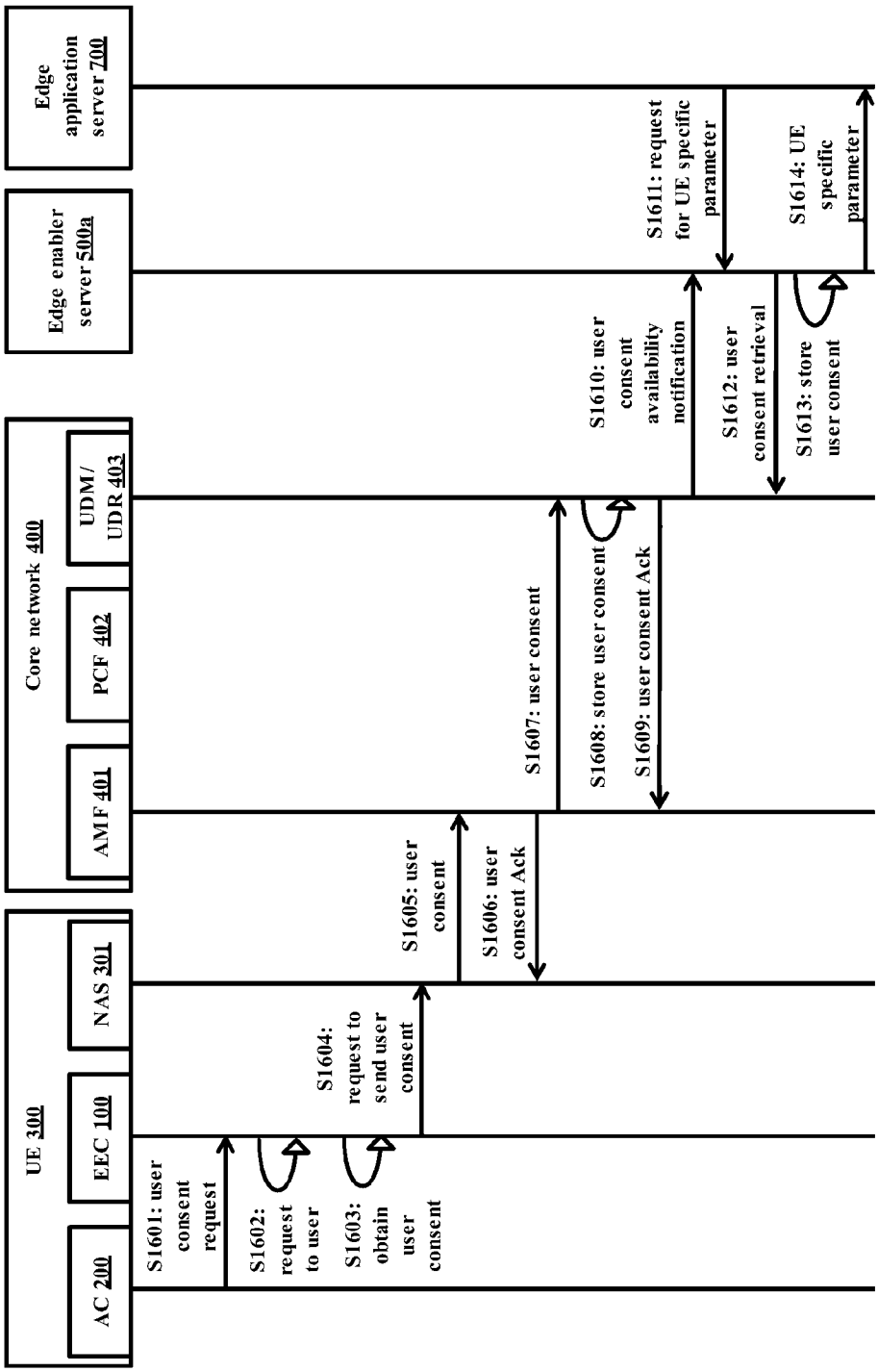
[Fig. 14]


Edge enabler client 100
Edge enabler server 500a
CAPIF core function device 500b
Edge application 600
S1401: authorization request
S1402: user consent request
S1403: user consent request
S1404: get user consent
S1405: user consent response
S1406: user consent response
S1407: store user consent
S1408: authorization response

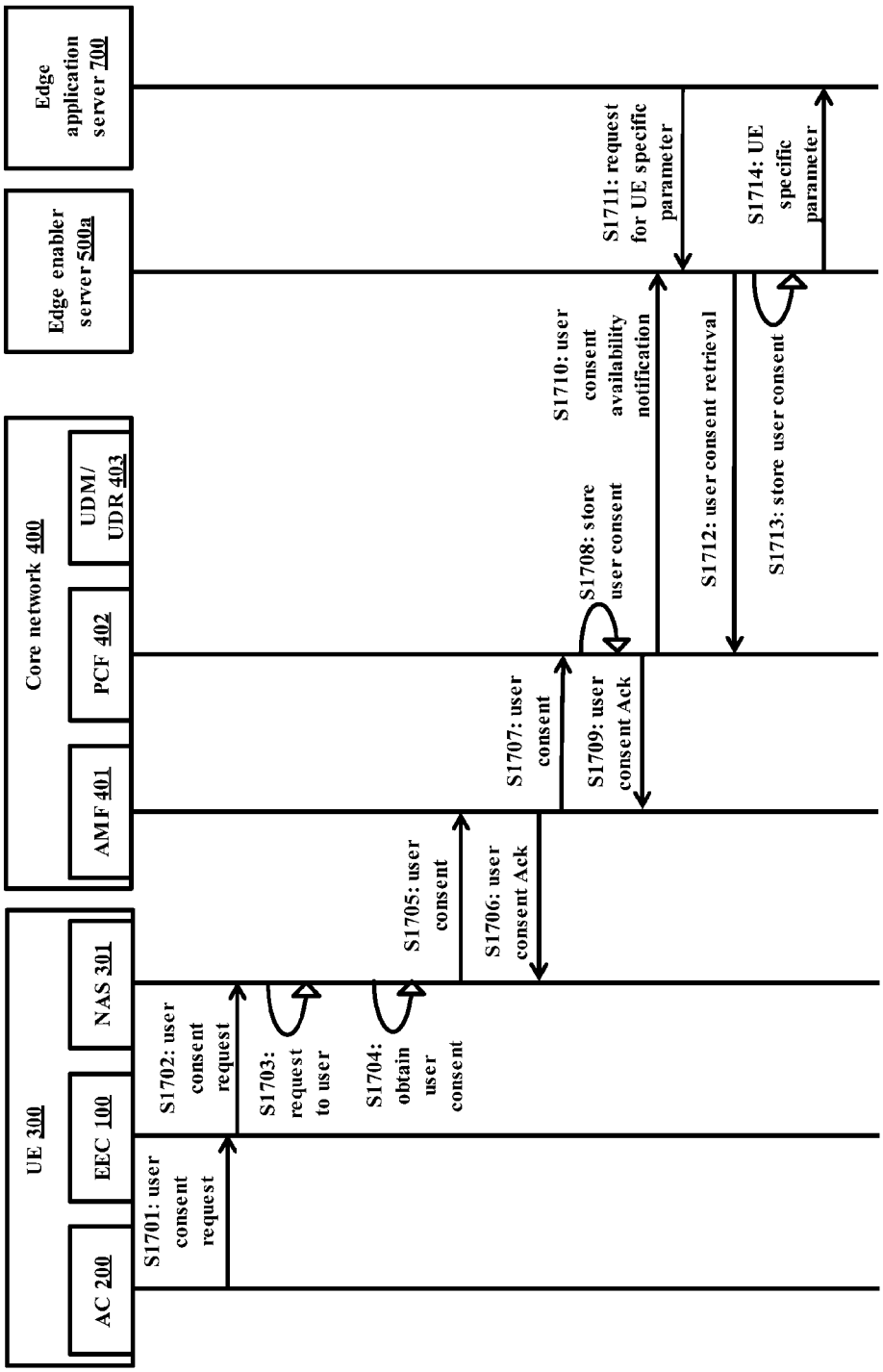
[Fig. 15]


UE 300
AC 200
EEC 100
NAS 301
Core network 400
AMF 401
PCF 402
UDM/ UDR 403
Edge enabler server 500a
Edge application server 700
S1501: user consent request
S1502: request to user
S1503: obtain user consent
S1504: request to send user consent
S1505: user consent
S1506: user consent Ack
S1507: user consent
S1508: store user consent
S1509: user consent Ack
S1510: user consent availability notification
S1511: request for UE specific parameter
S1512: user consent retrieval
S1513: store user consent
S1514: UE specific parameter

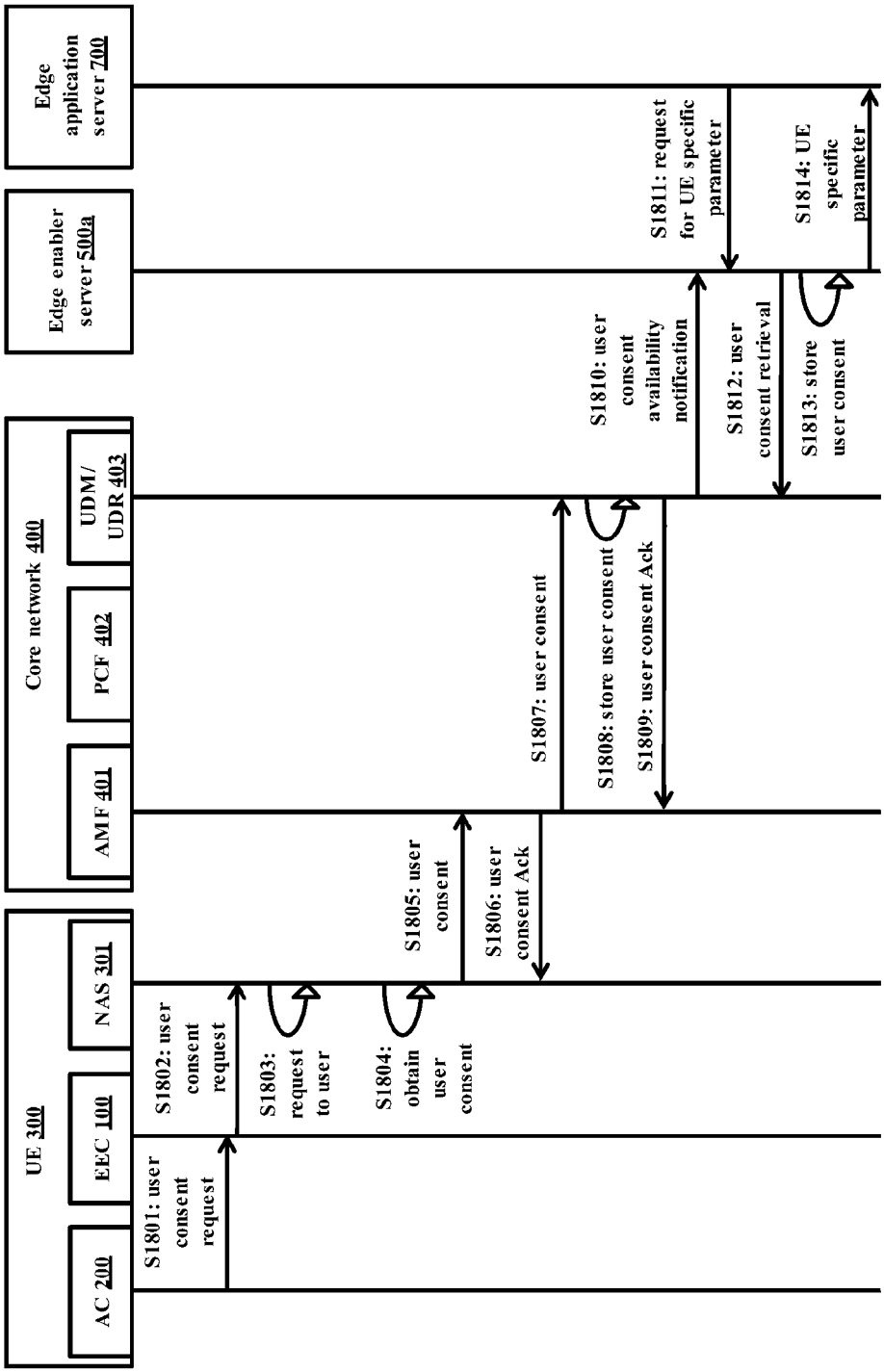
[Fig. 16]


UE 300
AC 200
EEC 100
NAS 301
Core network 400
AMF 401
PCF 402
UDM/ UDR 403
Edge enabler server 500a
Edge application server 700
S1601: user consent request
S1602: request to user
S1603: obtain user consent
S1604: request to send user consent
S1605: user consent
S1606: user consent Ack
S1607: user consent
S1608: store user consent
S1609: user consent Ack
S1610: user consent availability notification
S1611: request for UE specific parameter
S1612: user consent retrieval
S1613: store user consent
S1614: UE specific parameter

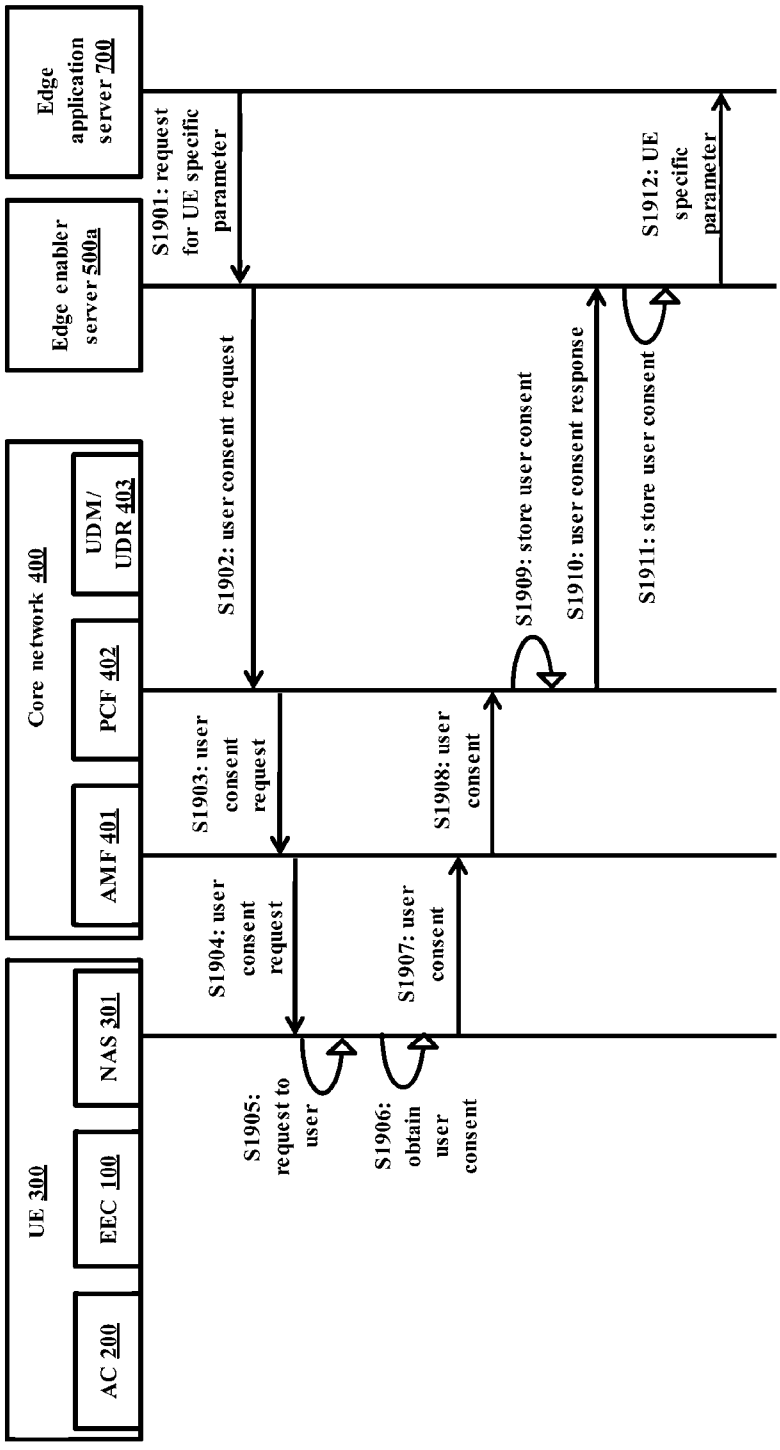
[Fig. 17]


UE 300
AC 200
EEC 100
NAS 301
Core network 400
AMF 401
PCF 402
UDM/ UDR 403
Edge enabler server 500a
Edge application server 700
S1701: user consent request
S1702: user consent request
S1703: request to user
S1704: obtain user consent
S1705: user consent
S1706: user consent Ack
S1707: user consent
S1708: store user consent
S1709: user consent Ack
S1710: user consent availability notification
S1711: request for UE specific parameter
S1712: user consent retrieval
S1713: store user consent
S1714: UE specific parameter

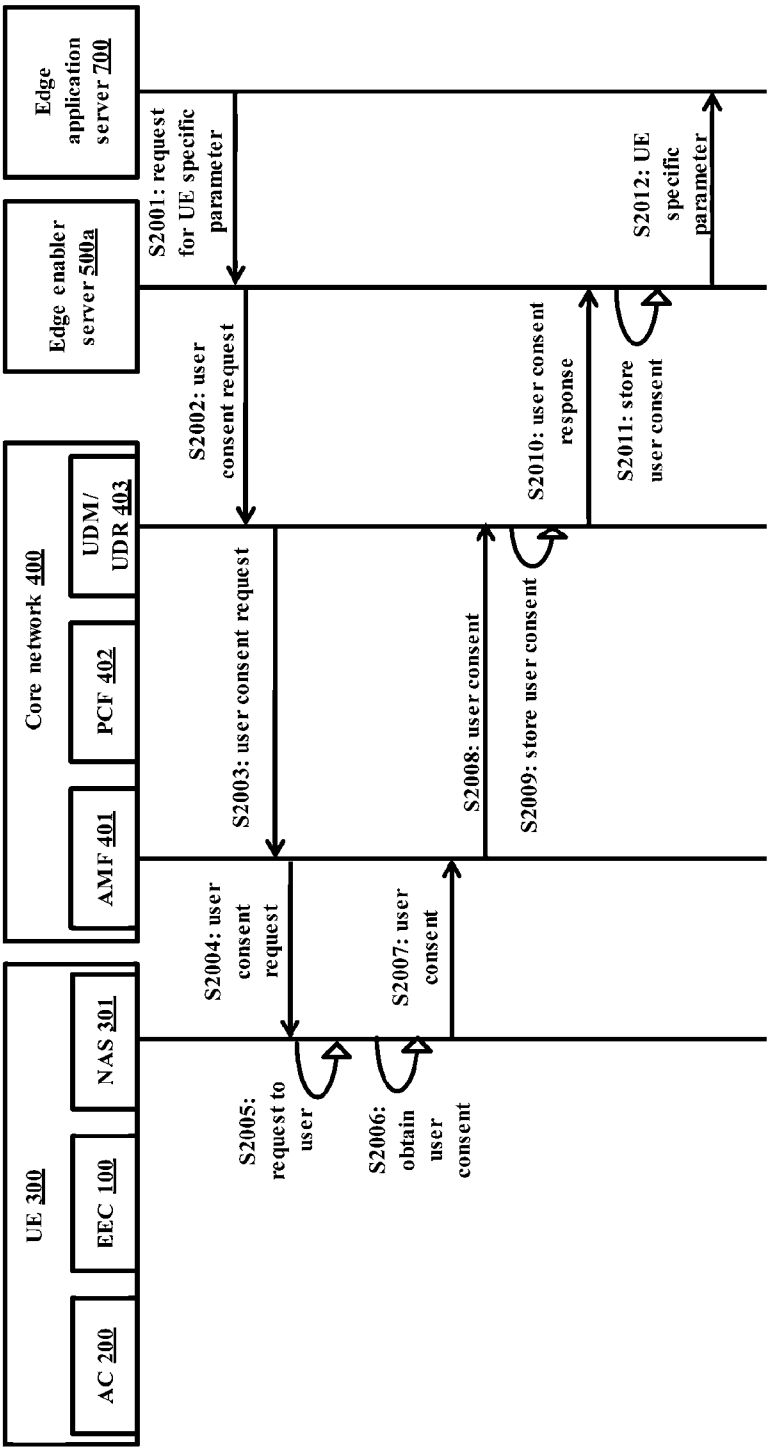
[Fig. 18]


UE 300
AC 200
EEC 100
NAS 301
Core network 400
AMF 401
PCF 402
UDM/ UDR 403
Edge enabler server 500a
Edge application server 700
S1801: user consent request
S1802: user consent request
S1803: request to user
S1804: obtain user consent
S1805: user consent
S1806: user consent Ack
S1807: user consent
S1808: store user consent
S1809: user consent Ack
S1810: user consent availability notification
S1811: request for UE specific parameter
S1812: user consent retrieval
S1813: store user consent
S1814: UE specific parameter

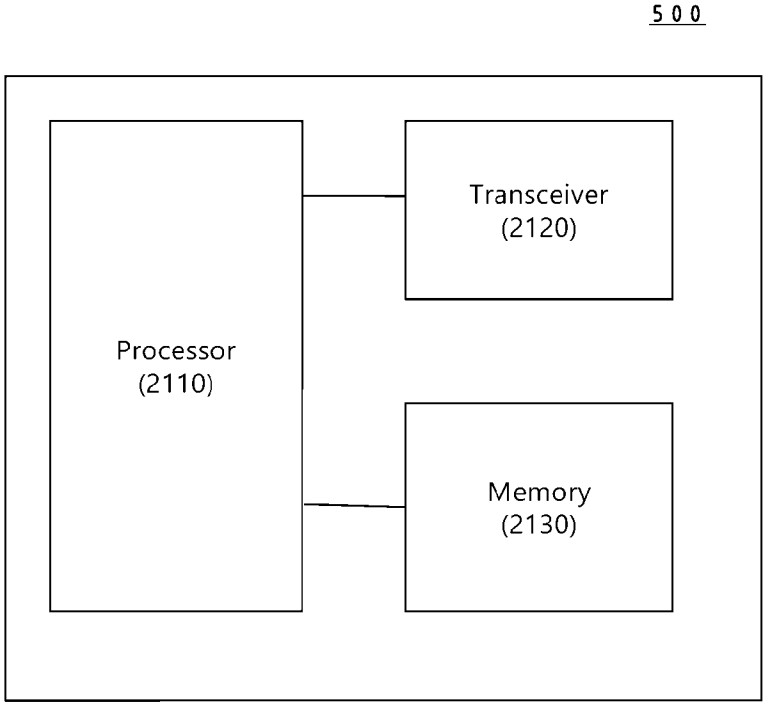
[Fig. 19]


Edge application server 700
Edge enabler server 500a
Core network 400
UDM/ UDR 403
PCF 402
AMF 401
UE 300
NAS 301
EEC 100
AC 200
S1901: request for UE specific parameter
S1902: user consent request
S1903: user consent request
S1904: user consent request
S1905: request to user
S1906: obtain user consent
S1907: user consent
S1908: user consent
S1909: store user consent
S1910: user consent response
S1911: store user consent
S1912: UE specific parameter

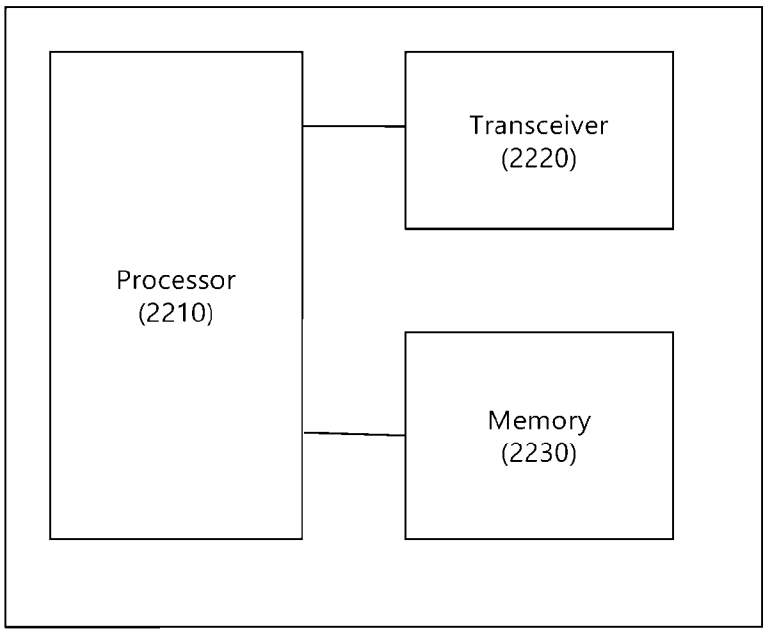
[Fig. 20]


Edge application server 700
Edge enabler server 500a
Core network 400
UDM/ UDR 403
PCF 402
AMF 401
UE 300
NAS 301
EEC 100
AC 200
S2001: request for UE specific parameter
S2002: user consent request
S2003: user consent request
S2004: user consent request
S2005: request to user
S2006: obtain user consent
S2007: user consent
S2008: user consent
S2009: store user consent
S2010: user consent response
S2011: store user consent
S2012: UE specific parameter

[Fig. 21]


500
Transceiver
(2120)
Processor
(2110)
Memory
(2130)

[Fig. 22]


2200
Transceiver
(2220)
Processor
(2210)
Memory
(2230)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/KR2020/007706

A. CLASSIFICATION OF SUBJECT MATTER

H04L 29/08(2006.01)i, H04L 29/06(2006.01)i

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)
H04L 29/08; G06F 15/16; H04L 29/06; H04L 9/08

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Korean utility models and applications for utility models
Japanese utility models and applications for utility models

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
eKOMPASS(KIPO internal) & Keywords: edge application, request, access, service, availability, user consent, authorizing, application specific user information, edge enabler client, one time password (OTP), update

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	'3GPP; TSG SA; Study on application architecture for enabling Edge Applications; (Release 17)', 3GPP TR 23.758 V0.2.0, 29 May 2019 sections 7.1.1, 7.6.1, 7.7.1; and figures 7.1.1-1, 7.6.1-1, 7.7.1-1	1-15
Y	'3GPP; TSG SA; Study on subscriber privacy impact in 3GPP; (Release 14)', 3GPP TR 33.849 V14.0.0, 22 March 2016 sections 3.2, 5.3.2.1, 5.4.1.1, 6.5.1-6.5.2, A.1.4	1-15
A	'3GPP; TSG SA; Security of the mission critical service; (Release 16)', 3GPP TS 33.180 V16.0.0, 13 June 2019 section 5.1.2.3	1-15
A	US 2019-0065731 A1 (INTERNATIONAL BUSINESS MACHINES CORPORATION) 28 February 2019 paragraphs [0003]-[0006], [0016]-[0022], [0068]-[0070]	1-15
A	US 10250708 B1 (AKAMAI TECHNOLOGIES, INC.) 02 April 2019 column 3, line 9 - column 4, line 48; and claims 1-10	1-15

☐ Further documents are listed in the continuation of Box C.

☒ 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
"D" document cited by the applicant in the international application
"E" earlier application or patent 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
22 September 2020 (22.09.2020)	**25 September 2020 (25.09.2020)**

Name and mailing address of the ISA/KR
International Application Division
Korean Intellectual Property Office
189 Cheongsa-ro, Seo-gu, Daejeon, 35208, Republic of Korea
Facsimile No. +82-42-481-8578

Authorized officer
YANG JEONG ROK
Telephone No. +82-42-481-5709

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.

PCT/KR2020/007706

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2019-0065731 A1	28/02/2019	CN 111034146 A	17/04/2020
		DE 112018004753 T5	10/06/2020
		GB 2579990 A	08/07/2020
		US 10586033 B2	10/03/2020
		US 10592656 B2	17/03/2020
		US 2019-0065730 A1	28/02/2019
		US 2020-0151318 A1	14/05/2020
		WO 2019-043539 A1	07/03/2019
US 10250708 B1	02/04/2019	US 2019-0230179 A1	25/07/2019
		WO 2019-133568 A1	04/07/2019