



HU000030670T2

(19) **HU****MAGYARORSZÁG****Szellemi Tulajdon Nemzeti Hivatala**(11) Lajstromszám: **E 030 670**(13) **T2**

EURÓPAI SZABADALOM SZÖVEGÉNEK FORDÍTÁSA

(21) Magyar ügyszám: **E 04 711904**(22) A bejelentés napja: **2004. 02. 17.**(51) Int. Cl.: **H04W 8/16** (2006.01)

(96) Az európai bejelentés bejelentési száma:

EP 20040711904

(86) A nemzetközi (PCT) bejelentési szám:

PCT/US 04/004670

(97) Az európai bejelentés közzétételi adatai:

EP 1593286 A1 **2004. 09. 02.**

(87) A nemzetközi közzétételi szám:

WO 04075594

(97) Az európai szabadalom megadásának meghirdetési adatai:

EP 1593286 B1 **2016. 11. 02.**

(30) Elsőbbségi adatok:

447563 P	2003. 02. 14.	US
490765 P	2003. 12. 12.	US
779109	2004. 02. 13.	US

(73) Jogosult(ak):

**QUALCOMM INCORPORATED, San Diego, CA
92121-1714 (US)**

(72) Feltaláló(k):

ARCENS, Suzanne, Santa Clara, CA 95051 (US)

(74) Képviselő:

**Danubia Szabadalmi és Jogi Iroda Kft.,
Budapest**(54) **Fokozott felhasználói magánszféra mobil állomás helymeghatározó szolgáltatások számára**

Az európai szabadalom ellen, megadásának az Európai Szabadalmi Közlönyben való meghirdetésétől számított kilenc hónapon belül, felszólalást lehet benyújtani az Európai Szabadalmi Hivatalnál. (Európai Szabadalmi Egyezmény 99. cikk(1))

A fordítást a szabadalmat az 1995. évi XXXIII. törvény 84/H. §-a szerint nyújtotta be. A fordítás tartalmi helyességét a Szellemi Tulajdon Nemzeti Hivatala nem vizsgálta.

(19)



(11)

EP 1 593 286 B1

(12)

EUROPEAN PATENT SPECIFICATION

(45) Date of publication and mention
of the grant of the patent:

02.11.2016 Bulletin 2016/44

(51) Int Cl.:

H04W 8/16 ^(2009.01)

(86) International application number:

PCT/US2004/004670

(21) Application number: **04711904.5**

(22) Date of filing: **17.02.2004**

(87) International publication number:

WO 2004/075594 (02.09.2004 Gazette 2004/36)

(54) ENHANCED USER PRIVACY FOR MOBILE STATION LOCATION SERVICES

ERHÖHTES BENUTZERPRIVATLEBEN FÜR MOBILSTATIONSPOSITIONSDIENSTLEISTUNGEN

RENFORCEMENT DE LA CONFIDENTIALITE DES DONNEES D'UN UTILISATEUR POUR DES
SERVICES D'EMPLACEMENT DE STATION MOBILE

(84) Designated Contracting States:
**AT BE BG CH CY CZ DE DK EE ES FI FR GB GR
HU IE IT LI LU MC NL PT RO SE SI SK TR**

(30) Priority: **14.02.2003 US 447563 P**
12.12.2003 US 490765 P
13.02.2004 US 779109

(43) Date of publication of application:
09.11.2005 Bulletin 2005/45

(60) Divisional application:
15190174.1 / 2 991 391
16164898.5 / 3 059 988

(73) Proprietor: **QUALCOMM INCORPORATED**
San Diego, CA 92121-1714 (US)

(72) Inventor: **ARCENS, Suzanne**
Santa Clara, CA 95051 (US)

(74) Representative: **Heselberger, Johannes**
Bardehle Pagenberg Partnerschaft mbB
Patentanwälte, Rechtsanwälte
Prinzregentenplatz 7
81675 München (DE)

(56) References cited:
WO-A1-02/093877 WO-A2-02/060191
US-A1- 2002 193 941 US-A1- 2003 008 672
US-B1- 6 360 102 US-B1- 6 505 048

EP 1 593 286 B1

Note: Within nine months of the publication of the mention of the grant of the European patent in the European Patent Bulletin, any person may give notice to the European Patent Office of opposition to that patent, in accordance with the Implementing Regulations. Notice of opposition shall not be deemed to have been filed until the opposition fee has been paid. (Art. 99(1) European Patent Convention).

Description

BACKGROUND

Field

[0001] 001 This invention relates to the field of location services for mobile devices, and more particularly to enhanced user control of privacy policy for responses to location requests.

Description of Related Art

[0002] 002 Location services (abbreviated as LCS, for "LoCation Services") for mobile telephones and wireless digital communication devices (collectively referred to hereinafter as Mobile Stations) are an increasingly important business area for wireless communication providers. This importance is reflected in the establishment of standards and functional specifications for LCS. Three exemplary LCS references are: 3rd Generation Partnership Project (3GPP), Technical Specification Group (TSG) Services and System Aspects, Functional stage 2 (SA2) description of LCS, Release 6, (3GPP TS 23.271 V6.0.0), June, 2002; Technical Document (TD) S2-022360, 3GPP TSG-SA2 Meeting #26, Toronto, Canada, August 19-23, 2002; and 3rd Generation Partnership Project (3GPP), Technical Specification Group (TSG) Services and System Aspects, Functional stage 2 (SA2) description of LCS, Release 6, (3GPP TS 23.271 V6.3.0), March, 2003. The references are referred to hereinafter as 3GPP-R1, 3GPP-R2, and 3GPP-R3 respectively.

[0003] 003 References 3GPP-R1 and 3GPP-R3 describe a functional model of an entire LCS system, including sections relating to user privacy. Reference 3GPP-R2 describes a network element, referred to as a Privacy Profile Register (PPR), that maintains the LCS privacy information of subscribers and that facilitates corresponding privacy functions. These references provide an overview of recent technology and standards relating to LCS and related LCS privacy operations. Numerous methods and apparatus for providing LCS to subscribers in accordance with these references are known to persons with ordinary skill in the communications arts.

[0004] 004 One known advantageous method for determining the location of a Mobile Station in a wireless communication system employs the Global Positioning System (GPS). Including a GPS device (or more generally, a Position Determination module, or "PDM") in the Mobile Station provides very accurate position determination capability. When a PDM is used as the primary means for providing accurate location information within a Mobile Station, the service provider network must contact the Mobile Station when requests for accurate location are received. Methods and apparatus for implementing the location service function using a PDM, such as using GPS in a Mobile Station, are well known to persons

of ordinary skill in the wireless communications arts. Handsets implementing LCS functions using GPS are currently available. An exemplary GPS system for mobile stations is described the reference "An Introduction to SnapTrack™ Server-Aided GPS Technology," M. Moe-glein and N. F. Krasner, Institute of Navigation (ION) GPS 1998 Proceedings, Sept. 15-18, 1998, pp. 333-344. A recent patent application that describes a GPS system suitable for mobile stations is "Method and Apparatus for Measurement Processing of Satellite Positioning System (SPS) Signals," L. Sheynblat and N. F. Krasner, United States Patent Application 20020050944, May 2, 2002.

[0005] 005 Disadvantageously, user control of privacy policy information is very limited and inflexible using existing LCS privacy methods wherein user privacy is managed by a service provided network. For example, in some exemplary prior art LCS privacy methods, various classes of requestor clients are defined by the service provider, and a user privacy profile, such as the PPR referred to above, based on these classes is established when the user initiates service. In accordance with these LCS privacy methods, the privacy profile designates certain requestor classes that have unrestricted access to the user location, and other requestor classes that have restricted access. Such restrictions may, for example, include an automatic denial of LCS information to specific restricted classes. The restrictions may also include a requirement that the user be notified and (optionally) approve LCS access requests by requestors from specified restricted classes. In these exemplary prior art systems, privacy profile modifications may only be effected by modifying the service agreement between the provider and the user. In cases where user location is primarily determined by a PDM resident within the Mobile Station, an additional modification option is effected by disabling the PDM. Although this option enhances privacy by enabling the user to prevent the retrieval of accurate position information, the usefulness of this approach is extremely limited because it prevents accurate location retrieval for all requestor classes until the PDM is once again enabled.

[0006] Another example is described in document WO02/060191. 006 The present disclosure is directed to a method and apparatus for LCS privacy management within a Mobile Station. The present disclosure enables convenient and flexible LCS control by a Mobile Station user.

SUMMARY

[0007] 007 The present disclosure relates to a method and apparatus for providing the geographical location of a wireless mobile station, and more particularly to methods and apparatus for providing enhanced user control of privacy policies that supervise responses to requests for location information. These requests are hereinafter referred to as location requests or, equivalently, as position requests.

[0008] 008 In one exemplary embodiment, a privacy control system for a Mobile Station comprises a Privacy Engine, a Position Determination Module (PDM), and a User Interface. The Privacy Engine is a software module that controls the responses of the Mobile Station to location requests.

[0009] 009 The Privacy Engine further includes a Privacy Policy. The Privacy Policy includes Privacy Classes for classifying location requestors and their associated location requests, and Privacy Rules for determining the response to location requests for each Privacy Class.

[0010] 010 A Privacy Class is defined by a list of location requestors and applications. The location requestors and applications may be individually specified, or grouped into categories or types, based on identifying information such as a URL, an Internet domain, or other data that may be supplied with a position request. A location request is classified according to the location requestor. Location requests can thereby be assigned to a Privacy Class based on information provided with the location request. Examples of Privacy Classes include, without limitation: a default Privacy Class for unknown or undeclared location request applications and requestor identities not specifically included in any other class; a default Privacy Class for trusted location request applications and requestor identities not specifically included in any other class; and user specified classes including location request applications and requestor identities identified by a URL or other identification data that may be provided with position request data.

[0011] 011 Each Privacy Class has an associated set of Privacy Rules for determining the response of the Privacy Engine to location requests. Examples include, without limitation: a rule specifying unrestricted access; a rule for default denial of access; a rule for access contingent on user notification and required approval; a rule for access with user notification but without required approval; a rule for access denial during user-selected time periods; a rule for access only for a defined approximation of location; *etc.* The Privacy Policy, the Privacy Classes, and the Privacy Rules determine how the Privacy Engine responds to each and all location requests.

[0012] 012 Advantageously, using the present inventive enhanced user privacy methods and apparatus, the Privacy Policy for a specific Mobile Station may be controlled or modified by the user via the User Interface in the Mobile Station. In one exemplary embodiment, the User Interface comprises a user interface having suitable input means such as a stylus, pointing device or keypad. In another embodiment of the present inventive concept, the Privacy Policy is controlled via a network application that connects to the Mobile Station through a wireless data network. In a further embodiment of the present inventive method, Privacy Policy may be controlled by an application residing in a local device, such as a laptop computer or personal digital assistant, wherein the device is operatively connected to the Mobile Station.

[0013] 013 Advantageously, the Mobile Station's Pri-

vacy Engine, including an initial Privacy Policy, may be received by (*i.e.*, downloaded to) the Mobile Station via a wireless data network.

5 BRIEF DESCRIPTION OF THE DRAWINGS

[0014]

10 014 FIGURE 1 is a block diagram of an exemplary communication system including a Mobile Station having a Privacy Engine adapted for use with the present inventive concept.

15 015 FIGURES 2A through 2D show a flow diagram of an exemplary method for providing Enhanced User Privacy in a Location Services application for use by Mobile Stations and other wireless communication devices.

20 016 Like reference numbers and designations in the various drawings indicate like elements.

DETAILED DESCRIPTION

25 **[0015]** 017 Throughout this description, embodiments and variations are described for the purpose of illustrating uses and implementations of the inventive concept. The illustrative description should be understood as presenting examples of the inventive concept, rather than as limiting the scope of the concept as disclosed herein.

30 **[0016]** 018 FIGURE 1 shows a block diagram of a wireless communication device and wireless communication system that can be adapted for use with the present inventive concept. As shown in FIGURE 1, one exemplary embodiment includes a Mobile Station 102 comprising a User Interface 106, a Wireless Network Communication Module 112, an Applications block 114, a Local Communication Module 118, a Privacy Engine 120, a Position Determination Module 122, and Other Modules 124.

35 **[0017]** 019 As shown in FIGURE 1, in one embodiment of the present inventive concept, the Wireless Network Communication Module 112 provides a wireless data connectivity between the Mobile Station 102 and external data networks 110. The external data networks 110 may comprise a variety of network systems. For example, in one embodiment an external data network may comprise wireless service provider network. As another example, an external data network may be an Internet Service Provider that provides a connection to receive and transmit data between the Mobile Station and the Internet. In general, the external data networks 110 comprise any data system capable of transmitting and receiving data to and from a Mobile Station using wireless communication. As shown in FIGURE 1, the Wireless Network Communication Module 112 is also operatively coupled to the Applications block 114 and the Privacy Engine 120. The Wireless Communication Module 112 receives and transmits data from the Application block 114 and the Privacy En-

gine 120.

[0018] 020 In one embodiment, the Applications block 114 comprises location applications that may require a position estimate of the Mobile Station. These location applications may be MS resident, which do not need interaction with the network, or may involve interaction with a location server in the network (e.g. module 108) and therefore act as a location client. For this exemplary embodiment the Applications block 114 also comprises other applications relating to network data communications and other functions of Mobile Station. Examples of such applications include, without limitation: email clients, web browsers, ftp clients, and other software applications for receiving or downloading data, data files and software instructions to the Mobile Station 102. The Applications block 114 is coupled to the Wireless Communication Module 112 to receive and transmit data and thereby communicate with the external data networks 110. The Applications block 114 is also operatively coupled to the User Interface 106 to receive and transmit data for user operation and communication with various applications. The Applications block 114 is further operatively coupled to the Privacy Engine 120 to receive and transmit data. Such data may comprise location request and response data. Such data may also comprise received or downloaded software instructions to create, modify, and implement functions and capabilities of the Privacy Engine 120. Alternatively, data to create, modify or implement functions of the Privacy Engine may be received directly from the Wireless Communication Module 112, which is also operatively coupled to the Privacy Engine 120 to receive and transmit data. As a further alternative, data to create, modify or implement functions of the Privacy Engine may be received and executed by components of the Mobile Station not shown in FIGURE 1. Such components are well known to those skilled in the communications arts, and may, for example, comprise Application Specific Integrated Circuits (ASICs), Application Programming Interfaces (API), Random Access Memory (RAM), Read Only Memory (ROM), etc. Exemplary methods and systems for downloading and executing applications in Mobile Stations via wireless networks are described by Lundblade, et al., "Safe Application Distribution and Execution in a Wireless Environment," U.S. Patent Application Publication No. US 2002/0183056 A1, Dec. 5, 2002.

[0019] 021 The Local Communication Module 118 provides a means for optionally receiving and transmitting data between the Mobile Station 102 and an external local applications module 116. In one embodiment, the external local applications module 116 resides on a locally connected device such as a personal computer, laptop, or personal digital assistant. The Module 118 provides connectivity to the locally connected device. The Local Communication Module 118 is also operatively coupled to the Privacy Engine 120 to receive and transmit data. Such data may include software instructions that create, modify, and implement the functions and capabilities of

the Privacy Engine 120. Additionally, these data may include input and output data for location applications (applications requiring location data) that are running on a separate device such as a laptop that is connected to the MS via infrared, Bluetooth, USB cable, or other means that are distinct from the network connectivity provided by the Wireless Communication module 112. Routing these location data to the Privacy Engine 120 facilitates privacy management for location requests by local applications as described hereinbelow.

[0020] 022 As described above, the Privacy Engine 120 is coupled to the elements 112, 114, and 118 to receive and transmit data. The Privacy Engine 120 is also coupled to receive and transmit data with the User Interface 106, the Position Determination Module 122, and the Other Modules 124. The functions and operation of the Privacy Engine 120 are specified hereinbelow.

[0021] 023 The User Interface 106 provides a means for a Mobile Station user to receive information from, provide instructions to, and operate the applications and functions embodied in the Applications block 114 and the Privacy Engine 120. The User Interface 106 may, for example, comprise a graphical user interface and suitable input means such as a touch screen, pointing device or keypad. The User Interface 106 may also comprise means to transmit and receive sounds, voice commands, or any other means for receiving information from, providing instructions to, and operating the software modules, applications and digital devices coupled to the Mobile Station 102.

[0022] 024 The Position Determination Module (PDM) 122 generates data that represents the location of the Mobile Station 102. One well known example of a suitable PDM employs a Global Positioning System (GPS) device or method. However, the current teachings comprehend the utilization of any PDM having a capability for providing position or location data to the Mobile Station 102. For example, the PDM may employ such well known positioning methods as assisted GPS (AGPS), Advanced Forward Link Trilateration (AFLT), Time of Arrival (TOA), Enhanced Observed Time Difference (E-OTD), positioning based on identifying the wireless communication cells within which the MS is operating (cell-based positioning), etc. These methods are well known to persons skilled in the communication arts and do not require description herein.

[0023] 025 The Other Modules block 124 represents software modules and hardware components for implementing or augmenting functions of the Mobile Station. These software modules and hardware components may, for example, include Application Specific Integrated Circuits (ASICs), Application Programming Interfaces (API), Random Access Memory (RAM), Read Only Memory (ROM), a Subscriber Identity Module (SIM) or Universal Subscriber Identity Module (USIM), a camera, etc. Although the connections for the Other Modules block 124 are not shown in FIGURE 1, persons skilled in the art will readily understand how the modules and compo-

nents in the Other Modules block 124 are operably coupled within the Mobile Station as required for functionality.

[0024] 026 Referring still to FIGURE 1, in one exemplary embodiment, a Privacy Management Server 104 comprises a Software application that is connected to the external data networks 110 to receive and transmit data. The Privacy Management Server 104 is coupled to the external data networks 110 to exchange data with the Wireless Network Communication Module 112. The Privacy Management Server 104 communicates with the Privacy Engine 120 via the external data networks 110 and the Wireless Network Communication Module 112. The Privacy Management Server 104 may receive and transmit data to the Network Applications block 114 via the external data networks 110 and the Wireless Network Communication Module 112. Data conveyed between the Privacy Management Server 104, the Network Applications block 114, and the Privacy Engine 120 may include software instructions that create, modify, and implement the functions or capabilities of the Privacy Engine 120. Likewise, data conveyed between the Privacy Management Server 104 and the Privacy Engine 120 via the Communication Module 112 may include software instructions that create, modify, and implement the functions and capabilities of the Privacy Engine 120. In general, data conveyed between the Privacy Management Server 104 and the elements comprising the Mobile Station 102 may be used to create, modify or implement software modules within the Mobile Station 102 that facilitate or relate to LCS and privacy management.

[0025] 027 The Location Request Application block 108 of FIGURE 1 represents Location Request Applications connected via the external data networks 110 to receive and transmit data to the Mobile Station 102. Location Request Applications 108 is coupled, via the external data network 110 and the Wireless Network Communication Module 112, to receive and transmit data to the Privacy Engine 120. The transmission and reception of Position Request and position reply data between the Location Request Applications block 108 and the Privacy Engine 120 is described hereinbelow.

Exemplary Privacy Policy

[0026] 028 In one exemplary embodiment, the Privacy Engine 120 is a software module that performs operations to control the responses of the Mobile Station to requests for location information. These requests are herein referred to as location requests or, equivalently, as position requests.

[0027] 029 The Privacy Engine further includes a Privacy Policy. The Privacy Policy is a component of the Privacy Engine that includes Privacy Classes for classifying location requestors and their associated location requests, and Privacy Rules for determining the response to location requests for each Privacy Class.

[0028] 030 A Privacy Class is defined by a list of loca-

tion requestors and applications. The location requestors and applications may be individually specified, or grouped into categories or types, based on identifying information such as a URL, an Internet domain, or other data which may be supplied with a position request. A location request is classified according to the location requestor. Location requests can thereby be assigned to a Privacy Class based on information provided with the location request. Examples of Privacy Classes include, without limitation: a default Privacy Class for unknown or undeclared location request applications and requestor identities not specifically included in any other class; a default Privacy Class for trusted location request applications and requestor identities not specifically included in any other class; and user specified classes including location request applications and requestor identities identified by a URL or other identification data that may be provided with position request data.

[0029] 031 Each Privacy Class has a related set of Privacy Rules for determining the response of the Privacy Engine to location requests. Examples include, without limitation: a rule specifying unrestricted access; a rule specifying default denial of access; a rule specifying access contingent on user notification and required approval; a rule specifying access with user notification but without required approval; a rule specifying access denial during user-selected time periods; a rule specifying access only for a defined approximation of location; *etc.* The Privacy Policy, the included Privacy Classes, and the included Privacy Rules determine how the Privacy Engine responds to each and all location requests.

Exemplary Initialization and Software Upgrade Method

[0030] 032 In one exemplary embodiment of the present inventive concept, a Mobile Station without user privacy control can be initially provided with software modules to implement Enhanced User Privacy for Mobile Station LCS by receiving or downloading data from a network server. The software data and instructions for installing and operatively implementing the Privacy Engine 120 (FIGURE 1), including an initial Privacy Policy, can be received or downloaded to the Mobile Station 102 from a network server (for example, the Privacy Management Server 104 of FIGURE 1, or other network servers not shown) via the Wireless Communication Module 112. Receiving and installing the received or downloaded data may be performed by a browser or other component in the Network Applications module 114 or by components included in the Other Modules 124. Methods for receiving or downloading applications and software modules to Mobile Stations via a wireless network connection are well known to persons of ordinary skill in the wireless communications arts. As noted hereinabove, exemplary methods and systems for downloading and executing applications in Mobile Stations via wireless networks are described by the Lundblade reference. In one embodiment, the Mobile Station includes a software platform to

assist interfacing applications to the Mobile Station, such as the Binary Runtime Environment for Wireless™ (BREW) software developed by QUALCOMM Incorporated, headquartered in San Diego, California.

[0031] 033 Software upgrades and modifications of the Privacy Engine 120 (still referring to FIGURE 1), the Privacy Policy and other Mobile Station software modules and components can also be received or downloaded from a network server as described above. In particular, the user (or other entity having permission to do so), may update the Privacy Policy using the wireless network connection. Alternatively, the user may also update the Privacy Policy using the User Interface 106. In another alternative, the user may update the Privacy Policy by inputting data using an external local application (as represented by External Local Applications block 116) connected via the Local Communication Module 118. In yet another alternative, the user may input user-specific Privacy Policy data using a removable data storage device (not shown in FIGURE 1). User-specific Privacy Policy data include Privacy Classes and Privacy Rules that may be selected, modified or created according to the requirements or preferences of the mobile station user. In one advantageous embodiment of the present inventive concept, the Mobile Station 102 is provided by the manufacturer or service provider with an initial or default Privacy Engine that includes a generic Privacy Policy. The generic Privacy Policy is then customized by the user to include user-specific Privacy Classes and Privacy Rules by one or more of the following methods: 1) downloading user-specific Privacy Policy data from a network; 2) inputting user-specific Privacy Policy data using the User Interface; 3) using an external local application in a locally connected device to input user-specific Privacy Policy data; or 4) using a removable data storage device to input previously stored user-specific Privacy Policy data. An exemplary implementation of removable data storage devices, such as Subscriber Identity Modules, Universal Subscriber Identity Modules or Removable Identity Modules, is described hereinbelow.

Exemplary Method of Operation for Enhanced User Privacy Control

[0032] 034 FIGURES 2(a)-2(d) illustrate a unified flow-chart diagram for an exemplary method of Enhanced User Privacy for use in Mobile Station LCS. Flow connections between FIGURES 2(a) and 2(b) are represented by the elements 214, 220, 230, and 232. Likewise, flow connections between FIGURES 2(a) and 2(c) are represented by the elements 202, 208 and 223. Flow connection between FIGURES 2(b) and 2(c) is represented by the element 258. Flow connections between FIGURES 2(b) and 2(d) are represented by the elements 214 and 246. Flow connection between FIGURES 2(c) and 2(d) is represented by the element 246.

[0033] 035 The element 202 in FIGURE 2(a) represents a state during which the Privacy Engine 120 (FIG-

URE 1) awaits reception of a request for location data information (i.e., a position request). At the STEP 204 the Privacy Engine 120 receives a position request via the data connections described hereinabove with reference to FIGURE 1. In reference to the present exemplary implementation, the Position Request data may comprise any of the following information: 1) network address and type of Location Request Application; 2) requestor category (e.g., emergency service, commercial service, individual person); 3) requestor identity, if applicable; 4) code word or digital certificate for verification of requestor identity; 5) requested Quality of Service (QoS). It shall be obvious to those of ordinary skill in the communications arts that the scope of the present teachings comprehends use of other types of Position Request data such as, for example, geographical area information, user information, requestor information, coordinate system, etc., as may be required to implement other embodiments.

[0034] 036 Referring again to FIGURE 2 (a), at the STEP 206, a Position Request Counter is initialized to a value of zero. The value zero represents the case where only one Position Request has been received. If subsequent Position Requests are received while a first Position Request is being processed, the Position Request Counter is incremented and decremented as described hereinbelow. The purpose of the Position Request Counter is for management of multiple concurrent position requests.

[0035] 037 The element 208 represents a flow connection from FIGURE 2(c). As described below, Position Request data will be processed by the inventive method subsequent to a STEP 286 of FIGURE 2(c) via the flow connection 208 only if a subsequent Position Request is received while a prior Position Request is being processed.

[0036] 038 At the STEP 210, the Privacy Engine 120 (FIGURE 1) invokes a selected Privacy Policy that assigns a Privacy Class to the Position Request received during STEP 204 (or via the element 208). As described above, the Privacy Policy comprises a list for assigning Privacy Classes to Position Requests, and Privacy Rules for decisions based on the assigned Privacy Classes.

[0037] 039 Referring again to FIGURE 1, the Privacy Engine 120 may optionally invoke the Applications module 114 the Other Modules 124, or Mobile Station modules and components not shown in the Figure, to perform classification of the Position Request data. For example, a network application may be invoked to verify digital certificate data.

[0038] 040 Referring again to FIGURE 2(a), at a STEP 212 the Position Request data are evaluated to determine whether the Position Request is an Emergency Service Request. In accordance with usual statutory requirements, an Emergency Service Request shall override the Privacy Policy, and position data shall be returned to the requestor as expeditiously as possible. For an Emergency Service Request the method proceeds

via the flow connection 214 to a STEP 256 (FIGURE 2(b)) to bypass the Privacy Policy and the expedite response. For a non-emergency request, the method proceeds to a STEP 216.

[0039] 041 At the STEP 216 the Position Request data are evaluated to determine if there are other requirements that necessitate overriding the Privacy Policy. For example, certain countries may require an override for requests originating from law enforcement or other government agencies. If an override is required, the method proceeds via the flow connection 214 to the STEP 256 to expedite processing. If an override is not required, the method proceeds to a STEP 218.

[0040] 042 Referring again to FIGURE 2(a), at the STEP 218, the Privacy Engine 120 (FIGURE 1) invokes the Privacy Policy to determine whether the Position Request should be denied based on the rules associated with the Privacy Class assigned to the request. Denial of a request position information may be determined based upon a plurality of criteria. In a first example, the request may be denied because the requestor is a commercial entity, and the assigned Privacy Class for commercial entities specifies automatic denial. In a second example, the request may be denied because the requestor identity is a private individual who has been placed in a Privacy Class with a rule specifying automatic denial. In a third example, the request may be denied because the Position Request data does not include a digital certificate or password that verifies identity of the requestor, and the default Privacy Class for this category includes a rule specifying automatic denial. In a fourth example, the user may have chosen to designate that all Position Requests, other than those related to emergency services, be placed in a Privacy Class specifying automatic denial during specified time periods. It will be obvious to those skilled in the wireless communications art that many other examples are comprehended within the scope of the present teachings.

[0041] 043 If a decision is made at the STEP 218 to deny the Position Request, then no position will be computed and the method proceeds to a STEP 222 whereat a denial of service message is transmitted to a Location Request Application. As described below in more detail in reference to the description of the flow diagram of FIGURE 2(b), the STEP 222 may also be implemented via flow connection 220 following STEPS 238 or 242 of FIGURE 2(b). Following the STEP 222, the inventive method proceeds to a STEP 282 of FIGURE 2(c) via the process flow connection 223. As will be explained more fully hereinbelow, at the STEP 282 the method checks the Position Request Counter to determine whether additional position requests are queued before either returning to the idle state process STEP 202, or executing further process steps.

[0042] 044 Returning to FIGURE 2(a), if a determination is made at the decision STEP 218 that the request should not be denied, a Privacy Policy is invoked at a STEP 224 to determine whether user notification is re-

quired. If user notification is determined not to be required at the STEP 224, the inventive method proceeds via the flow connection 230 to a STEP 250 of FIGURE 2(b) for further processing. This is described in more detail below in regard to the description of FIGURE 2(b).

[0043] 045 If user notification is determined at the STEP 224 to be required, then at a STEP 226 notification is conveyed to the user via the User Interface 106 (FIGURE 1). The User Interface 106 may employ a sound, image, vibration, or other means to alert the user that a Position Request has been granted, and graphical, text, or audible display or other presentation may be used to convey information relating to the Position Request, such as requestor category, requestor identity, and/or requested QoS.

[0044] 046 At a STEP 228 the Privacy Engine 120 invokes the Privacy Policy to determine if the Position Request requires user response in addition to user notification. If not, then the inventive method proceeds via flow connection 230 to the STEP 250 of FIGURE 2(b) for further processing. If a user response is required, then a timed wait for user response is initiated at a STEP 232.

[0045] 047 FIGURE 2(b) is a continuation of the unified flow diagram of FIGURE 2 (a)-2 (c), proceeding from the STEP 232 (timed wait for user response). STEPS 234, 236, and 238 represent possible events that may terminate the timed wait period at the STEP 232. The STEP 240 represents an event that may occur during the timed wait period at the STEP 232.

[0046] 048 If the timed wait for user response at the STEP 232 is terminated by the event represented at the STEP 234, User Accepts Request, then Position Request data are transferred to the STEP 250 for further processing.

[0047] 049 If the timed wait for user response at the STEP 232 is terminated without user response by the event represented at the STEP 236, Time Out, then Position Request data are transferred and the method proceeds to a STEP 242 for further processing. The STEP 242 invokes the Privacy Policy to determine if an absence of user response requires denial. If an absence of user response requires denial, then the inventive method proceeds via the flow connection 220 to the STEP 222 (shown in FIGURE 2(a)). If absence of user response does not require denial, then the method proceeds to the STEP 250 for further processing.

[0048] 050 If the timed wait for user response of the STEP 232 is terminated by the event represented at the STEP 238 (User Denies Request), then the inventive method proceeds via the flow connection 220 to the STEP 222, shown in FIGURE 2(a).

[0049] 051 As shown in FIGURE 2(b), if a new Position Request is received during the timed wait of the STEP 232, *i.e.*, the event represented at the STEP 240 (Possible Arrival of New Position Request During Wait) occurs prior to the termination of the timed wait for user response, then the new Position Request data received by the Privacy Engine 120 (FIGURE 1) are transferred, and

the method proceeds to a STEP 244.

[0050] 052 Still in reference to FIGURE 2(b), at the STEP 244 the new Position Request is evaluated to determine whether the request is an Emergency Service Request. For an Emergency Service Request the method proceeds via the flow connection 246 to a STEP 288 (FIGURE 2(d)). At the STEP 288 the Position Request Counter is incremented and the method proceeds to a STEP 290. At the STEP 290 the processing for the prior Position Request is suspended and placed in a queue for subsequent processing, as explained hereinbelow. In another embodiment (not shown) the method may instead abort processing of the prior Position Request at the STEP 290. In yet another embodiment (not shown), means are provided to enable the PD module 122 (FIGURE 1) to process a plurality of simultaneous requests. Following the STEP 290, the method proceeds to the STEP 256 (FIGURE 2(b)) via the flow connection 214 for expedited processing of the Emergency Service Request. If the new request is not an emergency request, the method proceeds directly from the STEP 244 to a STEP 248 (FIGURE 2(b)).

[0051] 053 At the STEP 248 the Position Request Counter is incremented. The method then proceeds to a STEP 260 and the new Position Request data are transferred to queuing. At the STEP 260, the method places the new Position Request data into a data queue. After completion of the STEP 260 the inventive method returns to the STEP 232, and awaits a response from the user. In alternative embodiments additional steps may be inserted and implemented prior to the STEP 248 for the purpose of deciding whether the new Position Request should be denied instead of queued. In these embodiments it may be advantageous to deny unacceptable requests if the added steps result in an overall improvement in efficiency. In one example, a request that stipulates an unacceptable QoS may be denied at once rather than placed in queue.

[0052] 054 As shown in FIGURE 2(b), the STEP 250 may be entered from any of the STEPS 234, 242, or (via flow connection 230) the STEP 228 (FIGURE 2(a)). At the STEP 250, Position Request data designating QoS are compared with Privacy Rules that apply for the current Position Request. For the purpose of describing the exemplary implementation, QoS may represent the accuracy of position data to be returned to the Location Request Application. The position data may comprise latitude and longitude coordinate data in conjunction with QoS data representing the accuracy of the position estimate. If the QoS specified by the Position Request data complies with limits specified by the Privacy Rules applicable for the present Position Request, the method proceeds to a STEP 256. If the QoS specified by the Position Request data do not comply with Privacy Policy limits, the QoS data are modified for compliance in a STEP 252 before further processing at the STEP 256. Further discussion to clarify the purpose and use of QoS specifications will be given in the *Exemplary Applications* section

described hereinbelow.

[0053] 055 At the STEP 256, the method activates the PD module 122 (FIGURE 1) in order to retrieve position data in accordance with Position Request data and current Privacy Policy specifications. As described hereinabove, when emergency or other privacy override requests are received, the method may implement STEP 256 via the flow connection 214, following from the STEPS 212, 216 (FIGURE 2(a)) or the STEP 290 (FIGURE 2(d)). The method then proceeds to a STEP 258. At the STEP 258, the method performs a timed wait for the PDM 122 response.

[0054] 056 FIGURE 2(c) is a continuation of the unified flow diagram of FIGURE 2, proceeding from the timed wait at the STEP 258 (FIGURE 2(b) (timed wait for PDM response)). The STEPS 262 and 264 represent events that may terminate the timed wait period of the STEP 258. The STEP 266 also represents an event that may occur during the timed wait period at the STEP 258. These steps are described in more detail in the following paragraphs.

[0055] 057 As shown in FIGURE 2(c), if the timed wait for the PDM response at the STEP 258 is terminated by the event represented at the STEP 262, *i.e.*, if the PDM 122 responds to the Privacy Engine 120 (FIGURE 1), the method proceeds from the STEP 262 to a decision STEP 270. If the timed wait of the STEP 258 "times-out", *i.e.*, is terminated by the event represented at the STEP 264, (Time Out), the method proceeds from the STEP 264 to a STEP 272 and an error message is transmitted to the Location Request Application. In alternative embodiment (not shown), position information previously stored may be transmitted in place of an error message. Following the STEP 272, the method proceeds to a STEP 282 to test for pending position requests in the new position request queue.

[0056] 058 As shown in FIGURE 2(c), if new position requests occur during the STEP 258, the method proceeds to a STEP 266 (Possible Arrival of New Position Request During Wait). At the STEP 266, new Position Request data is received by the Privacy Engine 120 (FIGURE 1). At the following STEP 268 the new Position Request is evaluated to determine whether the request is an Emergency Service Request. For an Emergency Service Request the method proceeds via the flow connection 246 to a STEP 288 (FIGURE 2(d)) for subsequent processing steps as described hereinabove. If the new request is not an emergency request, the method proceeds directly from the STEP 268 to a STEP 274.

[0057] 059 At the STEP 274, the method increments the Position Request Counter. At a following STEP 278, the method places new Position Request data into a data queue. After completion of the STEP 278 the method returns to the STEP 258 to continue to perform a timed wait for PDM response.

[0058] 060 When the timed wait at the STEP 258 is interrupted by the PDM 122 responding to the Privacy Engine 120 (FIGURE 1), the method proceeds from the

STEP 258 to the STEP 262 as shown in FIGURE 2(c). At the STEP 262, PDM data are transferred from the PDM 122 at the STEP 262, to the Privacy Engine 120. The PDM data comprise position coordinate data and QoS data. At the STEP 270, PDM data designating QoS are compared with Privacy Rules relating to the Privacy Class of the current Position Request. For the purpose of describing the exemplary implementation, QoS may represent an estimated accuracy of PDM position coordinate data to be returned to the Location Request Application. The PDM data, for example, may comprise latitude and longitude data in conjunction with QoS data representing the accuracy of the position estimate. If the QoS of the PDM data complies with limits specified by the Privacy Rules relating to the Privacy Class of the current Position Request, the method proceeds to a STEP 280 for further processing. If the QoS specified by the PDM data do not comply with Privacy Policy limits for the present instance, then the QoS data are modified for compliance at a STEP 276. After the position estimate is reformatted at the STEP 276, the method proceeds to the STEP 280. More detailed description of the purpose and use of QoS specifications is provided below in the *Exemplary Applications* section.

[0059] 061 The PDM data are transmitted to the Location Request Application at the STEP 280. The method then proceeds to the STEP 282, whereat the Position Request Counter is interrogated to determine if new Position Requests are pending. If the counter value is determined to be zero, indicating that no pending requests are present, then the method returns to the wait state 202 (FIGURE 2(a)). If the counter value is an integer greater than zero, then the method proceeds to a STEP 284. At the STEP 284, new Position Request data are retrieved from the new Position Request data queue.

[0060] 062 The method then proceeds to a STEP 286, whereat the Position Request Counter is decremented. The method then proceeds (via the flow connection 208) to the STEP 210 (FIGURE 2(a)) to further process new Position Request data.

Exemplary Applications

[0061] 063 In a typical application of the present teachings, several user-configurable Privacy Classes, and properties or rules appertaining thereto, can be defined. As described above in reference to FIGURE 1, user configurability may be effected via data connections between the Privacy Engine 120 and the User Interface 106, the Privacy Management Server 104 (or other network servers not shown in the Figures), or the External Local Applications 116. It is desirable to permit configuration and modification of the Privacy Engine 120 and Privacy Policy by secure means only. By way of example, secure means may comprise methods and means for providing secure digital communication, use of passwords, digital certificates, and other well known identity verification and authentication methods.

[0062] 064 Privacy Classes may include, without limitation, the following types:

1. default for unknown or undeclared (*i.e.*, non-trusted) Location Request Applications and requestor identities not specifically included in any other class;
2. default for trusted Location Request Applications and requestor identities not specifically included in any other class; and
3. user specified classes including Location Request Applications and requestor identities.

[0063] 065 Each Privacy Class may include, without limitation, the following Privacy Rules:

1. specification of default acceptance or denial, or acceptance contingent to specified restrictions;
2. specification of user notification requirements:
 - 2.a. user notification absolutely required or not required, notification based on requested QoS (*e.g.*, the user specifies that notification is required for position estimates more accurate than 10 meters. Hence, if Position Request data specifies QoS for position estimate with 5 meters accuracy, the user shall be notified.), and
 - 2.b. notification based on whether the request is periodic or initiated on demand;
 - 2.c. notification based on time of occurrence, such time of day, day of week, date, or similar time-dependent restrictions.
3. specification of display mode to be used for user notification (*e.g.*, pop-up icon in graphical user interface, notification by tone, music or other sound, notification by vibration, *etc.*), and information to be displayed, if any;
4. specification of notification requirements related to periodic requests such as whether explicit notification is required for each periodic request or required only for the first request of a periodic series;
5. specification of QoS or position estimate accuracy to be delivered (*e.g.*, a Privacy Policy class may be permitted only zip code accuracy, or permitted only for accuracy to within a radius greater than a specified number of meters);
6. specification of the default handling if the user does not respond to a notification (*e.g.*, request allowed or not allowed when the user does not respond to a notification such as a pop up window, with or without an "OK" button, which automatically disap-

pears after a few seconds);

7. specification of variable rule configurations based upon the Mobile Station location or the time of the day. [For example, the user may establish a rule modifying or prohibiting a response from certain locations or at certain times of day.]

[0064] 066 In one embodiment of the present inventive concept, the Mobile Station 102 (FIGURE 1) may include a Subscriber Identity Module (SIM), a Universal Subscriber Identity Module (USIM) or a Removable User Identity Module (RUIM). SIM, USIM and RUIM devices are removable storage components for Mobile Stations that enable secure storage of user-specific information. As previously described in reference to FIGURE 1, the SIM, USIM or RUIM device may be included in the Other Modules block 112. In this exemplary embodiment, user-specific Privacy Policy data are stored in the SIM, USIM or RUIM device. The devices are operatively coupled to the Privacy Engine 120 (connection not shown in FIGURE 1), and the user-specific Privacy Policy data are transmitted to the Privacy Engine 120 for implementation of the Privacy Engine 120 operations described hereinabove. User-specific Privacy Policy data are also received from the Privacy Engine for storage. This occurs when the Privacy Policy data are initially received for storage by the SIM, USIM or RUIM device, and when the data are changed or updated. When the SIM, USIM or RUIM is removed from the Mobile Station 102, the user-specific Privacy Policy information may then be advantageously deleted automatically from the Privacy Engine 120. The use of SIM, USIM or RUIM devices for removable storage of user-specific data in Mobile Stations is well known to persons skilled in the communication arts. Standards for implementation of SIM devices are described in the reference 3rd Generation Partnership Project (3GPP), Technical Specification (TS) Group Terminals, Subscriber Identity Module Application Programming Interface (SIM API), Stage 1, Release 1999, (3GPP TS 02.19 V8.0.0), June, 2001. This reference is hereby referenced for teachings relating to implementation of SKI devices. It will also be obvious to persons skilled in the art that the present teachings encompass embodiments wherein other removable storage devices (such as smart cards or memory sticks) are included in a Mobile Station and used in conjunction with the Privacy Engine for storage of user-specific Privacy Policy data.

[0065] 067 In light of the examples provided in the description above, those of ordinary skill in the communications art shall recognize that the teachings herein can be broadly and generally applied to user control and management of personal privacy information relating to LCS.

[0066] 068 Those of ordinary skill in the communications and computer arts shall also recognize that computer readable medium which tangibly embodies the method steps of any of the embodiments herein may be used in accordance with the present teachings. For ex-

ample, the method steps described above with reference to FIGURES 2(a)-2(c) may be embodied as a series of computer executable instructions stored on a the computer readable medium. Such a medium may include, without limitation, RAM, ROM, EPROM, EEPROM, floppy disk, hard disk, CD-ROM, etc. The disclosure also includes the method STEPS of any of the foregoing embodiments synthesized as digital logic in an integrated circuit, such as a Field Programmable Gate Array, or Programmable Logic Array, or other integrated circuits that can be fabricated or modified to embody computer program instructions.

[0067] 069 The Mobile Station 102 in accordance with the present teachings may include, without limitation: wireless telephone, a personal digital assistant with wireless communication capability, a laptop with wireless communication capability, and any other mobile digital device for personal communication via wireless connection.

[0068] 070 A number of embodiments of the present inventive concept have been described. Nevertheless, it will be understood that various modifications may be made without departing from the scope of the concept as disclosed herein. For example, the methods can be executed in software or hardware, or a combination of hardware and software embodiments. As another example, it should be understood that the functions described as being part of one module may in general be performed equivalently in another module. As yet another example, steps or acts shown or described in a particular sequence may generally be performed in a different order, except for those embodiments described in a claim that include a specified order for the steps.

[0069] 071 Accordingly, it is to be understood that the inventive concept is not to be limited by the specific illustrated embodiments, but only by the scope of the appended claims. The description may provide examples of similar features as are recited in the claims, but it should not be assumed that such similar features are identical to those in the claims unless such identity is essential to comprehend the scope of the claim. In some instances the intended distinction between claim features and description features is underscored by using slightly different terminology.

Claims

1. A privacy control system for use in a mobile station (102), wherein the mobile station (102) communicates with a wireless communication system, and wherein the privacy control system provides geographical location information associated with the mobile station (102), comprising:

a) a Privacy Engine (120), including a Privacy Policy component having at least one Privacy Rule, wherein the Privacy Engine (120) receives

location requests related to the geographical location of the mobile station generated by a location requestor external to the mobile station (102) and determines whether the location request should be denied based at least in part on the at least one Privacy Rule; and
 b) a Position Determination Module (122), operatively coupled and responsive to the Privacy Engine (120), wherein the Position Determination Module (122) provides estimates of the geographical location of the mobile station (102) to the Privacy Engine (120);

wherein, the Privacy Engine (120)

selectively activates the Position Determination Module (122) in accordance with the Privacy Policy component in order to receive the geographical location estimates from the Position Determination Module (122), and responds to the location requests by processing the location estimates, and provides response messages in accordance with the Privacy Policy component.

2. The privacy control system of Claim 1, wherein the Position Determination Module (122) operates according to one or more of the following methods:

Global Positioning System, assisted Global Positioning System, Advanced Forward Link Trilateration, Time of Arrival, Enhanced Observed Time Difference, and positioning based on identifying wireless communication cells within which the mobile station (102) is operating.

3. The privacy control system of Claim 1, further comprising a wireless network communication module (112) operatively coupled to the Privacy Engine (120) and to the wireless communication system, wherein the wireless network communication module (112) is configured to receive the location requests from the wireless communication system and to transmit the response messages to the wireless communication system, and further configured to receive data and software instructions from the wireless communication system and to transmit data and software instructions to the wireless communication system.
4. The privacy control system of Claim 3, wherein the Privacy Engine (120) comprises software that is downloaded from the wireless communication system.
5. The privacy control system of Claim 3, wherein the Privacy Engine (120) is modified with software upgrades downloaded from the wireless communication system.

tion system.

6. The privacy control system of Claim 3, wherein the Privacy Policy comprises software that is downloaded from the wireless communication system.
7. The privacy control system of Claim 3, wherein the Privacy Policy is modified with updates downloaded from the wireless communication system.
8. The privacy control system of Claim 7, wherein the updates include user-specific Privacy Policy data.
9. The privacy control system of Claim 3, wherein the location request is received from an external application operatively connected to the wireless communication system.
10. The privacy control system of Claim 1, further comprising a local communication module (118) operatively coupled to the Privacy Engine (120) and to external local applications (116), wherein the local communication module (118) is configured to receive the location requests from the external local applications (116) and to transmit the response messages to the external local applications (116), and further configured to receive data and software instructions from the external local applications (116) and to transmit data and software instructions to the external local applications (116).
11. The privacy control system of Claim 10, wherein the Privacy Engine (120) comprises software that is downloaded from an external local application (116).
12. The privacy control system of Claim 10, wherein the Privacy Engine (120) is modified with software upgrades by software instructions downloaded from an external local application (116).
13. The privacy control system of Claim 10, wherein the Privacy Policy comprises software that is downloaded from an external local application (116).
14. The privacy control system of Claim 10, wherein the Privacy Policy is modified with updates downloaded from an external local application (116).
15. The privacy control system of Claim 14, wherein the updates include user-specific Privacy Policy data.
16. The privacy control system of Claim 10, wherein the location request is received from an external local application (116).
17. The privacy control system of Claim 1, further comprising a User Interface (106), operatively coupled to the Privacy Engine (120), wherein the User Inter-

face (106) is configured to receive input from a user, and wherein the user input is used to modify the Privacy Policy with updates.

18. The privacy control system of Claim 17, wherein the updates include user-specific Privacy Policy data. 5
19. The privacy control system of Claim 17, wherein the User Interface (106) provides notifications of location requests to the user, in accordance with the Privacy Policy, and wherein the User Interface (106) is configured to receive responses from the user, responsive to the location request notifications. 10
20. The privacy control system of Claim 19, wherein the Privacy Policy includes a plurality of Privacy Classes, wherein the Privacy Classes classify the location requests received by the Privacy Engine (120), and wherein the Privacy Policy further includes Privacy Rules that determine responses to the location requests for each Privacy Class, and wherein the Privacy Rules include at least one of the following rules: 15
 - a) a rule requiring default acceptance or denial of a location request; 25
 - b) a rule requiring user notification of a location request;
 - c) a rule requiring user notification based upon a requested quality of service;
 - d) a rule requiring user notification based upon whether the location request is periodic or initiated on demand; 30
 - e) a rule requiring user notification based upon a time of occurrence of the location request;
 - f) a rule specifying a display mode to be used for user notification; 35
 - g) a rule specifying an accuracy range of the location estimate to be provided;
 - h) a rule requiring default handling of a response message if the user does not respond to a user notification; and 40
 - i) a rule specifying response message handling based on current geographical location of the mobile station.
21. The privacy control system of Claim 1, further comprising a removable data storage device, wherein the removable data storage device is operatively coupled to the Privacy Engine (120), and wherein the removable data storage device is configured to receive, store, and transmit user-specific Privacy Policy data. 50
22. The privacy control system of Claim 21, wherein the removable data storage device comprises a Subscriber Identity Module device. 55
23. The privacy control system of Claim 21, wherein the

removable data storage device comprises a Universal Subscriber Identity Module device.

24. The privacy control system of Claim 21, wherein the removable data storage device comprises a Removable User Identity Module device.
25. A method of providing privacy control in a mobile station (102) of the mobile station geographical location information, wherein the mobile station (102) communicates with a wireless communication system, and wherein the mobile station (102) includes a Privacy Engine (120) comprising software instructions, wherein the Privacy Engine software instructions also include Privacy Policy instructions having at least one Privacy Rule, and wherein the mobile station (102) further includes a Position Determination Module (122) capable of providing geographical location estimates of the mobile station (102); the method comprising the steps of:
 - a) receiving (204) location requests for a current geographical location of the mobile station (102) from a location requestor external to the mobile station (102);
 - b) processing the location requests in accordance with the Privacy Engine software instructions, wherein processing the location request includes determining whether the location request should be denied based at least in part on the at least one Privacy Rule;
 - c) selectively activating the Position Determination Module (122) in accordance with the Privacy Policy component for obtaining geographical location estimates of the mobile station (102);
 - d) processing the geographical location estimates in accordance with the location requests, the Privacy Engine software instructions, and the Privacy Rules; and
 - e) selectively providing response messages responsive to the location requests, in accordance with the Privacy Engine software instructions, the location estimates and the Privacy Rules.
26. The privacy control method of Claim 25, wherein the step b) of processing the location requests further includes a step of processing emergency location requests by overriding the Privacy Policy instructions to provide emergency response messages. 45
27. The privacy control method of Claim 26, wherein the step b) of processing the location requests includes processing a plurality of concurrent location requests.
28. The privacy control method of Claim 27, wherein pending location requests are suspended while the emergency location requests are processed.

29. The privacy control method of Claim 25, further comprising a step of notifying a user of location requests.

30. The privacy control method of Claim 29, wherein the Privacy Policy instructions include Privacy Classes for classifying the location requests received during the step a), and wherein the Privacy Policy instructions include Privacy Rules for determining a response to the location requests for each Privacy Class, and wherein the Privacy Rules include at least one of the following rules:

- a) a rule requiring default acceptance or denial of a location request;
- b) a rule requiring user notification of a location request;
- c) a rule requiring user notification based upon a requested quality of service;
- d) a rule requiring user notification based upon whether the location request is periodic or initiated on demand;
- e) a rule requiring user notification based upon a time of occurrence of the location request;
- f) a rule specifying a display mode to be used for user notification;
- g) a rule specifying an accuracy range of the location estimate to be provided;
- h) a rule requiring default handling of a response message if the user does not respond to a user notification; and
- i) a rule specifying response message handling based on current geographical location of the mobile station.

Patentansprüche

1. Ein Privatsphärenkontrollsystem zum Einsatz in einer Mobilstation (102), wobei die Mobilstation (102) mit einem drahtlosen Kommunikationssystem kommuniziert und wobei das Privatsphärenkontrollsystem geographische Standortinformationen bereitstellt, verbunden mit der Mobilstation (102), aufweisend:

- a) eine Privatsphäreneinheit (120), eine Privatsphärenrichtlinienkomponente beinhaltend, die über zumindest eine Privatsphärenregel verfügt, wobei die Privatsphäreneinheit (120) Standortanfragen empfängt, zugehörig zu dem geographischen Standort von der Mobilstation, erzeugt durch einen Standortanforderer, außerhalb der Mobilstation (102), und bestimmt, ob die Standortanfrage abgewiesen werden sollte, zumindest zum Teil basierend auf der zumindest einen Privatsphärenregel; und
- b) ein Positionsbestimmungsmodul (122), wirksam verbunden mit und reagierend auf die Pri-

vatsphäreneinheit (120), wobei das Positionsbestimmungsmodul (122) Schätzungen von dem geographischen Standort von der Mobilstation (102) an die Privatsphäreneinheit (120) bereitstellt;

wobei die Privatsphäreneinheit (120)

selektiv das Positionsbestimmungsmodul (122) aktiviert, in Übereinstimmung mit der Privatsphärenrichtlinienkomponente, um die geographischen Standortschätzungen von dem Positionsbestimmungsmodul (122) zu empfangen, und auf die Standortanfragen antwortet, durch Verarbeiten der Standortschätzungen, und Antwortnachrichten bereitstellt, in Übereinstimmung mit der Privatsphärenrichtlinienkomponente.

2. Das Privatsphärenkontrollsystem nach Anspruch 1, wobei das Positionsbestimmungsmodul (122) betrieben wird gemäß einem oder mehreren von den folgenden Verfahren:

globales Ortungssystem, unterstütztes globales Ortungssystem, weiterentwickelte Vorwärtsverbindungs-Trilateration, Ankunftszeit, erweiterter beobachteter Zeitunterschied und Ortung, basierend auf Identifizierung von drahtlosen Kommunikationszellen, innerhalb derer die Mobilstation (120) betrieben wird.

3. Das Privatsphärenkontrollsystem nach Anspruch 1, weiter aufweisend, ein Drahtlosnetzwerk-Kommunikationsmodul (112) betriebsfähig verbunden mit der Privatsphäreneinheit (120) und mit dem drahtlosen Kommunikationssystem, wobei das Drahtlosnetzwerk-Kommunikationsmodul (112) konfiguriert ist, die Standortanfragen von dem drahtlosen Kommunikationssystem zu empfangen und die Antwortnachrichten an das drahtlose Kommunikationssystem zu übertragen, und weiter konfiguriert ist, Daten und Softwareanweisungen von dem drahtlosen Kommunikationssystem zu empfangen und Daten und Softwareanweisungen an das drahtlose Kommunikationssystem zu übertragen.

4. Das Privatsphärenkontrollsystem nach Anspruch 3, wobei die Privatsphäreneinheit (120) Software aufweist, die von dem drahtlosen Kommunikationssystem heruntergeladen wird.

5. Das Privatsphärenkontrollsystem nach Anspruch 3, wobei die Privatsphäreneinheit (120) mit Softwareaktualisierungen modifiziert wird, heruntergeladen von dem drahtlosen Kommunikationssystem.

6. Das Privatsphärenkontrollsystem nach Anspruch 3, wobei die Privatsphärenrichtlinie Software aufweist, die von dem drahtlosen Kommunikationssystem heruntergeladen wird.
7. Das Privatsphärenkontrollsystem nach Anspruch 3, wobei die Privatsphärenrichtlinie mit Aktualisierungen modifiziert wird, heruntergeladen von dem drahtlosen Kommunikationssystem.
8. Das Privatsphärenkontrollsystem nach Anspruch 7, wobei die Aktualisierungen benutzerspezifische Privatsphärenrichtlinien-Daten beinhalten.
9. Das Privatsphärenkontrollsystem nach Anspruch 3, wobei die Standortanfrage empfangen wird von einer externen Anwendung, betriebsfähig verbunden mit dem drahtlosen Kommunikationssystem.
10. Das Privatsphärenkontrollsystem nach Anspruch 1, weiter aufweisend ein lokales Kommunikationsmodul (118), betriebsfähig verbunden mit der Privatsphäreneinheit (120) und mit externen lokalen Anwendungen (116), wobei das lokale Kommunikationsmodul (118) konfiguriert ist, die externen Standortanfragen von den externen lokalen Anwendungen (116) zu empfangen und die Antwortnachrichten zu den externen lokalen Anwendungen (116) zu übertragen und weiter konfiguriert ist, Daten und Softwareanweisungen von den externen lokalen Anwendungen (116) zu empfangen und Daten und Softwareanweisungen zu den externen lokalen Anwendungen (116) zu übertragen.
11. Das Privatsphärenkontrollsystem nach Anspruch 10, wobei die Privatsphäreneinheit (120) Software aufweist, die heruntergeladen wird von einer externen lokalen Anwendung (116).
12. Das Privatsphärenkontrollsystem nach Anspruch 10, wobei die Privatsphäreneinheit (120) modifiziert wird mit Softwareaktualisierungen durch Softwareanweisungen, heruntergeladen von einer externen lokalen Anwendung (116).
13. Das Privatsphärenkontrollsystem nach Anspruch 10, wobei die Privatsphärenrichtlinie Software aufweist, die von einer externen lokalen Anwendung heruntergeladen wird.
14. Das Privatsphärenkontrollsystem nach Anspruch 10, wobei die Privatsphärenrichtlinie modifiziert ist mit Aktualisierungen, heruntergeladen von einer externen lokalen Anwendung (116).
15. Das Privatsphärenkontrollsystem nach Anspruch 14, wobei die Aktualisierungen benutzerspezifische Privatsphärenrichtlinien-Daten beinhalten.
16. Das Privatsphärenkontrollsystem nach Anspruch 10, wobei die Standortanfrage empfangen wird von einer externen lokalen Anwendung (116).
17. Das Privatsphärenkontrollsystem nach Anspruch 1, weiter aufweisend eine Benutzerschnittstelle (106), betriebsfähig verbunden mit der Privatsphäreneinheit (120), wobei die Benutzerschnittstelle (106) konfiguriert ist, Eingabe von einem Benutzer zu empfangen und wobei die Benutzereingabe verwendet wird, die Privatsphärenrichtlinie mit Aktualisierungen zu modifizieren.
18. Das Privatsphärenkontrollsystem nach Anspruch 17, wobei die Aktualisierungen benutzerspezifische Privatsphärenrichtlinien-Daten beinhalten.
19. Das Privatsphärenkontrollsystem nach Anspruch 17, wobei die Benutzerschnittstelle (106) dem Benutzer Benachrichtigungen über Standortanfragen bereitstellt, in Übereinstimmung mit der Privatsphärenrichtlinie und wobei die Benutzerschnittstelle (106) konfiguriert ist, Antworten von dem Benutzer zu empfangen, reagierend auf die Standortanfragebenachrichtigungen.
20. Das Privatsphärenkontrollsystem nach Anspruch 19, wobei die Privatsphärenrichtlinie eine Vielzahl von Privatsphärenklassen beinhaltet, wobei die Privatsphärenklassen die Standortanfragen, empfangen von der Privatsphäreneinheit (120), klassifizieren und wobei die Privatsphärenrichtlinie weiter Privatsphärenregeln beinhaltet, die Antworten auf die Standortanfragen für jede Privatsphärenklasse bestimmen, und wobei die Privatsphärenregeln zumindest eine von den folgenden Regeln beinhalten:
 - a) eine Regel, Standardannahme oder Abweisung von einer Standortanfrage erfordernd;
 - b) eine Regel, Benutzerbenachrichtigung über eine Standortanfrage erfordernd;
 - c) eine Regel, Benutzerbenachrichtigung erfordernd, basierend auf einer angeforderten Servicequalität;
 - d) eine Regel, Benutzerbenachrichtigung erfordernd, basierend darauf, ob die Standortanfrage periodisch ist, oder auf Verlangen initiiert wird;
 - e) eine Regel, Benutzerbenachrichtigung erfordernd, basierend auf einem Zeitpunkt des Auftretens von der Standortanfrage;
 - f) eine Regel, die einen Anzeigemodus spezifiziert, der für Benutzerbenachrichtigung verwendet werden soll;
 - g) eine Regel, die einen Genauigkeitsbereich von der Standortschätzung spezifiziert, die bereitgestellt werden soll;
 - h) eine Regel, Standardhandhabung von einer Antwortnachricht erfordernd, wenn der Benut-

- zer nicht auf eine Benutzerbenachrichtigung antwortet; und
i) eine Regel, die Antwortnachrichthandhabung spezifiziert, basierend auf dem gegenwärtigen Standort von der Mobilstation.
21. Das Privatsphärenkontrollsystem nach Anspruch 1, weiter aufweisend ein entfernbare Datenspeicherendgerät, wobei das Datenspeicherendgerät betriebsfähig verbunden ist mit der Privatsphäreinheit (120) und wobei das entfernbare Datenspeicherendgerät konfiguriert ist zu empfangen, speichern und übertragen von benutzerspezifischen Privatsphärenrichtlinien-Daten.
22. Das Privatsphärenkontrollsystem nach Anspruch 21, wobei das entfernbare Datenspeicherendgerät ein Teilnehmeridentitätsmodul aufweist.
23. Das Privatsphärenkontrollsystem nach Anspruch 21, wobei das entfernbare Datenspeicherendgerät ein universelles Teilnehmeridentitätsmodul aufweist.
24. Das Privatsphärenkontrollsystem nach Anspruch 21, wobei das entfernbare Datenspeicherendgerät ein entfernbare Benutzeridentitätsmodul aufweist.
25. Ein Verfahren zum Bereitstellen von Privatsphärenkontrolle von der geographischen Standortinformation in einer Mobilstation (102), wobei die Mobilstation (102) mit einem drahtlosen Kommunikationssystem kommuniziert und wobei die Mobilstation (102) eine Privatsphäreinheit (120) beinhaltet, Softwareanweisungen aufweisend, wobei die Privatsphäreinheitsoftwareanweisungen auch Privatsphärenrichtlinienanweisungen beinhalten, die über zumindest eine Privatsphärenregel verfügen, und wobei die Mobilstation (102) weiter ein Positionsbestimmungsmodul (122) beinhaltet, das in der Lage ist, geographische Standortschätzungen von der Mobilstation (102) bereitzustellen; das Verfahren die Schritte aufweisend:
- a) Empfangen (204) von Standortanfragen für einen gegenwärtigen geographischen Standort von der Mobilstation (102) von einem Standortanforderer außerhalb der Mobilstation (102);
b) Verarbeiten der Standortanfragen in Übereinstimmung mit den Privatsphäreinheitsoftwareanweisungen, wobei das Verarbeiten der Standortanfragen beinhaltet, Bestimmen, ob die Standortanfrage abgewiesen werden sollte, zumindest zum Teil basierend auf der zumindest einen Privatsphärenregel;
c) selektives Aktivieren des Positionsbestimmungsmoduls (122), in Übereinstimmung mit der Privatsphärenrichtlinienkomponente zum Erhalten von geographischen Standortschätzungen von der Mobilstation (102);
d) Verarbeiten der geographischen Standortschätzungen in Übereinstimmung mit den Standortanfragen, den Privatsphäreinheitsoftwareanweisungen und den Privatsphärenregeln; und
e) selektives Bereitstellen von Antwortnachrichten, reagierend auf die Standortanfragen, in Übereinstimmung mit den Privatsphäreinheitsoftwareanweisungen, den Standortschätzungen und den Privatsphärenregeln.
26. Das Privatsphärenkontrollverfahren nach Anspruch 25, wobei der Schritt b) zum Verarbeiten der Standortanfragen weiter beinhaltet, einen Schritt zum Verarbeiten von Notfallstandortanfragen durch Überschriften der Privatsphärenrichtlinienanweisungen, um Notfallantwortnachrichten bereitzustellen.
27. Das Privatsphärenkontrollverfahren nach Anspruch 26, wobei der Schritt b) zum Verarbeiten der Standortanfragen beinhaltet, Verarbeiten einer Vielzahl von gleichzeitigen Standortanfragen.
28. Das Privatsphärenkontrollverfahren nach Anspruch 27, wobei anhängige Standortanfragen ausgesetzt werden, während die Notfallstandortanfragen verarbeitet werden.
29. Das Privatsphärenkontrollverfahren nach Anspruch 25, weiter aufweisend einen Schritt zum Benachrichtigen eines Benutzers über Standortanfragen.
30. Das Privatsphärenkontrollverfahren nach Anspruch 29, wobei die Privatsphärenrichtlinienanweisungen Privatsphärenklassen beinhalten zum Klassifizieren der Standortanfragen, die während des Schrittes a) empfangen wurden, und wobei die Privatsphärenrichtlinienanweisungen Privatsphärenregeln beinhalten zum Bestimmen einer Antwort auf die Standortanfragen für jede Privatsphärenklasse und wobei die Privatsphärenregeln zumindest eine von den folgenden Regeln beinhalten:
- a) eine Regel, Standardannahme oder Abweisung von einer Standortanfrage erfordernd;
b) eine Regel, Benutzerbenachrichtigung über eine Standortanfrage erfordernd;
c) eine Regel, Benutzerbenachrichtigung erfordernd, basierend auf einer angeforderten Servicequalität;
d) eine Regel, Benutzerbenachrichtigung erfordernd, basierend darauf, ob die Standortanfrage periodisch ist, oder auf Verlangen initiiert wird;
e) eine Regel, Benutzerbenachrichtigung erfordernd, basierend auf einem Zeitpunkt des Auftretens von der Standortanfrage;
f) eine Regel, die einen Anzeigemodus spezifi-

ziert, der für Benutzerbenachrichtigung verwendet werden soll;

g) eine Regel, die einen Genauigkeitsbereich von der Standortschätzung spezifiziert, die bereitgestellt werden soll;

h) eine Regel, Standardhandhabung von einer Antwortnachricht erfordernd, wenn der Benutzer nicht auf eine Benutzerbenachrichtigung antwortet; und

i) eine Regel, die Antwortnachrichthandhabung spezifiziert, basierend auf dem gegenwärtigen Standort von der Mobilstation.

Revendications

1. Système de contrôle de la confidentialité à utiliser dans une station mobile (102), dans lequel la station mobile (102) communique avec un système de communication sans fil, et dans lequel le système de contrôle de la confidentialité fournit des informations d'emplacement géographique associées à la station mobile (102), comprenant :

a) un moteur de confidentialité (120), incluant un composant de politique de confidentialité ayant au moins une règle de confidentialité, le moteur de confidentialité (120) recevant des demandes d'emplacement relatives à l'emplacement géographique de la station mobile générées par un demandeur d'emplacement externe à la station mobile (102) et détermine si la demande d'emplacement doit être refusée en se basant au moins en partie sur la au moins une règle de confidentialité ; et

b) un module de détermination de position (122), couplé opérationnellement et réactif au moteur de confidentialité (120), le module de détermination de position (122) fournissant des estimations de l'emplacement géographique de la station mobile (102) au moteur de confidentialité (120) ;

dans lequel, le moteur de confidentialité (120) active sélectivement le module de détermination de position (122) en conformité avec le composant de politique de confidentialité afin de recevoir les estimations d'emplacement géographique du module de détermination de position (122), et répond aux demandes d'emplacement en traitant les estimations d'emplacement, et fournit des messages de réponse en conformité avec le composant de politique de confidentialité.

2. Système de contrôle de la confidentialité selon la revendication 1, dans lequel le module de détermination de position (122) opère selon un ou plusieurs des procédés suivants :

système de positionnement global, système de positionnement global assisté, trilatération de liaison aller avancée, heure d'arrivée, calcul amélioré de la différence de temps observée, et positionnement basé sur l'identification de cellules de communication sans fil au sein desquelles la station mobile (102) opère.

3. Système de contrôle de la confidentialité selon la revendication 1, comprenant en outre un module de communication de réseau sans fil (112) couplé opérationnellement au moteur de confidentialité (120) et au système de communication sans fil, dans lequel le module de communication de réseau sans fil (112) est configuré pour recevoir les demandes d'emplacement du système de communication sans fil et pour transmettre les messages de réponse au système de communication sans fil, et en outre configuré pour recevoir des données et des instructions logicielles du système de communication sans fil et transmettre des données et instructions logicielles au système de communication sans fil.

4. Système de contrôle de la confidentialité selon la revendication 3, dans lequel le moteur de confidentialité (120) comprend un logiciel qui est téléchargé à partir du système de communication sans fil.

5. Système de contrôle de la confidentialité selon la revendication 3, dans lequel le moteur de confidentialité (120) est modifié avec des mises à niveau de logiciel téléchargées à partir du système de communication sans fil.

6. Système de contrôle de la confidentialité selon la revendication 3, dans lequel la politique de confidentialité comprend un logiciel qui est téléchargé à partir du système de communication sans fil.

7. Système de contrôle de la confidentialité selon la revendication 3, dans lequel la politique de confidentialité est modifiée avec des mises à jour téléchargées à partir du système de communication sans fil.

8. Système de contrôle de la confidentialité selon la revendication 7, dans lequel les mises à jour incluent des données de politique de confidentialité spécifiques de l'utilisateur.

9. Système de contrôle de la confidentialité selon la revendication 3, dans lequel la demande d'emplacement est reçue d'une application externe opérationnellement connectée au système de communication sans fil.

10. Système de contrôle de la confidentialité selon la revendication 1, comprenant en outre un module de communication local (118) couplé opérationnelle-

- ment au moteur de confidentialité (120) et à des applications locales externes (116), le module de communication local (118) étant configuré pour recevoir les demandes d'emplacement des applications locales externes (116) et transmettre les messages de réponse aux applications locales externes (116), et en outre configuré pour recevoir des données et des instructions logicielles des applications locales externes (116) et transmettre des données et des instructions logicielles aux applications locales externes (116).
11. Système de contrôle de la confidentialité selon la revendication 10, dans lequel le moteur de confidentialité (120) comprend un logiciel qui est téléchargé à partir d'une application locale externe (116).
 12. Système de contrôle de la confidentialité selon la revendication 10, dans lequel le moteur de confidentialité (120) est modifié avec des mises à niveau de logiciel par des instructions logicielles téléchargées à partir d'une application locale externe (116).
 13. Système de contrôle de la confidentialité selon la revendication 10, dans lequel la politique de confidentialité comprend un logiciel qui est téléchargé à partir d'une application locale externe (116).
 14. Système de contrôle de la confidentialité selon la revendication 10, dans lequel la politique de confidentialité est modifiée avec des mises à jour téléchargées à partir d'une application locale externe (116).
 15. Système de contrôle de la confidentialité selon la revendication 14, dans lequel les mises à jour incluent des données de politique de confidentialité spécifiques de l'utilisateur.
 16. Système de contrôle de la confidentialité selon la revendication 10, dans lequel la demande d'emplacement est reçue à partir d'une application locale externe (116).
 17. Système de contrôle de la confidentialité selon la revendication 1, comprenant en outre une interface utilisateur (106), couplée opérationnellement au moteur de confidentialité (120), l'interface utilisateur (106) étant configurée pour recevoir une entrée d'un utilisateur, et l'entrée d'utilisateur étant utilisée pour modifier la politique de confidentialité avec des mises à jour.
 18. Système de contrôle de la confidentialité selon la revendication 17, dans lequel les mises à jour incluent des données de politique de confidentialité spécifiques de l'utilisateur.
 19. Système de contrôle de la confidentialité selon la revendication 17, dans lequel l'interface utilisateur (106) fournit des notifications de demandes d'emplacement à l'utilisateur, en conformité avec la politique de confidentialité, et l'interface utilisateur (106) étant configurée pour recevoir des réponses de l'utilisateur, en réaction aux notifications de demande d'emplacement.
 20. Système de contrôle de la confidentialité selon la revendication 19, dans lequel la politique de confidentialité inclut une pluralité de classes de confidentialité, les classes de confidentialité classant les demandes d'emplacement reçues par le moteur de confidentialité (120), et la politique de confidentialité inclut en outre des règles de confidentialité qui déterminent des réponses aux demandes d'emplacement pour chaque classe de confidentialité, et les règles de confidentialité incluant au moins l'une des règles suivantes :
 - a) une règle requérant une acceptation ou un refus par défaut d'une demande d'emplacement ;
 - b) une règle requérant une notification d'utilisateur d'une demande d'emplacement ;
 - c) une règle requérant une notification d'utilisateur basée sur une qualité de service demandée ;
 - d) une règle requérant une notification d'utilisateur selon que la demande d'emplacement est périodique ou initiée à la demande ;
 - e) une règle requérant une notification d'utilisateur basée sur une heure d'occurrence de la demande d'emplacement ;
 - f) une règle spécifiant un mode d'affichage à utiliser pour une notification d'utilisateur ;
 - g) une règle spécifiant une plage de précision de l'estimation d'emplacement à fournir ;
 - h) une règle requérant un traitement par défaut d'un message de réponse si l'utilisateur ne répond pas à une notification d'utilisateur ; et
 - i) une règle spécifiant un traitement de message de réponse basée sur un emplacement géographique actuel de la station mobile.
 21. Système de contrôle de la confidentialité selon la revendication 1, comprenant en outre un dispositif de stockage de données amovible, le dispositif de stockage de données amovible étant couplé opérationnellement au moteur de confidentialité (120), et le dispositif de stockage de données amovible étant configuré pour recevoir, stocker, et transmettre des données de politique de confidentialité spécifiques de l'utilisateur.
 22. Système de contrôle de la confidentialité selon la revendication 21, dans lequel le dispositif de stock-

kage de données amovible comprend un dispositif de module d'identité d'abonné.

23. Système de contrôle de la confidentialité selon la revendication 21, dans lequel le dispositif de stockage de données amovible comprend un dispositif de module d'identité d'abonné universel.

24. Système de contrôle de la confidentialité selon la revendication 21, dans lequel le dispositif de stockage de données amovible comprend un dispositif de module d'identité d'utilisateur amovible.

25. Procédé permettant d'assurer un contrôle de la confidentialité dans une station mobile (102) des informations d'emplacement géographique de station mobile, la station mobile (102) communiquant avec un système de communication sans fil, et la station mobile (102) incluant un moteur de confidentialité (120) comprenant des instructions logicielles, les instructions logicielles du moteur de confidentialité incluant également des instructions de politique de confidentialité ayant au moins une règle de confidentialité, et la station mobile (102) incluant en outre un module de détermination de position (122) capable de fournir des estimations d'emplacement géographique de la station mobile (102) ; le procédé comprenant les étapes de :

- a) réception (204) de demandes d'emplacement d'un emplacement géographique actuel de la station mobile (102) par un demandeur d'emplacement externe à la station mobile (102) ;
- b) traitement des demandes d'emplacement en conformité avec les instructions logicielles de moteur de confidentialité, le traitement de la demande d'emplacement incluant le fait de déterminer si la demande d'emplacement doit être refusée en se basant au moins en partie sur la au moins une règle de confidentialité ;
- c) l'activation sélective du module de détermination de position (122) en conformité avec le composant de politique de confidentialité pour obtenir des estimations d'emplacement géographique de la station mobile (102) ;
- d) le traitement des estimations d'emplacement géographique en conformité avec les demandes d'emplacement, les instructions logicielles du moteur de confidentialité et les règles de confidentialité ; et
- e) la fourniture sélective de messages de réponse en réaction aux demandes d'emplacement, en conformité avec les instructions logicielles du moteur de confidentialité, les estimations d'emplacement et les règles de confidentialité.

26. Procédé de contrôle de la confidentialité selon la revendication 25, dans lequel l'étape b) de traitement

des demandes d'emplacement inclut en outre une étape de traitement de demandes d'emplacement d'urgence par écrasement des instructions de politique de confidentialité pour fournir des messages de réponse d'urgence.

27. Procédé de contrôle de la confidentialité selon la revendication 26, dans lequel l'étape b) de traitement des demandes d'emplacement inclut un traitement d'une pluralité de demandes d'emplacement simultanées.

28. Procédé de contrôle de la confidentialité selon la revendication 27, dans lequel des demandes d'emplacement en attente sont suspendues pendant que les demandes d'emplacement d'urgence sont traitées.

29. Procédé de contrôle de la confidentialité selon la revendication 25, comprenant en outre une étape de notification de demandes d'emplacement à un utilisateur.

30. Procédé de contrôle de la confidentialité selon la revendication 29, dans lequel les instructions de politique de confidentialité incluent des classes de confidentialité permettant de classer les demandes d'emplacement reçues durant l'étape a), et les instructions de politique de confidentialité incluant des règles de confidentialité permettant de déterminer une réponse aux demandes d'emplacement pour chaque classe de confidentialité, et les règles de confidentialité incluant au moins l'une des règles suivantes :

- a) une règle requérant une acceptation ou un refus par défaut d'une demande d'emplacement ;
- b) une règle requérant une notification d'utilisateur d'une demande d'emplacement ;
- c) une règle requérant une notification d'utilisateur basée sur une qualité de service demandée ;
- d) une règle requérant une notification d'utilisateur selon que la demande d'emplacement est périodique ou initiée à la demande ;
- e) une règle requérant une notification d'utilisateur basée sur une heure d'occurrence de la demande d'emplacement ;
- f) une règle spécifiant un mode d'affichage à utiliser pour une notification d'utilisateur ;
- g) une règle spécifiant une plage de précision de l'estimation d'emplacement à fournir ;
- h) une règle requérant un traitement par défaut d'un message de réponse si l'utilisateur ne répond pas à une notification d'utilisateur ; et
- i) une règle spécifiant un traitement de message de réponse basée sur un emplacement géographique actuel de la station mobile.

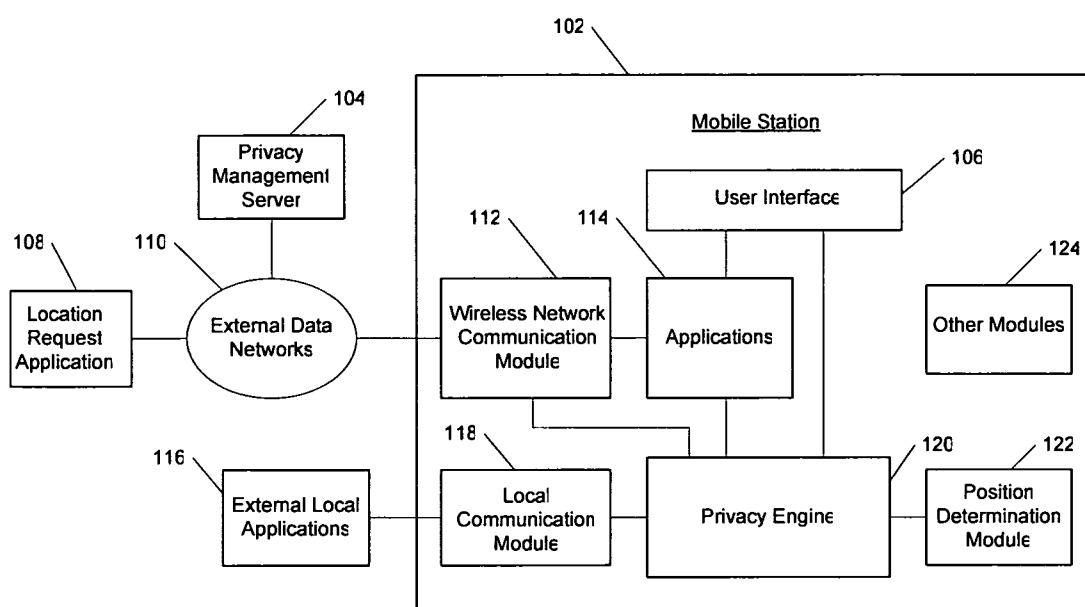


Figure 1

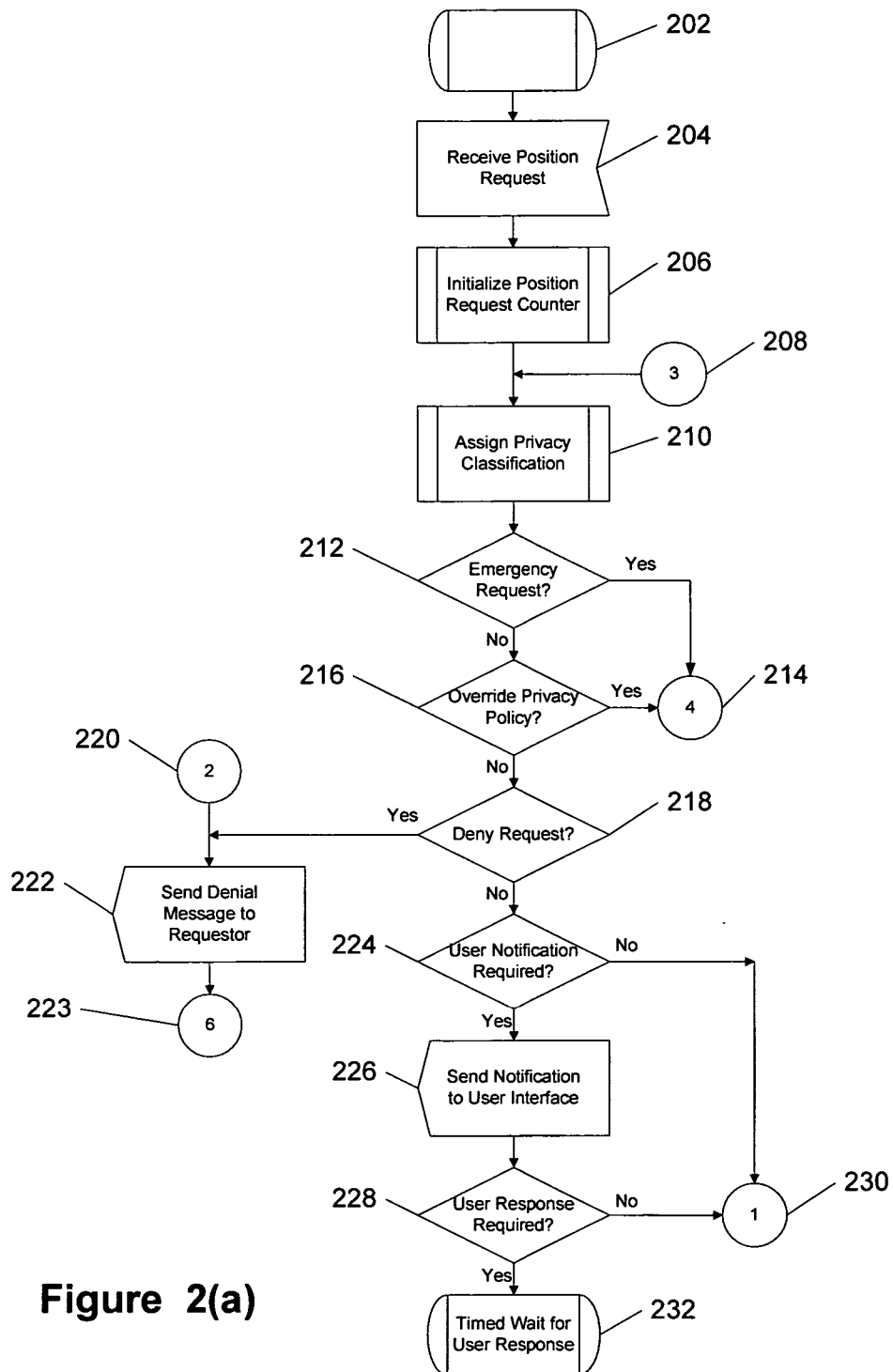


Figure 2(a)

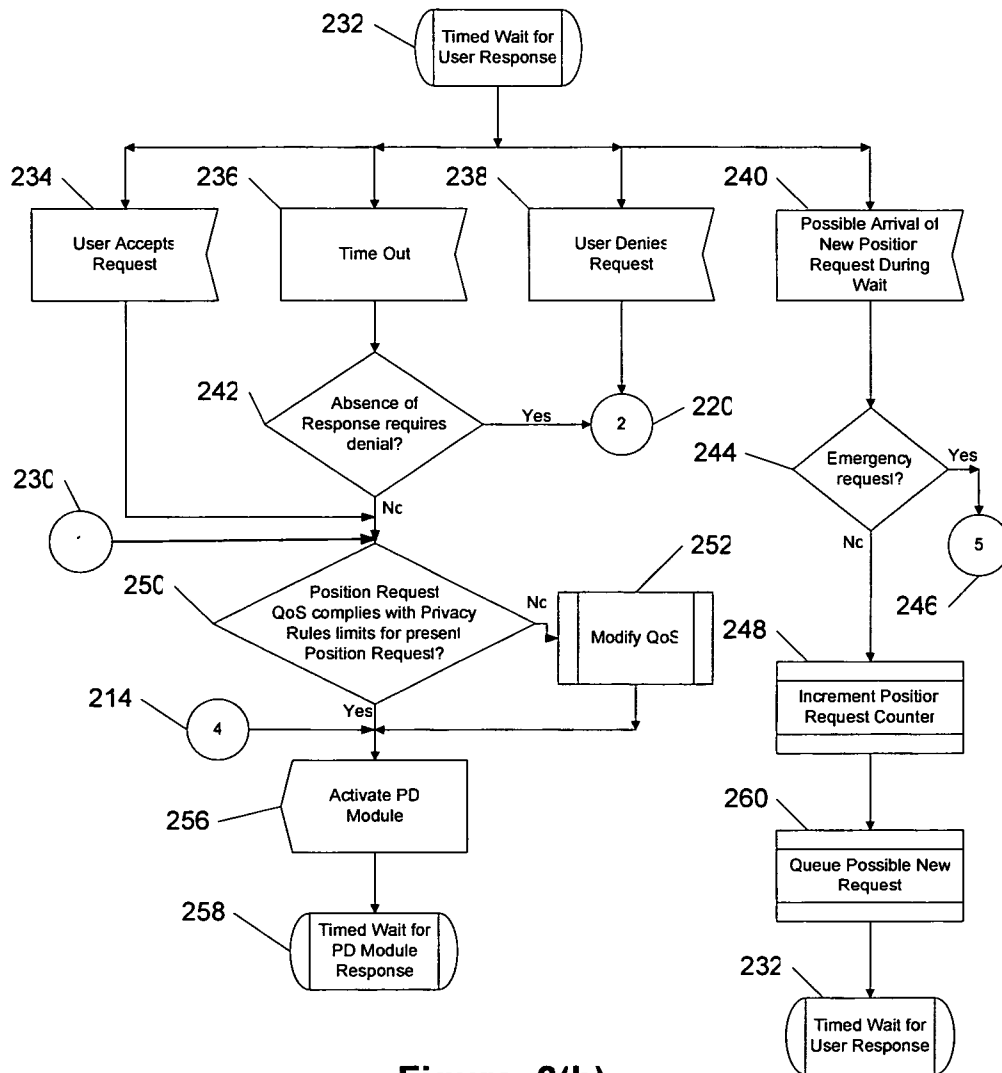


Figure 2(b)

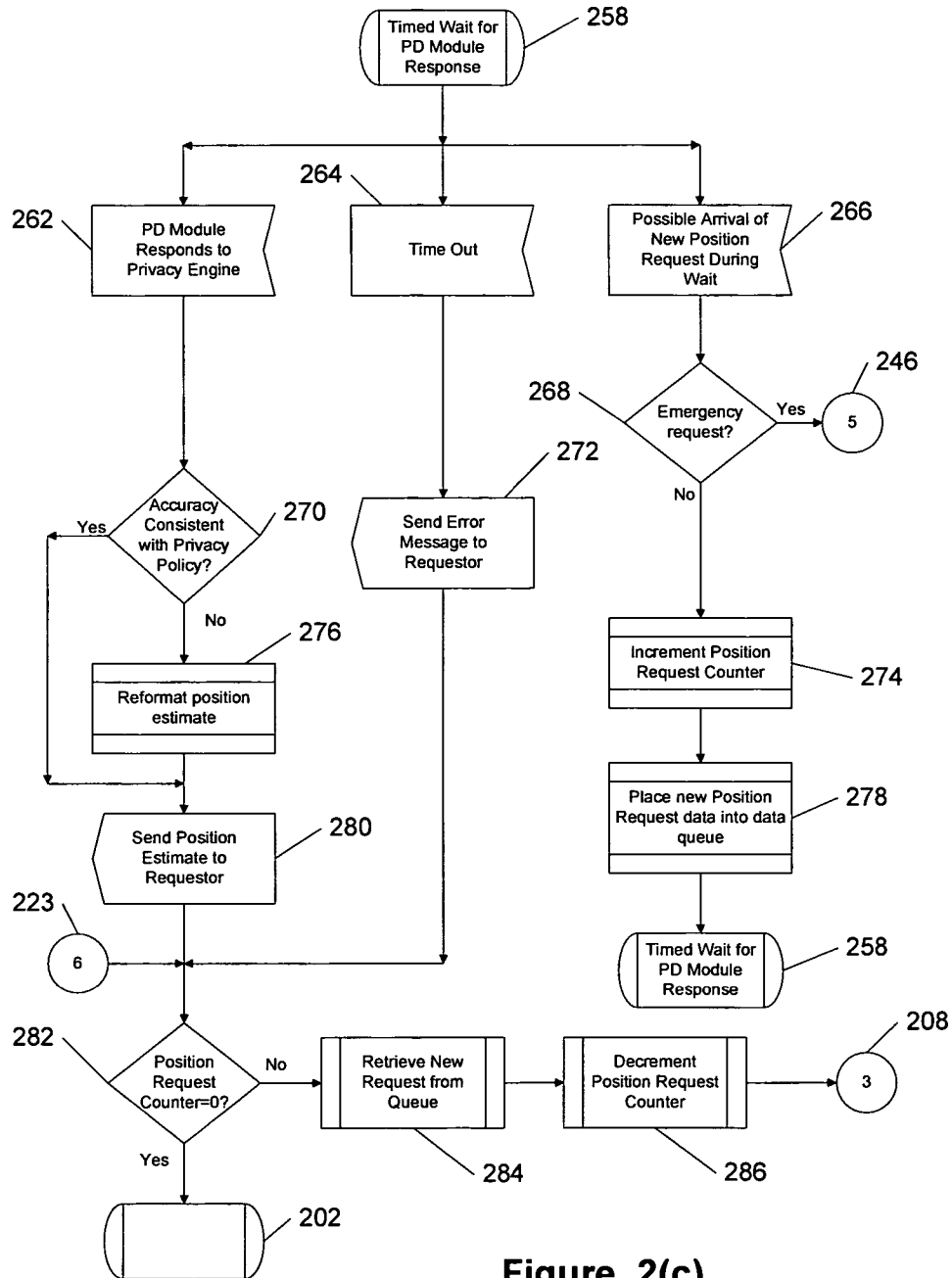


Figure 2(c)

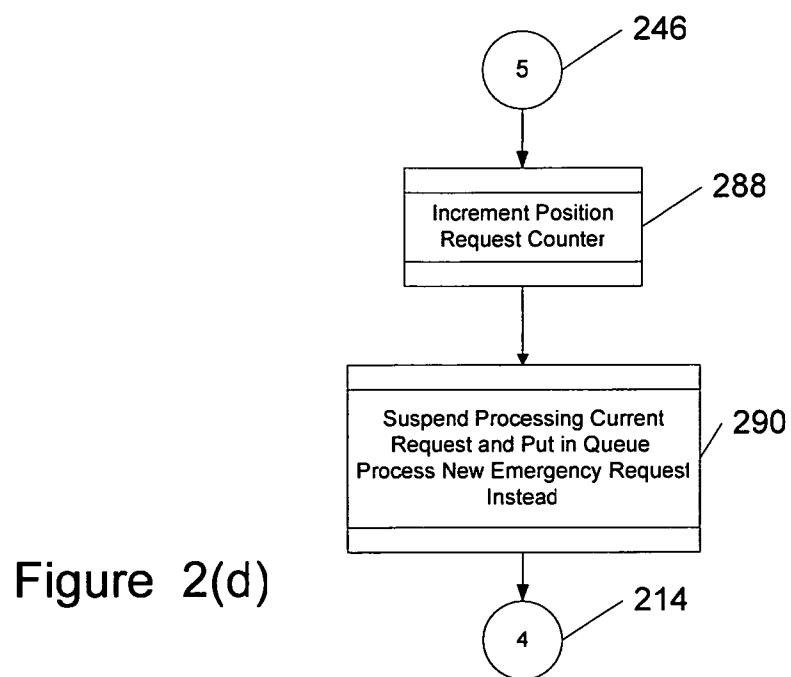


Figure 2(d)

REFERENCES CITED IN THE DESCRIPTION

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

Patent documents cited in the description

- US 20020050944 A [0004]
- WO 02060191 A [0006]
- US 20020183056 A1 [0018]

Non-patent literature cited in the description

- **M. MOEGLEIN ; N. F. KRASNER.** An Introduction to SnapTrack™ Server-Aided GPS Technology. *Institute of Navigation (ION) GPS 1998 Proceedings, Sept. 15-18, 1998, 333-344* [0004]

Fokozott felhasználói magánszféra mobil állomás helymeghatározó szolgáltatások számára

Szabadalmi igénypontok

1. Egy magánszféra (privacy) szabályozó rendszer egy mobil állomáson (102) való használatra, ahol a mobil állomás (102) egy vezeték nélküli kommunikációs rendszerrel kommunikál, és ahol a magánszféra szabályozó rendszer a mobil állomással (102) társított földrajzi hely információt szolgáltat, és tartalmaz:

a) egy magánszféra motort (120), amely legalább egy magánszféra szabályt tartalmazó magánszféra szabályrendszer komponensét foglal magában, ahol a magánszféra motor (120) a mobil állomás földrajzi helyére vonatkozó, egy a mobil állomáson (102) kívüli helykérelmező által előállított helyre vonatkozó kérelmeket vesz, és meghatározza, hogy a helyre vonatkozó kérelmet el kell-e utasítani legalább részben a legalább egy magánszféra szabály alapján; és

b) egy helymeghatározó modult (122), amely operatív módon kapcsolódik a magánszféra motorhoz (120) és azzal együttműködik, ahol a helymeghatározó modul (122) a mobil állomás (102) földrajzi helyére vonatkozó becsléseket szolgáltatja;

ahol a magánszféra motor (120)

szelektív módon aktiválja a helymeghatározó modult (122) a magánszféra szabályrendszer komponensnek megfelelően, annak érdekében, hogy vegye a földrajzi hely becsléseket a helymeghatározó modultól (122), és

válaszol a helyre vonatkozó kérelmekre a hely becslések feldolgozása útján, és

válaszúzeneteket nyújt a magánszféra szabályrendszer komponensnek megfelelően.

2. Az 1. igénypont szerinti magánszféra szabályozó rendszer, ahol a helymeghatározó modul (122) a következő eljárások közül egy vagy több szerint működik:

Global Positioning System, Assisted Global Positioning System, Advanced Forward Link Trilateration, Time of Arrival, Enhanced Observed Time Difference és pozícionálás azon vezeték nélküli kommunikációs cellák azonosítása alapján, amelyekben belül a mobil állomás (102) működik.

3. Az 1. igénypont szerinti magánszféra szabályozó rendszer, amely tartalmaz továbbá egy vezeték nélküli hálózati kommunikációs modult (112), amely operatív módon csatlakozik a magánszféra motorhoz (120) és a vezeték nélküli kommunikációs rendszerhez, ahol a vezeték nélküli hálózati kommunikációs modul (112) úgy van konfigurálva, hogy vegye a helyre vonatkozó kérelmeket a vezeték nélküli kommunikációs rendszertől és átvigye a válasz üzeneteket a vezeték nélküli kommunikációs rendszerhez, továbbá úgy van konfigurálva, hogy adatokat és szoftver utasításokat vegyen a vezeték nélküli kommunikációs rendszertől és adatokat és szoftver utasításokat vigyen át a vezeték nélküli kommunikációs rendszerhez.

4. A 3. igénypont szerinti magánszféra szabályozó rendszer, ahol a magánszféra motor (120) a vezeték nélküli kommunikációs rendszerből letöltött szoftvert tartalmaz.

5. A 3. igénypont szerinti magánszféra szabályozó rendszer, ahol a magánszféra motor (120) a vezeték nélküli kommunikációs rendszerből letöltött szoftver frissítésekkel módosított.

6. A 3. igénypont szerinti magánszféra szabályozó rendszer, ahol a magánszféra szabályrendszer a vezeték nélküli kommunikációs rendszerből letöltött szoftvert tartalmaz.



SZTNH-100049013

7. A 3. igénypont szerinti magánszféra szabályozó rendszer, ahol a magánszféra szabályrendszer a vezetéknélküli kommunikációs rendszerből letöltött frissítésekkel módosított.
8. A 7. igénypont szerinti magánszféra szabályozó rendszer, ahol a frissítések felhasználóra vonatkozó magánszféra szabályrendszer adatokat foglalnak magukban.
9. A 3. igénypont szerinti magánszféra szabályozó rendszer, ahol a helyre vonatkozó kérelmet egy a vezetéknélküli kommunikációs rendszerhez operatív módon csatlakoztatott külső alkalmazástól vesszük.
10. Az 1. igénypont szerinti magánszféra szabályozó rendszer, amely tartalmaz továbbá egy helyi kommunikációs modult (118), amely operatív módon kapcsolódik a magánszféra motorhoz (120) és külső helyi alkalmazásokhoz (116), ahol a helyi kommunikációs modul (118) úgy van konfigurálva, hogy vegye a helyre vonatkozó kérélmeket a külső helyi alkalmazásoktól (116) és átvigye a válasz üzeneteket a külső helyi alkalmazásokhoz (116), továbbá úgy van konfigurálva, hogy adatokat és szoftver utasításokat vegyen a külső helyi alkalmazásoktól (116) és adatokat és szoftver utasításokat vigyen át a külső helyi alkalmazásokhoz (116).
11. A 10. igénypont szerinti magánszféra szabályozó rendszer, ahol a magánszféra motor (120) egy külső helyi alkalmazástól (116) letöltött szoftvert tartalmaz.
12. A 10. igénypont szerinti magánszféra szabályozó rendszer, ahol a magánszféra motor (120) egy külső helyi alkalmazástól (116) letöltött szoftver utasítások révén szoftver frissítésekkel módosított.
13. A 10. igénypont szerinti magánszféra szabályozó rendszer, ahol a magánszféra szabályrendszer egy külső helyi alkalmazástól (116) letöltött szoftvert tartalmaz.
14. A 10. igénypont szerinti magánszféra szabályozó rendszer, ahol a magánszféra szabályrendszer egy külső helyi alkalmazástól (116) letöltött frissítésekkel módosított.
15. A 14. igénypont szerinti magánszféra szabályozó rendszer, ahol a frissítések felhasználóra vonatkozó magánszféra szabályrendszer adatokat foglalnak magukban.
16. A 10. igénypont szerinti magánszféra szabályozó rendszer, ahol a helyre vonatkozó kérelmet egy külső helyi alkalmazástól (116) vesszük.
17. Az 1. igénypont szerinti magánszféra szabályozó rendszer, amely tartalmaz továbbá egy a magánszféra motorhoz (120) operatív módon kapcsolódó felhasználói interfészt (106), ahol a felhasználói interfész (106) úgy van konfigurálva, hogy beviteli adatot fogadjon egy felhasználótól, és ahol a felhasználói beviteli adatot használjuk a magánszféra szabályrendszer frissítésekkel történő módosítására.
18. A 17. igénypont szerinti magánszféra szabályozó rendszer, ahol a frissítések felhasználóra vonatkozó magánszféra szabályrendszer adatokat foglalnak magukban.
19. A 17. igénypont szerinti magánszféra szabályozó rendszer, ahol a felhasználói interfész (106) helyre vonatkozó kérélmekre vonatkozó értesítéseket küld a felhasználónak, a magánszféra szabályrendszernek megfelelően, és ahol a felhasználói interfész (106) úgy van konfigurálva, hogy a helyre vonatkozó kérelem értesítésekre válaszképpen válaszokat fogadjon a felhasználótól.
20. A 19. igénypont szerinti magánszféra szabályozó rendszer, ahol a magánszféra szabályrendszer több

magánszféra osztályt foglal magában, ahol a magánszféra osztályok a magánszféra motor (120) által vett helyre vonatkozó kérelmeket osztályozzák, és ahol a magánszféra szabályrendszer tartalmaz továbbá magánszféra szabályokat, amelyek az egyes magánszféra osztályokra vonatkozóan a helyre vonatkozó kérelmekre adott válaszokat határozzák meg, és ahol a magánszféra szabályok a következő szabályok közül legalább egyet tartalmaznak:

- a) egy helyre vonatkozó kérelem alapértelmezett elfogadását vagy elutasítását szükségessé tevő szabály;
- b) egy helyre vonatkozó kérelemre vonatkozó felhasználói értesítést szükségessé tevő szabály;
- c) egy kért szolgáltatási minőségen alapuló felhasználói értesítést szükségessé tevő szabály;
- d) a helyre vonatkozó kérelem periodikusságán vagy kérelemre kezdeményezettségén alapuló felhasználói értesítést szükségessé tevő szabály;
- e) a helyre vonatkozó kérelem fellépésének időpontján alapuló felhasználói értesítést szükségessé tevő szabály;
- f) felhasználói értesítés céljára használandó kijelző üzemmódot meghatározó szabály;
- g) a rendelkezésre bocsátandó hely becslés pontossági tartományát meghatározó szabály;
- h) egy válaszüzenet alapértelmezett kezelését szükségessé tevő szabály, ha a felhasználó nem válaszol egy felhasználói értesítésre; és
- i) a mobil állomás aktuális földrajzi helyén alapuló válaszüzenet kezelést meghatározó szabály.

21. Az 1. igénypont szerinti magánszféra szabályozó rendszer, amely tartalmaz továbbá egy eltávolítható adattároló eszközt, ahol az eltávolítható adattároló eszköz operatív módon csatlakozik a magánszféra motorhoz (120), és ahol az eltávolítható adattároló eszköz úgy van konfigurálva, hogy felhasználó specifikus magánszféra szabályrendszer adatokat vegyen, tároljon és vigyen át.

22. A 21. igénypont szerinti magánszféra szabályozó rendszer, ahol az eltávolítható adattároló eszköz egy előfizetői azonosság modul eszközt tartalmaz.

23. A 21. igénypont szerinti magánszféra szabályozó rendszer, ahol az eltávolítható adattároló eszköz egy univerzális előfizetői azonosság modul eszközt tartalmaz.

24. A 21. igénypont szerinti magánszféra szabályozó rendszer, ahol az eltávolítható adattároló eszköz egy eltávolítható felhasználói azonosság modul eszközt tartalmaz.

25. Eljárás magánszféra (privacy) szabályozás biztosítására a mobil állomás földrajzi hely információ egy mobil állomásán (102), ahol a mobil állomás (102) egy vezeték nélküli kommunikációs rendszerrel kommunikál, és ahol a mobil állomás (102) szoftver utasításokat tartalmazó magánszféra motort (120) foglal magában, ahol a magánszféra motor szoftver utasítások magánszféra szabályrendszer utasításokat is magukban foglalnak, amelyek legalább egy magánszféra szabályt tartalmaznak, és ahol a mobil állomás (102) továbbá egy helymeghatározó modult (122) tartalmaz, amely képes a mobil állomás (102) földrajzi helyére vonatkozó becslések szolgáltatására, az eljárás a következő lépéseket foglalja magában:

- a) helyre vonatkozó kérelmek vétele (204) a mobil állomás (102) aktuális földrajzi helye vonatkozásában egy a mobil állomáson (102) kívüli helykérelmezőtől;

b) a helyre vonatkozó kérelmek feldolgozása a magánszféra motor szoftver utasítások szerint, ahol a helyre vonatkozó kérelem feldolgozása magában foglalja annak meghatározását, hogy a helyre vonatkozó kérelmet el kell-e utasítani legalább részben a legalább egy magánszféra szabály alapján,

c) a helymeghatározó modul (122) szelektív aktiválása a magánszféra szabályrendszer komponensnek megfelelően, a mobil állomás (102) földrajzi hely becsléseinek megszerzéséhez;

d) a földrajzi hely becslések feldolgozása a helyre vonatkozó kérelmeknek, a magánszféra motor szoftver utasításoknak és a magánszféra szabályoknak megfelelően; és

e) a helyre vonatkozó kérelmekre válaszoló válaszüzenetek szelektív szolgáltatása a magánszféra motor szoftver utasításoknak, a hely becsléseknek és a magánszféra szabályoknak megfelelően.

26. A 25. igénypont szerinti magánszféra szabályozó eljárás, ahol a helyre vonatkozó kérelmek feldolgozásának b) lépése tartalmaz továbbá egy vészeseti helyre vonatkozó kérelem feldolgozási lépést, a magánszféra szabályrendszer utasítások felülbírálata révén, vészeseti válasz üzenetek nyújtásához.

27. A 25. igénypont szerinti magánszféra szabályozó eljárás, ahol a helyre vonatkozó kérelmek feldolgozásának b) lépése konkurens helyre vonatkozó kérelmek feldolgozását is magában foglalja.

28. A 27. igénypont szerinti magánszféra szabályozó eljárás, ahol a függő helyre vonatkozó kérelmeket felfüggesztjük, amíg a vészeseti helyre vonatkozó kérelmek feldolgozása folyik.

29. A 25. igénypont szerinti magánszféra szabályozó eljárás, amely tartalmazza továbbá egy felhasználó értesítésének lépését a helyre vonatkozó kérelmekről.

30. A 29. igénypont szerinti magánszféra szabályozó eljárás, ahol a magánszféra szabályrendszer utasítások magánszféra osztályokat tartalmaznak az a) lépés során vett helyre vonatkozó kérelmek osztályozására, és ahol a magánszféra szabályrendszer utasítások magánszféra szabályokat foglalnak magukban minden egyes magánszféra osztályhoz a helyre vonatkozó kérelmekre egy válasz meghatározásához, és ahol a magánszféra szabályok a következő szabályok közül legalább egyet tartalmaznak:

a) egy helyre vonatkozó kérelem alapértelmezett elfogadását vagy elutasítását szükségessé tevő szabály;

b) egy helyre vonatkozó kérelemre vonatkozó felhasználói értesítést szükségessé tevő szabály;

c) egy kért szolgáltatási minőségen alapuló felhasználói értesítést szükségessé tevő szabály;

d) a helyre vonatkozó kérelem periodikusságán vagy kérelemre kezdeményezettségén alapuló felhasználói értesítést szükségessé tevő szabály;

e) a helyre vonatkozó kérelem fellépésének időpontján alapuló felhasználói értesítést szükségessé tevő szabály;

f) felhasználói értesítés céljára használandó kijelző üzemmódot meghatározó szabály;

g) a rendelkezésre bocsátandó hely becslés pontossági tartományát meghatározó szabály,

h) egy válaszüzenet alapértelmezett kezelését szükségessé tevő szabály, ha a felhasználó nem válaszol egy felhasználói értesítésre; és

i) a mobil állomás aktuális földrajzi helyén alapuló válaszüzenet kezelést meghatározó szabály.