(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 614 105**

(51) Int. CI.:

H04W 8/16 (2009.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **17.02.2004 PCT/US2004/004670**

(87) Fecha y número de publicación internacional: **02.09.2004 WO04075594**

(96) Fecha de presentación y número de la solicitud europea: **17.02.2004 E 04711904 (5)**

(97) Fecha y número de publicación de la concesión europea: **02.11.2016 EP 1593286**

(54) Título: **Privacidad de usuario mejorada para servicios de localización de estaciones móviles**

(30) Prioridad:

14.02.2003 US 447563 P
12.12.2003 US 490765 P
13.02.2004 US 779109

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
29.05.2017

(73) Titular/es:

QUALCOMM INCORPORATED (100.0%)
5775 Morehouse Drive
San Diego, CA 92121-1714, US

(72) Inventor/es:

ARCENS, SUZANNE

(74) Agente/Representante:

FORTEA LAGUNA, Juan José

DESCRIPCIÓN

Privacidad de usuario mejorada para servicios de localización de estaciones móviles

ANTECEDENTES

Campo

Esta invención se refiere al campo de los servicios de localización para dispositivos móviles, y más particularmente al control del usuario mejorado de la política de privacidad para las respuestas a las peticiones de localización.

Descripción de la técnica relacionada

Los servicios de localización (abreviados como LCS, por "Location Services") para teléfonos móviles y dispositivos de comunicación digitales inalámbricos (denominados colectivamente en lo sucesivo como estaciones móviles) son un área comercial cada vez más importante para los proveedores de comunicaciones inalámbricas. Esta importancia se refleja en el establecimiento de estándares y especificaciones funcionales para los LCS. Tres referencias ejemplares de los LCS son: Proyecto de Colaboración de Tercera Generación (3GPP), Grupo técnico de especificación (TSG) de Servicios y Aspectos del sistema, Descripción funcional de la etapa 2 (SA2) de LCS, versión 6, (3GPP TS 23.271 V6.0.0), junio de 2002; Documento Técnico (TD) S2-022360, 3GPP TSG-SA2 Reunión #26, Toronto, Canadá, 19-23 de agosto de 2002; y Proyecto de Colaboración de Tercera Generación (3GPP), Grupo técnico de especificación (TSG) de Servicios y Aspectos del sistema, Descripción funcional de la etapa 2 (SA2) de LCS, edición 6, (3GPP TS 23.271 V6.3.0), marzo de 2003. Las referencias se denominan en lo sucesivo como 3GPP-R1, 3GPP-R2 y 3GPP-R3 respectivamente.

Las referencias 3GPP-R1 y 3GPP-R3 describen un modelo funcional del sistema completo de los LCS, incluyendo secciones relacionadas con la privacidad del usuario. La referencia 3GPP-R2 describe un elemento de red, denominado como un registro de perfil privado (PPR), que mantiene la información de privacidad de los LCS de los abonados y que facilita las funciones de privacidad correspondientes. Estas referencias proporcionan una visión general de la tecnología y los estándares recientes relativos a los LCS y las operaciones de privacidad de los LCS. Las personas con conocimientos comunes en las técnicas de comunicación conocen numerosos procedimientos y aparatos para proporcionar LCS a los abonados de acuerdo con estas referencias.

Un procedimiento ventajoso conocido para determinar la localización de una estación móvil en un sistema de comunicación inalámbrica emplea el Sistema de Posicionamiento Global (GPS). La inclusión de un dispositivo GPS (o más en general, un módulo de determinación de la posición, o "PDM") en la estación móvil proporciona una capacidad de determinación de la posición muy precisa. Cuando se utiliza un PDM como medio principal para proporcionar información de localización precisa en una estación móvil, la red del proveedor de servicios debe ponerse en contacto con la estación móvil cuando se reciben peticiones para una localización exacta. Los procedimientos y aparatos para la implementación de la función del servicio de localización usando un PDM, como por ejemplo el uso de un GPS en una estación móvil, son bien conocidos para las personas con conocimientos comunes en las técnicas de comunicaciones inalámbricas. Actualmente se dispone de terminales que implementan las funciones de los LCS utilizando un GPS. Un sistema GPS ejemplar para estaciones móviles se describe en la referencia "Una introducción a la tecnología de GPS asistido por servidor SnapTrack™," M. Moeglein y N.F. Krasner, Actas de GPS del Instituto de Navegación (ION) de 1998, 15-18 de septiembre de 1998, págs. 333-344. Una solicitud de patente reciente que describe un sistema GPS adecuado para estaciones móviles es "Method and Apparatus for Measurement Processing of Satellite Positioning System (SPS) Signals", L. Sheynblat y N.F. Krasner, solicitud de Patente de Estados Unidos 20020050944, 2 de mayo de 2002.

De manera desventajosa, el control del usuario de la información de la política de privacidad es muy limitado y poco flexible utilizando los procedimientos existentes de privacidad de los LCS, en los que la privacidad del usuario se gestiona mediante una red de provisión de servicios. Por ejemplo, en algunos procedimientos de privacidad de los LCS de la técnica anterior a modo de ejemplo, el proveedor de servicios define diversas clases de clientes peticionarios, y cuando el usuario inicia el servicio se establece un perfil de privacidad del usuario, tal como el PPR al que se hace referencia más arriba, sobre la base de estas clases. De acuerdo con estos procedimientos privacidad de los LCS, el perfil de privacidad designa ciertas clases de peticionarios que tienen un acceso sin restricciones a la localización del usuario, y otras clases de peticionarios que tienen un acceso restringido. Por ejemplo, dichas restricciones pueden incluir un rechazo automático de la información de los LCS a unas clases restringidas específicas. Las restricciones también pueden incluir un requisito de notificación al usuario y (opcionalmente) aprobación de las peticiones de acceso a los LCS realizadas por los peticionarios de clases restringidas específicas. En estos sistemas ejemplares de la técnica anterior, las modificaciones del perfil de privacidad sólo se pueden llevar a cabo mediante la modificación del acuerdo de servicios entre el proveedor y el usuario. En los casos en los que la localización del usuario se determina principalmente mediante un PDM residente en la estación móvil, se efectúa una opción de modificación adicional mediante la desactivación del PDM. Aunque esta opción mejora la privacidad al permitir que el usuario impida la recuperación de la información precisa de la posición, la utilidad de esta solución es extremadamente limitada, ya que impide la recuperación de la localización

precisa para todas las clases de peticionarios hasta que el PDM se habilite una vez más.

Otro ejemplo se describe en el documento WO02/060191.

La presente divulgación está dirigida a un procedimiento y aparato para la gestión de la privacidad de los LCS en una estación móvil. La presente divulgación permite que un usuario de una estación móvil controle los LCS de manera cómoda y flexible.

RESUMEN

La presente divulgación se refiere a un procedimiento y aparato para proporcionar la localización geográfica de una estación móvil inalámbrica, y más particularmente a procedimientos y aparatos para proporcionar un control del usuario mejorado de las políticas de privacidad que supervisan las respuestas a las peticiones de información de localización. Estas peticiones se denominan en lo sucesivo como peticiones de localización o, de manera equivalente, como peticiones de posición.

En un modo de realización ejemplar, un sistema de control de la privacidad para una estación móvil comprende un motor de privacidad, un módulo de determinación de la posición (PDM) y una interfaz de usuario. El motor de privacidad es un módulo de software que controla las respuestas de la estación móvil a las peticiones de localización.

El motor de privacidad incluye además una política de privacidad. La política de privacidad incluye clases de privacidad para la clasificación de los peticionarios de localización y sus peticiones de localización asociadas, y reglas de privacidad para la determinación de la respuesta a las peticiones de localización para cada clase de privacidad.

Una clase de privacidad está definida mediante una lista de aplicaciones y peticionarios de localización. Las aplicaciones y los peticionarios de localización se pueden especificar de forma individual o agrupados por categorías o tipos, en base a la información de identificación como por ejemplo una URL, un dominio de Internet u otros datos que se pueden proporcionar con una petición de posición. Una petición de localización se clasifica según el peticionario de localización. De este modo, las peticiones de localización se pueden asignar a una clase de privacidad basándose en la información proporcionada con la petición de localización. Ejemplos de clases de privacidad incluyen, sin limitación: una clase de privacidad predeterminada para aplicaciones de petición de localización desconocidas o no declaradas e identidades de peticionarios no incluidas específicamente en ninguna otra clase; una clase de privacidad predeterminada para aplicaciones de petición de localización de confianza e identidades de peticionarios no incluidas específicamente en ninguna otra clase; y clases especificadas por el usuario que incluyen aplicaciones de petición de localización e identidades de peticionarios identificadas por una URL u otros datos de identificación que se pueden proporcionar con los datos de petición de la posición.

Cada clase de privacidad tiene un conjunto asociado de reglas de privacidad para la determinación de la respuesta del motor de privacidad a las peticiones de localización. Los ejemplos incluyen, sin limitación: una regla que especifica un acceso sin restricciones; una regla para el rechazo de acceso predeterminado; una regla para el acceso dependiente de la notificación al usuario y la aprobación requerida; una regla para el acceso con notificación al usuario pero sin aprobación requerida; una regla para el rechazo de acceso durante periodos de tiempo seleccionados por el usuario; una regla para el acceso a una aproximación definida de la localización únicamente; *etc*. La política de privacidad, las clases de privacidad y las reglas de privacidad determinan cómo responde el motor de privacidad a todas y cada una de las peticiones de localización.

Ventajosamente, usando los presentes procedimientos y aparatos de privacidad del usuario mejorada de la invención, el usuario puede controlar o modificar la política de privacidad de una estación móvil específica a través de la interfaz de usuario en la estación móvil. En un modo de realización ejemplar, la interfaz de usuario comprende una interfaz de usuario que tiene medios de entrada adecuados tales como un lápiz, un dispositivo de señalización o un teclado. En otra realización del concepto de la presente invención, la política de privacidad se controla a través de una aplicación de red que se conecta a la estación móvil a través de una red de datos inalámbrica. En un modo de realización adicional del procedimiento de la presenta invención, la política de privacidad se puede controlar mediante una aplicación residente en un dispositivo local, tal como un ordenador portátil o un asistente personal digital, en el que el dispositivo está conectado operativamente a la estación móvil.

Ventajosamente, el motor de privacidad de la estación móvil, que incluye una política de privacidad inicial, puede ser recibido por *(es decir*, descargado a) la estación móvil a través de una red de datos inalámbrica.

BREVE DESCRIPCIÓN DE LOS DIBUJOS

La figura 1 es un diagrama de bloques de un sistema de comunicación ejemplar que incluye una estación móvil que tiene un motor de privacidad adaptado para su uso con el concepto de la presente invención.

Las figuras 2A a 2D muestran un diagrama de flujo de un procedimiento ejemplar para proporcionar una privacidad del usuario mejorada en una aplicación de servicios de localización para su uso por estaciones móviles y otros dispositivos de comunicación inalámbrica.

Los números de referencia y designaciones similares en los diversos dibujos indican elementos similares.

DESCRIPCIÓN DETALLADA

A lo largo de esta descripción, se describen los modos de realización y variaciones con el propósito de ilustrar los usos e implementaciones del concepto de la invención. La descripción ilustrativa debe entenderse como una presentación de ejemplos del concepto de la invención, y no como una limitación del alcance del concepto tal y como se describe en el presente documento.

La figura 1 muestra un diagrama de bloques de un dispositivo de comunicación inalámbrica y un sistema de comunicación inalámbrica que se puede adaptar para su uso con el concepto de la presente invención. Como se muestra en la figura 1, un modo de realización ejemplar incluye una estación móvil 102 que comprende una interfaz de usuario 106, un módulo de comunicación de red inalámbrica 112, un bloque de aplicaciones 114, un módulo de comunicación local 118, un motor de privacidad 120, un módulo de determinación de la posición 122 y otros módulos 124.

Como se muestra en la figura 1, en un modo de realización del concepto de la presente invención, el módulo de comunicación de red inalámbrica 112 proporciona una conectividad inalámbrica de datos entre la estación móvil 102 y las redes de datos externas 110. Las redes de datos externas 110 pueden comprender una variedad de sistemas de red. Por ejemplo, en un modo de realización una red de datos externa puede comprender una red inalámbrica del proveedor de servicios. Como otro ejemplo, una red de datos externa puede ser un proveedor de servicios de Internet que proporciona una conexión para recibir y transmitir datos entre la estación móvil e Internet. En general, las redes de datos externas 110 comprenden cualquier sistema de datos capaz de transmitir y recibir datos hacia y desde una estación móvil usando la comunicación inalámbrica. Como se muestra en la figura 1, el módulo de comunicación de red inalámbrica 112 también está acoplado operativamente al bloque de aplicaciones 114 y al motor de privacidad 120. El módulo de comunicación inalámbrico 112 recibe y transmite datos desde el bloque de aplicaciones 114 y el motor de privacidad 120.

En un modo de realización, el bloque de aplicaciones 114 comprende aplicaciones de localización que pueden requerir una estimación de la posición de la estación móvil. Estas aplicaciones de localización pueden residir en la MS, con lo que no necesitan la interacción con la red, o pueden implicar la interacción con un servidor de localización en la red (por ejemplo, el módulo 108) y por lo tanto actuar como un cliente de localización. Para este modo de realización ejemplar, el bloque de aplicaciones 114 también comprende otras aplicaciones relacionadas con las comunicaciones de datos de red y otras funciones de la estación móvil. Los ejemplos de dichas aplicaciones incluyen, sin limitación: clientes de correo electrónico, navegadores web, clientes de ftp y otras aplicaciones de software para la recepción o descarga de datos, archivos de datos e instrucciones de software en la estación móvil 102. El bloque de aplicaciones 114 está acoplado al módulo de comunicación inalámbrica 112 para recibir y transmitir datos y, por lo tanto, comunicarse con las redes de datos externas 110. El bloque de aplicaciones 114 también está acoplado operativamente a la interfaz de usuario 106 para recibir y transmitir datos para la operación del usuario y la comunicación con diversas aplicaciones. El bloque de aplicaciones 114 también está acoplado operativamente al motor de privacidad 120 para recibir y transmitir datos. Dichos datos pueden comprender peticiones de localización y datos de respuesta. Dichos datos también pueden comprender instrucciones software recibidas o descargadas para crear, modificar e implementar las funciones y capacidades del motor de privacidad 120. Como alternativa, los datos para crear, modificar o implementar las funciones del motor de privacidad se pueden recibir directamente desde el módulo de comunicación inalámbrica 112, que también está acoplado operativamente al motor de privacidad 120 para recibir y transmitir datos. Como una alternativa adicional, los datos para crear, modificar o implementar las funciones del motor de privacidad se pueden recibir y ejecutar mediante los componentes de la estación móvil no mostrados en la figura 1. Dichos componentes son bien conocidos por los expertos en las técnicas de comunicación, y pueden comprender, por ejemplo, circuitos integrados específicos de la aplicación (ASIC), interfaces de programación de aplicaciones (API), memoria de acceso aleatorio (RAM), memoria de sólo lectura (ROM), *etc.* Procedimientos y sistemas ejemplares para la descarga y ejecución de aplicaciones en las estaciones móviles a través de redes inalámbricas se describen por Lundblade, y otros, en "Distribución y ejecución segura de aplicaciones en un entorno inalámbrico," publicación de solicitud de Patente de Estados Unidos nº US 2002/0183056 Al, 5 de diciembre de 2002.

El módulo de comunicación local 118 proporciona un medio para recibir y transmitir datos opcionalmente entre la estación móvil 102 y un módulo de aplicaciones locales externas 116. En un modo de realización, el módulo de aplicaciones locales externas 116 reside en un dispositivo conectado localmente como por ejemplo un ordenador personal, un ordenador portátil o un asistente personal digital. El módulo 118 proporciona conectividad con el dispositivo conectado localmente. El módulo de comunicación local 118 también está acoplado operativamente al motor de privacidad 120 para recibir y transmitir datos. Dichos datos pueden incluir instrucciones software que crean, modifican e implementan las funciones y capacidades del motor de privacidad 120. Además, estos datos pueden

incluir datos de entrada y de salida para las aplicaciones de localización (aplicaciones que requieren datos de localización) que se ejecutan en un dispositivo independiente tal como un ordenador portátil que está conectado a la MS a través de infrarrojos, Bluetooth, cable USB u otros medios que son distintos de la conectividad de red proporcionada por el módulo de comunicación inalámbrica 112. El enrutamiento de estos datos de localización hacia el motor de privacidad 120 facilita la gestión de la privacidad para las peticiones de localización de las aplicaciones locales, tal como se describe a continuación.

Como se ha descrito anteriormente, el motor de privacidad 120 está acoplado a los elementos 112, 114 y 118 para recibir y transmitir datos. El motor de privacidad 120 también está acoplado para recibir y transmitir datos con la interfaz de usuario 106, el módulo de determinación de la posición 122 y los otros módulos 124. A continuación se especifican las funciones y el funcionamiento del motor de privacidad 120.

La interfaz de usuario 106 proporciona un medio para que un usuario de la estación móvil reciba información procedente de, proporcione instrucciones a y utilice las aplicaciones y funciones incorporadas en el bloque de aplicaciones 114 y el motor de privacidad 120. Por ejemplo, la interfaz de usuario 106 puede comprender una interfaz gráfica de usuario y medios de entrada adecuados tales como una pantalla táctil, un dispositivo de señalización o un teclado. La interfaz de usuario 106 puede comprender también medios para transmitir y recibir sonidos, comandos de voz o cualquier otro medio para recibir información procedente de, proporcionar instrucciones a y utilizar los módulos de software, las aplicaciones y los dispositivos digitales acoplados a la estación móvil 102.

El módulo de determinación de la posición (PDM) 122 genera datos que representan la localización de la estación móvil 102. Un ejemplo bien conocido de un PDM adecuado emplea un procedimiento o dispositivo de un Sistema de Posicionamiento Global (GPS). Sin embargo, las presentes instrucciones comprenden la utilización de cualquier PDM que tenga la capacidad de proporcionar datos de posición o datos de localización a la estación móvil 102. Por ejemplo, el PDM puede emplear dichos procedimientos de posicionamiento bien conocidos como el GPS asistido (AGPS), la Trilateración avanzada de Enlace Directo (AFLT), la Hora de llegada (TOA), la Diferencia temporal observada mejorada (E-OTD), el posicionamiento basado en la identificación de las celdas de comunicación inalámbrica en donde está funcionando la MS (posicionamiento basado en celdas), etc. Estos procedimientos son bien conocidos por los expertos en las técnicas de comunicación y no es necesario describirlos en este documento.

El bloque de otros módulos 124 representa los módulos de software y los componentes hardware para la implementación o el aumento de las funciones de la estación móvil. Por ejemplo, estos módulos de software y componentes de hardware pueden incluir circuitos integrados específicos de la aplicación (ASIC), interfaces de programación de aplicaciones (API), memoria de acceso aleatorio (RAM), memoria de sólo lectura (ROM), Módulo de Identidad de Abonado (SIM) o un Módulo de Identidad de Abonado Universal (USIM), una cámara, etc. Aunque las conexiones para el bloque de otros módulos 124 no se muestran en la figura 1, las personas expertas en la técnica comprenderán fácilmente cómo los módulos y componentes del bloque de otros módulos 124 están acoplados operativamente en la estación móvil según sea necesario para la funcionalidad.

Haciendo aún referencia a la figura 1, en un modo de realización ejemplar, un servidor de gestión de privacidad 104 comprende una aplicación de software que está conectada a las redes de datos externas 110 para recibir y transmitir datos. El servidor de gestión de privacidad 104 está acoplado a las redes de datos externas 110 para intercambiar datos con el módulo de comunicación de red inalámbrica 112. El servidor de gestión de privacidad 104 se comunica con el motor de privacidad 120 a través de las redes de datos externas 110 y el módulo de comunicación de red inalámbrica 112. El servidor de gestión de privacidad 104 puede recibir y transmitir datos al bloque de aplicaciones de red 114 a través de las redes de datos externas 110 y el módulo de comunicación de red inalámbrica 112. Los datos transmitidos entre el servidor de gestión de privacidad 104, el bloque de aplicaciones de red 114 y el motor de privacidad 120 pueden incluir instrucciones de software que crean, modifican e implementan las funciones o capacidades del motor de privacidad 120. Del mismo modo, los datos transmitidos entre el servidor de gestión de privacidad 104 y el motor de privacidad 120 a través del módulo de comunicación 112 pueden incluir instrucciones de software que crean, modifican e implementan las funciones y capacidades del motor de privacidad 120. En general, los datos transmitidos entre el servidor de gestión de privacidad 104 y los elementos que comprenden los datos hacia la estación móvil 102. Por ejemplo, el PDM puede emplear dichos procedimientos de posicionamiento bien conocidos como el GPS asistido (AGPS), la Trilateración de Enlace Directo avanzada (AFLT), la Hora de llegada (TOA), la Diferencia temporal observada mejorada (E-OTD), el posicionamiento basado en la identificación de las celdas de comunicación inalámbrica en donde está funcionando la MS (posicionamiento basado en celdas), *etc.* Estos procedimientos son bien conocidos por los expertos en las técnicas de comunicación y no es necesario describirlos en este documento.

El bloque de otros módulos 124 representa los módulos de software y los componentes hardware para la implementación o el aumento de las funciones de la estación móvil. Por ejemplo, estos módulos de software y componentes de hardware pueden incluir circuitos integrados específicos de la aplicación (ASIC), interfaces de programación de aplicaciones (API), memoria de acceso aleatorio (RAM), memoria de sólo lectura (ROM), un Módulo de Identidad de Abonado (SIM) o un Módulo de Identidad de Abonado Universal (USIM), una cámara, *etc.* Aunque las conexiones para el bloque de otros módulos 124 no se muestran en la figura 1, las personas expertas en la técnica comprenderán fácilmente cómo los módulos y componentes del bloque de otros módulos 124 están

acoplados operativamente en la estación móvil según sea necesario para la funcionalidad.

Haciendo aún referencia a la figura 1, en un modo de realización ejemplar, un servidor de gestión de privacidad 104 comprende una aplicación de software que está conectada a las redes de datos externas 110 para recibir y transmitir datos. El servidor de gestión de privacidad 104 está acoplado a las redes de datos externas 110 para intercambiar datos con el módulo de comunicación de red inalámbrica 112. El servidor de gestión de privacidad 104 se comunica con el motor de privacidad 120 a través de las redes de datos externas 110 y el módulo de comunicación de red inalámbrica 112. El servidor de gestión de privacidad 104 puede recibir y transmitir datos al bloque de aplicaciones de red 114 a través de las redes de datos externas 110 y el módulo de comunicación de red inalámbrica 112. Los datos transmitidos entre el servidor de gestión de privacidad 104, el bloque de aplicaciones de red 114 y el motor de privacidad 120 pueden incluir instrucciones de software que crean, modifican e implementan las funciones o capacidades del motor de privacidad 120. Del mismo modo, los datos transmitidos entre el servidor de gestión de privacidad 104 y el motor de privacidad 120 a través del módulo de comunicación 112 pueden incluir instrucciones de software que crean, modifican e implementan las funciones y capacidades del motor de privacidad 120. En general, los datos transmitidos entre el servidor de gestión de privacidad 104 y los elementos que comprenden la estación móvil 102 pueden utilizarse para crear, modificar o implementar módulos de software en la estación móvil 102 que facilitan o se refieren a los LCS y a la gestión de privacidad.

El bloque de aplicaciones de petición de localización 108 de la figura 1 representa las aplicaciones de petición de localización conectadas a través de las redes de datos externas 110 para recibir y transmitir datos a la estación móvil 102. Las aplicaciones de petición de localización 108 están acopladas, a través de la red de datos externa 110 y el módulo de comunicación de red inalámbrica 112, para recibir y transmitir datos al motor de privacidad 120. A continuación se describe la transmisión y recepción de la petición de posición y los datos de respuesta de posición entre el bloque de aplicaciones de petición de localización 108 y el motor de privacidad 120.

Política de privacidad ejemplar

En un modo de realización ejemplar, el motor de privacidad 120 es un módulo de software que realiza operaciones para controlar las respuestas de la estación móvil a las peticiones de información de localización. Estas peticiones se denominan en el presente documento como peticiones de localización o, de manera equivalente, como peticiones de posición.

El motor de privacidad incluye además una política de privacidad. La política de privacidad es un componente del motor de privacidad que incluye clases de privacidad para la clasificación de los peticionarios de localización y sus peticiones de localización asociadas, y reglas de privacidad para la determinación de la respuesta a las peticiones de localización para cada clase de privacidad.

Una clase de privacidad está definida mediante una lista de aplicaciones y peticionarios de localización. Las aplicaciones y los peticionarios de localización se pueden especificar de forma individual o agrupados por categorías o tipos, en base a información de identificación como por ejemplo una URL, un dominio de Internet u otros datos que se pueden proporcionar con una petición de posición. Una petición de localización se clasifica según el peticionario de localización. De este modo, las peticiones de localización se pueden asignar a una clase de privacidad basándose en la información proporcionada con la petición de localización. Ejemplos de clases de privacidad incluyen, sin limitación: una clase de privacidad predeterminada para aplicaciones de petición de localización desconocidas o no declaradas e identidades de peticionarios no incluidas específicamente en ninguna otra clase; una clase de privacidad predeterminada para aplicaciones de petición de localización de confianza e identidades de peticionarios no incluidas específicamente en ninguna otra clase; y clases especificadas por el usuario que incluyen aplicaciones de petición de localización e identidades de peticionarios identificadas por una URL u otros datos de identificación que se pueden proporcionar con los datos de petición de la posición.

Cada clase de privacidad tiene un conjunto asociado de reglas de privacidad para la determinación de la respuesta del motor de privacidad a las peticiones de localización. Los ejemplos incluyen, sin limitación: una regla que especifica un acceso sin restricciones; una regla que especifica el rechazo de acceso predeterminado; una regla que especifica el acceso dependiente de la notificación al usuario y la aprobación requerida; una regla que especifica el acceso con notificación al usuario pero sin aprobación requerida; una regla que especifica el rechazo de acceso durante periodos de tiempo seleccionados por el usuario; una regla que especifica el acceso para una aproximación definida de la localización únicamente; etc. La política de privacidad, las clases de privacidad incluidas y las reglas de privacidad incluidas determinan cómo responde el motor de privacidad a todas y cada una de las peticiones de localización.

Inicialización ejemplar y procedimiento de actualización de software

En un modo de realización ejemplar del concepto de la presente invención, una estación móvil sin control de privacidad del usuario se puede equipar inicialmente con módulos de software para implementar la privacidad del usuario mejorada para los LCS de la estación móvil mediante la recepción o la descarga de datos desde un servidor de red. Los datos e instrucciones de software para la instalación y la implementación operativa del motor de

privacidad 120 (figura 1), que incluye una política de privacidad inicial, se pueden recibir o descargar en la estación móvil 102 desde un servidor de red (por ejemplo, el servidor de gestión de privacidad 104 de la figura 1, u otros servidores de red que no se muestran) a través del módulo de comunicación inalámbrica 112. La recepción y la instalación de los datos recibidos o descargados se puede realizar mediante un navegador u otro componente en el módulo de aplicaciones de red 114 o mediante los componentes incluidos en los otros módulos 124. Los procedimientos para la recepción o la descarga de aplicaciones y módulos de software a las estaciones móviles a través de una conexión de red inalámbrica son bien conocidos para las personas de experiencia común en las técnicas de comunicaciones inalámbricas. Como se ha señalado anteriormente, la referencia Lundblade describe los procedimientos y sistemas ejemplares para la descarga y ejecución de aplicaciones en las estaciones móviles a través de redes inalámbricas. En un modo de realización, la estación móvil incluye una plataforma de software para ayudar a la comunicación de las aplicaciones con la estación móvil, tal como el software Binary Runtime Environment for Wireless™ (BREW) desarrollado por QUALCOMM Incorporated, con sede en San Diego, California.

Las actualizaciones de software y las modificaciones del motor de privacidad 120 (todavía haciendo referencia a la figura 1), la política de privacidad y otros módulos y componentes de software de la estación móvil también se pueden recibir o descargar desde un servidor de red tal como se describió anteriormente. En particular, el usuario (u otra entidad que tenga permisos para hacerlo), puede actualizar la política de privacidad mediante la conexión de red inalámbrica. Como alternativa, el usuario también puede actualizar la política de privacidad mediante la interfaz de usuario 106. En otra alternativa, el usuario puede actualizar la política de privacidad mediante la introducción de datos utilizando una aplicación local externa (como la representada por el bloque de aplicaciones locales externas 116) conectada a través del módulo de comunicación local 118. En otra alternativa adicional, el usuario puede introducir datos de la política de privacidad específicos del usuario utilizando un dispositivo extraíble de almacenamiento de datos (no mostrado en la figura 1). Los datos de la política de privacidad específicos del usuario incluyen las clases de privacidad y las reglas de privacidad que se pueden seleccionar, modificar o crear de acuerdo a las necesidades o preferencias del usuario de la estación móvil. En un modo de realización ventajoso del concepto de la presente invención, el fabricante o el proveedor de servicios equipa la estación móvil 102 con un motor de privacidad inicial o predeterminado que incluye una política de privacidad genérica. El usuario personaliza entonces la política de privacidad genérica para incluir las clases de privacidad y las reglas de privacidad específicas del usuario mediante uno o más de los siguientes procedimientos: 1) la descarga de datos de la política de privacidad específicos del usuario desde una red; 2) la introducción de datos de la política de privacidad específicos del usuario utilizando la interfaz de usuario; 3) el uso de una aplicación local externa en un dispositivo conectado localmente para introducir los datos de la política de privacidad específicos del usuario; o 4) el uso de un dispositivo extraíble de almacenamiento de datos para introducir los datos previamente almacenados de la política de privacidad específicos del usuario. A continuación se describe una implementación ejemplar de dispositivos extraíbles de almacenamiento de datos, como por ejemplo los Módulos de Identidad de Abonado, los Módulos de Identidad de Abonado Universales o los Módulos de Identidad Extraíbles.

Procedimiento de operación ejemplar para el control de privacidad del usuario mejorada

Las figuras 2(a)-2(d) ilustran un diagrama de flujo unificado para un procedimiento ejemplar de la privacidad del usuario mejorada para su uso en los LCS de las estaciones móviles. Las conexiones de flujo entre las figuras 2(a) y 2(b) están representadas por los elementos 214, 220, 230 y 232. Del mismo modo, las conexiones de flujo entre las figuras 2(a) y 2(c) están representadas por los elementos 202, 208 y 223. La conexión de flujo entre las figuras 2(b) y 2(c) está representada por el elemento 258. Las conexiones de flujo entre las figuras 2(b) y 2(d) están representadas por los elementos 214 y 246. La conexión de flujo entre las figuras 2(c) y 2(d) está representada por el elemento 246.

El elemento 202 en la figura 2(a) representa un estado durante el cual el motor de privacidad 120 (figura 1) espera la recepción de una petición de información de datos de localización (*es decir*, una petición de posición). En el PASO 204 el motor de privacidad 120 recibe una petición de posición a través de las conexiones de datos descritas anteriormente con referencia a la figura 1. En referencia a la presente implementación ejemplar, los datos de petición de posición pueden comprender cualquiera de los siguientes datos: 1) la dirección de red y el tipo de aplicación de petición de localización; 2) la categoría de peticionario (por ejemplo, servicios de emergencia, servicios comerciales, persona individual); 3) la identidad del peticionario, en su caso; 4) la palabra de código o el certificado digital para la verificación de la identidad del peticionario; 5) la calidad de servicio (QoS) solicitada. Será obvio para las personas de experiencia común en las técnicas de comunicación que el alcance de las presentes instrucciones incluye el uso de otros tipos de datos de petición de posición tales como, por ejemplo, la información de la zona geográfica, la información del usuario, la información del peticionario, el sistema de coordenadas, *etc.,* que puedan ser necesarios para implementar otros modos de realización.

Haciendo referencia de nuevo a la figura 2(a), en el PASO 206, un contador de peticiones de posición se inicializa a un valor de cero. El valor cero representa el caso en el que se ha recibido una sola petición de posición. Si se reciben más peticiones de posición mientras que se está procesando una primera petición de posición, el contador de peticiones de posición se incrementa y disminuye tal como se describe a continuación. El objetivo del contador de peticiones de posición es la gestión de múltiples peticiones de posición concurrentes.

El elemento 208 representa una conexión de flujo de la figura 2(c). Como se describe a continuación, los datos de petición de posición serán procesados mediante el procedimiento de la invención después de un PASO 286 de la figura 2(c) a través de la conexión de flujo 208 solamente si se recibe una petición de posición posterior mientras que se está procesando una petición de posición previa.

En el PASO 210, el motor de privacidad 120 (figura 1) invoca una política de privacidad seleccionada que asigna una clase de privacidad a la petición de posición recibida durante el PASO 204 (o a través del elemento 208). Como se describió anteriormente, la política de privacidad comprende una lista para la asignación de clases de privacidad a peticiones de posición, y reglas de privacidad para las decisiones basadas en las clases de privacidad asignadas.

Haciendo referencia de nuevo a la figura 1, el motor de privacidad 120 puede invocar opcionalmente al módulo de aplicaciones 114, a los otros módulos 124 o a los módulos y componentes de la estación móvil que no se muestran en la figura, para llevar a cabo la clasificación de los datos de petición de posición. Por ejemplo, se puede invocar una aplicación de red para verificar los datos de certificados digitales.

Haciendo referencia nuevamente a la figura 2(a), en un PASO 212 se evalúan los datos de petición de posición para determinar si la petición de posición es una petición de servicios de emergencia. De conformidad con los requisitos legales habituales, una petición de servicios de emergencia anulará la política de privacidad, y se devolverán al peticionario los datos de posición con la mayor rapidez posible. Para una petición de servicios de emergencia el procedimiento continúa a través de la conexión de flujo 214 hasta el PASO 256 (figura 2(b)) para eludir la política de privacidad y la agilizar la respuesta. Para una petición que no sea de emergencia, el procedimiento continúa en el PASO 216.

En el PASO 216 se evalúan los datos de petición de posición para determinar si hay otros requisitos que requieran que se anule la política de privacidad. Por ejemplo, ciertos países pueden requerir una anulación para las peticiones procedentes de las autoridades policiales u otras agencias gubernamentales. Si se requiere una anulación, el procedimiento avanza a través de la conexión de flujo 214 al PASO 256 para acelerar el proceso. Si no se requiere una anulación, el procedimiento continúa en el PASO 218.

Haciendo referencia nuevamente a la figura 2(a), en el PASO 218, el motor de privacidad 120 (figura 1) invoca la política de privacidad para determinar si se debe rechazar la petición de posición basándose en las normas asociadas a la clase de privacidad asignada a la petición. El rechazo de una petición de información de posición se puede determinar en base a una pluralidad de criterios. En un primer ejemplo, la petición se puede rechazar debido a que el peticionario es una entidad comercial, y la clase de privacidad asignada para las entidades comerciales especifica un rechazo automático. En un segundo ejemplo, la petición se puede rechazar debido a que la identidad del peticionario es una persona física que ha sido colocada en una clase de privacidad con una norma que especifica el rechazo automático. En un tercer ejemplo, la petición se puede rechazar debido a que los datos de petición de posición no incluyen un certificado digital o una contraseña que verifique la identidad del peticionario, y la clase de privacidad predeterminada para esta categoría incluye una norma que especifica el rechazo automático. En un cuarto ejemplo, el usuario puede haber elegido la designación de que todas las peticiones de posición, distintas de las relacionadas con los servicios de emergencia, se coloquen en una clase de privacidad que especifica el rechazo automático durante unos períodos de tiempo especificados. Será obvio para los expertos en la técnica de las comunicaciones inalámbricas que dentro del alcance de las presentes instrucciones se incluyen muchos otros ejemplos.

Si se toma una decisión en el PASO 218 para rechazar la petición de posición, entonces no se computará ninguna posición y el procedimiento pasa a un PASO 222 en donde se transmite un mensaje de rechazo de servicio a una aplicación de petición de localización. Como se describe a continuación con más detalle haciendo referencia a la descripción del diagrama de flujo de la figura 2(b), el PASO 222 también se puede implementar a través de conexión de flujo 220 siguiendo los pasos 238 o 242 de la figura 2(b). Tras el PASO 222, el procedimiento de la invención continúa en el PASO 282 de la figura 2(c) a través de la conexión de flujo del proceso 223. Como se explicará más a fondo en lo que sigue, en el PASO 282 el procedimiento comprueba el contador de peticiones de posición para determinar si las peticiones de posición adicionales se ponen en cola antes de volver al PASO 202 del proceso de estado inactivo o bien ejecutar más pasos del proceso.

Volviendo a la figura 2(a), si en el PASO de decisión 218 se determina que la petición no se debe rechazar, se invoca una política de privacidad en un PASO 224 para determinar si se requiere una notificación al usuario. Si en el PASO 224 se determina que no se requiere la notificación al usuario, el procedimiento de la invención continúa a través de la conexión de flujo 230 hasta un PASO 250 de la figura 2(b) para su posterior procesamiento. Esto se describe en más detalle a continuación en relación con la descripción de la figura 2(b).

Si en el PASO 224 se determina que se requiere la notificación al usuario, entonces en un PASO 226 se transmite una notificación al usuario a través de la interfaz de usuario 106 (figura 1). La interfaz de usuario 106 puede emplear sonido, imagen, vibraciones u otros medios para alertar al usuario de que se ha concedido una petición de posición, y se puede utilizar un gráfico, texto, una pantalla acústica u otra presentación para transmitir información relativa a la petición de posición, como por ejemplo la categoría del peticionario, la identidad del peticionario y/o la QoS

solicitada.

En el PASO 228 el motor de privacidad 120 invoca la política de privacidad para determinar si la petición de posición requiere respuesta del usuario además de la notificación al usuario. Si no es así, entonces el procedimiento de la invención procede a través de la conexión de flujo 230 al PASO 250 de la figura 2(b) para su posterior procesamiento. Si se requiere una respuesta del usuario, entonces se inicia una espera temporizada para la respuesta del usuario en el PASO 232.

La figura 2(b) es una continuación del diagrama de flujo unificado de la figura 2(a)-2(c), procedente del PASO 232 (espera temporizada para la respuesta del usuario). Los PASOS 234, 236 y 238 representan los posibles eventos que pueden finalizar el período de espera temporizada en el PASO 232. El PASO 240 representa un evento que puede ocurrir durante el período de espera temporizada en el PASO 232.

Si la espera temporizada para la respuesta del usuario en el PASO 232 finaliza mediante el evento representado en el PASO 234, el usuario acepta la petición, entonces los datos de petición de posición se transfieren al PASO 250 para su posterior procesamiento.

Si la espera temporizada para la respuesta del usuario en el PASO 232 finaliza sin respuesta del usuario mediante el evento representado en el PASO 236, vencimiento de temporización, entonces se transmiten los datos de petición de posición y el procedimiento procede al PASO 242 para su posterior procesamiento. El PASO 242 invoca la política de privacidad para determinar si una ausencia de respuesta del usuario requiere un rechazo. Si una ausencia de respuesta del usuario requiere un rechazo, entonces el procedimiento de la invención procede a través de la conexión de flujo 220 al PASO 222 (mostrado en la figura 2(a)). Si una ausencia de respuesta del usuario no requiere un rechazo, entonces el procedimiento continúa en el PASO 250 para su posterior procesamiento.

Si la espera temporizada para la respuesta del usuario del PASO 232 finaliza mediante el evento representado en el PASO 238 (el usuario rechaza la petición), entonces el procedimiento de la invención procede a través de la conexión de flujo 220 al PASO 222, que se muestra en la figura 2(a).

Como se muestra en la figura 2(b), si se recibe una nueva petición de posición durante la espera temporizada del PASO 232, *es decir*, el caso representado en el PASO 240 (posible llegada de una nueva petición de posición durante la espera) se produce antes de la finalización de la espera temporizada de la respuesta del usuario, entonces se transmiten los nuevos datos de petición de posición recibidos por el motor de privacidad 120 (figura 1), y el procedimiento continúa en el paso 244.

Todavía en referencia a la figura 2(b), en el PASO 244 se evalúa la nueva petición de posición para determinar si la petición es una petición de servicios de emergencia. Para una petición de servicios de emergencia el procedimiento continúa a través de la conexión de flujo 246 hasta el PASO 288 (figura 2(d)). En el PASO 288 se incrementa el contador de peticiones de posición y el procedimiento continúa en el PASO 290. En el PASO 290 se suspende el procesamiento para la petición de posición previa y se pone en una cola para su posterior procesamiento, como se explica en lo que sigue. En otro modo de realización (no mostrado) el procedimiento puede en cambio cancelar el procesamiento de la petición de posición previa en el PASO 290. En otro modo de realización adicional (no mostrado), se proporcionan medios para permitir que el módulo PD 122 (figura 1) procese una pluralidad de peticiones simultáneas. Tras el PASO 290, el procedimiento pasa al PASO 256 (figura 2 (b)) a través de la conexión de flujo 214 para el procesamiento acelerado de la petición de servicios de emergencia. Si la nueva petición no es una petición de emergencia, el procedimiento pasa directamente del PASO 244 a un PASO 248 (figura 2(b)).

En el PASO 248 se incrementa el contador de peticiones de posición. El procedimiento pasa entonces a un PASO 260 y los nuevos datos de petición de posición se envían a la cola. En el PASO 260, el procedimiento coloca los nuevos datos de petición de posición en una cola de datos. Tras completar el PASO 260 el procedimiento de la invención vuelve al PASO 232, y espera una respuesta del usuario. En modos de realización alternativos se pueden insertar e implementar pasos adicionales antes del PASO 248 con el fin de decidir si la nueva petición de posición se debe rechazar en lugar de ponerse en cola. En estos modos de realización, puede ser ventajoso rechazar las peticiones inaceptables si los pasos adicionales dan como resultado una mejora global en la eficiencia. En un ejemplo, se puede rechazar inmediatamente una petición que estipula una QoS inaceptable en lugar de ponerla en la cola.

Como se muestra en la figura 2(b), se puede entrar en el PASO 250 desde cualquiera de los PASOS 234, 242 o (a través de conexión de flujo 230) el PASO 228 (figura 2(a)). En el PASO 250, los datos de petición de posición que designan la QoS se comparan con las reglas de privacidad que aplican para la petición de posición actual. Con el fin de describir la implementación ejemplar, la QoS puede representar la precisión de los datos de posición que se devuelven a la aplicación de petición de localización. Los datos de posición pueden comprender datos de coordenadas de latitud y longitud junto con datos de QoS que representan la precisión de la estimación de la posición. Si la QoS especificada por los datos de petición de posición se ajusta a los límites especificados por las reglas de privacidad aplicables a la petición de posición actual, el procedimiento continúa en el PASO 256. Si la QoS especificada por los datos de petición de posición no cumple con los límites de la política de privacidad, los datos de

QoS se modifican para su cumplimiento en un PASO 252 antes del procesamiento adicional en el PASO 256. En la sección *Aplicaciones ejemplares* descrita a continuación se proporcionará un análisis adicional para aclarar la finalidad y el uso de las especificaciones de QoS .

En el PASO 256, el procedimiento activa el módulo PD 122 (figura 1) con el fin de recuperar los datos de posición de acuerdo con los datos de petición de posición y las especificaciones de la política de privacidad actual. Como se ha descrito anteriormente, cuando se reciben peticiones de emergencia u otras peticiones de anulación de privacidad, el procedimiento puede implementar el PASO 256 a través de la conexión de flujo 214, tras los PASOS 212, 216 (figura 2(a)) o el PASO 290 (figura 2(d)). El procedimiento pasa entonces a un PASO 258. En el PASO 258, el procedimiento realiza una espera temporizada para la respuesta del PDM 122.

La figura 2(c) es una continuación del diagrama de flujo unificado de la figura 2, procedente de la espera temporizada en el PASO 258 (figura 2(b)) (espera temporizada para la respuesta del PDM). Los PASOS 262 y 264 representan los posibles eventos que pueden finalizar el período de espera temporizada del PASO 258. El PASO 266 también representa un evento que puede ocurrir durante el período de espera temporizada en el PASO 258. Estos pasos se describen con más detalle en los párrafos siguientes.

Como se muestra en la figura 2(c), si la espera temporizada para la respuesta del PDM en el PASO 258 finaliza mediante el evento representado en el PASO 262, *es decir*, si el PDM 122 responde al motor de privacidad 120 (figura 1), el procedimiento avanza desde el PASO 262 a un PASO de decisión 270. Si la espera temporizada del PASO 258 "agota el tiempo de espera", *es decir*, finaliza mediante el evento representado en el PASO 264, (vencimiento del tiempo de espera), el procedimiento pasa del PASO 264 a un PASO 272 y se transmite un mensaje de error a la aplicación de petición de localización. En un modo de realización alternativo (no mostrado), se puede transmitir la información de posición guardada previamente en lugar de un mensaje de error. Tras el PASO 272, el procedimiento pasa a un PASO 282 para comprobar las peticiones de posición pendientes en la cola de nuevas peticiones de posición.

Como se muestra en la figura 2(c), si las nuevas peticiones de posición se producen durante el PASO 258, el procedimiento continúa en el PASO 266 (posible llegada de una nueva petición de posición durante la espera). En el PASO 266, se reciben los nuevos datos de petición de posición mediante el motor de privacidad 120 (figura 1). En el PASO 268 siguiente se evalúa la nueva petición de posición para determinar si la petición es una petición de servicios de emergencia. Para una petición de servicios de emergencia el procedimiento continúa a través de la conexión de flujo 246 hasta el PASO 288 (figura 2(d)) para los pasos de procesamiento posteriores tal como se describe más arriba. Si la nueva petición no es una petición de emergencia, el procedimiento pasa directamente del PASO 268 a un PASO 274.

En el PASO 274, el procedimiento incrementa el contador de peticiones de posición. En un PASO 278 siguiente, el procedimiento coloca los nuevos datos de petición de posición en una cola de datos. Después de completar el PASO 278 el procedimiento vuelve al PASO 258 para continuar y realizar una espera temporizada para la respuesta del PDM.

Cuando la espera temporizada en el PASO 258 se interrumpe debido a la respuesta del PDM 122 al motor de privacidad 120 (figura 1), el procedimiento pasa del PASO 258 al PASO 262 como se muestra en la figura 2(c). En el PASO 262, los datos del PDM se transmiten desde el PDM 122 en el PASO 262 al motor de privacidad 120. Los datos del PDM comprenden datos de coordenadas de posición y datos de QoS. En el PASO 270, los datos de PDM que designan la QoS se comparan con las reglas de privacidad en relación con la clase de privacidad de la petición de posición actual. Con el fin de describir la implementación ejemplar, la QoS puede representar una precisión estimada de los datos de coordenadas de posición del PDM que se devuelven a la aplicación de petición de localización. Por ejemplo, los datos del PDM pueden comprender datos de latitud y longitud junto con datos de QoS que representan la precisión de la estimación de la posición. Si la QoS de los datos del PDM cumple con los límites especificados por las reglas de privacidad relativas a la clase de privacidad de la petición de posición actual, el procedimiento pasa a un PASO 280 para su posterior procesamiento. Si la QoS especificada por los datos del PDM no cumple con los límites de la política de privacidad para el caso actual, entonces los datos de QoS se modifican para su cumplimiento en el PASO 276. Una vez que se vuelve a formatear la estimación de la posición en el PASO 276, el procedimiento continúa en el PASO 280. A continuación, en la sección *Aplicaciones ejemplares* se proporciona una descripción más detallada de la finalidad y el uso de las especificaciones de QoS.

Los datos del PDM se transmiten a la aplicación de petición de localización en el PASO 280. A continuación, el procedimiento continúa en el PASO 282, en donde se consulta el contador de peticiones de posición para determinar si hay nuevas peticiones de posición pendientes. Si se determina que el valor del contador es cero, lo que indica que no hay presente ninguna petición pendiente, entonces el procedimiento vuelve al estado de espera 202 (figura 2(a)). Si el valor del contador es un número entero mayor que cero, entonces el procedimiento continúa en el PASO 284. En el PASO 284, se recuperan los nuevos datos de petición de posición de la cola de nuevos datos de petición de posición.

El procedimiento pasa entonces al PASO 286, en donde se disminuye el contador de peticiones de posición. El

procedimiento continúa entonces (a través de la conexión de flujo 208) en el PASO 210 (figura 2(a)) para procesar adicionalmente los nuevos datos de petición de posición.

Aplicaciones ejemplares

En una aplicación típica de las presentes instrucciones, se pueden definir varias clases de privacidad configurables por el usuario, y las propiedades o normas pertenecientes a las mismas. Como se ha descrito anteriormente en referencia a la figura 1, la configurabilidad de usuario se puede efectuar a través de conexiones de datos entre el motor de privacidad 120 y la interfaz de usuario 106, el servidor de gestión de privacidad 104 (u otros servidores de red que no se muestran en las figuras), o las aplicaciones locales externas 116. Es deseable permitir la configuración y la modificación del motor de privacidad 120 y la política de privacidad únicamente mediante medios seguros. A modo de ejemplo, los medios seguros pueden comprender procedimientos y medios para proporcionar una comunicación digital segura, el uso de contraseñas, certificados digitales, y otros procedimientos de verificación de identidad y autenticación bien conocidos.

Las clases de privacidad pueden incluir, sin limitación, los siguientes tipos:

1. predeterminado para aplicaciones de petición de localización desconocidas o no declaradas (es decir, no fiables) e identidades de peticionarios no incluidas específicamente ninguna otra clase;

2. predeterminado para aplicaciones de petición de localización fiables e identidades de peticionarios no incluidas específicamente ninguna otra clase; y

3. clases específicas del usuario incluyendo aplicaciones de petición de localización e identidades de peticionarios.

Cada clase de privacidad puede incluir, sin limitación, las siguientes reglas de privacidad:

1. especificación de la aceptación o rechazo predeterminados, o aceptación dependiente de las restricciones especificadas;

2. especificación de los requisitos de notificación al usuario:

2.a. notificación al usuario absolutamente necesaria o no necesaria, notificación basada en la QoS solicitada (por ejemplo, el usuario especifica que se requiere una notificación para estimaciones de posición con una precisión superior a 10 metros. Por lo tanto, si los datos de petición de posición especifican una QoS para la estimación de la posición con una precisión de 5 metros, se notificará al usuario.), y

2.b. notificación basada en si la petición es periódica o iniciada bajo demanda;

2.c. notificación basada en el momento de ocurrencia, como la hora del día, el día de la semana, la fecha o restricciones dependientes del tiempo similares.

3. especificación del modo de visualización que se utilizará para la notificación al usuario (por ejemplo, icono emergente en la interfaz gráfica de usuario, notificación mediante un tono, música u otro sonido, notificación mediante vibración, *etc.*), y la información que se mostrará, en su caso;

4. especificación de los requisitos de notificación relacionados con peticiones periódicas, como por ejemplo si se requiere una notificación explícita para cada petición periódica o se requiere sólo para la primera petición de una serie periódica;

5. especificación de la QoS o precisión estimada de la posición a entregar (por ejemplo, se puede permitir una clase de la política de privacidad con una precisión de código postal únicamente, o se puede permitir únicamente para una precisión que sea inferior a un radio mayor que un número determinado de metros);

6. especificación del funcionamiento predeterminado si el usuario no responde a una notificación (por ejemplo, petición permitida o no permitida cuando el usuario no responde a una notificación tal como una ventana emergente, con o sin un botón "Aceptar", que desaparece automáticamente al cabo de unos segundos);

7. especificación de configuraciones de reglas variables basadas en la localización de la estación móvil o en la hora del día. [Por ejemplo, el usuario puede establecer una regla que modifique o prohíba una respuesta procedente de ciertas localizaciones o a ciertas horas del día.]

En un modo de realización del concepto de la presente invención, la estación móvil 102 (figura 1) puede incluir un Módulo de Identidad de Abonado (SIM), un Módulo de Identidad de Abonado Universal (USIM) o un Módulo de Identidad de Usuario Extraíble (RUIM). Los dispositivos SIM, USIM y RUIM son componentes de almacenamiento

extraíbles para estaciones móviles que permiten el almacenamiento seguro de información específica del usuario. Como se ha descrito anteriormente en referencia a la figura 1, el dispositivo SIM, USIM o RUIM se puede incluir en el bloque de otros módulos 112. En este modo de realización ejemplar, los datos de la política de privacidad específicos del usuario se almacenan en el dispositivo SIM, USIM o RUIM. Los dispositivos están acoplados operativamente al motor de privacidad 120 (conexión no mostrada en la figura 1), y los datos de la política de privacidad específicos del usuario se transmiten al motor de privacidad 120 para la implementación de las operaciones del motor de privacidad 120 descritas anteriormente. Los datos de la política de privacidad específicos del usuario también se reciben desde el motor de privacidad para su almacenamiento. Esto ocurre cuando se los datos de la política de privacidad se reciben inicialmente para el almacenamiento mediante el dispositivo SIM, USIM o RUIM, y cuando se modifican o se actualizan los datos. Cuando la SIM, USIM o RUIM se retira de la estación móvil 102, la información de la política de privacidad específica del usuario se puede borrar entonces ventajosamente de forma automática del motor de privacidad 120. El uso de dispositivos SIM, USIM o RUIM para el almacenamiento extraíble de los datos específicos del usuario en las estaciones móviles es bien conocido por los expertos en las técnicas de la comunicación. Los estándares para la implementación de los dispositivos SIM se describen en el Proyecto de Colaboración de Tercera Generación (3GPP), Grupo técnico de especificación (TS) de Terminales, interfaz de programación de aplicaciones del Módulo de Identidad de Abonado (API de SIM), fase 1, edición 1999 (3GPP TS 02.19 V8.0.0), junio de 2001. Por la presente se hace referencia a esta referencia para obtener instrucciones relativas a la implementación de los dispositivos SIM. También será evidente para las personas expertas en la técnica que las presentes instrucciones abarcan modos de realización en los que se incluyen otros dispositivos de almacenamiento extraíbles (como por ejemplo tarjetas inteligentes o lápices de memoria) en una estación móvil y se utilizan junto con el motor de privacidad para el almacenamiento de datos de la política de privacidad específicos del usuario.

A la luz de los ejemplos proporcionados en la descripción anterior, los expertos en la técnica de comunicaciones reconocerán que las instrucciones del presente documento se pueden aplicar de manera amplia y general al control del usuario y a la gestión de la información de privacidad personal relativa a los LCS.

Los expertos en las técnicas de comunicaciones e informática también reconocerán que el medio legible por ordenador que incorpora tangiblemente las etapas del procedimiento de cualquiera de los modos de realización del presente documento puede utilizarse de acuerdo con las presentes instrucciones. Por ejemplo, las etapas del procedimiento descritas anteriormente con referencia a las figuras 2(a)-2(c) se pueden realizar como una serie de instrucciones ejecutables por ordenador almacenadas en un medio legible por el ordenador. Dicho medio puede incluir, sin limitación, RAM, ROM, EPROM, EEPROM, disco flexible, disco duro, CD-ROM, *etc*. La divulgación también incluye los PASOS del procedimiento de cualquiera de los modos de realización anteriores sintetizados como lógica digital en un circuito integrado, como una matriz de puertas programables de campo, o una matriz de lógica programable, u otros circuitos integrados que se pueden fabricar o modificar para incorporar instrucciones de programas informáticos.

La estación móvil 102 de acuerdo con las presentes instrucciones puede incluir, sin limitación: un teléfono inalámbrico, un asistente personal digital con capacidad de comunicación inalámbrica, un ordenador portátil con capacidad de comunicación inalámbrica y cualquier otro dispositivo digital móvil para la comunicación personal a través de una conexión inalámbrica.

Se han descrito diversos modos de realización del presente concepto inventivo. Sin embargo, se entenderá que se pueden realizar diversas modificaciones sin apartarse del alcance del concepto tal como se describe en el presente documento. Por ejemplo, los procedimientos se pueden ejecutar en software o hardware, o en una combinación de modos de realización hardware y software. Como otro ejemplo, se debe entender que las funciones descritas como parte de un módulo en general se pueden llevar a cabo de forma equivalente en otro módulo. Como otro ejemplo, los pasos o etapas mostrados o descritos en una secuencia particular por lo general se pueden realizar en un orden diferente, con excepción de los modos de realización descritos en una reivindicación que incluya un orden específico para los pasos.

En consecuencia, se debe comprender que el concepto de la invención no ha de estar limitado por los modos de realización específicos ilustrados, sino solamente por el alcance de las reivindicaciones adjuntas. La divulgación puede proporcionar ejemplos de características similares a las descritas en las reivindicaciones, pero no debe suponerse que tales características similares son idénticas a las de las reivindicaciones a menos que dicha identidad sea esencial para comprender el alcance de la reivindicación. En algunos casos, la distinción pretendida entre las características de las reivindicaciones y las características de la divulgación se acentúa mediante el uso de una terminología ligeramente diferente.

REIVINDICACIONES

1. Un sistema de control de privacidad para su uso en una estación móvil (102), en el que la estación móvil (102) se comunica con un sistema de comunicación inalámbrica, y en el que el sistema de control de privacidad proporciona información de localización geográfica asociada con la estación móvil (102), que comprende:

a) un motor de privacidad (120), que incluye un componente de política de privacidad que tiene al menos una regla de privacidad, en el que el motor de privacidad (120) recibe peticiones de localización relacionadas con la localización geográfica de la estación móvil generadas por un peticionario de localización externo a la estación móvil (102) y determina si la petición de localización se debe rechazar basándose al menos en parte en al menos una regla de privacidad; y

b) un módulo de determinación de la posición (122), operativamente acoplado y que reacciona al motor de privacidad (120), en el que el módulo de determinación de la posición (122) proporciona estimaciones de la localización geográfica de la estación móvil (102) al motor de privacidad (120) ;

en el que, el motor de privacidad (120)

activa selectivamente el módulo de determinación de la posición (122) de acuerdo con el componente de política de privacidad con el fin de recibir las estimaciones de localización geográfica del módulo de determinación de la posición (122), y responde a las peticiones de localización mediante el procesamiento de las estimaciones de localización, y proporciona mensajes de respuesta de acuerdo con el componente de política de privacidad.

2. El sistema de control de privacidad, de acuerdo con la reivindicación 1, en el que el módulo de determinación de la posición (122) funciona de acuerdo con uno o más de los siguientes procedimientos:

Sistema de Posicionamiento Global, Sistema de Posicionamiento Global Asistido, Trilateración de enlace directo avanzada, Hora de llegada, Diferencia temporal observado mejorada, y posicionamiento basado en la identificación de las celdas de comunicación inalámbrica en las que funciona la estación móvil (102).

3. El sistema de control de la privacidad, de acuerdo con la reivindicación 1, que comprende además un módulo de comunicación de red inalámbrica (112) acoplado operativamente al motor de privacidad (120) y al sistema de comunicación inalámbrica, en el que el módulo de comunicación de red inalámbrica (112) está configurado para recibir las peticiones de localización del sistema de comunicación inalámbrica y para transmitir los mensajes de respuesta al sistema de comunicación inalámbrica, y está configurado además para recibir datos e instrucciones de software del sistema de comunicación inalámbrica y para transmitir datos e instrucciones de software al sistema de comunicación inalámbrica.

4. El sistema de control de la privacidad, de acuerdo con la reivindicación 3, en el que el motor de privacidad (120) comprende un software que se descarga desde el sistema de comunicación inalámbrica.

5. El sistema de control de la privacidad, de acuerdo con la reivindicación 3, en el que el motor de privacidad (120) se modifica con las actualizaciones de software descargadas desde el sistema de comunicación inalámbrica.

6. El sistema de control de la privacidad, de acuerdo con la reivindicación 3, en el que la política de privacidad comprende un software que se descarga desde el sistema de comunicación inalámbrica.

7. El sistema de control de la privacidad, de acuerdo con la reivindicación 3, en el que la política de privacidad se modifica con actualizaciones descargadas desde el sistema de comunicación inalámbrica.

8. El sistema de control de la privacidad, de acuerdo con la reivindicación 7, en el que las actualizaciones incluyen datos de la política de privacidad específicos del usuario.

9. El sistema de control de la privacidad, de acuerdo con la reivindicación 3, en el que la petición de localización se recibe desde una aplicación externa conectada operativamente al sistema de comunicación inalámbrica.

10. El sistema de control de la privacidad, de acuerdo con la reivindicación 1, que comprende además un módulo de comunicación local (118) acoplado operativamente al motor de privacidad (120) y a aplicaciones locales externas (116), en el que el módulo de comunicación local (118) está configurado para recibir las peticiones de localización de las aplicaciones locales externas (116) y para transmitir los mensajes de respuesta de las aplicaciones locales externas (116), y además está configurado para recibir datos e instrucciones de software de las aplicaciones locales externas (116) y para transmitir datos e instrucciones de software a las aplicaciones locales externas (116).

11. El sistema de control de la privacidad, de acuerdo con la reivindicación 10, en el que el motor de privacidad (120) comprende un software que se descarga desde una aplicación local externa (116).

12. El sistema de control de la privacidad, de acuerdo con la reivindicación 10, en el que el motor de privacidad (120) se modifica con actualizaciones de software mediante las instrucciones de software que se descargan desde una aplicación local externa (116).

13. El sistema de control de la privacidad, de acuerdo con la reivindicación 10, en el que la política de privacidad comprende un software que se descarga desde una aplicación local externa (116).

14. El sistema de control de la privacidad, de acuerdo con la reivindicación 10, en el que la política de privacidad se modifica con actualizaciones que se descargan desde una aplicación local externa (116).

15. El sistema de control de la privacidad, de acuerdo con la reivindicación 14, en el que las actualizaciones incluyen datos de la política de privacidad específicos del usuario.

16. El sistema de control de la privacidad, de acuerdo con la reivindicación 10, en el que la petición de localización se recibe desde una aplicación local externa (116).

17. El sistema de control de la privacidad, de acuerdo con la reivindicación 1, que comprende además una interfaz de usuario (106), acoplada operativamente al motor de privacidad (120), en el que la interfaz de usuario (106) está configurada para recibir la entrada de un usuario, y en el que la entrada de usuario se utiliza para modificar la política de privacidad con las actualizaciones.

18. El sistema de control de la privacidad, de acuerdo con la reivindicación 17, en el que las actualizaciones incluyen datos de la política de privacidad específicos del usuario.

19. El sistema de control de la privacidad, de acuerdo con la reivindicación 17, en el que la interfaz de usuario (106) proporciona notificaciones de peticiones de localización al usuario, de acuerdo con la política de privacidad, y en el que la interfaz de usuario (106) está configurada para recibir las respuestas del usuario, que reacciona a las notificaciones de petición de localización.

20. El sistema de control de la privacidad, de acuerdo con la reivindicación 19, en el que la política de privacidad incluye una pluralidad de clases de privacidad, en el que las clases de privacidad clasifican las peticiones de localización recibidas mediante el motor de privacidad (120), y en el que la política de privacidad incluye además reglas de privacidad que determinan respuestas a las peticiones de localización para cada clase de privacidad, y en el que las reglas de privacidad incluyen al menos una de las siguientes reglas:

a) una regla que requiere la aceptación o el rechazo, por defecto, de una petición de localización;

b) una regla que requiere la notificación al usuario de una petición de localización;

c) una regla que requiere la notificación al usuario en base a una calidad de servicio solicitada;

d) una regla que requiere la notificación al usuario en base a si la petición de localización es periódica o iniciada bajo demanda;

e) una regla que requiere la notificación al usuario en base a un tiempo de ocurrencia de la petición de localización;

f) una regla que especifica un modo de visualización que se utilizará para la notificación al usuario;

g) una regla que especifica un intervalo de precisión de la estimación de localización a entregar;

h) una regla que requiere un manejo, por defecto, de un mensaje de respuesta si el usuario no responde a una notificación al usuario; y

i) una regla que especifica el manejo de mensaje de respuesta en base a la localización geográfica actual de la estación móvil.

21. El sistema de control de la privacidad, de acuerdo con la reivindicación 1, que comprende además un dispositivo de almacenamiento de datos extraíble, en el que el dispositivo de almacenamiento de datos extraíble está acoplado operativamente al motor de privacidad (120), y en el que el dispositivo de almacenamiento de datos extraíble está configurado para recibir, almacenar y transmitir datos de la política de privacidad específicos del usuario.

22. El sistema de control de la privacidad, de acuerdo con la reivindicación 21, en el que el dispositivo de almacenamiento de datos extraíble comprende un dispositivo de Módulo de Identidad de Abonado.

23. El sistema de control de la privacidad, de acuerdo con la reivindicación 21, en el que el dispositivo de almacenamiento de datos extraíble comprende un dispositivo de Módulo de Identidad de Abonado Universal.

24. El sistema de control de la privacidad, de acuerdo con la reivindicación 21, en el que el dispositivo de almacenamiento de datos extraíble comprende un dispositivo de módulo de Identidad de Usuario Extraíble.

25. Un procedimiento para proporcionar un control de la privacidad en una estación móvil (102) de la información de localización geográfica de la estación móvil, en el que la estación móvil (102) se comunica con un sistema de comunicación inalámbrica, y en el que la estación móvil (102) incluye un motor de privacidad (120) que comprende instrucciones de software, en el que las instrucciones de software del motor de privacidad también incluyen instrucciones de la política de privacidad que tienen al menos una regla de privacidad, y en el que la estación móvil (102) incluye además un módulo de determinación de posición (122) capaz de proporcionar estimaciones de la localización geográfica de la estación móvil (102); comprendiendo el procedimiento los pasos de:

a) recepción (204) de peticiones de localización para una localización geográfica actual de la estación móvil (102) a partir de un peticionario de localización externo a la estación móvil (102);

b) procesamiento de las peticiones de localización de acuerdo con las instrucciones de software del motor de privacidad, en el que el procesamiento de la petición de localización incluye la determinación de si la petición de localización se debe rechazar basándose al menos en parte en al menos una regla de privacidad;

c) activación selectiva del módulo de determinación de posición (122) de acuerdo con el componente de la política de privacidad para obtener estimaciones de la localización geográfica de la estación móvil (102);

d) procesamiento de las estimaciones de la localización geográfica, de acuerdo con las peticiones de localización, las instrucciones de software del motor de privacidad y las reglas de privacidad; y

e) entrega selectiva de los mensajes de respuesta que responden a las peticiones de localización, de acuerdo con las instrucciones de software del motor de privacidad, las estimaciones de localización y las reglas de privacidad.

26. El procedimiento de control de la privacidad, de acuerdo con la reivindicación 25, en el que el paso b) de procesamiento de las peticiones de localización incluye además un paso de procesamiento de las peticiones de localización de emergencia mediante la anulación de las instrucciones de la política de privacidad para proporcionar mensajes de respuesta de emergencia.

27. El procedimiento de control de la privacidad, de acuerdo con la reivindicación 26, en el que el paso b) de procesamiento de las peticiones de localización incluye el procesamiento de una pluralidad de peticiones de localización concurrentes.

28. El procedimiento de control de la privacidad, de acuerdo con la reivindicación 27, en el que las peticiones de localización pendientes se suspenden mientras se procesan las peticiones de localización de emergencia.

29. El procedimiento de control de la privacidad, de acuerdo con la reivindicación 25, que comprende además un paso de notificación a un usuario de las peticiones de localización.

30. El procedimiento de control de la privacidad, de acuerdo con la reivindicación 29, en el que las instrucciones de la política de privacidad incluyen clases de privacidad para clasificar las peticiones de localización recibidas durante el paso a), y en el que las instrucciones de la política de privacidad incluyen reglas de privacidad para la determinación de una respuesta a las peticiones de localización para cada clase de privacidad, y en el que las reglas de privacidad incluyen al menos una de las siguientes normas:

a) una regla que requiere la aceptación o el rechazo, por defecto, de una petición de localización;

b) una regla que requiere la notificación al usuario de una petición de localización;

c) una regla que requiere la notificación al usuario en base a una calidad de servicio solicitada;

d) una regla que requiere la notificación al usuario en base a si la petición de localización es periódica o

iniciada bajo demanda;

e) una regla que requiere la notificación al usuario en base a un tiempo de ocurrencia de la petición de localización;

f) una regla que especifica un modo de visualización que se utilizará para la notificación al usuario;

g) una regla que especifica un intervalo de precisión de la estimación de localización a entregar;

h) una regla que requiere un manejo, por defecto, de un mensaje de respuesta si el usuario no responde a una notificación al usuario; y

i) una regla que especifica el manejo de un mensaje de respuesta en base a la localización geográfica actual de la estación móvil.

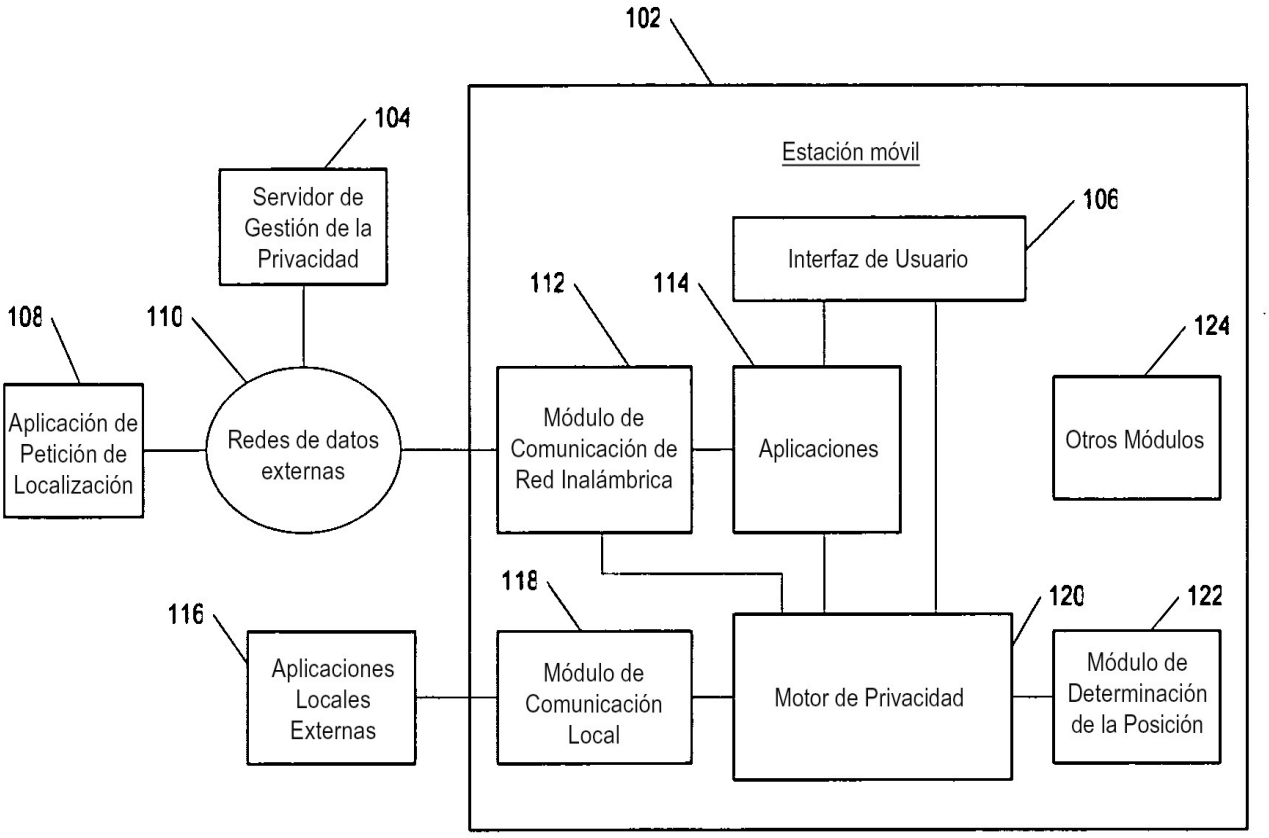
102
Estación móvil
104
Servidor de Gestión de la Privacidad
106
Interfaz de Usuario
108
110
112
114
124
Aplicación de Petición de Localización
Redes de datos externas
Módulo de Comunicación de Red Inalámbrica
Aplicaciones
Otros Módulos
116
118
120
122
Aplicaciones Locales Externas
Módulo de Comunicación Local
Motor de Privacidad
Módulo de Determinación de la Posición

Figura 1

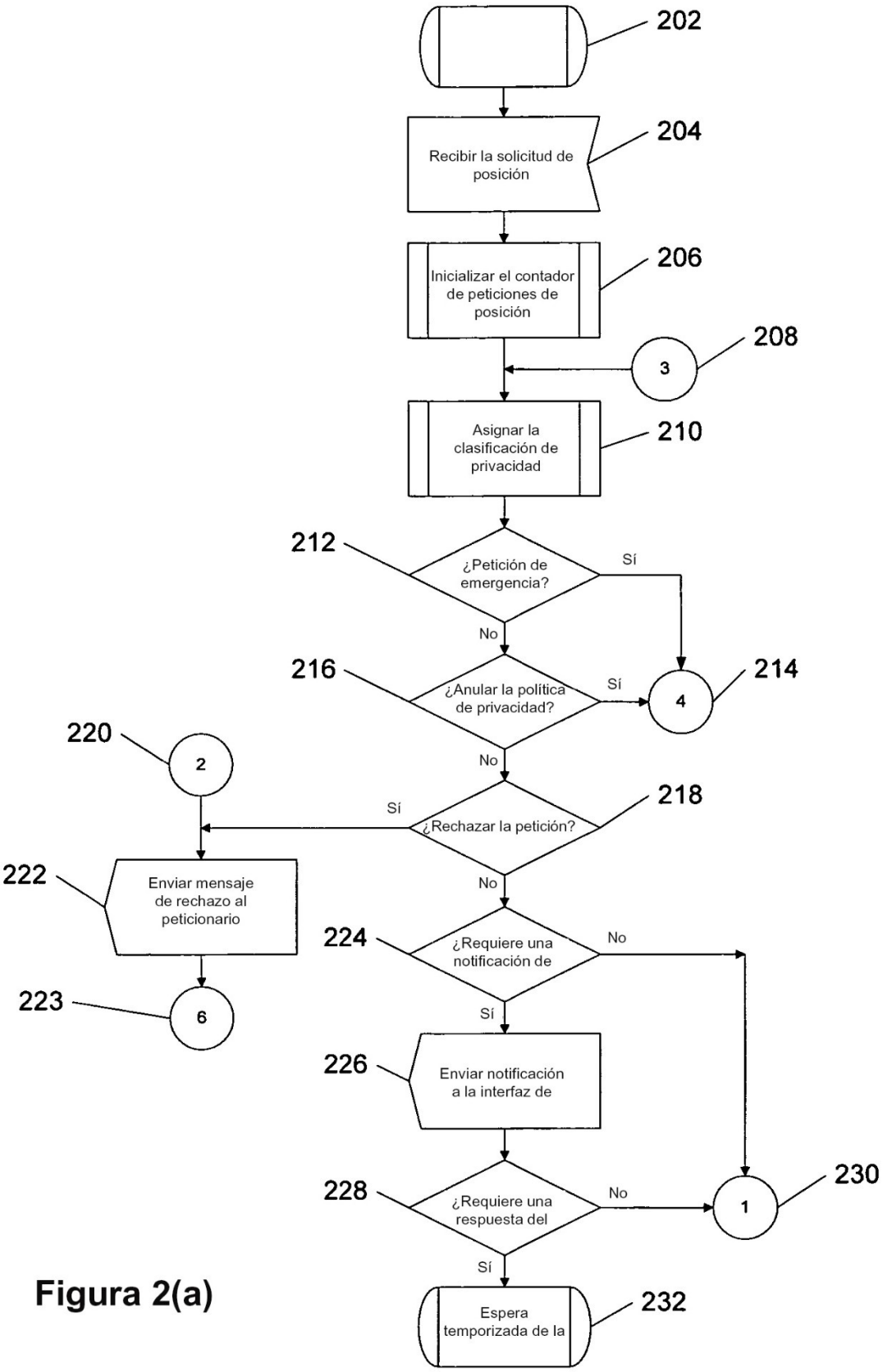
202
Recibir la solicitud de posición
204
Inicializar el contador de peticiones de posición
206
3
208
Asignar la clasificación de privacidad
210
212
¿Petición de emergencia?
Sí
No
216
¿Anular la política de privacidad?
Sí
4
214
No
220
2
Sí
218
¿Rechazar la petición?
222
Enviar mensaje de rechazo al peticionario
No
224
¿Requiere una notificación de
No
Sí
223
6
226
Enviar notificación a la interfaz de
228
¿Requiere una respuesta del
No
1
230
Sí
Espera temporizada de la
232

Figura 2(a)

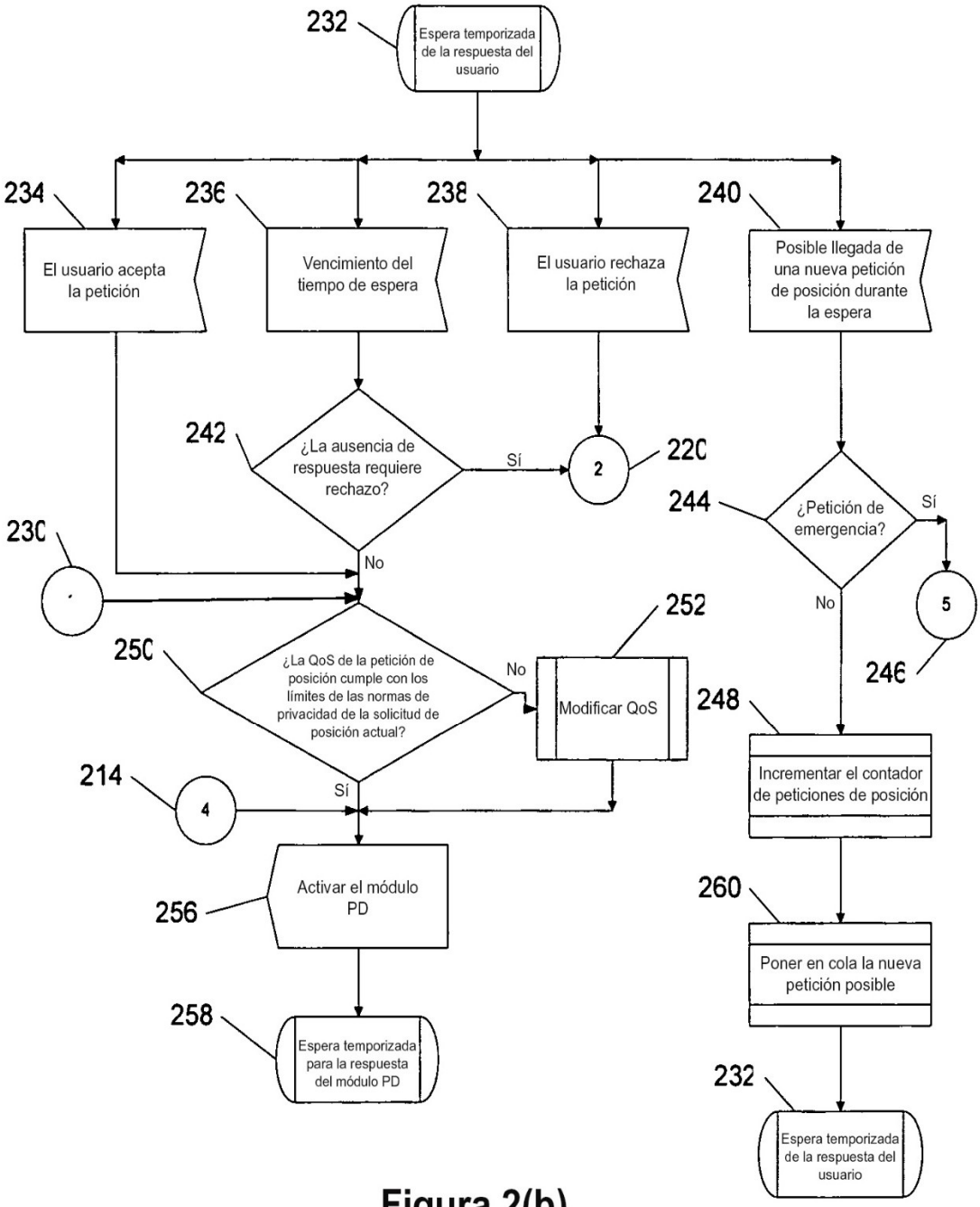
232
Espera temporizada de la respuesta del usuario
234
El usuario acepta la petición
236
Vencimiento del tiempo de espera
238
El usuario rechaza la petición
240
Posible llegada de una nueva petición de posición durante la espera
242
¿La ausencia de respuesta requiere rechazo?
Sí
2
220
No
230
244
¿Petición de emergencia?
Sí
No
5
246
250
¿La QoS de la petición de posición cumple con los límites de las normas de privacidad de la solicitud de posición actual?
No
252
Modificar QoS
248
Incrementar el contador de peticiones de posición
214
4
Sí
Activar el módulo PD
256
260
Poner en cola la nueva petición posible
258
Espera temporizada para la respuesta del módulo PD
232
Espera temporizada de la respuesta del usuario

Figura 2(b)

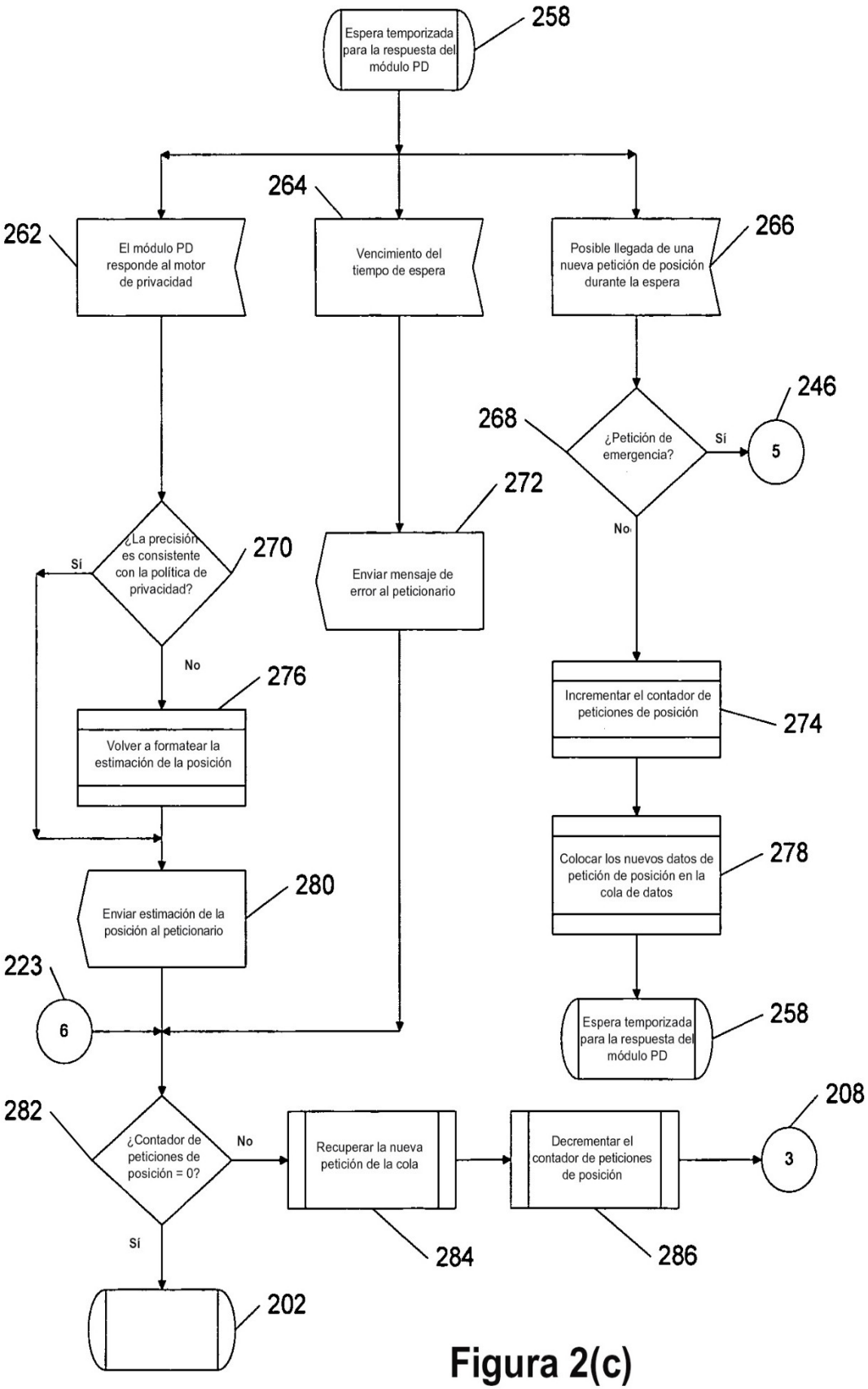
Espera temporizada para la respuesta del módulo PD
258
El módulo PD responde al motor de privacidad
262
Vencimiento del tiempo de espera
264
Posible llegada de una nueva petición de posición durante la espera
266
¿Petición de emergencia?
268
Sí
246
5
No
¿La precisión es consistente con la política de privacidad?
270
Sí
No
Enviar mensaje de error al peticionario
272
Incrementar el contador de peticiones de posición
274
Volver a formatear la estimación de la posición
276
Colocar los nuevos datos de petición de posición en la cola de datos
278
Enviar estimación de la posición al peticionario
280
223
6
Espera temporizada para la respuesta del módulo PD
258
¿Contador de peticiones de posición = 0?
282
No
Sí
Recuperar la nueva petición de la cola
284
Decrementar el contador de peticiones de posición
286
208
3
202

Figura 2(c)

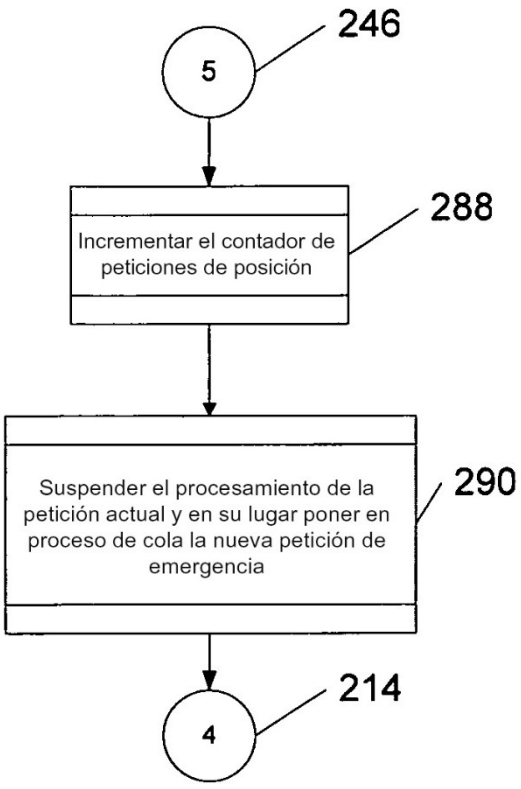
246
5
Incrementar el contador de peticiones de posición
288
Suspender el procesamiento de la petición actual y en su lugar poner en proceso de cola la nueva petición de emergencia
290
214
4

Figura 2(d)