(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 495 740**

(51) Int. CI.:

H04L 29/06 (2006.01)
H04W 12/12 (2009.01)
H04W 8/26 (2009.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **05.06.2007 E 07394015 (7)**

(97) Fecha y número de publicación de la concesión europea: **13.08.2014 EP 1865744**

(54) Título: **Detección de dispositivo en redes móviles**

(30) Prioridad:

08.06.2006 US 811792 P

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
17.09.2014

(73) Titular/es:

MARKPORT LIMITED (100.0%)
53 Merrion Square South
Dublin 2, IE

(72) Inventor/es:

WOLLERSHEIM, MAURICE y
WIJBRANS, KLAAS

(74) Agente/Representante:

UNGRÍA LÓPEZ, Javier

DESCRIPCIÓN

Detección de dispositivo en redes móviles

Introducción

Campo de la invención

La invención se refiere a detección de dispositivos usados por abonados de operadores móviles.

Explicación de la técnica anterior

Lo que sigue son definiciones de algunos términos usados en esta memoria descriptiva.

- Identidad de dispositivo: término usado para la identidad única de un dispositivo específico. En general, dentro de una red GSM/UMTS es la IMEI de un dispositivo.

- EIR (Registro de Identidad de Equipo) mantiene una lista de identificadores de dispositivo móvil que han de ser excluidos de la red o supervisados (destinado originalmente al seguimiento de teléfonos robados). Al unirse a la red o al tiempo de establecimiento de llamada (dependiendo del vendedor del sistema de conmutación de red), el conmutador contactará el EIR para comprobar si dicho dispositivo específico puede estar presente en la red. El EIR intercambia las listas de teléfonos (robados) con un EIR central de modo que los dispositivos robados no puedan ser usados en ninguna de las redes conectadas.

- IMEI: Identidad de Equipo Móvil Internacional. Un número de identificación asignado a estaciones móviles GSM que identifica de forma única a cada uno. La IMEI (14 dígitos más dígito de verificación) o IMEISV (16 dígitos) incluye información acerca del origen, modelo, y número de serie del dispositivo, incluyendo la Identidad de Equipo Móvil Internacional y el número de versión de software (IMEISV) también un elemento que identifica el número de versión de software del equipo móvil.

- IMSI: Identidad de Abonado Móvil Internacional. Un número que identifica de forma única un abonado GSM. El número contiene dos partes: la primera identifica el operador de red GSM con quien el abonado tiene una cuenta. La segunda parte del número es asignada por el operador de red para identificar de forma única el abonado. IMSI = MCC + MNC + MSIN, donde MCC significa Código de País de Móvil, MNC significa Código de Red Móvil, MSIN significa Número de Identificación de Abonado Móvil.

- Tipo de dispositivo. Término usado para un conjunto de dispositivos con idénticas capacidades.

- MDN: Número de Directorio Móvil. Un número de directorio de 10 dígitos usado para llamar a un teléfono inalámbrico.

- MEID: (Identificador de Equipo Móvil): una alternativa no GSM a la IMEI.

- MIN: Número de Identificación de Móvil (MIN): identifica de forma única una unidad móvil dentro de una red de portadoras inalámbricas.

- Identidad de Abonado: término usado para la identidad de un abonado específico. En general se usa la MSISDN. A veces se usa la identidad SIM (IMSI).

WO2004/004390 A1 describe los cambios de detección de dispositivo usando prueba de enlaces de señalización al MSC o el HLR y el uso de una aplicación MSISDN/IMEI para determinar las propiedades del dispositivo.

WO2005/036916 A1 describe cambios de detección de dispositivo basados en SIM usando SMS para indicar el cambio de dispositivo a la aplicación de detección de dispositivo.

US 6.275.692 B1 describe la adaptación de servicio a un dispositivo específico usando información obtenida de la red.

US2006/0009214 A1 describe el uso de la identificación IMEI/SIM conjuntamente con una base de datos para notificar cambios de dispositivo a proveedores de servicios.

EP1331833 A1 describe la detección de cambio de dispositivo basada en red detectando pares MSISDN-IMEI circulantes en la red telefónica móvil y almacenándolos en una base de datos que puede ser consultada.

WO01/31840 describe la identificación de un usuario usando almacenamiento de un identificador de usuario, un identificador de dispositivo y un sello de tiempo. Las búsquedas se introducen en uno de los identificadores.

La tecnología actual para detección de dispositivo se basa en el uso de paradigmas de bases de datos convencionales bajo el supuesto de que la identidad de dispositivo y la identidad de abonado son identificaciones únicas que constituyen conjuntamente una identificación única de un caso de dispositivo+abonado. En base a dicho paradigma, estos sistemas piden el almacenamiento de la identidad de dispositivo y el abonado o la identidad SIM como una 2-tupla (es decir, un par ordenado) en una base de datos. Esto no tiene en cuenta que:

- Un solo abonado puede tener múltiples teléfonos simultáneamente, cada uno con la misma identificación de abonado (SIM clonado), o cambiar el SIM entre estos teléfonos.

- Muchos teléfonos pueden dar la impresión de estar usando la misma identidad de dispositivo. Esto sucede especialmente porque, en las marcas principales, el valor de la IMEI es programable cuando el teléfono es flasheado, siendo reflasheados posteriormente muchos teléfonos provistos originalmente de un bloqueo SIM con la misma IMEI o parte de ella para quitar el bloqueo SIM.

Como resultado, el almacenamiento de la identidad actual de dispositivo y abonado en una base de datos como una 2-tupla es altamente ineficiente en la mayoría de las bases de datos debido a la relación n:m y la alta reutilización del mismo valor de clave. Esto prohíbe la eficiente detección de cambios de dispositivo. Dado que la detección de dispositivo en base a registro de red de un dispositivo puede generar cientos, si no miles, de peticiones por segundo, la eficiencia en la base de datos es muy importante para evitar onerosos requisitos de hardware.

Ya existen bases de datos que enlazan la identidad de un abonado con la identidad de un dispositivo. Un ejemplo de tal base de datos es el HLR propiamente dicho, que es capaz de almacenar la IMEI de un aparato conjuntamente con la MSISDN y la IMSI de un abonado. La implementación HLR tiene la desventaja de que la información solamente se describe al nivel MAP interrogando el HLR con las peticiones MAP apropiadas.

Tradicionalmente, la detección de dispositivo se basa en el uso de bases de datos que almacenan tanto la identidad de un dispositivo como la identidad de un abonado (por ejemplo, MSISDN o IMSI) o una tarjeta SIM (por ejemplo, IMSI si se usan diferentes IMSIs para múltiples dispositivos del mismo abonado). Estas bases de datos almacenan solamente el último aparato que tiene un abonado específico entre todos los aparatos usados por dicho abonado almacenando tuplas MSISDN/IMSI e IMEI.

Una base de datos que solamente almacena el último dispositivo usado no es capaz de distinguir entre una combinación nueva de abonado/dispositivo y una combinación de abonado/dispositivo ya vista. Una base de datos que almacena la relación entre abonados y dispositivos debe mantener un conjunto dinámico de relaciones, puesto que los usuarios de tarjetas múltiples (usuarios que usan múltiples dispositivos cada uno con tarjetas SIM clonadas) y los usuarios que cambian regularmente sus tarjetas SIM a dispositivos diferentes dan lugar a múltiples relaciones entre la identidad de abonado y dispositivo. Además, debido a copia de IMEI, si, por ejemplo, se quita el bloqueo SIM, la base de datos experimentará una indexación ineficiente puesto que habrá gran número de dispositivos con la misma IMEI exactamente. Almacenar de esta forma la identidad de abonado y dispositivo no es una forma eficiente de detectar cambios en la combinación de abonado y dispositivo, y así detectar cuándo un dispositivo es nuevo para dicho abonado y así deberá ser tenido en cuenta por el sistema de gestión de dispositivos.

Por lo tanto, la invención tiene la finalidad de proporcionar un método y sistema mejorados para la detección de dispositivo.

Resumen de la invención

Según la invención, se facilita un método realizado en una red móvil, incluyendo el método los pasos expuestos en la reivindicación 1.

En una realización, la firma es generada por un algoritmo hash usando como entradas los identificadores de dispositivo y abonado tal como una IMEI y una IMSI.

En una realización, la firma es un número binario.

En una realización, el método es implementado en respuesta a una activación de EIR.

En una realización, se almacena un sello de tiempo en la memoria de firmas para indicar el tiempo de escritura de la firma en la memoria.

En una realización, el método incluye el paso adicional, si la firma ya está almacenada, de actualizar el sello de tiempo asociado con la firma en la memoria para indicar la última vez que la firma fue procesada.

En una realización, los sellos de tiempo se usan para determinar la edad.

En otra realización, el método incluye los pasos adicionales de archivar o borrar firmas que tengan una edad superior a un umbral.

En una realización, la firma es almacenada en la memoria en una posición indicativa de edad.

En una realización, la notificación incluye el identificador de dispositivo y el identificador de abonado.

En una realización, la notificación incluye el sello de tiempo.

En una realización, la notificación incluye tanto el sello de tiempo actualizado como el sello de tiempo previo, donde el sello de tiempo es actualizado.

En otra realización, la firma es generada por una aplicación de detección que se ejecuta en un elemento de red.

En una realización, la aplicación de detección opera como un proxy para un EIR de red existente.

En una realización, la aplicación genera automáticamente una respuesta positiva EIR simulada además de realizar las operaciones de procesado de firma.

En una realización, la aplicación de detección opera conjuntamente con una base de datos EIR para sustituir un EIR de legado.

En una realización, la aplicación de detección construye una respuesta MAP CHECK_IMEI a partir del estado devuelto de la base de datos EIR

En una realización, se genera una notificación solamente cuando se determina que la combinación de dispositivo/abonado no existe en la red.

En otra realización, el método incluye el paso adicional de almacenar la firma y el identificador de abonado en una segunda base de datos.

En una realización, la segunda actualización de base de datos se realiza con un par de clave-valor en el que el identificador de abonado es la clave y la firma es el valor.

En una realización, el sistema genera una notificación que indica el dispositivo de abonado actual después de actualizar la segunda base de datos.

En otro aspecto, la invención proporciona un sistema de detección de dispositivo de red móvil incluyendo medios para realizar cualquier método definido anteriormente.

En otro aspecto, la invención proporciona un medio legible por ordenador incluyendo código de software para realizar cualquier método definido anteriormente al ejecutarse en un procesador digital.

Descripción detallada de la invención

Descripción detallada de la invención

La invención se entenderá más claramente por la descripción siguiente de algunas de sus realizaciones, dada a modo de ejemplo solamente con referencia a los dibujos acompañantes en los que:

Las figuras 1 a 3 son diagramas que representan la operación de sistemas de detección de dispositivo de la invención.

La figura 4 es un diagrama de flujo para un método de detección de dispositivo.

Descripción de las realizaciones

Con referencia a la figura 1 un sistema de detección de dispositivo incluye una aplicación de detección de dispositivo 1 y una memoria de firmas 2. El sistema se representa comunicando con un MSC 3.

La figura 2 representa un sistema de detección de dispositivo que tiene una aplicación 10, y una memoria de firmas 11. La aplicación 10 comunica con un EIR de legado 13 enlazado con una base de datos EIR 14, y con un MSC 12.

La figura 3 representa un sistema de detección de dispositivo incluyendo una aplicación 20 y una memoria de firmas 21. La aplicación se representa comunicando con un MSC 22 y con una base de datos EIR 23.

Los sistemas de detección de dispositivo generan una firma en base a una combinación de identidades de abonado y dispositivo. La firma no tiene significado semántico, es decir, los identificadores individuales que le dan origen no son una firma directamente legible con sello de tiempo, y la firma es almacenada en una memoria de datos conjuntamente con el sello de tiempo asociado. Lo siguiente es un ejemplo:

Ejemplo de número IMEI/IMEISV:

35-19300-123456-1-28
Ejemplo de número IMSI

310-150-123456789

La firma se crea usando un algoritmo hash MD5 que usa los números IMEI e IMSI concatenados como variables de entrada.

Paso 1. Concatenar <IMEI> más <IMSI>: “351930012345612831010150123456789”

Paso 2. Calcular la firma hash MD5: “e1765e21365b1a05e09062d133859565”

Esta firma no tiene significado semántico, es decir, los identificadores individuales (IMEI o IMSI) no pueden ser reconstruidos a partir de la firma. En esta realización, un algoritmo unidireccional genera la firma. En otra realización, el algoritmo que genera la firma a partir de las identidades puede ser reversible; sin embargo, los elementos de los identificadores originales todavía no son directamente discernibles en la firma. Solamente se pueden recuperar realizando el procedimiento inverso al elemento original. A causa de la naturaleza pseudoaleatoria de la firma generada (que no tiene significado semántico) se genera una clave única, asegurando que la búsqueda sea muy eficiente. La memoria de firmas tiene una estructura simple y eficiente, direccionada por un par de clave-valor en la que la clave es la firma y el sello de tiempo es el valor.

La firma se usa para determinar si una combinación de dispositivo/abonado existe en la red, y una notificación de estado de dispositivo/abonado es transmitida a un sistema externo. Éste último puede ser, por ejemplo, un sistema de gestión de dispositivos, una base de datos de atención a cliente, un sistema de provisión automático para un elemento de red tal como un MMSC, un sistema de provisión WAP, un sistema de registro, o un sistema de provisión de libro de direcciones.

Lo siguiente establece los escenarios ilustrados para implementación de la invención.

Realización de la figura 1

Para redes que no proporcionan funcionalidad EIR, el sistema de detección de dispositivo 1, 2 está integrado directamente en la red en lugar de un EIR. El MSC 3 está configurado para ver la aplicación de detección de dispositivo 1 como un EIR. La aplicación 1 responde con un reconocimiento positivo por defecto (“retorno blanco”, indicando que el dispositivo está permitido en la red) puesto que no está disponible la funcionalidad EIR. Además, la aplicación 1 genera una firma a partir de los identificadores de dispositivo y abonado incluidos en la petición MAP CHECK_IMEI transmitida desde el MSC 3. Usa la firma para comprobar (mediante la verificación eficiente de si la firma está en la memoria 2) si esta combinación de dispositivo/abonado existe en la red, es decir, ha sido detectada previamente en la red. En esta realización, la comprobación tiene la finalidad de determinar si la combinación fue detectada en un intervalo de tiempo anterior. El intervalo de tiempo es configurable en esta realización. En una realización alternativa, la comprobación determina si la combinación fue detectada alguna vez en la red, y no solamente en un intervalo de tiempo. La aplicación 1 genera una notificación para un sistema externo para indicar el resultado de esta comprobación.

Realización de la figura 2

En redes con un EIR de legado existente, la aplicación de detección de dispositivo 10 está integrada en el recorrido de señalización del EIR. Las peticiones de una comprobación EIR se pasan al EIR 13 por proxy. La respuesta del EIR 13 es aceptada y devuelta al MSC 12 como la respuesta a la petición original MAP CHECK_IMEI. Se lleva a cabo una comprobación de combinación de dispositivo/abonado como se ha descrito anteriormente.

Realización de la figura 3

En redes que requieren funcionalidad EIR, el sistema de la invención se extiende con la capacidad de consultar la base de datos EIR 23 conteniendo información específica EIR (en la práctica una lista de IMEIs con su estado asociado). El sistema 20, 21 determina y pasa la respuesta al MSC 22. De nuevo, se realiza una comprobación similar para la combinación de dispositivo/abonado. La aplicación de detección construye una respuesta MAP CHECK_ IMEI a partir del estado devuelto por la base de datos EIR 23.

Lo siguiente son los pasos primarios implementados por los sistemas de detección de dispositivo, con referencia a la figura 4.

1. MSC envía una operación MAP CHECK_IMEI conteniendo IMEI e IMSI. La señal 1 incorpora la respuesta EIR, una respuesta simulada (figura 1) o una respuesta real (figuras 2 y 3). La respuesta en esta realización es generada en paralelo con la realización de las operaciones siguientes.

2. La aplicación de detección de dispositivo comprueba si existe una firma en la memoria, y si la firma existe, actualiza el sello de tiempo asociado con el tiempo actual. Si la firma no existe, entonces se escribe la nueva firma en la memoria, con un sello de tiempo asociado puesto al tiempo actual.

3. Si la firma generada no estaba en la base de datos, indica que es una nueva combinación de dispositivo/abonado y la aplicación de detección de dispositivo envía una activación conteniendo la IMEI e IMSI de la petición original.

4. Activada por el tiempo, la aplicación de detección de dispositivo activa el envejecimiento de firmas. Para evitar la presencia de firmas atrasadas en la memoria, esta facilidad de limpieza pone a todas las entradas una edad más antigua que un período configurable y quita dichas entradas.

5. Si la firma está atrasada, es quitada de la base de datos.

La aplicación de detección es especialmente adecuada para la detección de nuevas combinaciones de abonado/dispositivo puesto que usa una base de datos simple y eficiente que permite lecturas muy rápidas en tiempo real. La estructura de base de datos surge a causa del hecho de que las firmas no tienen significado semántico y por ello no son indexadas usando los identificadores. Se deberá indicar que los pasos de detección de dispositivo 2-5 se realizan independientemente de la respuesta EIR. Esto es ventajoso cuando, por ejemplo, un dispositivo ha sido robado, la aplicación de detección de dispositivo proporciona una comprobación en tiempo real de si el dispositivo robado ha sido usado.

Cuando una activación de EIR llega a la aplicación de detección, calcula la firma del aparato a partir de la IMSI e IMEI en la activación de EIR y los compara con las firmas almacenadas. Si se halla la firma, la aplicación de detección ha detectado que el abonado ha cambiado a una combinación de abonado/dispositivo ya conocida, y se actualiza un sello de tiempo indicando la última vez que se vio esta firma. Si no se halla la firma (esto indica que se ha detectado una combinación nueva de abonado/dispositivo), la firma es añadida a la memoria por la aplicación de detección de dispositivo y se lleva a cabo una acción para enviar una activación conteniendo el par IMEI/IMSI detectado. Como resultado, cada vez que se detecta una combinación nueva de una IMEI y una IMSI, se añade una firma nueva a la memoria de firmas. La notificación de salida es especialmente útil como una activación para la provisión de un dispositivo nuevo.

En otra realización, el sistema tiene una segunda base de datos, principalmente para detectar un cambio en el aparato de un abonado usado por última vez. La segunda base de datos contiene mapeados de identificador de abonado a firma tal como mapeados de IMSI a firma o mapeados de MSISDN a firma. La segunda base de datos es direccionada usando un par de clave-valor, en el que el identificador de abonado es la clave y la firma es el valor. Tal base de datos está separada de la memoria de firmas y por ello no afecta a las operaciones centrales de verificación de firma descritas anteriormente.

Después de calcular la firma, como un segundo paso, la aplicación de detección de dispositivo consulta la segunda base de datos para consultar (y actualizar) la última firma vista que pertenece al abonado. Si la firma ha cambiado, se sabe que un cambio en el dispositivo activo de un abonado ha sido detectado y se envía una activación de cambio de dispositivo. Esto es útil para la gestión de distribución de servicios. Por ejemplo, si el usuario conmuta regularmente entre dos dispositivos diferentes, la memoria de firmas no detectará un cambio de combinación de usuario/dispositivo dentro de un intervalo de tiempo preconfigurado. Sin embargo, la segunda base de datos seguirá la pista de qué dispositivo está usando actualmente el usuario.

En resumen, las interacciones básicas de la base de datos son:

1) La aplicación recibe una activación de EIR del MSC y calcula una firma derivada de las identidades de abonado y dispositivo.

2) La aplicación usa la memoria de firmas para detectar nuevas combinaciones de abonado/dispositivo como se ha descrito anteriormente.

3) La aplicación consulta la segunda base de datos con el identificador de abonado (IMSI, MSISDN) y compara la firma presente con la firma calculada para detectar combinaciones de abonado/dispositivo cambiadas, sobreescribiendo la firma previa con la última firma cuando se ha producido un cambio de dispositivo.

La descripción anterior describe la invención en términos de las identificaciones de dispositivo GSM y abonado y en

términos de tecnología de base de datos como una realización preferida. Sin embargo, la invención no se limita a la tecnología GSM (por ejemplo, el uso de MEID y MIN/MDN en redes CDMA es una alternativa) o a una implementación de base de datos (por ejemplo, la implementación en memoria usando estructuras de datos es una alternativa).

Se apreciará que el sistema de la invención detecta nuevas combinaciones de abonado y dispositivo supervisando y siguiendo la pista combinaciones únicas de identidad de abonado y dispositivo usando una base de datos simple aplanada con una sola clave. Mediante lógica simple (es decir, esta firma existe en base a datos) se determina entonces que un nuevo dispositivo es detectado para dicho abonado, dando lugar a una activación al sistema de gestión de dispositivos o cualquier otro sistema para el que esta información sea relevante (por ejemplo, la provisión de dicho dispositivo, registrar dicho evento, etc). Si la firma ya existe, la invención conoce que la combinación de dispositivos se vio antes y por ello no generará una activación de aprovisionamiento.

Centrándose en la detección de nuevas combinaciones de abonado/aparato, y almacenando solamente la firma, la invención no sufre los problemas de una base de datos relacional, un servidor de directorio o estructuras de datos dinámicas. Esta firma es un número (por ejemplo, binario o hexadecimal) construido a partir de la identidad SIM (IMSI) y la IMEI proporcionados por la red en una activación de EIR usando una función matemática apropiada. Dado que la firma no tiene significado semántico, por ser de naturaleza pseudoaleatoria, su implementación en la base de datos es altamente eficiente. El uso de tal firma no solamente simplificará la base de datos especializada, sino que también permite implementaciones en memoria eficientes que dan lugar a significativas mejoras de funcionamiento.

La invención no se limita a las realizaciones descritas, sino que su construcción y detalle se pueden variar.

REIVINDICACIONES

1. Un método realizado por una red móvil, incluyendo el método los pasos realizados por uno o más elementos de red de:

detectar una señal procedente de un elemento de red que indica que un abonado desea estar activo en la red usando un dispositivo móvil; y

transmitir una notificación de estado de existencia de la combinación de dispositivo y abonado en la red, donde el método determina dicho estado:

generando una firma derivada de un identificador de dispositivo y un identificador de abonado, no teniendo la firma un significado semántico,

verificar si la firma está en una memoria de firmas, y:

si no lo está, determinar que la combinación de dispositivo y abonado no existe en la red, y almacenar la firma en la memoria de firmas, y

si lo está, determinar que la combinación de dispositivo y abonado ya existe en la red.

2. Un método según la reivindicación 1, donde la firma es generada por un algoritmo hash usando como entradas los identificadores de dispositivo y abonado tal como una IMEI y una IMSI.

3. Un método según la reivindicación 2, donde la firma es un número binario.

4. Un método según cualquier reivindicación precedente, donde el método es implementado en respuesta a una activación de EIR.

5. Un método según cualquier reivindicación precedente, donde se guarda un sello de tiempo en la memoria de firmas para indicar el tiempo de escritura de la firma en la memoria.

6. Un método según la reivindicación 5, incluyendo el paso adicional de, si la firma ya está almacenada, actualizar el sello de tiempo asociado con la firma en la memoria para indicar la última vez que la firma fue procesada.

7. Un método según las reivindicaciones 5 o 6, donde los sellos de tiempo se usan para determinar la edad.

8. Un método según cualquier reivindicación precedente, incluyendo el método los pasos adicionales de archivar o borrar firmas que tienen una edad superior a un umbral.

9. Un método según la reivindicación 8, donde la firma se almacena en la memoria en una posición indicativa de la edad.

10. Un método según cualquier reivindicación precedente, donde la notificación incluye el identificador de dispositivo y el identificador de abonado.

11. Un método según cualquiera de las reivindicaciones 5 a 10, donde la notificación incluye el sello de tiempo.

12. Un método según las reivindicaciones 10 o 11, donde la notificación incluye tanto el sello de tiempo actualizado como el sello de tiempo previo, donde el sello de tiempo es actualizado.

13. Un método según cualquier reivindicación precedente, donde la firma es generada por una aplicación de detección que se ejecuta en un elemento de red.

14. Un método según la reivindicación 13, donde la aplicación de detección opera como un proxy para un EIR de red existente.

15. Un método según la reivindicación 14, donde la aplicación genera automáticamente una respuesta positiva EIR simulada además de realizar las operaciones de procesado de firma.

16. Un método según la reivindicación 13, donde la aplicación de detección opera conjuntamente con una base de datos EIR para sustituir un EIR de legado.

17. Un método según la reivindicación 16, donde la aplicación de detección construye una respuesta MAP CHECK_IMEI a partir del estado devuelto por la base de datos EIR

18. Un método según cualquier reivindicación precedente, donde solamente se genera una notificación cuando se determina que la combinación de dispositivo/abonado no existe en la red.

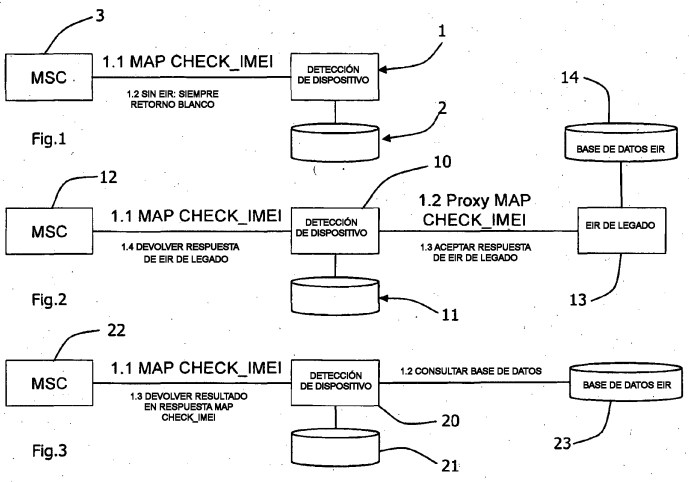
19. Un método según cualquier reivindicación precedente, incluyendo el paso adicional de almacenar la firma y el identificador de abonado en una segunda base de datos.

20. Un método según la reivindicación 19, donde la segunda actualización de base de datos se realiza con un par de clave-valor en el que el identificador de abonado es la clave y la firma es el valor.

21. Un método según las reivindicaciones 19 o 20, donde el sistema genera una notificación que indica el dispositivo de abonado actual después de actualizar la segunda base de datos.

22. Un sistema de detección de dispositivo de red móvil incluyendo medios para realizar un método según cualquier reivindicación precedente.

23. Un medio legible por ordenador incluyendo código de software para realizar un método de cualquiera de las reivindicaciones 1 a 21 cuando se ejecuta en un procesador digital.


3
MSC
1.1 MAP CHECK_IMEI
1.2 SIN EIR: SIEMPRE RETORNO BLANCO
DETECCIÓN DE DISPOSITIVO
1
2
14
BASE DE DATOS EIR
Fig.1
12
MSC
1.1 MAP CHECK_IMEI
1.4 DEVOLVER RESPUESTA DE EIR DE LEGADO
DETECCIÓN DE DISPOSITIVO
10
1.2 Proxy MAP CHECK_IMEI
1.3 ACEPTAR RESPUESTA DE EIR DE LEGADO
EIR DE LEGADO
11
13
Fig.2
22
MSC
1.1 MAP CHECK_IMEI
1.3 DEVOLVER RESULTADO EN RESPUESTA MAP CHECK_IMEI
DETECCIÓN DE DISPOSITIVO
1.2 CONSULTAR BASE DE DATOS
BASE DE DATOS EIR
20
21
23
Fig.3

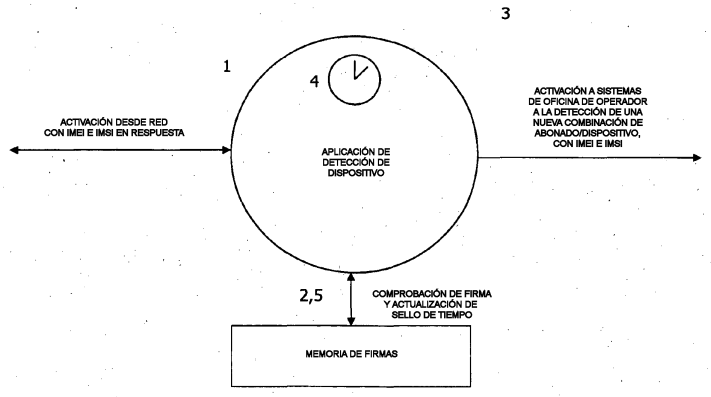

3
1
4
ACTIVACIÓN DESDE RED CON IMEI E IMSI EN RESPUESTA
APLICACIÓN DE DETECCIÓN DE DISPOSITIVO
ACTIVACIÓN A SISTEMAS DE OFICINA DE OPERADOR A LA DETECCIÓN DE UNA NUEVA COMBINACIÓN DE ABONADO/DISPOSITIVO, CON IMEI E IMSI
2,5
COMPROBACIÓN DE FIRMA Y ACTUALIZACIÓN DE SELLO DE TIEMPO
MEMORIA DE FIRMAS

Fig.4