(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 723 972**

(51) Int. CI.:

H04W 12/06 (2009.01)
H04W 4/14 (2009.01)
H04W 4/50 (2008.01)
H04L 29/08 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **15.09.2015 PCT/EP2015/071005**

(87) Fecha y número de publicación internacional: **31.03.2016 WO16046015**

(96) Fecha de presentación y número de la solicitud europea: **15.09.2015 E 15763903 (0)**

(97) Fecha y número de publicación de la concesión europea: **06.02.2019 EP 3198912**

(54) Título: **Método para detectar dinámicamente que unos elementos seguros son idóneos para una campaña OTA y el correspondiente servidor OTA**

(30) Prioridad:

22.09.2014 EP 14306451

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
04.09.2019

(73) Titular/es:

THALES DIS FRANCE SA (100.0%)
6, rue de la Verrerie
92190 Meudon, FR

(72) Inventor/es:

PEREIRA, GABRIEL;
BOITEUX, TRISTAN y
DEPUSSE, KIM

(74) Agente/Representante:

ELZABURU, S.L.P

DESCRIPCIÓN

Método para detectar dinámicamente que unos elementos seguros son idóneos para una campaña OTA y el correspondiente servidor OTA

La presente invención pertenece al campo de las telecomunicaciones y, más específicamente, a la administración remota de elementos seguros, tales como UICC (tarjetas universales de circuitos integrados), ESi (elementos seguros integrados), tarjetas de memoria, tarjetas micro-SD o eUICC (UICC integrados) que interactúan con dispositivos; por ejemplo, dispositivos portátiles como teléfonos, teléfonos inteligentes, agendas electrónicas u ordenadores. Los elementos seguros también pueden tener la forma de circuitos instalados en máquinas, como circuitos en el área M2M (máquina a máquina). Pueden no estar físicamente conectados a los terminales, pero pueden comunicarse con ellos mediante una conexión de corta distancia, en la que un elemento seguro se ubica de forma remota y se comunica a través de un canal de corta distancia con el terminal (por ejemplo, Bluetooth o Wi-Fi).

Dicha administración de elementos seguros se realiza normalmente por vía aérea (OTA) para actualizar o instalar programas o datos en elementos seguros. La administración de este tipo usa el protocolo HTTP (protocolo de transferencia de hipertexto) y también es denominada “RFM” (Administración remota de archivos) o “RAM” (gestión de administración remota) por HTTP.

Hay dos formas de administrar elementos seguros:

Una primera forma es direccionar los elementos seguros en un modo de envío sin solicitud; por ejemplo, utilizando listas estáticas de elementos seguros. Una lista de elementos seguros se construye utilizando criterios de selección antes de la realización de la campaña y estos elementos seguros son objeto de direccionamiento durante la campaña. Sin embargo, la lista específica de elementos seguros que se actualizarán a través de una campaña OTA evoluciona permanentemente durante la realización de una campaña (se pueden activar nuevos abonos, se pueden cambiar las tarjetas o elementos seguros de un dispositivo a otro, se pueden reemplazar las tarjetas, …). Esta limitación se vuelve crítica cuando el número de elementos seguros es grande (puede ser de varios millones) y cuando la campaña dura un largo periodo (varias semanas o incluso meses) para llegar a todos los elementos seguros en el campo. Por ejemplo, si un MNO (operador de red móvil) está aprovisionando nuevos abonos en la plataforma OTA mientras se está realizando una campaña para la cual los elementos recientemente aprovisionados podrían ser idóneos para una campaña, será preciso que el MNO realice una segunda campaña para actualizar los abonos recién aprovisionadas.

Una segunda forma es realizar la gestión de campañas a través de HTTP en modo de obtención por solicitud con un mecanismo de idoneidad dinámica: en esta solución, no se crea una lista específica, sino que los elementos seguros se definen a través de un criterio de idoneidad. Los elementos seguros realizan sondeos regularmente para ponerse en contacto con la plataforma OTA y para comprobar si hay una actualización pendiente para ellos. El criterio de idoneidad se evalúa cuando el elemento seguro está realizando el sondeo, lo que brinda el beneficio de permitir alcanzar elementos que se desplegaron después del inicio de la campaña. Sin embargo, esta solución tiene una gran limitación: solo está soportada con elementos seguros que soportan el portador HTTP. Además, tiene un inconveniente importante cuando no es necesario actualizar ninguno o pocos elementos seguros (se crea un tráfico importante de red para soportar las sesiones periódicas de sondeo HTTP entre millones de elementos seguros y la plataforma OTA).

El documento US2011252240 da a conocer la combinación de un marco de envío sin solicitud con un marco de obtención por solicitud para transferir actualizaciones para los dispositivos inalámbricos. En respuesta a la recepción de una notificación (envío sin solicitud) del servidor de administración, se verifica la confianza de la notificación. Si la confianza se verifica positivamente, se puede establecer una sesión de red (obtención por solicitud) con el servidor de administración.

El problema es encontrar una forma de administrar campañas OTA con listas específicas dinámicas, independientemente del portador (SMS, CAT-TP, HTTP, …) que haya de usarse para realizar las operaciones remotas. CAT-TP significa protocolo de transporte del juego de herramientas para aplicaciones de tarjetas.

Este objetivo se alcanza gracias a un método para la administración remota de elementos seguros, cooperando cada elemento seguro con un terminal de telecomunicaciones en una red de telecomunicaciones, realizándose dicha administración remota mediante un servidor OTA, consistiendo el método en:

- Detectar qué elementos seguros no han sondeado el servidor OTA durante un periodo de tiempo determinado;

- Comprobar la idoneidad para estos elementos seguros;

- Actualizar los elementos seguros que no sondearon el servidor OTA durante este periodo de tiempo determinado y que son idóneos para la campaña OTA enviando, sin solicitud, mensajes a estos elementos seguros.

Por lo tanto, la invención propone aplicar el modo de envío sin solicitud descrito anteriormente a elementos seguros que no sondearon el servidor OTA desde una fecha dada y que son idóneos para una actualización.

Ventajosamente, los mensajes que se envían sin solicitud a los elementos seguros son mensajes SMS, independientemente de los portadores que estén soportados por los elementos seguros.

La invención también se refiere a un servidor OTA para actualizar elementos seguros que cooperan con terminales de telecomunicaciones en una red de telecomunicaciones, comprendiendo este servidor OTA:

- Medios para detectar qué elementos seguros no han sondeado el servidor OTA durante un periodo de tiempo determinado;

- Medios para comprobar la idoneidad de estos elementos seguros;

- Medios para actualizar estos elementos seguros que no han sondeado el servidor OTA durante este periodo de tiempo determinado y que son idóneos para la campaña OTA enviando, sin solicitud, mensajes a estos elementos seguros.

En la siguiente descripción de una implementación preferida de la invención, dada con referencia a la figura 1, aparecerán otras características y ventajas.

La figura 1 representa un sistema que implementa la presente invención.

En esta figura, se proporciona un servidor OTA 10 para actualizar elementos seguros 11, representándose un único elemento seguro 11. La actualización de los elementos seguros 11 se realiza normalmente durante las campañas OTA. Cada elemento seguro 11 coopera con un terminal de telecomunicaciones (no representado) en una red de telecomunicaciones. Un elemento seguro es, por ejemplo, una UICC, una tarjeta SIM o un elemento seguro integrado (ESi).

Según la segunda forma de administrar los elementos seguros 11 descritos anteriormente, cada elemento seguro sondea regularmente (durante una etapa 20) sobre HTTP el servidor OTA 10 para comprobar si este servidor OTA 10 tiene que actualizar el elemento seguro 11. El servidor 10 tiene medios 12 para comprobar la idoneidad del elemento seguro 11 para una actualización. Esta idoneidad consiste en comprobar si hay datos o programas que deben descargarse en el elemento seguro 11. Si el ES es idóneo para una actualización, un administrador 13 de ES envía instrucciones OTA al ES 11 a través de una capa 14 de conectividad, también usada durante la etapa de sondeo 20. Después de haber enviado las instrucciones al ES 11 (y después de comprobar que la actualización se realizó con éxito), la capa 14 de conectividad envía un registro a una base de datos 15 para registrar qué instrucciones han sido enviadas al ES 11 (qué programas se han descargado o actualizado) y la fecha de la actualización de este ES 11. Esta fecha es denominada en lo sucesivo Last_Polling_Date y corresponde a la última vez que el ES 11 ha sondeado al servidor OTA 10, consultando las posibles actualizaciones que se enviarán por el aire. El servidor OTA 10 puede comunicarse con elementos seguros 11 utilizando los portadores SMS, CAT-TP y HTTP. El mecanismo de sondeo de los elementos seguros a la plataforma solo utiliza el portador HTTP (canal de datos).

Esta forma corresponde a la forma clásica (conocida) de administrar elementos seguros 11 (modo de obtención por solicitud).

Según la invención, el servidor OTA comprende un simulador 16 de sondeo que analiza periódicamente toda la base de datos 15 de elementos seguros 11 y simula un sondeo (etapa 21) para cada ES 11 que no está sondeando de manera natural el servidor OTA 10. Estos elementos seguros 11 que no efectúan un sondeo son aquellos que usan solo el portador de SMS (abonos 2G o 3G en general), aquellos que no soportan el protocolo HTTP, aquellos que cooperan con terminales de telecomunicaciones que no son compatibles con BIP (protocolo independiente del portador) pero también elementos seguros que se supone que sondean pero que no son están realizando sondeos debido a su posición geográfica (problemas de cobertura de datos, situaciones de itinerancia, …). El simulador 16 de sondeo utilizará los criterios de Last_Polling_Date para simular un sondeo (etapa 21) de estos elementos seguros 11, como si realmente hubieran realizado un sondeo. Los sondeos simulados se dirigen a los medios 12 para comprobar la idoneidad para actualizar estos elementos seguros 11. Después de una comprobación de idoneidad de estos elementos seguros que no realizaron sondeos durante un periodo de tiempo determinado, se indican aquellos para los cuales es necesaria o está disponible una actualización al administrador 13 de ES, que envía instrucciones OTA a estos elementos seguros 11. Estos elementos seguros se actualizan aunque no sondearan al servidor OTA. La comprobación de idoneidad es la misma que la utilizada anteriormente en la gestión de campañas a través de HTTP en modo de obtención por solicitud.

Así, el simulador 16 de sondeo emula el sondeo de los elementos seguros que no sondearon el servidor OTA 10 durante un periodo de tiempo determinado (desde un momento dado). Estos elementos seguros son considerados por el servidor OTA (en el nivel de los medios 12 de comprobación de idoneidad) como si hubieran sondeado realmente.

Así, la invención propone entrar en un modo de envío sin solicitud para elementos seguros que no se pusieron en contacto con el servidor OTA 10 desde un momento dado (por ejemplo, sin encuesta alguna desde hace dos semanas).

El servidor OTA 10 usa un portador adaptado a cada ES que haya de actualizarse: los elementos seguros que solo soportan SMS se actualizarán a través de SMS (envío SMS sin solicitud), los que soportan HTTP se actualizarán a

través de HTTP (envío HTTP sin solicitud). También se puede considerar el volumen de los datos o las instrucciones que se enviarán a los elementos seguros: Si estos datos o instrucciones pueden caber en un SMS (tamaño inferior a aproximadamente 1 Kb), se puede preferir un envío SMS sin solicitud al establecimiento, por ejemplo, de una sesión HTTP.

Otra solución es direccionar los elementos seguros independientemente del portador que soportan. Esto significa que todos los elementos seguros serán objeto de direccionamiento solo a través de SMS. Esto garantiza, por ejemplo, que se actualicen los elementos seguros que no están bajo la cobertura de datos (no es posible HTTP) pero que están bajo la cobertura de la red (pueden recibir mensajes SMS). Esto permite también la actualización de elementos seguros comprendidos en los terminales en los que los usuarios han desactivado la recepción de datos; por ejemplo, mientras se encuentran en el extranjero para evitar la facturación del tráfico de datos.

La invención permite desplegar elementos seguros HTTP sin activar el sondeo periódico, simulando el sondeo y, en caso de idoneidad, los elementos seguros pueden actualizarse en modo de envío sin solicitud. El beneficio es optimizar los recursos de la red.

Además, en el caso de elementos seguros implementados con el sondeo periódico activado, las tarjetas que se inserten en terminales que no tengan prestaciones BIP nunca podrán sondear el servidor OTA. La invención, gracias al emulador de sondeo, permite realizar operaciones remotas OTA en ellos utilizando un portador alternativo (SMS).

REIVINDICACIONES

1. Método para la administración remota de elementos seguros (11), cooperando cada elemento seguro (11) con un terminal de telecomunicaciones en una red de telecomunicaciones, realizándose dicha administración remota mediante un servidor OTA (10), caracterizándose dicho método por comprender:

- Detectar qué elementos seguros (11) no han sondeado dicho servidor OTA (10) durante un periodo de tiempo determinado;

- Comprobación de idoneidad para dichos elementos seguros (11);

- Actualizar dichos elementos seguros (11) que no sondearon dicho servidor OTA (10) para dicho periodo de tiempo determinado y que son idóneos para dicha administración remota enviando, sin solicitud, mensajes a dichos elementos seguros (11).

2. Método según la reivindicación 1, en el que dichos mensajes enviados, sin solicitud, a dichos elementos seguros (11) son mensajes SMS, independientemente de los portadores que estén soportados por dichos elementos seguros (11).

3. El servidor OTA (10) para actualizar elementos seguros (11) que cooperan con terminales de telecomunicaciones en una red de telecomunicaciones, caracterizándose dicho servidor OTA (10) por comprender:

- Medios (16) para detectar qué elementos seguros (11) no han sondeado a dicho servidor OTA (10) durante un periodo de tiempo determinado;

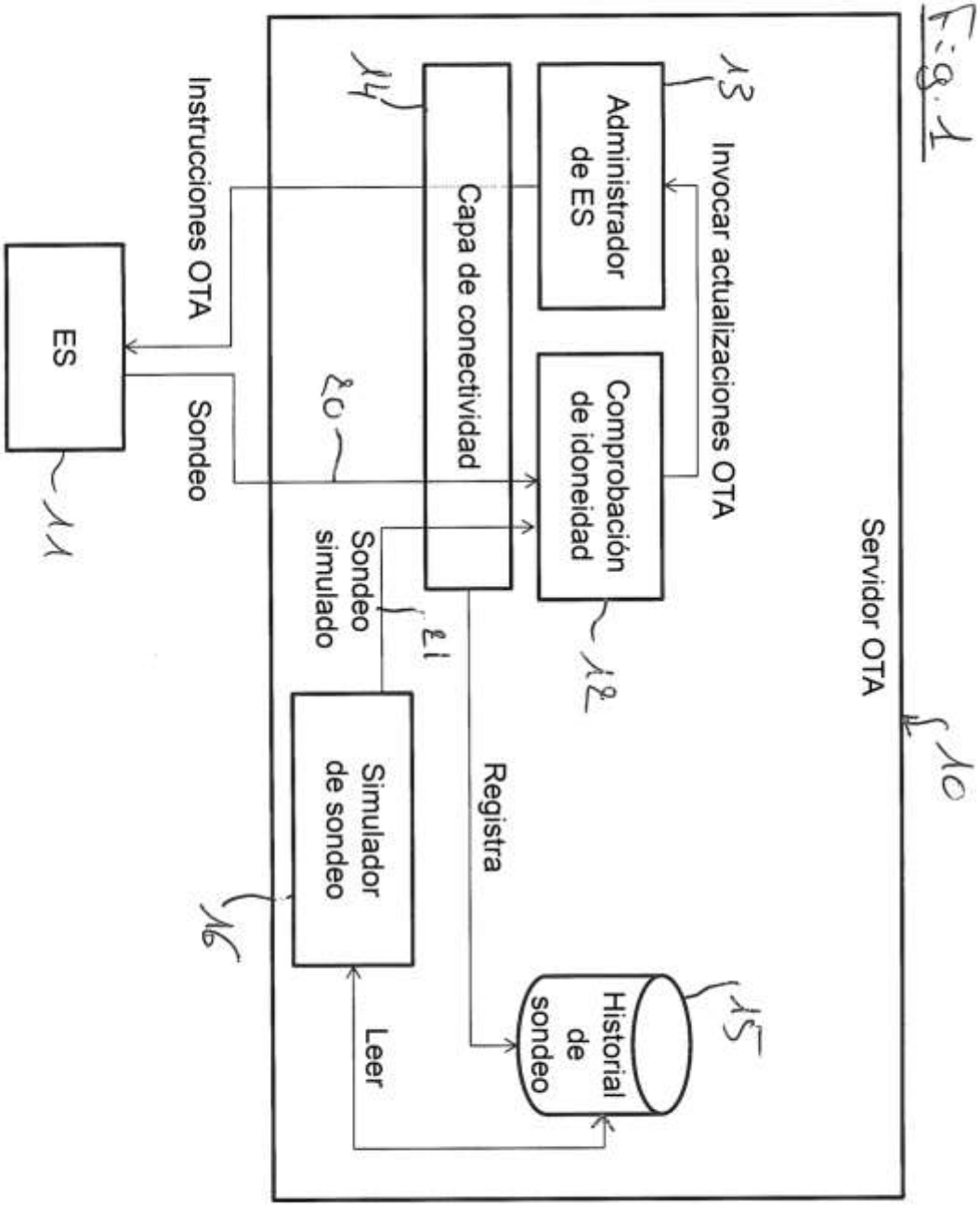
- Medios (12) para comprobar la idoneidad de dichos elementos seguros (11);

- Medios para actualizar dichos elementos seguros (11) que no han sondeado dicho servidor OTA (10) para dicho periodo de tiempo determinado y que son idóneos para una administración remota enviando, sin solicitud, mensajes a dichos elementos seguros (11).

4. Servidor OTA (10) según la reivindicación 3, en el que dichos medios (16) para detectar qué elementos seguros (11) que no han interrogado a dicho servidor OTA (10) durante un periodo de tiempo determinado están constituidos por un simulador (16) de sondeo.

5. Servidor OTA según cualquiera de las reivindicaciones 3 y 4, en el que dichos mensajes enviados, sin solicitud, a dichos elementos seguros (11) son mensajes SMS, independientemente de los portadores que estén soportados por dichos elementos seguros (11).

Fig. 1


Servidor OTA
10
Administrador de ES
13
Invocar actualizaciones OTA
Comprobación de idoneidad
12
Capa de conectividad
14
Instrucciones OTA
Sondeo
20
Sondeo simulado
21
Simulador de sondeo
16
Registra
Leer
Historial de sondeo
15
ES
11