

19



OFICINA ESPAÑOLA DE  
PATENTES Y MARCAS

ESPAÑA



11 Número de publicación: **2 533 831**

51 Int. Cl.:

**H04L 29/06** (2006.01)

**H04L 12/22** (2006.01)

12

TRADUCCIÓN DE PATENTE EUROPEA

T3

96 Fecha de presentación y número de la solicitud europea: **21.04.2005** **E 05008812 (9)**

97 Fecha y número de publicación de la concesión europea: **31.12.2014** **EP 1592195**

54 Título: **Estación móvil y método de control de comunicación**

30 Prioridad:

**28.04.2004 JP 2004134262**

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

**15.04.2015**

73 Titular/es:

**NTT DOCOMO, INC. (100.0%)**  
**11-1, Nagatacho 2-chome, Chiyoda-ku**  
**Tokyo 100-6150, JP**

72 Inventor/es:

**ASAI, MAO;**  
**OI, TATSURO;**  
**NAKATSUCHI, MASAHARU;**  
**KAKUNO, KOSUKE y**  
**SHIBUTANI, AKIRA**

74 Agente/Representante:

**LLAGOSTERA SOTO, María Del Carmen**

**ES 2 533 831 T3**

Aviso: En el plazo de nueve meses a contar desde la fecha de publicación en el Boletín europeo de patentes, de la mención de concesión de la patente europea, cualquier persona podrá oponerse ante la Oficina Europea de Patentes a la patente concedida. La oposición deberá formularse por escrito y estar motivada; sólo se considerará como formulada una vez que se haya realizado el pago de la tasa de oposición (art. 99.1 del Convenio sobre concesión de Patentes Europeas).

## Descripción

### ANTECEDENTES DE LA INVENCION

#### Campo de la invención

La presente invención se refiere a un procedimiento para una estación móvil para  
5 realizar una conexión con un dispositivo externo a la vez que se mantiene un nivel de  
seguridad predeterminado.

#### Técnicas relacionadas

Convencionalmente, las estaciones móviles, incluyendo los teléfonos móviles pueden  
10 disfrutar de diversos servicios, utilizando un programa de aplicaciones preinstalado (en  
lo sucesivo, una "aplicación") o una aplicación descargada a través de una red. Algunos  
de estos servicios implican la transmisión y recepción de diversas señales hacia y desde  
un dispositivo externo. En este caso, la estación móvil necesita seleccionar un  
interlocutor fiable a fin de mantener un nivel de seguridad predeterminado durante la  
15 comunicación. Por ejemplo, el Documento de Patente 1 es un documento que describe  
esta tecnología, y que describe una característica técnica de determinación de la  
propiedad de conexión de acuerdo con un nivel de seguridad de un interlocutor.

[Documento de Patente 1] Solicitud de Patente Japonesa abierta No. 2002-281558

La solicitud de patente GB 2348568 A describe un sistema para adaptar el nivel de  
20 seguridad de una aplicación que se ejecuta en un terminal móvil de acuerdo con unas  
configuraciones de aplicación almacenadas en el terminal, y de acuerdo con parámetros  
externos.

RESUMEN DE LA INVENCION

Sin embargo, la tecnología convencional mencionada anteriormente presenta un problema preocupante, ya que, dependiendo del nivel de seguridad del interlocutor de la comunicación, la estación móvil no está autorizada a comunicarse con el dispositivo  
5 externo a pesar del deseo de un usuario. Uno de los medios eficaces para resolver este problema es garantizar la seguridad en un nivel alto, como por ejemplo la introducción de un PIN (Número de Identificación Personal), para todas las aplicaciones que requieran una conexión con un dispositivo externo.

En realidad, los niveles de seguridad de las respectivas aplicaciones necesarias para la  
10 conexión con un dispositivo externo son diferentes según los tipos de servicios deseados por el usuario. Por esta razón, el establecimiento de un ajuste del nivel de seguridad igual para todas las aplicaciones no siempre resulta eficiente en términos de reducción de la carga de proceso y de carga de comunicación en la estación móvil, del tiempo de comunicación de la misma, etc. En particular, si se solicita la introducción del PIN  
15 incluso en una conexión de la estación móvil con un dispositivo externo que no requiere seguridad en un nivel tan alto, por ejemplo, en un caso de conexión con un terminal registrado en la estación móvil, ello puede contribuir a la impedancia de la comunicación simple y rápida.

Por lo tanto, un objeto de la presente invención es permitir que una estación móvil  
20 establezca rápidamente la comunicación a la vez que se mantiene la seguridad en un nivel determinado, cambiando un procedimiento de conexión con un dispositivo externo, de acuerdo con un nivel de seguridad establecido en una aplicación.

Con el fin de resolver el problema anterior, se describe una estación móvil de acuerdo con la reivindicación 1.

Un método de control de comunicación de acuerdo con la presente invención se describe en la reivindicación 4.

De acuerdo con estos aspectos de la invención, el procedimiento de conexión entre la estación móvil y el dispositivo externo se determina de acuerdo con el nivel de seguridad establecido en la aplicación para realizar la comunicación con el dispositivo externo. Específicamente, cuando se ha establecido un alto nivel de seguridad en la aplicación activada, se aplica una condición más estricta para la conexión; por ejemplo, se exige que el dispositivo externo transmita un PIN. Por otro lado, cuando se determina un nivel de seguridad bajo en la aplicación activada, se aplican unas condiciones más flexibles para la conexión; por ejemplo, se omite la petición de transmisión de un PIN para el dispositivo externo. Mediante esta configuración en la que la estación móvil cambia el procedimiento de conexión con el dispositivo externo de acuerdo con el nivel de seguridad establecido en la aplicación, la estación móvil evita la ejecución indiscriminada de autenticación y cifrado complejos como consecuencia de la comunicación con un interlocutor de comunicación que no exige un nivel de seguridad tan alto, como por ejemplo un dispositivo externo registrado. Como resultado, resulta factible establecer rápidamente la comunicación entre la estación móvil y el dispositivo externo a la vez que se mantiene la seguridad en un cierto nivel.

La estación móvil de acuerdo con la presente invención puede estar configurada en una configuración que comprende además medios de selección para seleccionar un dispositivo externo que puede someterse a una conexión automática utilizando una aplicación con un alto nivel de seguridad determinado en el mismo, en el que cuando el nivel de seguridad captado por el medio de captación es el nivel de seguridad alto, el

medio de conexión realiza la conexión automática con el dispositivo externo seleccionado por el medio de selección.

La conexión en el nivel de seguridad alto puede eliminar la relación con terceros no autorizados tanto como sea posible, incluso en los casos en que se intenta la conexión automática sin la intervención de una operación de usuario. De acuerdo con la presente invención, la conexión automática con el dispositivo externo se ejecuta si el usuario permite la conexión automática y sólo si el nivel de seguridad se encuentra alto en la aplicación en acción. Ello permite que la estación móvil establezca rápidamente la comunicación por el procedimiento simple y sin necesidad de una operación de usuario, a la vez que se mantiene el nivel de seguridad fijado.

La estación móvil de acuerdo con la presente invención también se puede configurar en una configuración que comprende además medios de selección para seleccionar un dispositivo externo que puede someterse a una conexión mediante una aplicación con un alto nivel de seguridad fijado en el mismo, en el que cuando el nivel de seguridad captado por los medios de captación es el nivel de seguridad alto, el medio de conexión realiza la conexión con el dispositivo externo en caso de recibir una solicitud de conexión desde el dispositivo externo seleccionado por el medio de selección.

Posiblemente existen terceras partes que intentan realizar un acceso no autorizado entre los dispositivos externos, por lo que resulta deseable, en términos de mantenimiento de la seguridad, que la estación móvil realice conexiones con una mayoría no especificada de dispositivos externos realizando una búsqueda (solicitud de conexión) de la propia estación móvil. Por otro lado, limitar la búsqueda de entidades independientemente de los niveles de seguridad de las aplicaciones resulta ineficiente en términos de facilidad de conexión en la ejecución de una aplicación que no requiere un nivel de seguridad tan

alto. Por lo tanto, la estación móvil hace caso omiso de una búsqueda desde un dispositivo externo (un dispositivo externo no especificado) no seleccionado por el usuario, sólo si la aplicación en ejecución se ha fijado en el nivel de seguridad alto. A continuación la estación móvil sólo acepta una búsqueda desde un dispositivo externo  
5 específico seleccionado como conectable, y permite una conexión con el dispositivo. Ello elimina la necesidad de que el usuario de la estación móvil envíe manualmente una respuesta de búsqueda para una búsqueda desde un dispositivo externo. Como resultado, resulta posible reducir el tiempo y el esfuerzo hasta el establecimiento de la comunicación, a la vez que se mantiene el nivel de seguridad predeterminado. Dado que  
10 la estación móvil de acuerdo con la presente invención puede administrar objetivos de conexión en el nivel de seguridad alto en una sola operación, funciona más eficazmente a medida que el número de peticiones de conexión de dispositivos externos aumenta.

En la estación móvil de acuerdo con la presente invención, preferiblemente, el medio de conexión realiza la conexión entre la estación móvil y el dispositivo externo mediante el  
15 uso de BLUETOOTH (marca registrada).

La comunicación utilizada para la conexión entre la estación móvil y el dispositivo externo es preferiblemente, por ejemplo, la comunicación Bluetooth. Dado que BLUETOOTH permite desde una a múltiples conexiones en su forma estándar y se puede instalar en muchos tipos de dispositivos, presenta muchas ventajas adecuadas  
20 para productos de consumo. Por este motivo, es necesario anticipar el uso no autorizado por parte de terceros, por un lado, y considerar adecuadamente la conveniencia del usuario por otro lado. En consecuencia, la aplicación de la tecnología de acuerdo con la presente invención a la comunicación BLUETOOTH puede producir el efecto antes

mencionado de permitir la comunicación rápida más eficazmente a la vez que se mantiene la seguridad.

La presente invención implica cambiar el procedimiento de conexión con el dispositivo externo de acuerdo con el nivel de seguridad establecido en la aplicación, y de esta  
5 manera permite un rápido establecimiento de la comunicación, a la vez que se mantiene la seguridad en el nivel predeterminado.

### BREVE DESCRIPCIÓN DE LOS DIBUJOS

La Fig. 1 es un diagrama de bloques que muestra una configuración funcional de  
10 una estación móvil de acuerdo con la presente invención.

La Fig. 2 es una ilustración que muestra un ejemplo de la correspondencia entre las aplicaciones y los niveles de seguridad del ADF.

La Fig. 3 es un diagrama de flujo que muestra un ejemplo de un proceso de conexión BLUETOOTH donde se selecciona un dispositivo registrado con una  
15 clave de enlace de dispositivos externos detectados.

La Fig. 4 es una ilustración que muestra una pantalla de visualización. La Fig. 4(a) es una ilustración que muestra una pantalla de visualización donde se selecciona un dispositivo registrado con una clave de enlace a partir de una lista de los dispositivos detectados que se muestran en el caso de ejecutar el proceso de  
20 conexión BLUETOOTH que se muestra en la Fig. 3. La Fig. 4(b) es una ilustración que muestra una pantalla de visualización donde se selecciona un dispositivo registrado sin una clave de enlace a partir de la lista anterior. La Fig.

4(c) es una ilustración que muestra una pantalla de visualización donde se selecciona un dispositivo no registrado de la lista anterior.

La Fig. 5 es un diagrama de flujo que muestra un ejemplo de un proceso de conexión BLUETOOTH donde se selecciona un dispositivo registrado sin una clave de enlace a partir de dispositivos externos detectados.

La Fig. 6 es un diagrama de flujo que muestra un ejemplo de un proceso de conexión BLUETOOTH donde se selecciona un dispositivo no registrado a partir de dispositivos externos detectados.

## 10 DESCRIPCIÓN DE LAS REALIZACIONES PREFERENTES

A continuación se describirá una realización de la presente invención con referencia a los dibujos adjuntos que se presentan con fines ilustrativos. En primer lugar, se describirá una configuración de estación móvil 10 en la presente realización. La Fig. 1 es un diagrama de bloques que muestra una configuración funcional de la estación móvil 10. Tal como se muestra en la Fig. 1, la estación móvil 10 tiene una memoria de aplicación 11, una parte de ejecución de aplicación 12 (correspondiente a los medios de activación), una parte de búsqueda de dispositivo 13, una parte de visualización 14, una parte de entrada 15 (correspondiente al medio de selección), un captador de nivel de seguridad 16 (correspondiente al medio de captación), y una parte de conexión BLUETOOTH 17 (correspondiente al medio de conexión). Estas partes están conectadas de manera que sean capaces de implementar la entrada/salida de varias señales a través de un bus.

A continuación se describirá en detalle cada uno de los componentes de la estación móvil 10.

El almacenamiento de aplicaciones 11 se compone físicamente de la memoria integrada, como por ejemplo una EEPROM (Memoria Eléctricamente Borrable y Programable de Sólo Lectura). El almacenamiento de aplicaciones 11 almacena una pluralidad de programas de aplicación que la estación móvil 10 puede ejecutar mediante el uso de BLUETOOTH. Los programas de aplicación son, por ejemplo, los de i-appli (marca registrada). Tal como se muestra en la Fig. 2, cada programa de aplicación se correlaciona con un ADF (Archivo de Descripción de Aplicación), y se establece un nivel de seguridad en cada uno de estos ADF. Cuando se ejecuta un programa de aplicación para realizar una conexión BLUETOOTH, la estación móvil 10 cambia el procedimiento de conexión de acuerdo con el nivel de seguridad.

Los ADF de todos los programas de aplicaciones que hacen uso de Bluetooth deben contener una descripción de clave UseBluetooth. Por ejemplo, cuando un parámetro de la clave UseBluetooth descrito en un ADF es "alto", la estación móvil 10 realiza una conexión a un nivel de seguridad alto, es decir, un procedimiento de conexión que incluye la autenticación y el cifrado, mediante la introducción del PIN. Por otra parte, cuando el parámetro es "bajo", la estación móvil 10 realiza una conexión en un nivel de seguridad bajo, es decir, un procedimiento de conexión sin la autenticación y el cifrado mediante la introducción del PIN. El parámetro se describe en el formato ASCII y distingue entre mayúsculas y minúsculas.

Cuando el usuario introduce un comando de activación de una aplicación, a través de la parte de entrada 15, la parte de ejecución de la aplicación 12 recupera esta aplicación desde el almacenamiento de aplicaciones 11 en un área de memoria. Cuando la

aplicación se activa de esta manera, la parte de ejecución de la aplicación 12 ordena a la parte de búsqueda de dispositivos 13 que busque dispositivos externos. Los dispositivos externos como objetivos de la búsqueda son dispositivos externos que existen dentro de un intervalo de transmisión (por ejemplo, aproximadamente 10-100 m de radio) de la estación móvil 10 y que pueden someterse a una conexión Bluetooth. Además, la parte de ejecución de aplicaciones 12 emite el nivel de seguridad que se describe en el ADF de la aplicación en acción, en respuesta a una petición del captador de nivel de seguridad 16 que se describe más adelante.

Cuando se recibe un comando de conexión desde una aplicación en acción, la parte de búsqueda de dispositivos 13 envía una señal de búsqueda al entorno (sondeo) para buscar dispositivos externos como candidatos para la conexión BLUETOOTH. La parte de ejecución de aplicaciones 12 mencionada anteriormente es notificada sobre los dispositivos externos detectados como resultado de la búsqueda. Con referencia a la Fig. 1, en la presente realización se detectan los dispositivos externos 20, 30 y 40, y por lo tanto la información de identificación de estos dispositivos es enviada desde la parte de búsqueda de dispositivos 13 a la parte de ejecución de aplicaciones 12.

La parte de visualización 14 presenta el resultado de la búsqueda realizada por la parte de búsqueda de dispositivos 13 al usuario de la estación móvil 10 de acuerdo con un comando de la parte de ejecución de aplicaciones 12. Preferiblemente, la parte de pantalla 14 muestra registros de conexión con los dispositivos externos detectados en una forma que el usuario puede reconocer visualmente.

La parte de entrada 15 se compone de un botón como hardware y, al detectar una operación de presión o contacto sobre el botón por parte del usuario, la parte de entrada 15 da la instrucción a la parte que ejecuta las aplicaciones 12 para ejecutar la aplicación.

La parte de entrada 15 lleva a cabo la selección de un dispositivo externo con el que la estación móvil 10 intenta conectar, a partir de los dispositivos externos que se muestran en la parte de visualización 14, de acuerdo con la operación de selección de un usuario.

La parte de entrada 15 selecciona un dispositivo externo específico a partir de una pluralidad de dispositivos externos registrados con antelación, según una operación de selección de acuerdo con un propósito del usuario. El dispositivo externo específico es, por ejemplo, un dispositivo externo como un interlocutor cuando la estación móvil 10 realiza una conexión automática mediante el uso de una aplicación con el nivel de seguridad alto establecido en la misma. En este caso, la estación móvil 10 transmite una solicitud de conexión al dispositivo externo específico.

El dispositivo externo específico es también un dispositivo externo como un interlocutor cuando la estación móvil 10 se busca y se conecta mediante el uso de una aplicación con el nivel de seguridad alto establecido en la misma. En este caso, el dispositivo externo específico transmite una petición de conexión a la estación móvil 10.

El captador de nivel de seguridad 16 pregunta a la parte de ejecución de aplicaciones 12 sobre el nivel de seguridad ("alto" o "bajo") descrito en el ADF de la aplicación en acción para captarlo. El captador de nivel de seguridad 16 da instrucciones a la parte de conexión BLUETOOTH 17 para que realice una conexión Bluetooth utilizando un procedimiento basado en el nivel de seguridad captado.

De acuerdo con la instrucción del captador nivel de seguridad 16, la pieza de conexión BLUETOOTH 17 ejecuta la conexión Bluetooth con el dispositivo externo seleccionado por la parte de entrada 15. Por ejemplo, cuando se describe "UseBluetooth =" <high> como la clave UseBluetooth del ADF de la aplicación en acción (cf. Fig. 2), la parte de

conexión BLUETOOTH 17 realiza un proceso de conexión BLUETOOTH que incluye la autenticación y el cifrado.

A continuación, se describirá el funcionamiento de la estación móvil 10 junto con un método de control de comunicación de acuerdo con la presente invención. Las Fig. 3 a 6 son diagramas de flujo para explicar los procesos de conexión BLUETOOTH de acuerdo con los interlocutores seleccionados. Los procesos de conexión BLUETOOTH son implementados mediante el funcionamiento coordinado de los componentes de la estación móvil 10, pero las Fig. 3 a 6 se representan basándose en la clasificación de las entidades de procesos de aplicación directa en una aplicación común y una aplicación nativa por motivos de conveniencia de la descripción. La aplicación ordinaria es, por ejemplo, i-appli y se describe como "aplicación" en los dibujos. La aplicación nativa es, por ejemplo, una libreta de direcciones o un navegador, y se abrevia como "nativa" en los dibujos.

Como premisa para la descripción de la operación, se supone en la presente realización que los dispositivos externos 20, 30, y 40 se detectan como candidatos para un interlocutor Bluetooth. El dispositivo externo 20 es un teléfono móvil de Ichiro Suzuki y tiene un registro de conexión anterior en el nivel de seguridad alto. Es decir, la estación móvil 10 contiene una clave de enlace registrada. El dispositivo externo 30 es un PHS (Sistema de Teléfono de Mano Personal) de Jiro Tanaka, y tiene un registro de conexión anterior en el nivel de seguridad bajo. Por lo tanto, la estación móvil 10 contiene un nombre de dispositivo registrado pero no una clave de enlace registrada. No hay registro de conexión del dispositivo externo 40.

En S1 en la Fig. 3, la parte de ejecución de la aplicación 12 de la estación móvil 10 primero activa una aplicación para proporcionar un servicio deseado por el usuario. La

activación de la aplicación puede ser desencadenada por activación automática mediante la detección de un dispositivo externo o por una activación manual mediante un comando por parte del usuario de la estación móvil 10.

En S2, a menos que se produzca una excepción de algún tipo, la aplicación emite un comando para la conexión BLUETOOTH (conectar (código largo)) a la nativa. Los ejemplos de casos en que se produce una excepción incluyen un caso en el que la clave UseBluetooth mencionada no se describe en el ADF, un caso en el que el parámetro de la clave UseBluetooth descrito en el ADF es una cadena de caracteres a excepción de "alta" y "baja", un caso en el que la conexión BLUETOOTH es rechazada en la configuración de la aplicación, y así sucesivamente. En estos casos en los que se produce una excepción, resulta deseable que la estación móvil 10 esté configurada para llamar la atención del usuario con su contenido.

Al recibir el comando de conexión, la nativa envía una señal de búsqueda (pregunta) para la búsqueda de una pluralidad de dispositivos externos, incluyendo el dispositivo externo 20 (S3). Entre los dispositivos externos que reciben la señal de búsqueda, los dispositivos externos 20, 30 y 40 con capacidad de conexión BLUETOOTH envían una señal de respuesta de búsqueda (Respuesta de mensaje) con el fin de notificar a la estación móvil 10 sobre la detección (S4).

La nativa hace que la parte de pantalla 14 muestre UI (identificaciones de usuario) de los dispositivos externos detectados, como resultado de la búsqueda de dispositivos. Estos dispositivos externos son candidatos para ser un interlocutor. El usuario de la estación móvil 10 selecciona el dispositivo externo 20 como interlocutor deseado para la conexión Bluetooth, a través de la parte de entrada 15 (S5). En la presente realización, el dispositivo externo 20 se corresponde con el teléfono móvil del Sr. Ichiro

Suzuki. La Fig. 4(a) muestra un estado de la parte de visualización 14 donde se selecciona el "teléfono móvil de Ichiro Suzuki" como interlocutor.

Más específicamente, la nativa gestiona la información sobre interlocutores. La información acerca de un interlocutor de comunicación es, por ejemplo, BD\_ADDR, un  
5 nombre de dispositivo, una clave de enlace, y una clave de cifrado. BD\_ADDR es una dirección específica para cada conexión BLUETOOTH, que puede ser visualizada por el usuario, pero que no puede ser modificada por el usuario (aunque se puede eliminar). El nombre del dispositivo es una cadena de caracteres (por ejemplo, el teléfono móvil de Ichiro Suzuki) registrado personalmente por el usuario, que puede ser sometido a  
10 todos los procesos de pantalla, cambio y eliminación. La clave de enlace es una clave de autenticación de 128 bits, y se registra automáticamente entre la estación móvil 10 y el dispositivo externo 20 en una conexión en el nivel de seguridad alto. La clave de enlace no puede ser visualizada por el usuario, pero puede ser borrada por el usuario. La clave de cifrado es una clave de cifrado de 128 bits, y se registra automáticamente entre la  
15 estación móvil 10 y el dispositivo externo 20 en una conexión en el nivel de seguridad alto. La clave de cifrado no puede ser visualizada por el usuario, pero puede ser borrada por el usuario sólo en combinación con la clave de enlace.

Convencionalmente, el BD\_ADDR de un interlocutor, el nombre del dispositivo registrado en el lado del interlocutor, etc. se mostraban como la interfaz de usuario en la  
20 búsqueda de dispositivos externos por parte de Bluetooth. Por esta razón, surgió el problema de que resultaba difícil para el usuario de la estación móvil 10 en el lado de la búsqueda identificar los interlocutores, y existía una posibilidad de suplantación de identidad. En la presente realización, sin embargo, el nombre del dispositivo registrado en el lado de búsqueda se muestra para cada interlocutor en la comunicación ya

registrado en una base de datos de las nativas en el lado de la búsqueda, y un interlocutor no registrado en el lado de búsqueda se muestra por su BD\_ADDR en el lado de búsqueda. Por lo tanto, los problemas anteriormente mencionados quedan superados.

- 5 Además, se ha registrado una clave de enlace en el nivel de seguridad alto para cada interlocutor en la comunicación que ha sido conectado anteriormente en la base de datos de las nativas. En la Fig. 4 (a), la marca ★ indica un interlocutor con una clave de enlace, es decir, un interlocutor cuyo nombre de dispositivo está registrado y con el que se ha realizado una conexión en el nivel de seguridad alto. En contraste con ello, la
- 10 marca ☆ indica un interlocutor sin una clave de enlace, es decir, un interlocutor cuyo nombre de dispositivo está registrado pero con el que no se ha establecido conexión en el nivel de seguridad alto. Además, cada interfaz de usuario sin marca ("XXXXXX" en la misma cifra) indica un interlocutor no registrado. Al permitir la referencia a la presencia o ausencia de la clave de enlace en combinación con cada interfaz de usuario
- 15 de esta manera, el usuario de la estación móvil 10 puede comprobar fácilmente la fiabilidad del interlocutor deseado antes del establecimiento de la conexión. Dado que la estación móvil 10 muestra el resultado de la búsqueda de un interlocutor en la pantalla nativa, también se puede esperar que proporcione el efecto de impedir que la aplicación se tome la libertad de reescribir el BD\_ADDR y mostrar el BD\_ADDR reescrito.
- 20 El usuario de la estación móvil 10 realiza una operación de selección en un botón de conexión 141 para dar instrucciones de realización de una conexión con el dispositivo externo 20 seleccionado como interlocutor. Volviendo a la Fig. 3, en S6, tal como se activa a través de esta instrucción, la nativa transmite una señal de solicitud de conexión (Page) al dispositivo externo 20. Al recibir la señal de solicitud de conexión, el

dispositivo externo 20 envía una señal de respuesta de petición (PageResponse) a la estación móvil 10 (S7).

A continuación, la estación móvil 10 hace que el captador de nivel de seguridad 16 capte el nivel de seguridad desde el ADF de la aplicación activada en S1 (S8). La

5 estación móvil 10 se refiere a la clave UseBluetooth descrita en el ADF para determinar si el nivel de seguridad establecido en la solicitud es alto o bajo (S9). Cuando el resultado de la determinación es que "UseBluetooth =" <high> se describe como la clave de UseBluetooth (S9; SÍ), la estación móvil 10 determina que el nivel de seguridad de la aplicación en acción es alto, y pasa a S10.

10 En S10, los procesos de autenticación y cifrado se llevan a cabo entre el dispositivo externo 20 como interlocutor y la estación móvil 10. Los procesos de autenticación y encriptación son tecnologías de seguridad de la comunicación conocidas y por lo tanto se omiten en la descripción detallada. Sin embargo, el proceso de autenticación es para examinar la validez del interlocutor de comunicación y de ese modo evitar el acceso no

15 autorizado, y el proceso de encriptación es para cifrar los datos transmitidos y recibidos y de este modo asegurar la confidencialidad de la comunicación. En este caso, para el dispositivo externo 20, la clave de enlace del mismo está ya registrada tal como se describe anteriormente, y por lo tanto no hay necesidad de introducir el PIN en la autenticación.

20 También se puede contemplar que, antes de la ejecución de los procesos en S10, el usuario de la estación móvil 10 establezca preliminarmente la propiedad de la conexión automática con cada dispositivo externo bajo el establecimiento del nivel de seguridad alto. Ello permite a la estación móvil 10 referirse al contenido establecido y realizar automáticamente una conexión con un dispositivo externo autorizado para realizar una

conexión automática. Dado que la conexión automática no requiere que el usuario introduzca un PIN o similar, se ejecuta deseablemente sólo con un interlocutor fiable. En este sentido, los dispositivos externos como objetivos de la conexión automática se limitan a los dispositivos designados por el usuario, y la comunicación con los  
5 dispositivos se ejecuta en el nivel de seguridad alto. Por este motivo, se implementa la conexión automática con alta comodidad para el usuario asegurando al mismo tiempo una alta seguridad.

Cuando el resultado de la determinación en S9 es que se describe "UseBluetooth =" <low> como la clave UseBluetooth (S9; NO), el flujo pasa a un proceso en S11 sin  
10 pasar los procesos de autenticación y cifrado en S10.

En S11, se establece un enlace por BLUETOOTH entre la estación móvil 10 y el dispositivo externo 20. Después del establecimiento del enlace, se envía una señal PAN\_EVENT\_CONNECTED para notificar a la aplicación sobre este hecho. En este momento, la estación móvil 10 puede estar configurada para presentar el nivel de  
15 seguridad que se aplica actualmente, durante la conexión BLUETOOTH. La presentación puede ser implementada, por ejemplo, mediante la adopción de una técnica de mostrar una cadena de caracteres que indica el nivel de seguridad, o una técnica de cambiar el color de un icono que indica el progreso de la comunicación, de acuerdo con el nivel de seguridad. Ello permite al usuario captar fácil y rápidamente en qué nivel de  
20 seguridad está funcionando la comunicación con el interlocutor.

Posteriormente, se describirá el proceso de conexión BLUETOOTH ejecutado entre la estación móvil 10 y el dispositivo externo 30 con referencia a la Fig. 5. Este proceso de conexión BLUETOOTH incluye una pluralidad de fases comunes para el proceso de conexión BLUETOOTH que se detallan con referencia a la Fig. 3. En concreto, los

procesos en S21-S29, S31, S32 y en la Fig. 5 son equivalentes a los de S1-S9, S10, y S11, respectivamente, que se muestran en la Fig. 3. Sin embargo, estos procesos son algo diferentes en detalle y, en particular, el interlocutor seleccionado en S25 es el PHS de Jiro Tanaka. La Fig. 4(b) muestra un estado de la parte de visualización 14 donde se  
5 selecciona el "PHS de Jiro Tanaka" como interlocutor.

Un proceso en S30 en la Fig. 5 son los procesos de entrada y la recopilación de un código PIN, que se ejecuta después de la determinación de si el nivel de seguridad es alto o bajo. Estos procesos se ejecutan cuando se determina que el nivel de seguridad es alto (S29; SI), es decir, cuando "UseBluetooth =" <high> se describe como la clave  
10 UseBluetooth del ADF. Dado que no se ha registrado ninguna clave de enlace para el dispositivo externo 30, la entrada de un PIN se lleva a cabo en la estación móvil 10 y se genera una clave de enlace basada en el PIN de entrada. La clave de enlace generada se registra en la estación móvil 10 en el momento del establecimiento de un enlace (S32). De esta manera, la estación móvil 10 registra la clave de enlace primero después de una  
15 autenticación (emparejamiento) satisfactoria, asegurando de este modo la credibilidad del emparejamiento de comunicación que tiene la clave de enlace.

A continuación, se describirá el proceso de conexión BLUETOOTH ejecutado entre la estación móvil 10 y el dispositivo externo 40 con referencia a la Fig. 6. El proceso de conexión BLUETOOTH incluye una pluralidad de fases comunes con el proceso de  
20 conexión BLUETOOTH detallado con referencia a la Fig. 3. En concreto, los procesos en S41-S49, S51, S52 y en la Fig. 6 son equivalentes a los de S1-S9, S10, y S11, respectivamente, que se muestran en la Fig. 3. Sin embargo, estos procesos se diferencian en que el interlocutor seleccionado en S45 es el dispositivo externo 40 no registrado. Cuando se selecciona una conexión con un dispositivo no registrado como

en este modo, resulta deseable visualizar una pantalla de diálogo 142 para preguntar la necesidad de registro del usuario, en combinación con una lista de dispositivos detectados (cf. Fig. 4 (c)), en consideración de los casos de reconexión. La estación móvil 10 también puede estar configurada para notificar simultáneamente al usuario que  
5 el objetivo al que se intenta conectar no se ha registrado, mediante un mensaje de texto para llamar su atención.

Los otros procesos en S50 y S52 son los mismos procesos que en S30 y S32, respectivamente, que se muestran en la Fig. 5. Los anteriores describen los procedimientos de conexión de la estación móvil 10 con los dispositivos externos 20, 30  
10 y 40, pero los procesos de conexión BLUETOOTH antes mencionados también se pueden ejecutar de manera similar entre la estación móvil 10 y todos los dispositivos externos detectados, sin limitarse a estos dispositivos externos descritos anteriormente.

Tal como se ha descrito anteriormente, la estación móvil 10 de la presente realización realiza la conexión Bluetooth con el dispositivo externo seleccionado como interlocutor  
15 por parte del usuario de la estación móvil 10, a partir de la pluralidad de dispositivos externos 20, 30, y 40 detectados en conjunción con la activación de la aplicación. Los dispositivos externos generalmente se clasifican en tres tipos, registrados (con una clave de enlace), registrados (sin una clave de enlace), y no registrados, dependiendo de las diferencias de los registros de conexión. La estación móvil 10 cambia el procedimiento  
20 para la conexión con el dispositivo externo por BLUETOOTH, de acuerdo con el nivel de seguridad establecido en la aplicación activada. Específicamente, cuando se establece el nivel de seguridad bajo en la solicitud, la estación móvil 10 omite los procesos de autenticación de dispositivos y cifrado, independientemente de las diferencias de los registros de conexión. Ello simplifica el procedimiento de conexión y reduce el tiempo

de conexión. Cuando se establece el nivel de seguridad alto en la solicitud, la estación móvil 10 ejecuta los procesos de autenticación y cifrado de dispositivos, independientemente de las diferencias de los registros de conexión. Ello evita las conexiones con terceros no autorizados y asegura la seguridad predeterminada de las comunicaciones.

Finalmente, en el desarrollo de una aplicación, el nivel de seguridad se puede ajustar de forma variable de acuerdo con un tipo de servicio implementado por la aplicación. Es decir, un desarrollador puede desarrollar una aplicación con un nivel de seguridad adecuado para un servicio individual.

10 La presente invención no se limita a la realización descrita anteriormente, y se puede modificar adecuadamente en diversas formas de modificación, sin apartarse del ámbito de la invención.

Por ejemplo, en la realización anterior el terminal para cambiar el método de visualización del resultado de la búsqueda de acuerdo con el nivel de seguridad era la estación móvil 10, es decir, el terminal que realizó la búsqueda mediante la transmisión de la señal de búsqueda. Sin embargo, la tecnología de la presente invención también es aplicable a los casos en que la estación móvil 10 es un terminal que se busca mediante la recepción de una señal de búsqueda transmitida (comando aceptar). En este modo, la estación móvil 10 cambia un método de visualización de una entidad de solicitud de la conexión (entidad de búsqueda) de acuerdo con el nivel de seguridad.

Específicamente, el usuario de la estación móvil 10 registra la propiedad de la conexión de cada dispositivo externo en el caso en que está establecido el nivel de seguridad alto en una aplicación, como un proceso preliminar. En otras palabras, aquí la propiedad de conexión es si se va a permitir o rechazar la aceptación de una solicitud de conexión.

Cuando una aplicación con el nivel de seguridad alto está activada al ser buscada, la estación móvil 10 hace caso omiso de una petición de conexión desde un dispositivo externo cuya conexión no está permitida por parte del usuario, de acuerdo con el contenido registrado. En contraste con ello, cuando se recibe una solicitud de conexión

5 desde un dispositivo externo al que está permitido conectar por parte del usuario (por ejemplo, un dispositivo externo que tiene un registro de conexión en el nivel de seguridad alto), la estación móvil 10 muestra la interfaz de usuario del dispositivo externo de la parte de visualización 14. Por otra parte, cuando una aplicación con el nivel de seguridad bajo está activada al ser buscada, la estación móvil 10 acepta una

10 solicitud de conexión de todos los dispositivos externos, independientemente de sus registros de conexión, y muestra las interfaces de usuario de estos dispositivos en serie de tiempo.

Esto permite al usuario de la estación móvil 10 comprobar fácilmente la fiabilidad del interlocutor de comunicación antes de la conexión, de acuerdo con el contenido del

15 servicio proporcionado por la aplicación. Particularmente, cuando el nivel de seguridad alto está establecido en la aplicación, el proceso anteriormente mencionado reduce de manera preliminar los interlocutores para los que se acepta la solicitud de conexión (búsqueda). Por este motivo, el número de respuestas enviadas manualmente en respuesta a la solicitud se reduce para el usuario en el lado buscado (estación móvil 10).

20 Ello se traduce en una reducción del tiempo y el esfuerzo necesarios para el establecimiento de un enlace entre la estación móvil 10 y un dispositivo externo. La realización indicada más arriba adoptó el proceso de autenticación y el proceso de encriptación basados en la introducción de PIN como medios para garantizar la seguridad en el nivel alto. Sin embargo, también es posible adoptar una configuración

25 en la que la estación móvil 10 establece de forma variable la propiedad de conexión

automática y desactiva la conexión automática sólo si se encuentra el nivel de seguridad alto activado en la aplicación. Ello elimina la preocupación de que los datos se transmitan y se reciban contra de la intención del usuario entre la estación móvil 10 y un dispositivo externo que no pasa a través del proceso de autenticación.

- 5 La estación móvil 10 es, por ejemplo, un teléfono móvil, pero puede ser cualquier equipo de información proporcionado con una función de comunicación, como por ejemplo una PDA (Asistente Digital Personal) o una PHS, y la función y el tamaño de los mismos no limitan los objetos a los que se aplica la presente invención.

Por otra parte, la realización anterior se ha configurado en el supuesto de la  
10 comunicación BLUETOOTH como la comunicación inalámbrica de corto alcance entre la estación móvil 10 y los dispositivos externos 20, 30, 40. Sin embargo, es una cuestión de rutina que la presente invención también es aplicable a la comunicación por infrarrojos incluyendo IrDA (Asociación de Datos por Infrarrojos) y para la comunicación LAN (Red de Área Local) inalámbrica.

- 15 A partir de la invención así descrita, resultará obvio que las realizaciones de la invención pueden variarse de muchas maneras. Tales variaciones no deberán ser consideradas como una desviación del alcance de la invención, y todas estas modificaciones, como resultará obvio para un experto en la técnica, tienen la finalidad de estar incluidas dentro del alcance de las siguientes reivindicaciones.

20

## Reivindicaciones

**1.** Una estación móvil (10) que comprende:

- medio de activación (12) para activar una aplicación para comunicarse con un dispositivo externo (20, 30, 40);

5 - medio de captación (16) para captar un nivel de seguridad establecido en la aplicación activada por el medio de activación (12); y

- medio de conexión (17) para realizar una conexión con el dispositivo externo (20, 30, 40) mediante un procedimiento de acuerdo con el nivel de seguridad captado por el medio de captación.

10 - medio de selección (15) para seleccionar un dispositivo externo que pueda someterse a una conexión cuando una aplicación con un nivel de seguridad alto establecido en la misma esté en uso,

- en que cuando el nivel de seguridad captado por el medio de captación (16) es el nivel de seguridad alto, el medio de conexión (17) realiza la conexión con el

15 dispositivo externo seleccionado por el medio de selección después de realizar una autenticación y codificación con el dispositivo externo.

**2.** La estación móvil (10) de acuerdo con la reivindicación 1, en que cuando el nivel de seguridad captado por el medio de captación (16) es el nivel de seguridad alto, el medio de conexión (17) realiza la conexión automática con el dispositivo externo en el caso de  
20 recibir una solicitud de conexión a partir del dispositivo externo seleccionado por el medio de selección (15).

3. La estación móvil (10) de acuerdo con la reivindicación 1, en que cuando el nivel de seguridad captado por el medio de captación (16) es un nivel de seguridad bajo, el medio de conexión (17) no realiza la autenticación ni la codificación.

4. Un método de control de comunicación que comprende las siguientes fases llevadas a

5 cabo por una estación móvil (10):

- una fase de activación (S1, S21, S41) que activa una aplicación para comunicarse con un dispositivo externo (20, 30, 40);

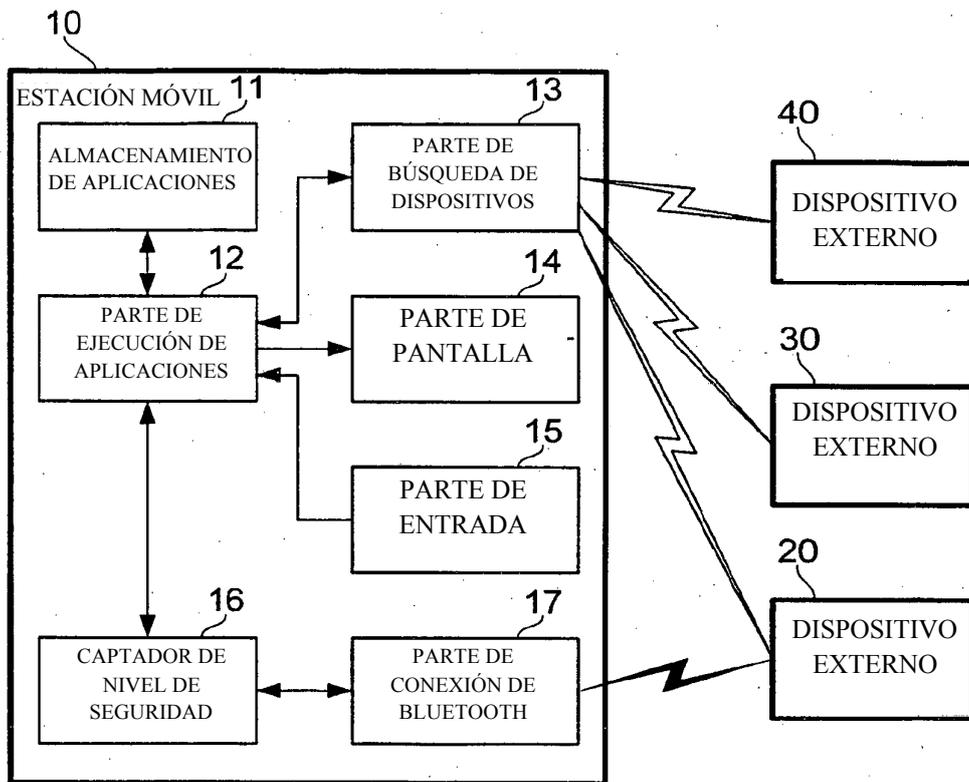
- una fase de captación (S8, S28, S48) que capta un nivel de seguridad establecido en la aplicación activada en la fase de activación (S1, S21, S41); y

10 - una fase de conexión (S10, S11, S31, S32, S51, S52) que realiza una conexión con el dispositivo externo (20, 30, 40) mediante un procedimiento de acuerdo con el nivel de seguridad captado en la fase de captación (S8, S28, S48); y

- una fase de selección que selecciona un dispositivo externo que puede someterse a una conexión cuando una aplicación con un nivel de seguridad alto establecido se encuentra en uso,

15 - en que cuando el nivel de seguridad captado en la fase de captación (S8, S28, S48) es el nivel de seguridad alto, la conexión con el dispositivo externo seleccionado en la fase de selección (S8, S28, S48) se realiza en la fase de conexión (S10, S11, S31, S32, S51, S52), después de llevar a cabo una autenticación y codificación con el  
20 dispositivo externo.

**Fig.1**



**Fig.2**

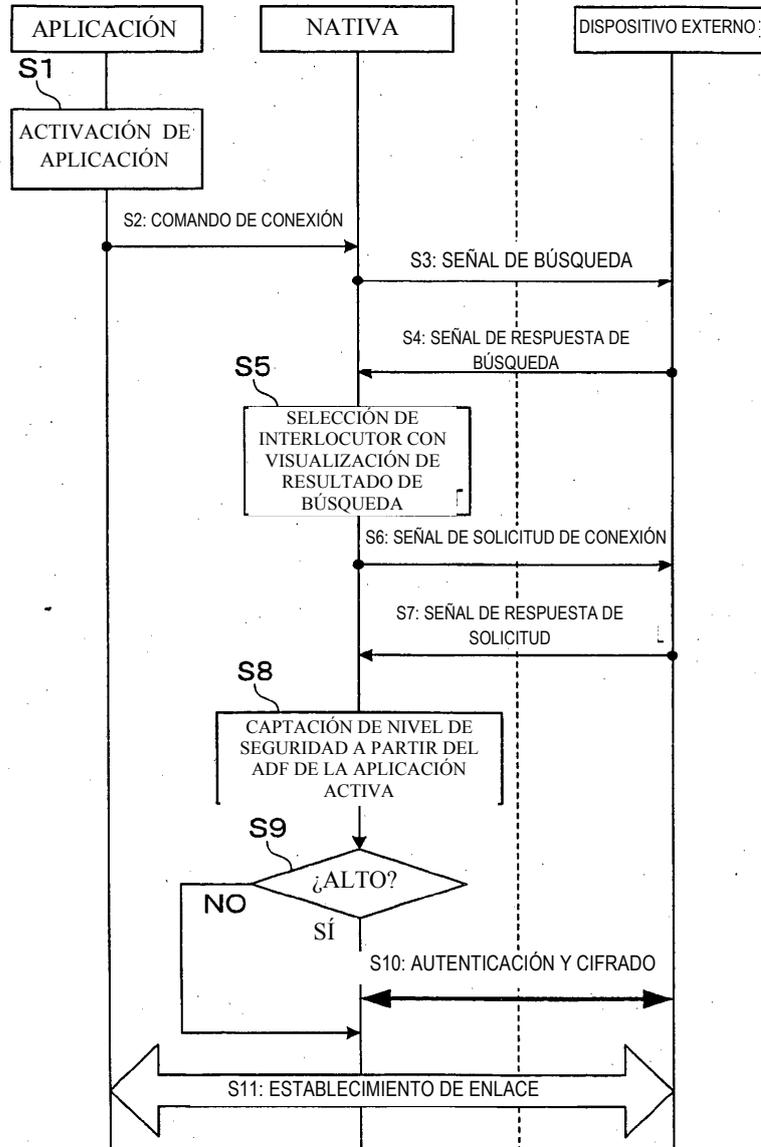
11

11a No	11b APLICACIÓN	11c CLAVE DE ADF de UseBluetooth
1	APLICACIÓN A	"UseBluetooth="<high>
2	APLICACIÓN B	"UseBluetooth="<low>
3	APLICACIÓN C	"UseBluetooth="<high>
4	APLICACIÓN D	"UseBluetooth="<xxx>
⋮	⋮	⋮

**Fig.3**

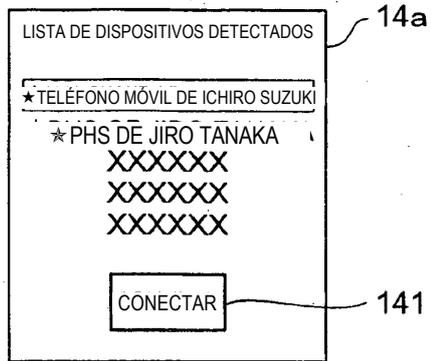
PROCESAMIENTO EN EL LADO DE LA ESTACIÓN MÓVIL 10

PROCESAMIENTO EN EL LADO DEL  
DISPOSITIVO EXTERNO 20

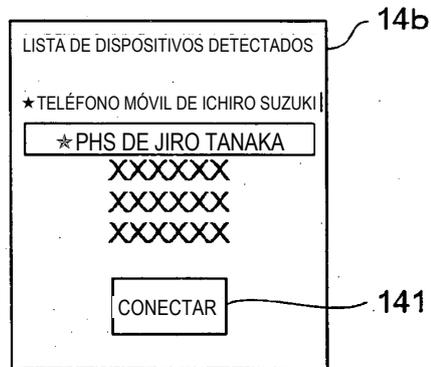


**Fig.4**

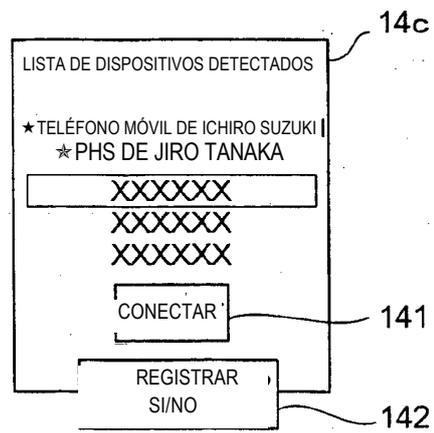
(a)



(b)

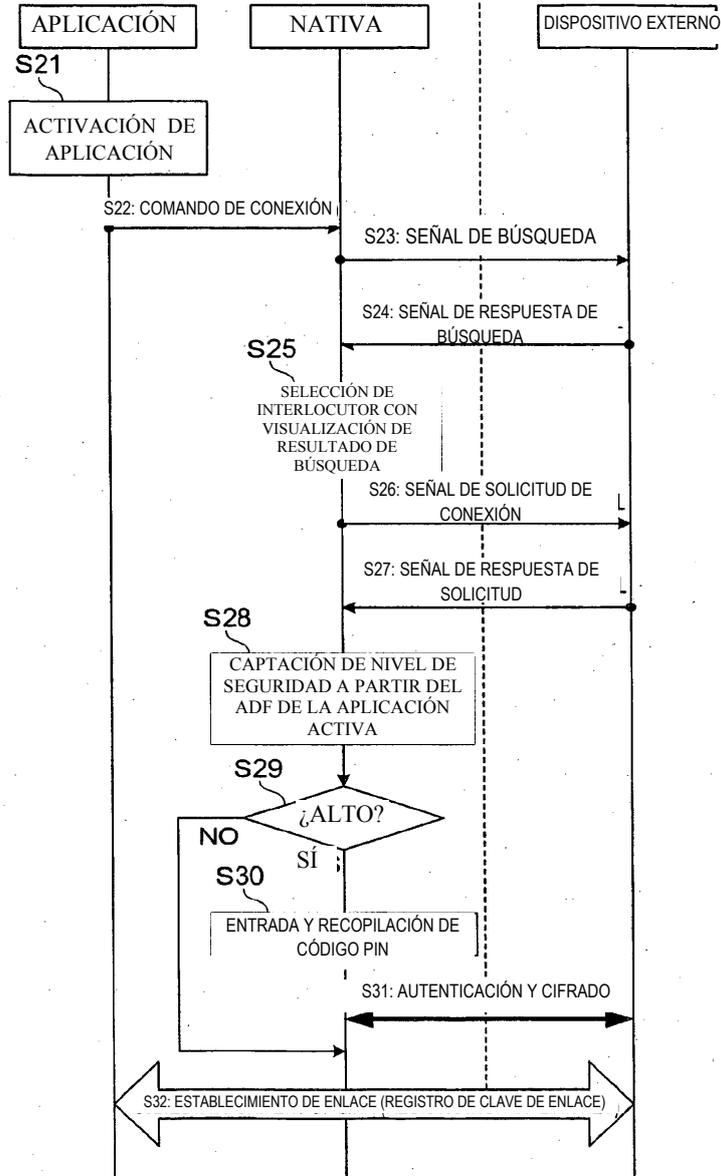


(c)



**Fig.5**  
 PROCESAMIENTO EN EL LADO DE LA ESTACIÓN MÓVIL 10

PROCESAMIENTO EN EL LADO DEL DISPOSITIVO EXTERNO 20



**Fig.6**

