(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 625 789**

(51) Int. CI.:

G06F 15/177 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **30.12.2004 PCT/FI2004/000810**

(87) Fecha y número de publicación internacional: **06.07.2006 WO06070045**

(96) Fecha de presentación y número de la solicitud europea: **30.12.2004 E 04805205 (4)**

(97) Fecha y número de publicación de la concesión europea: **12.04.2017 EP 1839182**

(54) Título: **Uso de configuraciones en un dispositivo con múltiples configuraciones**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
20.07.2017

(73) Titular/es:

NOKIA TECHNOLOGIES OY (100.0%)
KEILALAHDENTIE 4
02150 ESPOO, FI

(72) Inventor/es:

PULKKINEN, MARKKU y
LINDROOS, MARTTI

(74) Agente/Representante:

VALLEJO LÓPEZ, Juan Pedro

DESCRIPCIÓN

Uso de configuraciones en un dispositivo con múltiples configuraciones

Campo de la invención

La invención se refiere a disponer el uso de configuraciones en dispositivos con múltiples configuraciones, más en concreto a disponer un control de acceso en conjuntos de datos de configuración gestionables por uno o más dispositivos de gestión externos.

Antecedentes de la invención

A medida que diferentes dispositivos de procesamiento de datos, tales como estaciones móviles, se vuelven más complejos, la importancia de la gestión de dispositivos se vuelve más pronunciada. Los dispositivos requieren varios ajustes diferentes, tales como ajustes en relación con puntos de acceso a Internet, y el ajuste manual de los mismos es laborioso y difícil para un usuario. Para solucionar este problema, se han desarrollado soluciones de gestión de dispositivos de tal modo que el administrador del sistema de información de una empresa o un teleoperador puede ajustar una configuración apropiada en el dispositivo. La gestión de dispositivos se refiere, en general, a acciones mediante las cuales una persona que no está usando el dispositivo puede cambiar la configuración del dispositivo; por ejemplo, cambiar los ajustes o incluso un protocolo que es usado por el dispositivo. Además de los ajustes específicos del dispositivo, también es posible transmitir datos específicos del usuario, tales como perfiles de usuario, logotipos, tonos de llamada y menús con los que el usuario puede modificar personalmente los ajustes del dispositivo, o la modificación tiene lugar de forma automática en conexión con la gestión de dispositivos.

Una de las normas de gestión de dispositivos es DM (*Device Management*, Gestión de dispositivos) de OMA (Open Mobile Alliance), que está basada, en parte, en el protocolo de SyncML (*Synchronization Markup Language*, lenguaje de marcado de sincronización). Por ejemplo, un ordenador personal (PC, *personal computer*) puede actuar como un servidor de gestión de dispositivos en un protocolo de gestión de dispositivos, y una estación móvil como un cliente de gestión de dispositivos. Los elementos que se gestionan en el cliente de gestión de dispositivos están dispuestos como objetos de gestión. Los objetos de gestión son entidades que pueden ser gestionadas por instrucciones de gestión de servidor en el cliente de gestión de dispositivos. Por ejemplo, el objeto de gestión puede ser un número o una entidad grande, tal como una imagen de segundo plano o un salvapantallas. En la gestión de dispositivos de OMA, los objetos de gestión están dispuestos en un árbol de gestión.

Algunos elementos gestionables típicos comprenden ajustes de conexión específicos del operador, por ejemplo, ajustes de conexión de GPRS (*General Packet Radio Service*, servicio radioeléctrico general por paquetes). Mediante procedimientos de DM de OMA, estos conjuntos de ajustes específicos del operador, a los que también se puede hacer referencia como configuraciones, en un dispositivo de terminal de usuario pueden ser mantenidos por un servidor de gestión controlado por operador. Por ejemplo, se pueden proveer ajustes de WAP (*Wireless Application Protocol*, protocolo de aplicaciones inalámbricas) para usar servicios de WAP de un proveedor de servicios como un contexto de configuración para el dispositivo de terminal.

Algunos elementos gestionados pueden comprender una información controlada por y específica del usuario, tal como salvapantallas y tonos de llamada. Además, el dispositivo se puede usar para acceder a un sistema de información corporativo, por ejemplo, un sistema de archivos, páginas de intranet y un sistema de correo electrónico en las mismas. Para este fin, es necesario que el dispositivo comprenda una o más configuraciones para disponer el acceso a estos servicios de sistema de información corporativos. Por razones de seguridad, es deseable que el personal de TI corporativo sea capaz de controlar estos ajustes. Por lo tanto, un dispositivo puede comprender múltiples configuraciones procedentes de diferentes partes de gestión y debería ser posible habilitar el acceso a una configuración específica solo para una parte de gestión autorizada. De acuerdo con el protocolo de DM de OMA, que se especifica en la especificación de OMA "*SyncML Device Management Protocol*", versión 1.1.2, 12 de diciembre de 2003, 41 páginas, en la fase de configuración de una sesión de gestión, un servidor de gestión se autentica sobre la base de las credenciales que se reciben del servidor de gestión. Además, tal como se ilustra en la especificación de OMA "*SyncML Management Tree and Description*", versión 1.1.2, 2 de diciembre de 2003, 44 páginas, un nodo de un árbol de gestión se puede especificar mediante una lista de control de acceso (ACL, *access control list*) que comprende una lista de identificadores y derechos de acceso que están asociados a cada identificador. Tal como se describe en el Capítulo 7.7.1, los derechos de acceso que se conceden mediante ACL definen identificadores de servidor de gestión que están autorizados para obtener, añadir, sustituir y/o eliminar un nodo. Por lo tanto, se pueden dar diferentes derechos de acceso a diversos servidores de gestión de dispositivos, y las instrucciones de gestión de dispositivos procedentes de servidores de gestión no autorizados no se realizan sobre el árbol de gestión. No obstante, aparte de una capacidad de controlar el acceso de los servidores de gestión a los nodos de un árbol de gestión, existe adicionalmente una necesidad general de limitar el uso de las configuraciones en el dispositivo. Por ejemplo, las empresas desean controlar los terminales que se usan para acceder a los servicios de TI de la empresa de un mejor modo con el fin de proteger datos y servicios corporativos.

El documento US2004/0123147 divulga un sistema y un método para controlar la seguridad o accesibilidad de un dispositivo de comunicación inalámbrico. El dispositivo de comunicación inalámbrico está configurado con ajustes de preferencias de seguridad que especifican quién puede acceder a un dispositivo de comunicación inalámbrico y el grado de accesibilidad del dispositivo inalámbrico. Las preferencias se pueden modificar en tiempo real y de forma remota desde el dispositivo de comunicación inalámbrico. Dependiendo de los ajustes de preferencias de seguridad, la interfaz o interfaces de usuario del dispositivo de comunicación inalámbrico se pueden cambiar de forma apropiada para proporcionar el nivel establecido de seguridad o accesibilidad del dispositivo.

Breve descripción de la invención

A continuación se proporcionan un método, un sistema de gestión de dispositivos, unos dispositivos de procesamiento de datos y un producto de programa informático que están caracterizados por lo que se expone en las reivindicaciones independientes. Algunas realizaciones de la invención se describen en las reivindicaciones dependientes.

De acuerdo con un aspecto de la invención, se proporciona un método para un sistema de gestión de dispositivos de acuerdo con la reivindicación 1.

De acuerdo con un aspecto de la invención, se proporciona un dispositivo de procesamiento de datos para un sistema de gestión de dispositivos de acuerdo con la reivindicación 8.

De acuerdo con un aspecto de la invención, se proporciona un producto de programa informático de acuerdo con la reivindicación 18.

De acuerdo con un aspecto de la invención, un dispositivo con múltiples conjuntos de datos de configuración comprende una información de control de acceso que es originada y/o controlada por una entidad de gestión externa para definir un derecho de una aplicación a acceder a un conjunto de datos de configuración. La información de control de acceso se comprueba en respuesta a una indicación procedente de una aplicación que requiere acceso a un conjunto de datos de configuración. Si, sobre la base de la información de control de acceso, la aplicación tiene autorización a acceder al conjunto de datos de configuración, se dispone para la aplicación el acceso al conjunto de datos de configuración.

La expresión “conjunto de datos de configuración” se refiere, en general, a un conjunto de datos que comprenden una información de configuración que tiene un efecto directo o indirecto sobre una o más funciones del dispositivo o una aplicación en el dispositivo. Por ejemplo, el conjunto de datos de configuración puede comprender una dirección de IP o un nombre de dominio de un servidor sobre la base del cual se dispone una conexión desde el dispositivo.

La invención hace posible controlar el acceso de las aplicaciones a los datos de configuración. Más en particular, los derechos de acceso se pueden especificar y/o controlar mediante una entidad externa. Un dispositivo puede comprender múltiples conjuntos de datos de configuración con diferentes propiedades de control de acceso. Por ejemplo, un conjunto de datos de configuración que especifica ajustes de acceso para un sistema de información corporativo se puede controlar mediante un soporte lógico de gestión de configuración que es operado por personal de TI corporativo.

Breve descripción de las figuras

La invención se describe a continuación con mayor detalle por medio de algunas realizaciones y con referencia a los dibujos adjuntos, en los que

la figura 1 ilustra un sistema de gestión,
la figura 2 ilustra un dispositivo con múltiples configuraciones,
la figura 3 ilustra un método de acuerdo con una realización de la invención; y
las figuras 4a y 4b ilustran un método de acuerdo con una realización de la invención.

Descripción detallada de algunas realizaciones de la invención

Una realización de la invención se describirá en lo sucesivo en un sistema que soporta la gestión de dispositivos de OMA; no obstante, se debería hacer notar que la invención se puede aplicar a cualquier sistema de gestión de dispositivos en el que las configuraciones en un dispositivo gestionado puedan ser gestionadas por una entidad de gestión externa.

La figura 1 ilustra un sistema en red. Por lo general, un servidor de red o un PC sirve como un servidor S. Por ejemplo, una estación móvil, un PC, un ordenador portátil, un dispositivo de PDA (*Personal Digital Assistant*, asistente personal digital), o un módulo para el mismo puede servir como un terminal TE. En las siguientes realizaciones, se supone que, para la gestión de dispositivos, el terminal TE sirve como un cliente de gestión de dispositivos y el servidor S como un servidor de gestión de dispositivos. El servidor S puede gestionar varios clientes

TE.

En el primer ejemplo de la figura 1, los clientes TE y los servidores de gestión S están conectados con una red de área local LAN. Un cliente TE que está conectado con la red LAN comprende una funcionalidad, tal como una tarjeta de red y soporte lógico que controla la transmisión de datos, para comunicarse con los dispositivos en la red LAN. La red de área local LAN puede ser cualquier tipo de red de área local y el TE también se puede conectar con el servidor S a través de Internet usando, por lo general, un cortafuegos FW. El terminal TE también se puede conectar con la red de área local LAN de forma inalámbrica a través de un punto de acceso AP.

En el segundo ejemplo, el cliente TE se comunica con el servidor S a través de una red móvil MNW. Un terminal TE que está conectado con la red MNW comprende una funcionalidad de estación móvil para comunicarse de forma inalámbrica con la red MNW. También pueden existir otras redes, tales como una red de área local LAN, entre la red móvil MNW y el servidor S. La red móvil MNW puede ser cualquier red inalámbrica, por ejemplo, una red que soporta servicios de GSM, una red que soporta servicios de GPRS (*General Packet Radio Service*, servicio radioeléctrico general por paquetes), una red móvil de tercera generación, tal como una red de acuerdo con las especificaciones de red de 3GPP (*3rd Generation Partnership Project*, Proyecto de Asociación de 3ª Generación), una red de área local inalámbrica WLAN, una red privada, o una combinación de varias redes. Además de los ejemplos en lo que antecede, también son posibles muchas otras configuraciones de gestión de dispositivos, tales como una conexión de gestión entre los terminales TE o una conexión de gestión directa entre el terminal TE y el servidor S mediante el uso de una conexión inalámbrica o una cableada sin otros elementos de red.

El terminal TE y el servidor S comprenden una memoria, una interfaz de usuario, unos medios de E/S para la transmisión de datos, y una unidad central de procesamiento que comprende uno o más procesadores. La memoria has una porción no volátil para almacenar aplicaciones que controlan la unidad central de procesamiento y para otra información a almacenar, y una porción volátil a usar en un procesamiento de datos temporal.

Las porciones de código de programa informático que se ejecutan en la unidad central de procesamiento pueden dar lugar a que el servidor S implemente los medios de la invención para establecer y gestionar contextos de servicio en el terminal TE, algunas realizaciones de lo cual se ilustran en conexión con la figura 4a. Las porciones de código de programa informático que se ejecutan en la unidad central de procesamiento del terminal TE pueden dar lugar a que el terminal TE también implemente los medios de la invención para disponer las configuraciones en el terminal y para disponer el uso de configuraciones en el terminal TE, algunas realizaciones de lo cual se ilustran en conexión con las figuras 2, 3, 4a y 4b. Se ha de hacer notar que una o más entidades pueden llevar a cabo las funciones de la invención. Por ejemplo, algunas de las características que se ilustran en la figura 3 son llevadas a cabo por un controlador de acceso específico en el terminal TE, mientras que algunas otras características son llevadas a cabo por una aplicación en el terminal TE. El programa informático se puede almacenar en cualquier medio de almacenamiento, desde el cual se puede cargar el mismo en la memoria del dispositivo TE; ejecutando S el programa informático. El programa informático también se puede cargar a través de la red mediante el uso de una pila de protocolo TCP/IP, por ejemplo. También es posible usar soluciones de soporte físico o una combinación de soluciones de soporte físico y de soporte lógico para implementar los medios de la invención. Una unidad de chip o algún otro tipo de módulo para controlar el dispositivo TE y/o S puede, en una realización, dar lugar a que el dispositivo TE y/o S realice las funciones de la invención. Una estructura de datos que comprende una información específica del contexto de servicio se puede transferir a través de una red de transmisión de datos, por ejemplo, del servidor S al terminal TE y almacenarse en la memoria del terminal TE.

En una realización, el terminal TE y el servidor S están dispuestos para soportar la gestión de dispositivos (DM, *device management*) de OMA. El terminal TE que sirve como un cliente de gestión de dispositivos de OMA comprende una funcionalidad de agente de cliente que se ocupa de funciones en relación con la sesión de gestión en el cliente. El servidor S que sirve como un servidor de gestión de dispositivos comprende un agente de servidor o una funcionalidad maestra de servidor que gestiona la sesión de gestión. No obstante, se ha de hacer notar que la aplicación de estas funcionalidades no se limita a dispositivo específico alguno, e incluso es posible que las funcionalidades de cliente y de servidor se implementen en un único dispositivo físico. Uno o más árboles de gestión que están almacenados en la memoria de TE representan los objetos gestionables en el terminal TE. El árbol de gestión está constituido por nodos y este define al menos un objeto de gestión que está formado por uno o más nodos o al menos un parámetro de un nodo. El nodo puede ser un parámetro individual, un árbol secundario o un conjunto de datos. El nodo puede comprender al menos un parámetro que puede ser un valor de configuración o un archivo, tal como un archivo de imagen de segundo plano en el nodo. Los contenidos del nodo también pueden ser un enlace a otro nodo. Cada nodo puede ser abordado por un identificador de recursos uniforme (URI, *uniform resource identifier*). Un servidor de gestión de dispositivos autorizado puede añadir (de forma dinámica) y cambiar los contenidos de los nodos en el árbol de gestión.

La figura 2 ilustra el entorno 200 de un terminal TE con múltiples configuraciones. El entorno 200 se dota de uno o más contextos de servicio 203. Un contexto de servicio 203 se puede considerar como un área en el terminal TE al cual se controla el acceso. Por lo tanto, la información que está almacenada en un área de almacenamiento específico del contexto de servicio en el terminal TE puede especificar o formar el contexto de servicio 203. En una realización, los contextos de servicio 203 representan diferentes configuraciones en el terminal TE que se usa para

acceder a servicios, por ejemplo, un servicio de acceso a Internet. Tal como se ilustra mediante flechas a partir del contexto de servicio 203, un contexto de servicio 203 que representa una configuración puede comprender unos certificados 206, unos ajustes 205 y/o algún otro tipo de datos 208 específicos del contexto de servicio. Tal como se ilustra en la figura 2, la información que pertenece a un contexto de servicio 203 se puede almacenar en múltiples ubicaciones de almacenamiento, o en una única posición de almacenamiento. Por ejemplo, un contexto de servicio 203 puede comprender o estar asociado a unos datos de usuario 208 sensibles que están almacenados en un sistema de archivos 207, los ajustes 205 y los certificados 206 que están almacenados en un depósito central 204, que puede ser un almacenamiento específico para la información de contexto de servicio. Los datos 208 que pertenecen a un contexto de servicio 203 pueden ser cualesquiera datos que se reciban en el terminal TE o que sean originados por una aplicación 202. Por ejemplo, un usuario puede introducir una entrada de calendario que se almacena como los datos 208 que pertenecen al contexto de servicio 203.

Un entorno de ejecución segura 201 puede controlar el acceso a la información del contexto de servicio 203, y se pueden asegurar posiciones de almacenamiento que comprenden contenidos de contextos de servicio. A pesar de que no se muestra en la figura 2, el entorno de ejecución 201 puede comprender un controlador de acceso que está dispuesto para controlar el acceso a la información de contexto de servicio. Una entidad de gestión externa, en una realización de un gestor de contextos de servicio 211, puede conceder derechos para que las aplicaciones 202 accedan a una información que pertenece a un contexto de servicio 203. La información de control de acceso (ACI, *access control information*) 212 que es originada y/o controlada por la entidad de gestión externa (211) se puede almacenar en el terminal TE para definir derechos de acceso a los contextos de servicio 203. Además, el entorno de ejecución 201 puede ayudar a asegurar la transferencia de datos entre la aplicación 202 autorizada a acceder al contexto de servicio 203 y una o más posiciones de almacenamiento que comprenden la información de contexto de servicio. En una realización, al menos algunos servicios de seguridad se disponen mediante un sistema operativo del terminal TE.

Las aplicaciones 202 se pueden ejecutar en el interior del entorno de ejecución segura 201 del entorno 200 del terminal. El acceso a uno o más contextos de servicio 203 se dispone para una aplicación 202 con el fin de iniciar un servicio para un usuario del terminal TE, si la información de control de acceso 212 posibilita esto. Esta información de control de acceso 212 se puede definir de muchas formas en el terminal TE. Por ejemplo, un archivo que identifica entidades que tienen autorización a acceder a un contexto de servicio 203 se puede almacenar en el terminal TE, y el terminal TE está dispuesto para proporcionar acceso al contexto de servicio 203 solo para entidades que se identifican directa o indirectamente en el archivo. La información de control de acceso 212 se podría definir en el terminal TE como parámetros para un componente de soporte lógico que implementa funciones de control de acceso de contextos de servicio, por ejemplo. Por lo tanto, el terminal TE se dota de reglas de control de acceso para definir la autorización a acceder a un contexto de servicio 203. El archivo de información de control de acceso puede ser una lista de identificadores de aplicación o una lista de identificadores de fuente de aplicaciones. No obstante, en lugar de o además de identificadores de aplicación, la información de control de acceso podría especificar la información de control de acceso de otras entidades en el terminal TE, tal como grupos de aplicaciones o entornos de ejecución de aplicaciones. La información de control de acceso 212 puede ser específica del contexto de servicio o de grupos de contextos de servicio. Por ejemplo, la información de control de acceso 212 puede comprender una pluralidad de diferentes perfiles para un acceso corporativo, que están adaptados para diferentes situaciones de uso. En una realización, esta información de control de acceso administrativo 212 pertenece a la información de contexto de servicio.

De acuerdo con una realización, un certificado 206 de una aplicación 202 se comprueba con el fin de definir de forma fiable un identificador que está asociado a la aplicación 202. Sobre la base de este identificador, entonces el terminal TE se dispone para comprobar si la aplicación 202 tiene, o no, autorización a acceder al contexto de servicio 203. Estos certificados 206 se pueden almacenar dentro de la información de contexto de servicio (por ejemplo, el certificado 206 en el depósito central 204) y/o fuera del contexto de servicio 203, por ejemplo, dentro de los datos de la aplicación 202 en el sistema de archivos 207. El certificado 206 está asociado a al menos una aplicación 202 en el terminal TE. El certificado 206 ha sido emitido y firmado digitalmente por una tercera parte de confianza, tal como una autoridad de certificación general o un desarrollador de aplicaciones, para probar la integridad y la fuente de la aplicación 202 asociada. El certificado 206 se podría obtener para el terminal TE por separado de la información de control de acceso 212, por ejemplo, durante la instalación de la aplicación, o este puede incluso formar una parte de la información de contexto de servicio o la información de control de acceso procedente de la entidad de gestión. Se ha de hacer notar que, en una realización, el certificado 206 se puede adquirir durante el procedimiento de control de acceso para comprobar el derecho de la aplicación 206 a acceder a un determinado contexto de servicio 203. El certificado 206 puede incluir al menos algunos de los siguientes: un nombre del titular del certificado, un número de serie, una fecha de caducidad, una copia de la clave pública del titular del certificado, y la firma digital del emisor de tal modo que un destinatario puede verificar que el certificado es auténtico.

Tal como también se ilustra mediante las líneas de trazo discontinuo en la figura 2, los contextos de servicio 203 pueden ser gestionados por la entidad de gestión autorizada externa 211. Esto puede querer decir que parte o la totalidad de la información que pertenece al contexto de servicio 203 puede ser leída, añadida, modificada y/o eliminada por la entidad de gestión externa 211. En una realización, la DM de OMA se aplica a gestionar los

contextos de servicio 203. Al menos parte de la información del contexto de servicio 203 se puede almacenar en un árbol de gestión, que es modificado por un agente de gestión de dispositivos sobre la base de instrucciones de gestión de dispositivos procedentes de un servidor (S) de gestión de dispositivos de OMA.

La figura 3 ilustra un método de una realización para usar los contextos de servicio en el terminal TE. En la etapa 301, puede existir una necesidad de iniciar un servicio mediante una aplicación 202 de tal modo que la aplicación 202 requiera una información que está almacenada bajo uno o más contextos de servicio 203 para la configuración de servicios, o para algún otro fin. Por lo general, esta necesidad se plantea basándose en una entrada de usuario, pero un servicio también se puede iniciar basándose en algún otro mecanismo desencadenante, tal como una instrucción procedente de un dispositivo externo. Los contextos de servicio 203 disponibles para el servicio se pueden comprobar en la etapa 302. Si la comprobación 302, 303 revela más de un contexto de servicio 203 disponible, se selecciona 305 un contexto de servicio 203 preferido. Por ejemplo, el terminal TE puede almacenar una lista de preferencias que indica los contextos de servicio 203 en un orden de preferencias. Un contexto de servicio 203 por defecto se podría seleccionar en la etapa 305. De lo contrario, se selecciona 304 un contexto de servicio 203 disponible. La aplicación 202, o un gestor de aplicaciones, se puede adaptar para realizar las etapas 301 a 305. A pesar de que no se muestra en la figura 3, se ha de hacer notar que el procedimiento de selección de contextos de servicio puede involucrar solicitar a un usuario del terminal TE que seleccione un contexto de servicio y/o que confirme la selección del contexto de servicio.

A continuación, el método avanza a la etapa 306, en la que se solicita el acceso a un contexto de servicio seleccionado o se indica de otro modo una necesidad de acceder a los datos específicos del contexto de servicio. Sobre la base de la información de control de acceso 212 procedente de y/o que está controlada por una entidad de gestión, se comprueba 307 si la aplicación 202 está autorizada a acceder al contexto de servicio 203. La información de control de acceso 212 relevante se puede obtener de la memoria del TE o, en una realización, el terminal TE se puede disponer para solicitar y recibir una información de control de acceso a partir de una entidad externa, tal como la entidad de gestión externa 212. La entidad de gestión puede ser el gestor de contextos de servicio 211 o alguna otra entidad, por ejemplo, una entidad que ha emitido el certificado 206. Si la aplicación 202 no está autorizada, se deniega 308 el acceso para la aplicación 202 al contexto de servicio 203.

De acuerdo con una realización, la etapa 307 comprende dos subetapas. En primer lugar, se comprueba un certificado 206 que está asociado a la aplicación 202 que requiere acceso al contexto de servicio 203. Mediante la comprobación del certificado 206, es posible asegurar la integridad y/o la fuente de la aplicación 202. En una segunda subetapa, un identificador que se obtiene del certificado 206 de la aplicación 202 se compara con los identificadores en una información de control de acceso 212 previamente determinada. En una realización, un identificador de fuente de aplicaciones procedente del certificado 206 se puede comparar en la segunda subetapa con unos identificadores de fuente de aplicaciones previamente determinados en la información de control de acceso 212. En la presente realización, la información de control de acceso 212 especifica aquellas aplicaciones, grupos de aplicaciones o fuentes de aplicaciones que están autorizadas a usar el contexto de servicio 203. Por lo tanto, si se puede hallar el identificador procedente del certificado 206 de la aplicación 202 en la información de control de acceso 212, la aplicación está autorizada.

Si la aplicación 202 está autorizada sobre la base de una comprobación 307, la aplicación puede acceder 309 a una información que está asociada al contexto de servicio 203 y, entonces, la aplicación 202 puede iniciar 310 el servicio sobre la base de la información de contexto de servicio asociada.

En una realización, el contexto de servicio 203 comprende o está asociado a unos ajustes que se requieren para disponer una conexión del terminal TE a uno o más recursos de red para acceder a un servicio. Por lo tanto, en la etapa 310, la aplicación 202 puede establecer una conexión que usa estos ajustes. Estos ajustes podrían especificar el acceso a recursos de intranet corporativos, tales como un servidor de correo electrónico y una cuenta de correo electrónico. No obstante, también existen muchos otros servicios para los cuales se puede usar el contexto de servicio 203.

En una realización, el terminal TE comprende unos datos (específicos) de aplicación controlados por acceso 208 que pertenecen a o que están asociados a un contexto de servicio 203 de tal modo que el acceso a los datos de aplicación 208 se dispone solo para las aplicaciones 202 que son autorizadas por la entidad de gestión externa 211. Por lo general, estos datos de aplicación 208 están relacionados con el usuario y son almacenados por una aplicación 202 en el terminal TE sobre la base de una entrada de usuario. En la etapa 310, los datos de aplicación 208, tales como un archivo que comprende correos electrónicos corporativos, se pueden visualizar y, posiblemente, procesarse adicionalmente mediante una aplicación 202 (una aplicación de cliente de correo electrónico en el presente ejemplo).

Un contexto de servicio 203 se puede seleccionar o definir cuando se usa una aplicación 202. Un contexto de servicio 203 se puede seleccionar cuando se activa una aplicación 202 y/o cuando se van a especificar nuevos contenidos como una información de contexto de servicio. Por ejemplo, cuando se activa una aplicación de correo electrónico, el usuario selecciona una cuenta de correo electrónico o perfil deseado, por lo que también se selecciona un contexto de servicio que está asociado a la cuenta de correo electrónico o perfil. Por lo tanto, cuando

la aplicación 202 requiere posteriormente acceso a la información del contexto de servicio 203, las etapas 302 a 305 son innecesarias pero se puede usar información en el contexto de servicio 203 asociado, por ejemplo, para establecer una conexión con un servidor de correo electrónico remoto. En otra realización, un contexto de servicio 203 se puede especificar para un elemento de datos de usuario, tal como un mensaje de correo electrónico. Este contexto de servicio 203 se podría seleccionar en conexión con el almacenamiento de un elemento de datos. Por ejemplo, cuando el usuario ha acabado de preparar un elemento de correo electrónico y selecciona almacenar el elemento, se muestran al usuario los contextos de servicio 203 disponibles (para la aplicación de correo electrónico). Entonces, el usuario puede seleccionar el contexto de servicio 203 al que se va a asociar el elemento de datos y, por lo tanto, posiblemente la posición de almacenamiento del elemento de datos, y el elemento de datos se almacena en consecuencia. Posteriormente, el elemento de datos se puede usar como cualesquiera otros datos específicos del contexto de servicio 203, es decir, el acceso al elemento de datos se permite solo para las aplicaciones 202 autorizadas.

En una realización, el acceso a los contextos de servicio 203 se controla (las etapas 307 a 309) mediante un procedimiento de seguridad en el entorno de ejecución segura 201, tal como una entidad de controlador de acceso específico. También es factible que el entorno de ejecución 201 compruebe 303 y seleccione 304, 305 un contexto de servicio 203 para la aplicación 202. Se puede proporcionar un selector de contextos de servicio específico en el entorno de ejecución segura 201.

En otra realización, los contextos de servicio 203 disponibles para la aplicación 202 que requiere acceso al contexto de servicio 203 ya se han comprobado en la etapa 302. En la presente realización, solo se consideran para el servicio los contextos de servicio 203 para los cuales el certificado de la aplicación 202 permite el acceso (o para los cuales la aplicación tiene autorización de acceso por algún otro medio). En la presente realización, el acceso a un contexto de servicio 203 es intentado solo por las aplicaciones 202 autorizadas y, por lo tanto, se evitan las solicitudes innecesarias.

Las figuras 4a y 4b ilustran un método para establecer y/o modificar un contexto de servicio 203 en el terminal TE mediante el servidor S de acuerdo con una realización. En la figura 4a, se ilustran características del servidor S que funciona como el servidor de gestión de dispositivos. En la etapa 401, existe una necesidad de crear un nuevo contexto de servicio 203 y/o de modificar un contexto de servicio 203 existente en el dispositivo de terminal TE gestionado. En otra realización, existe una necesidad de añadir o modificar la información de control de acceso 212 en relación con un contexto de servicio 203.

Entonces, se dispone 402 una sesión de gestión de dispositivos entre la funcionalidad del servidor de gestión de dispositivos en el servidor S y la funcionalidad del cliente de gestión de dispositivos en el terminal TE. Se pueden utilizar las funciones convencionales de establecimiento de sesiones de DM de OMA que se ilustran en la especificación de OMA “*SyncML Device Management Protocol*”, versión 1.1.2, 12 de diciembre de 2003, 41 páginas.

La información relacionada con el contexto de servicio, por ejemplo, los ajustes de conexión 205, y/o la información de control de acceso 212, se especifica 403 en una o más instrucciones de gestión de dispositivos. En la presente realización, al menos parte de la información de contexto de servicio en la instrucción o instrucciones de gestión de dispositivos es dirigida a uno o más nodos de árbol de gestión de dispositivos específicos del contexto de servicio. La instrucción de gestión se transmite 404 al terminal TE.

La figura 4b ilustra funciones en el terminal TE que recibe una información relacionada con el contexto de servicio. En la etapa 410, una instrucción de gestión de dispositivos se recibe de un servidor de gestión de dispositivos (S). Los datos relacionados con el contexto de servicio, incluyendo la información de control de acceso, se pueden almacenar en el terminal TE. Más en concreto, en la etapa 411 el cliente de gestión de dispositivos en el terminal TE define las acciones requeridas sobre la base de la instrucción de gestión de dispositivos recibida. Entonces, el árbol de gestión de dispositivos en el terminal TE puede ser modificado por la información nueva y/o modificada en relación con el contexto de servicio 203. Por ejemplo, se puede añadir un nuevo nodo con una lista ACL que define el servidor S como que es el único servidor de gestión de dispositivos autorizado para modificar el nodo. Se ha de hacer notar que el árbol de gestión solo puede servir como una vista de la información gestionada, por lo que la información gestionada se puede almacenar fuera del árbol de gestión.

Si el contexto de servicio 203 se crea por primera vez y no se ha provisto una gestión de dispositivos para el terminal TE, en primer lugar se pueden usar métodos de aprovisionamiento de cliente de OMA para iniciar y configurar la gestión de dispositivos antes de instrucciones de gestión específicas del contexto de servicio. Por lo tanto, en las etapas 402 y 410, se puede utilizar una conexión para disponer el aprovisionamiento.

El árbol de gestión puede comprender uno o más nodos para la información de control de acceso 212, incluso si la información de control de acceso 212 no es parte del contexto de servicio 203. De una forma similar a la que se ha ilustrado en lo que antecede, mediante la utilización de una instrucción de gestión de dispositivos que es dirigida a un nodo para la información de control de acceso 212, es posible disponer la modificación, la supresión o la adición de la información de control de acceso 212. Por lo tanto, una entidad de gestión externa puede cambiar fácilmente la configuración de control de acceso en el dispositivo TE gestionado. Se ha de hacer notar que las figuras 4a y 4b son

solo a modo de ejemplo. Por ejemplo, la instrucción de gestión de dispositivos se podría formar antes del establecimiento de la sesión de gestión. En una realización, un contexto de servicio 203 puede ser creado o modificado por una parte autorizada en el terminal TE, por ejemplo, un usuario. Procedimientos similares a los que ya se han ilustrado en conexión con la figura 3, las etapas 306 - 309 se pueden utilizar cuando se accede a la información de contexto de servicio. Por lo tanto, es innecesario aplicar mecanismos de gestión de dispositivos para modificar la información del contexto de servicio 203.

En una realización, el gestor de contextos de servicio 211 o un proveedor de servicios, en la realización de la figura 4a el servidor S, puede comprobar que un contexto de servicio adecuado se ha puesto en práctica y/o que se usa de forma apropiada en el terminal TE. Por lo tanto, el proveedor de servicios puede comprobar que se han puesto en práctica unos ajustes correctos y solo se usan aplicaciones procedentes de una fuente de confianza. Esta comprobación se podría implementar mediante el uso de instrucciones GET de DM de OMA para los nodos que comprenden estos datos de contexto de servicio. La presente realización se puede implementar después de las etapas 404 y 412 o en algún otro punto en el tiempo, por ejemplo, después de recibir una solicitud de servicio procedente de una aplicación 202 en el terminal TE.

En las etapas 402, 403, 410 y 411, es posible utilizar los mecanismos del protocolo de gestión de dispositivos y los mensajes que se definen para el mismo; para una descripción más detallada del protocolo de gestión de dispositivos de OMA y otras instrucciones, por ejemplo, se hace referencia a la especificación de OMA "*SyncML Device Management Protocol*", versión 1.1.2, 12 de diciembre de 2003, 41 páginas, y la especificación de OMA "*SyncML Representation Protocol Device Management Usage*", versión 1.1.2, 12 de junio de 2003, 39 páginas.

De acuerdo con una realización, los contenidos de un contexto de servicio 203 se pueden asociar con diferentes reglas de control de acceso y/o niveles de derechos de acceso sobre la base de la información de control de acceso 212. En una realización adicional, diferentes reglas de acceso se aplican a diferentes porciones del contexto de servicio 203. Por ejemplo, los ajustes 205 del contexto de servicio 203 que especifican una conexión con un servidor de correo electrónico corporativo se pueden leer (por una aplicación 202 autorizada a acceder al contexto de servicio 203) pero se pueden no modificar, mientras que el acceso a los datos 208 en un sistema de archivos 207 que está asociado al contexto de servicio 203 se puede tanto leer como modificar. En la presente realización, los contenidos de los contextos de servicio 203 se pueden diferenciar con respecto al control de acceso.

Algunas reglas a modo de ejemplo que se pueden aplicar como la realización que se ha ilustrado en lo que antecede son: derecho de lectura (de la totalidad o solo una parte específica de los datos de contexto de servicio), derecho de eliminación y derecho de adición. Las reglas de control y/o niveles de derechos de acceso se pueden especificar dentro de la información de control de acceso 212 o algún otro almacenamiento. En una realización, las directivas de acceso se especifican mediante XACML (*Extensible Access Markup Language*, lenguaje de marcado de acceso extensible). Si se aplica la DM de OMA, las listas de control de acceso se pueden especificar en un árbol de gestión para determinar uno o más servidores de gestión de dispositivos externos autorizados a acceder a los datos relacionados con el contexto de servicio asociados, es decir, las entidades de gestión externas se pueden especificar mediante listas de control de acceso de DM de OMA.

En una realización alternativa o complementaria, diferentes reglas de control de acceso están asociadas a diferentes usuarios de los contextos de servicio 203 sobre la base de la información de control de acceso 212. En la presente realización, es posible aplicar diferentes derechos de acceso para diferentes aplicaciones 202 y usuarios del terminal TE, por ejemplo. Como un ejemplo, un contexto de servicio 203 (o parte del mismo) se puede ajustar para ser modificable solo por el usuario de o el abonado al terminal TE y una entidad de gestión externa que origina y/o que controla el contexto de servicio 203.

En una realización, el usuario de o el abonado al terminal TE siempre tiene autorización a eliminar o suprimir los contextos de servicio 203 con respecto al terminal TE. Debido a que ser requiere un contexto de servicio 203 para obtener un servicio, el terminal TE no se puede usar para acceder al servicio después de que se haya suprimido el contexto de servicio 203. Por lo tanto, no es necesario dar pleno control a administrador 211 alguno de un contexto de servicio 203, y los usuarios no han de renunciar a un derecho de control de sus terminales. No es necesario forzar contexto de servicio alguno en ninguno de los terminales, pero el usuario / abonado puede desear usar un servicio y, por lo tanto, aceptar un contexto de servicio en el terminal TE. Debido a que el propio contexto de servicio 203 se puede ajustar para ser modificable solo por la entidad de gestión autorizada (211), es posible evitar el acceso del usuario para modificar el contexto de servicio 203.

En una realización adicional, se proporciona una capacidad de informar a la entidad de gestión autorizada 211 acerca de los contextos de servicio 203 suprimidos por el usuario. Una característica o aplicación 203 que maneja la supresión de un contexto de servicio 203 sobre la base de una entrada de usuario se puede configurar para transmitir un mensaje a la entidad de gestión autorizada 211 que informa acerca de la supresión del contexto de servicio 203 con respecto al terminal TE. En otra realización, la entidad de gestión autorizada 211 está configurada para comprobar los contextos de servicio 203 (que la misma está autorizada a ver) en el terminal TE con el fin de detectar los suprimidos. Por ejemplo, se pueden realizar comprobaciones periódicas mediante procedimientos de DM de OMA en los nodos que comprenden datos de contexto de servicio.

Se debería hacer notar que las realizaciones que se han descrito en lo que antecede también se podrían aplicar en cualquier combinación de las mismas. Es obvio a un experto en la materia que, a medida que avanza la tecnología, la idea básica de la invención se puede implementar de muchas formas diferentes. Por lo tanto, la invención y sus realizaciones no se limitan a los ejemplos que se han descrito en lo que antecede, sino que pueden variar dentro del alcance de las reivindicaciones.

REIVINDICACIONES

1. Un método para un sistema de gestión de dispositivos para disponer el uso de configuraciones en un dispositivo con múltiples conjuntos de datos de configuración y una pluralidad de aplicaciones, **caracterizado por que** el sistema comprende una información de control de acceso que es originada y/o controlada por una entidad de gestión externa para definir un derecho de una aplicación a acceder a un conjunto de datos de configuración, comprendiendo el método:

certificar, en respuesta a una indicación procedente de una aplicación que requiere acceso a un conjunto de datos de configuración (302), una fuente de la aplicación y comprobar, a partir de la información de control de acceso, el derecho de una aplicación a acceder a un conjunto de datos de configuración mediante la comparación de unos identificadores previamente determinados en la información de control de acceso con un identificador en un certificado que está asociado a la aplicación; y
disponer, en respuesta a que la aplicación tenga autorización a acceder al conjunto de datos de configuración, el acceso al conjunto de datos de configuración para la aplicación (309), en donde al menos un contexto de servicio (203) está almacenado en el dispositivo, comprendiendo el contexto de servicio al menos el conjunto de datos de configuración, y se permite el acceso al contexto de servicio para la aplicación sobre la base de la información de control de acceso si la aplicación está autorizada sobre la base de una información de control de acceso que está asociada al contexto de servicio.

2. Un método de acuerdo con la reivindicación 1, **caracterizado por** disponer la selección (305) de un conjunto de datos de configuración para la aplicación en respuesta a una pluralidad de conjuntos de datos de configuración que se encuentran disponibles para la aplicación.

3. Un método de acuerdo con una cualquiera de las reivindicaciones anteriores, **caracterizado por** disponer un servicio mediante la aplicación sobre la base de al menos parte del conjunto de datos de configuración.

4. Un método de acuerdo con una cualquiera de las reivindicaciones anteriores, **caracterizado por** disponer el conjunto de datos de configuración y/o la información de control de acceso en el mismo en el dispositivo mediante:

el establecimiento (402) de una sesión de gestión de dispositivos o una conexión para disponer el aprovisionamiento entre un servidor de gestión de dispositivos de la entidad de gestión externa y el dispositivo,
la recepción del conjunto de datos de configuración y/o la información de control de acceso mediante la sesión de gestión de dispositivos o la conexión para el aprovisionamiento, y
el almacenamiento del conjunto de datos de configuración y/o la información de control de acceso en el dispositivo.

5. Un método de acuerdo con la reivindicación 1, **caracterizado por que** la información de control de acceso se comprueba en respuesta a una solicitud procedente de la aplicación para acceder al conjunto de datos de configuración.

6. Un método de acuerdo con la reivindicación 1, **caracterizado por que** el conjunto de datos de configuración comprende unos ajustes que se requieren para disponer una conexión desde el dispositivo con uno o más recursos de red para acceder a un servicio, y
el dispositivo de procesamiento de datos está dispuesto para establecer una conexión con uno o más recursos de red sobre la base de los ajustes.

7. Un método de acuerdo con la reivindicación 1, **caracterizado por que** una transferencia de datos entre la aplicación autorizada a acceder al conjunto de datos de configuración y una posición de almacenamiento que comprende el conjunto de datos de configuración está asegurada.

8. Un sistema de gestión de dispositivos que comprende un servidor de gestión de dispositivos y un cliente de gestión de dispositivos a gestionar, estando dispuesto el sistema de gestión de dispositivos para gestionar al menos un cliente de gestión de dispositivos por medio de una estructura de gestión que comprende al menos un nodo, **caracterizado por que** el sistema comprende un dispositivo de procesamiento de datos de acuerdo con la reivindicación 9.

9. Un dispositivo de procesamiento de datos para un sistema de gestión de dispositivos, comprendiendo el dispositivo unos medios para almacenar múltiples conjuntos de datos de configuración y una pluralidad de aplicaciones, **caracterizado por que** el dispositivo de procesamiento de datos comprende:

una memoria para almacenar una información de control de acceso para definir un derecho de una aplicación a acceder a un conjunto de datos de configuración,
unos medios para certificar una fuente de la aplicación y comprobar la información de control de acceso mediante la comparación de unos identificadores previamente determinados en la información de control de acceso con un identificador en un certificado que está asociado a la aplicación en respuesta a una indicación

procedente de una aplicación que requiere acceso a un conjunto de datos de configuración (302), y
unos medios para disponer el acceso al conjunto de datos de configuración para la aplicación en respuesta a que la aplicación tenga autorización a acceder al conjunto de datos de configuración (309), en donde el dispositivo de procesamiento de datos está dispuesto para almacenar al menos un contexto de servicio (203) que comprende al menos el conjunto de datos de configuración, y
el dispositivo de procesamiento de datos está dispuesto para permitir que la aplicación acceda al contexto de servicio sobre la base de la información de control de acceso si la aplicación está autorizada sobre la base de una información de control de acceso que está asociada al contexto de servicio.

10. Un dispositivo de procesamiento de datos de acuerdo con la reivindicación 9, **caracterizado por que** el dispositivo de procesamiento de datos está dispuesto para comprobar la información de control de acceso en respuesta a una solicitud procedente de la aplicación para acceder al conjunto de datos de configuración.

11. Un dispositivo de procesamiento de datos de acuerdo con las reivindicaciones 9 o 10, **caracterizado por que** el dispositivo de procesamiento de datos comprende unos medios para disponer (310) un servicio mediante la aplicación sobre la base de al menos parte del conjunto de datos de configuración.

12. Un dispositivo de procesamiento de datos de acuerdo con la reivindicación 9, **caracterizado por que** el contexto de servicio comprende adicionalmente datos relacionados con el usuario que son almacenados por una aplicación del dispositivo de procesamiento de datos.

13. Un dispositivo de procesamiento de datos de acuerdo con una cualquiera de las reivindicaciones 9 a 12, **caracterizado por que** el conjunto de datos de configuración comprende unos ajustes que se requieren para disponer una conexión desde el dispositivo a uno o más recursos de red para acceder a un servicio, y
el dispositivo de procesamiento de datos está dispuesto para establecer una conexión a uno o más recursos de red sobre la base de los ajustes.

14. Un dispositivo de procesamiento de datos de acuerdo con una cualquiera de las reivindicaciones 9 a 13, **caracterizado por que** el dispositivo de procesamiento de datos comprende unos medios para disponer la selección (305) de un conjunto de datos de configuración para la aplicación en respuesta a una pluralidad de conjuntos de datos de configuración que se encuentran disponibles para la aplicación.

15. Un dispositivo de procesamiento de datos de acuerdo con una cualquiera de las reivindicaciones 9 a 14, **caracterizado por que** una transferencia de datos entre la aplicación autorizada a acceder al conjunto de datos de configuración y una posición de almacenamiento que comprende el conjunto de datos de configuración está asegurada.

16. Un dispositivo de procesamiento de datos de acuerdo con una cualquiera de las reivindicaciones 9 a 15, **caracterizado por que** el dispositivo de procesamiento de datos comprende un cliente de gestión de dispositivos de acuerdo con una norma de gestión de dispositivos de la Alianza Móvil Abierta, y
el dispositivo de procesamiento de datos está dispuesto para añadir y/o modificar (412) un conjunto de datos de configuración sobre la base de una instrucción de gestión de dispositivos desde un servidor de gestión de dispositivos a un nodo de un árbol de gestión en el dispositivo de procesamiento de datos.

17. Un producto de programa informático descargable en una memoria de un dispositivo de procesamiento de datos, **caracterizado por que** el producto de programa informático comprende un código de programa informático que, cuando se ejecuta en un procesador del dispositivo de procesamiento de datos, da lugar a que el dispositivo de procesamiento de datos:

certifique, en respuesta a una indicación procedente de una aplicación que requiere acceso a un conjunto de datos de configuración (302), una fuente de la aplicación y compruebe una información de control de acceso para definir un derecho de una aplicación a acceder a un conjunto de datos de configuración mediante la comparación de unos identificadores previamente determinados en la información de control de acceso con un identificador en un certificado que está asociado a la aplicación y
disponga, en respuesta a que la aplicación tenga autorización a acceder al conjunto de datos de configuración, el acceso al conjunto de datos de configuración para la aplicación (309), en donde al menos un contexto de servicio (203) está almacenado en el dispositivo, comprendiendo el contexto de servicio al menos el conjunto de datos de configuración, y se permite el acceso al contexto de servicio para la aplicación sobre la base de la información de control de acceso si la aplicación está autorizada sobre la base de una información de control de acceso que está asociada al contexto de servicio.

18. Un producto de programa informático de acuerdo con la reivindicación 17, en donde el producto de programa informático comprende un código de programa informático para dar lugar a que el dispositivo de procesamiento de datos disponga la selección (305) de un conjunto de datos de configuración para la aplicación en respuesta a una pluralidad de conjuntos de datos de configuración que se encuentran disponibles para la aplicación.

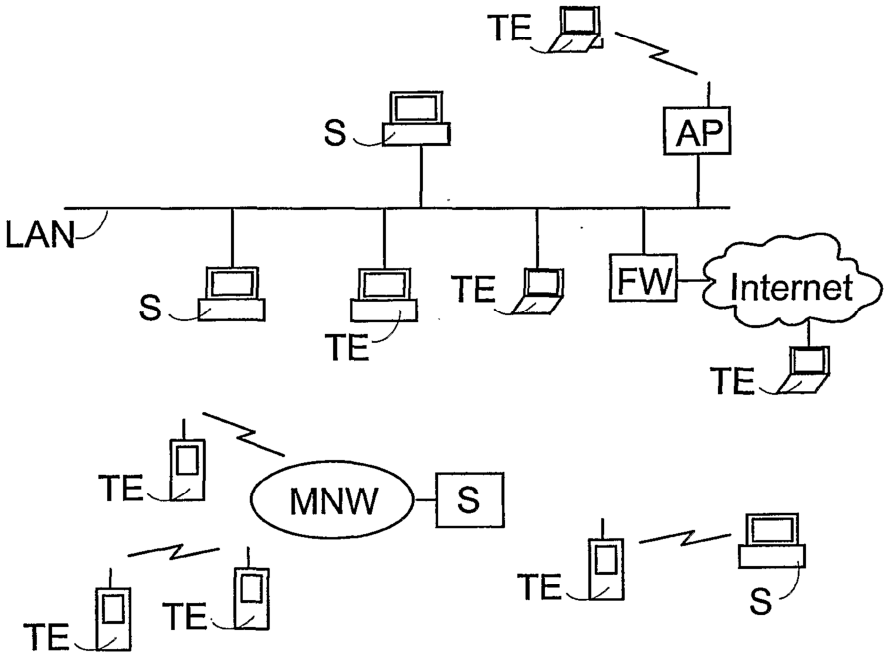
TE
S
AP
LAN
S
TE
TE
FW
Internet
TE
TE
MNW
S
TE
TE
TE
S

Fig. 1

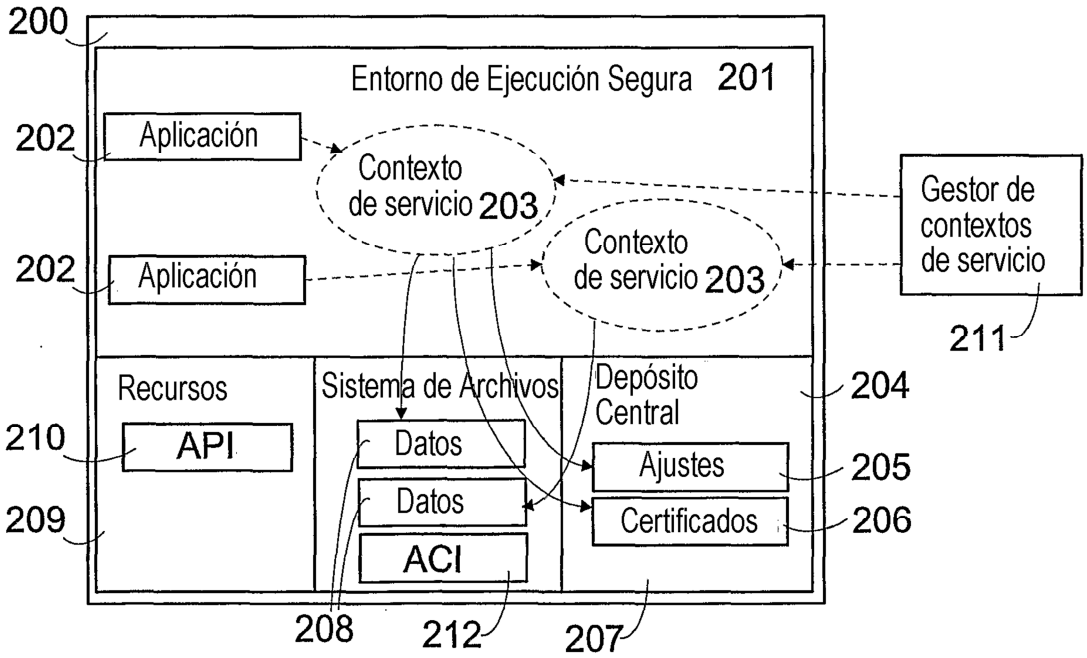
200
Entorno de Ejecución Segura 201
202
Aplicación
Contexto de servicio 203
Gestor de contextos de servicio
202
Aplicación
Contexto de servicio 203
211
Recursos
Sistema de Archivos
Depósito Central
204
210
API
Datos
Ajustes
205
209
Datos
Certificados
206
ACI
208
212
207

Fig. 2

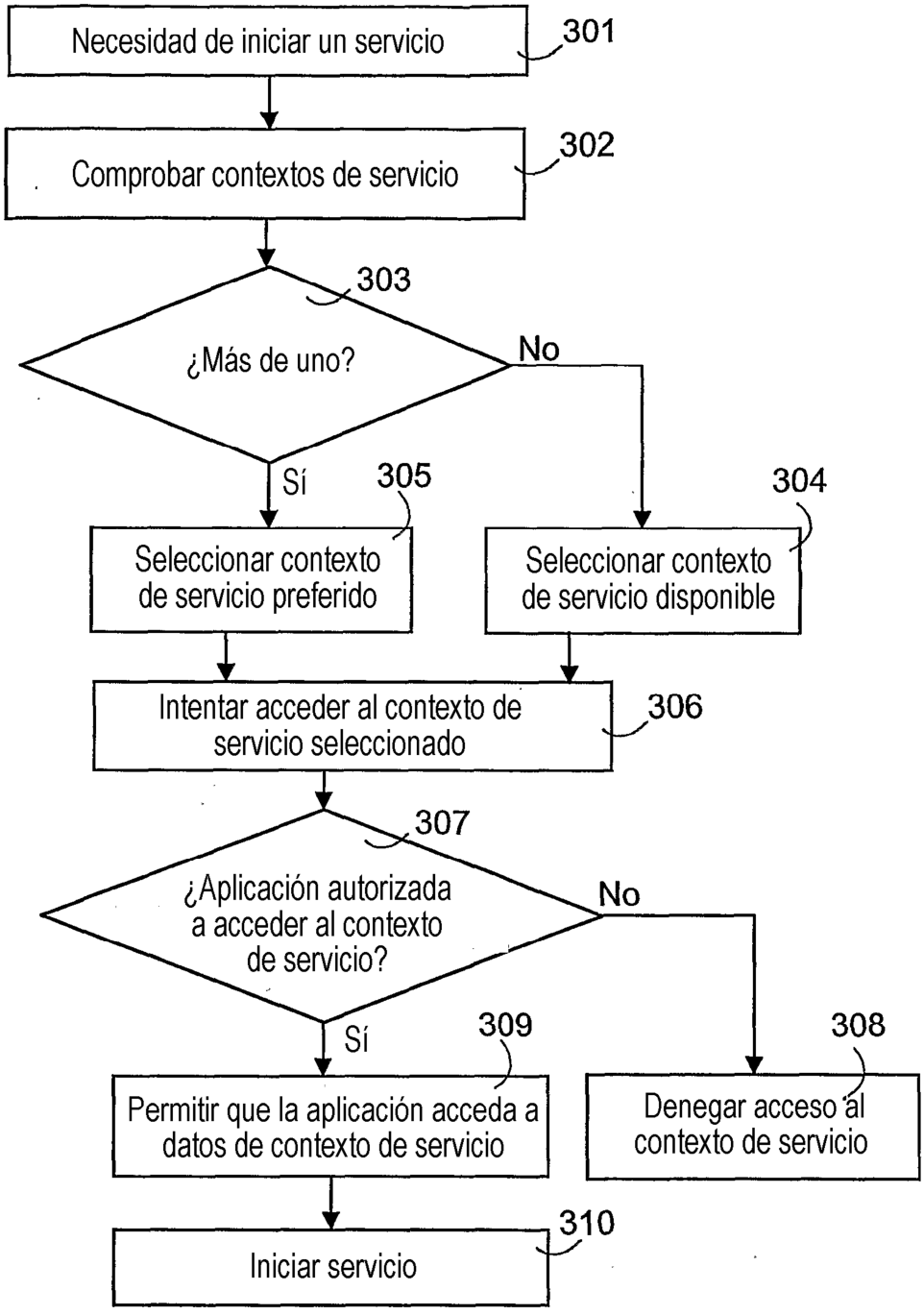
Necesidad de iniciar un servicio
301
Comprobar contextos de servicio
302
303
¿Más de uno?
No
Sí
305
Seleccionar contexto de servicio preferido
304
Seleccionar contexto de servicio disponible
Intentar acceder al contexto de servicio seleccionado
306
307
¿Aplicación autorizada a acceder al contexto de servicio?
No
Sí
309
Permitir que la aplicación acceda a datos de contexto de servicio
308
Denegar acceso al contexto de servicio
310
Iniciar servicio

Fig. 3

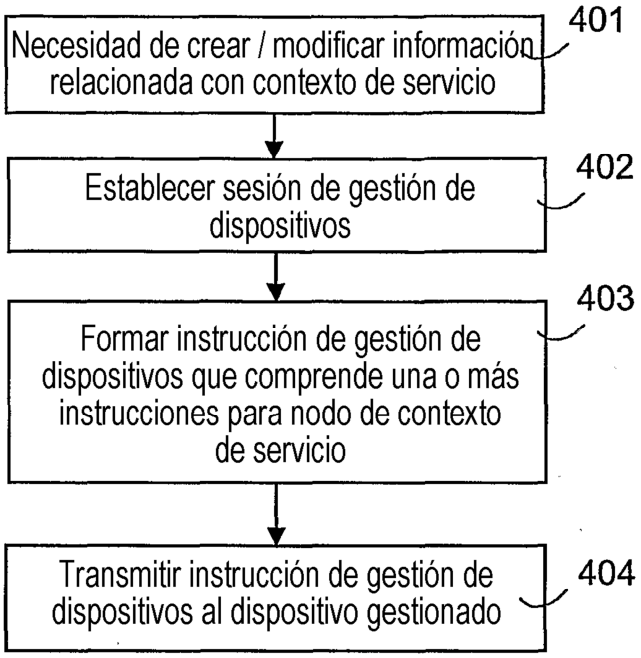
Necesidad de crear / modificar información relacionada con contexto de servicio
401
Establecer sesión de gestión de dispositivos
402
Formar instrucción de gestión de dispositivos que comprende una o más instrucciones para nodo de contexto de servicio
403
Transmitir instrucción de gestión de dispositivos al dispositivo gestionado
404

Fig. 4a

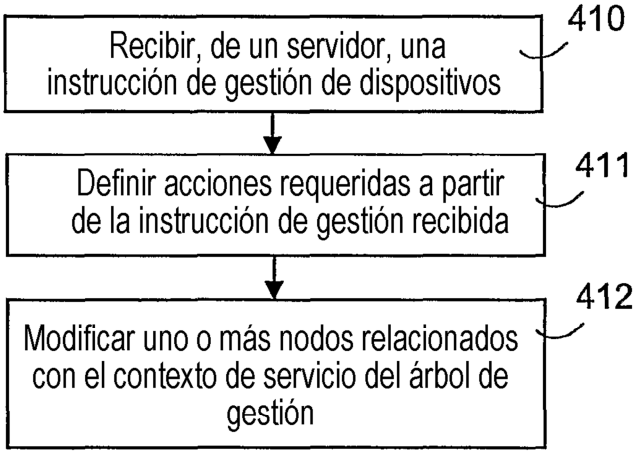
Recibir, de un servidor, una instrucción de gestión de dispositivos
410
Definir acciones requeridas a partir de la instrucción de gestión recibida
411
Modificar uno o más nodos relacionados con el contexto de servicio del árbol de gestión
412

Fig. 4b