(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 384 473**

(51) Int. CI.:
G06F 21/00 (2006.01)
H04L 29/08 (2006.01)
H04L 12/24 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **07020544 .8**
(96) Fecha de presentación: **19.10.2007**
(97) Número de publicación de la solicitud: **1939780**
(97) Fecha de publicación de la solicitud: **02.07.2008**

(54) Título: **Gestión de dispositivos**

(30) Prioridad:
20.10.2006 GB 0620927

(45) Fecha de publicación de la mención BOPI:
05.07.2012

(45) Fecha de la publicación del folleto de la patente:
05.07.2012

(73) Titular/es:
VODAFONE GROUP PLC
VODAFONE HOUSE THE CONNECTION
NEWBURY
BERKSHIRE RG14 2FN, GB

(72) Inventor/es:
Bone, Nicholas;
Belrose, Caroline Jessica;
Wright, Timothy y
Babbage, Stephen

(74) Agente/Representante:
Carpintero López, Mario

DESCRIPCIÓN

Gestión de dispositivos

La invención se refiere a un sistema para gestión de dispositivos. En particular, la invención se refiere a la provisión de un marco en el que los terminales móviles son configurados y gestionados por un servidor central.

La gestión de dispositivos (DM) en sistemas de telecomunicaciones móviles hace posible que el operador móvil de la red gestione y actualice diversos aspectos de los terminales móviles individuales (esto es, los aparatos telefónicos móviles). Por ejemplo, pueden ser gestionados unos parámetros de configuración y el software y / o el firmware pueden ser actualizados “sobre el aire” (OTA).

La DM ha sido implementada de múltiples formas. Un ejemplo de un esquema de la DM es el esquema desarrollado por la OMA (Alianza Móvil Abierta [Open Mobile Alliance]) del cuerpo de estándares de la industria. Las especificaciones de la DM de la OMA introducen la noción de objetos de gestión (MOs). Los MOs son entidades que pueden ser manipuladas mediante acciones de gestión (por control remoto). En este esquema los MOs están lógicamente agrupados en una estructura jerárquica designada como “árbol de gestión”.

Cada terminal móvil susceptible de DM está provisto de una aplicación de cliente de la DM: un elemento de software que interactúa con un servidor de gestión (situado en la red de telecomunicaciones móviles) y acepta los MOs procedentes del servidor de gestión. Los MOs son utilizados para actualizar el árbol de gestión y, a su vez, las funciones de gestión son implementadas. Los MOs contendrán generalmente unos parámetros de configuración y / o unos datos para unas aplicaciones y unos servicios dispuestos sobre el terminal, sin embargo las especificaciones de la DM no dan instrucciones acerca de qué datos pueden o no pueden ser acarreados dentro de un MO, o qué efecto tendrán esos datos sobre el terminal. Las especificaciones de los datos autorizados se configuran de acuerdo con lo requerido por cualquier implementación determinada.

Para evitar problemas de seguridad, un cliente de la DM debe identificar y autenticar un servidor de la DM antes de aceptar los MOs desde el servidor y, de modo similar, el servidor de la DM debe identificar y autenticar al cliente de la DM. El cliente de la DM debe, por consiguiente, poseer unas determinadas credenciales y configuraciones para instruirle acerca de cómo contactar con el servidor de la DM correcta y cómo manejar correctamente la autenticación mutua requerida.

Tradicionalmente, un agente de la DM situado en un terminal es capaz de gestionar un entorno de ejecución principal único (esto es, un entorno en el cual puedan ser ejecutadas unas aplicaciones u otro software, como por ejemplo el OS principal y las aplicaciones ejecutadas por encima de él) en un terminal.

En terminales más avanzados, sin embargo, se contempla que puede disponerse más de un entorno de ejecución (EE) en un terminal. Estos terminales más recientes son con ello susceptibles de ejecutar aplicaciones en un primer EE que esté eficazmente separado de un segundo EE (y por supuesto de EEs adicionales). Esta separabilidad es conveniente por razones de seguridad, fiabilidad y posiblemente de eficiencia. Un ejemplo de dicho terminal sería un terminal que ejecutara un OS complejo, por ejemplo un Symbian, (primer EE) y un EE protegido separado, donde las aplicaciones o tareas de confianza pudieran discurrir dentro de un entorno aislado y de confianza (segundo EE).

Múltiples OSs pueden, así mismo, coexistir en la misma plataforma cuando el terminal está dispuesto con un “hipervisor” (o software de virtualización) y / o una arquitectura de procesador dual.

El documento WO2006/070045 divulga un procedimiento para disponer el uso de configuraciones en un dispositivo que incorpora unos entornos de ejecución principal únicos. Los contextos de los servicios pueden ser gestionados por una entidad de gestión autorizada externa – esto es, un agente de DM.

El documento de la Alianza Móvil Abierta (OMA) “Clase de Aplicaciones de Gestión EFI” [“EFI Manage Application Class”] OMA – WAP – EFIMAC-V1_1-20040609-C divulga una clase de aplicación que proporciona unos servicios que pueden ser utilizados por una aplicación que se ejecute dentro de un primer entorno de aplicaciones para interactuar con unas aplicaciones nativas que se ejecutan dentro de otros entornos de aplicaciones.

El documento WO03/073306 se refiere a una técnica de descarga de software apropiada para descargar software en múltiples terminales en redes de comunicaciones inalámbricas.

El documento WO2005/091108 se refiere a la provisión de un entorno de ejecución seguro en dispositivos tales como terminales de telecomunicaciones móviles.

Tal y como se podrá apreciar con facilidad a partir de lo expuesto, la gestión de entornos de ejecución diferentes en un dispositivo único representa una carga adicional considerable sobre la capacidad de procesamiento del dispositivo. Aunque un agente de la DM puede llevar a cabo una operación de gestión idéntica en cada EE u OS, la separación de los EEs necesitará una estructura jerárquica nueva de los MOs (árbol de gestión) así como una duplicación del código de la DM, una configuración y unos datos de autenticación del servidor para cada EE.

Incluso cuando existan restricciones técnicas, como por ejemplo un aislamiento que no necesite las duplicaciones referidas, puede haber circunstancias en las cuales los activos en diferentes áreas o entornos de los terminales deben ser gestionados por diferentes partes, y ello puede significar que dos entornos necesiten ser gestionados por servidores de la DM diferentes. Siempre que se requiera más de un servidor de la DM para gestionar entornos y / o activos de terminales diferentes, se requieren múltiples árboles y conjuntos de gestión de configuración de la DM y de los datos de autenticación.

Por consiguiente, constituye un objetivo de la invención obviar o al menos mitigar los problemas mencionados con anterioridad.

De acuerdo con un aspecto de la presente invención, se proporciona un terminal de telecomunicaciones móviles que incorpora una plataforma de ejecución que incluye un primer entorno de ejecución y un segundo entorno de ejecución, estando cada entorno de ejecución dispuesto para ejecutar un agente de gestión de dispositivos respectivo y emitiendo cada agente, de acuerdo con las instrucciones procedentes de un servidor de gestión de dispositivos, unas acciones de gestión que actúan sobre una o más entidades de gestión respectivas que se ejecutan dentro de uno o más entornos de ejecución; en el que las entidades de gestión del segundo entorno de ejecución están agrupadas en una estructura de gestión, siendo la estructura de gestión una de las entidades de gestión situadas dentro del primer entorno de ejecución, de forma que el servidor de gestión de dispositivos está autorizado para gestionar aplicaciones y / o servicios ejecutados dentro tanto de los primero como de los segundos entornos de ejecución.

De acuerdo con un aspecto adicional de la presente invención, se proporciona un procedimiento para procesar la gestiones de gestión recibidas de un servidor de gestión de dispositivos por un terminal, que comprende:

la provisión de una plataforma de gestión que incorpora un primer entorno de ejecución y un segundo entorno de ejecución;

en el primer entorno de ejecución, la ejecución de un primer agente de gestión de dispositivos, emitiendo el primer agente, de acuerdo con las instrucciones procedentes de un servidor de gestión de dispositivos, unas acciones de gestión que actúan sobre una o más entidades de gestión respectivas ejecutadas dentro del primer entorno de ejecución;

en el segundo entorno de ejecución, la ejecución de un segundo agente de gestión de dispositivos, emitiendo el segundo agente, de acuerdo con las instrucciones procedentes de un servidor de gestión de dispositivos, unas acciones de gestión que actúan sobre una o más entidades de gestión respectivas ejecutadas dentro del segundo entorno de ejecución;

en el que las entidades de gestión del segundo entorno de ejecución están agrupadas en una estructura de gestión, siendo la estructura de gestión una de las entidades de gestión situadas dentro del primer entorno de ejecución.

Los dispositivos pueden incorporar más de un entorno de ejecución (EE). Por ejemplo, el dispositivo puede incorporar más de un Sistema Operativo ejecutado, o puede incorporar un segundo entorno / área protegido y un entorno de ejecución no protegido, donde el entorno protegido podría estar aislado por unos controles de software y / o hardware o podría incluso ser un elemento protegido basado en hardware situado dentro del terminal. Incluso una tarjeta inteligente extraíble, como por ejemplo una tarjeta SIM podría ser considerada como un EE del dispositivo.

Tradicionalmente, hay un agente de la DM separado en cada EE y un árbol de gestión separado en cada EE para gestionar los dos sistemas operativos separados. Sin embargo, esto requiere dos canales de comunicación separados con el servidor y dos conjuntos de configuración. Cada agente de la DM es requerido para mantener instancias separadas de credenciales, configuraciones y canales con el (los) servidor(es) del DM. Ello, a su vez, requiere un ancho de banda, una capacidad de procesamiento y de coste suplementarios. En resumen, dicha propuesta no lleva a cabo un cambio de escala efectivo.

Cuando existe una pluralidad de entornos de ejecución, sería conveniente poder gestionar estos EEs de una manera análoga a la forma en que se gestiona el EE principal.

En la invención, las entidades de gestión (esto es los MOs) del segundo entorno de ejecución están agrupadas en una estructura de gestión de los MOs (esto es, un árbol de gestión) y esta estructura de gestión está ella misma definida como un MO del primer EE. Una estructura de gestión para un EE tratado como un MO para otro EE es designada como un “árbol de gestión virtual” (VMT) y se basa en el hecho de que las especificaciones de la DM no plantean restricciones acerca de qué datos pueden ser acarreados dentro de un MO.

El servidor de la DM para el primer EE puede, por consiguiente, gestionar tanto el árbol de gestión para el primer EE como el árbol de gestión para el segundo EE, (utilizando el VMT) por medio de la conexión con el agente de la DM existente en el primer EE.

El servidor de la DM es responsable del suministro de los MOs a un agente de la DM, pero no es necesariamente el autor original de los MOs. Por ejemplo, el autor del MO puede firmar el MO y, a continuación, suministrarlo al

servidor de la DM el cual sería responsable de la distribución del MO a los terminales. En este caso, el agente de la DM autenticaría el servidor de la DM suministrando los MOs, pero, así mismo, autenticaría de manera específica los MOs que se suministran para asegurar que procedieran del autor correcto del MO. De modo similar, el uso de los VMTs es, así mismo, posible incluso cuando el autor de los MOs para el segundo EE difiera del autor de los MOs para el primer EE.

Una vez que el VMT ha sido suministrado al agente de la DM del primer EE, esta agente de la DM puede, a continuación, pasar el contenido del VMT directamente al agente de la DM del segundo EE para su procesamiento.

De modo ventajoso, el agente de la DM del primer EE podría incluso ser considerado como un servidor de la DM apoderado del agente de la DM del segundo EE si es necesario. En este caso, la estructura del cliente de la DM del segundo EE y los protocolos de comunicaciones serían casi estándar excepto porque el agente de la DM del segundo EE no necesita establecer comunicaciones con un servidor remoto de la DM. Esto podría ser especialmente útil si un EE es una tarjeta inteligente.

Mediante el anidamiento de los árboles de gestión (mediante el uso de los VMTs), la invención proporciona una solución más eficiente que la provisión a cada EE de un agente de la DM completamente independiente, dado que se requieren menos conexiones de servidor.

En una forma de realización de la invención, el terminal está provisto de una pluralidad de EEs, y es capaz de ejecutar un agente de la DM. No hay un MO para cada objeto gestionado (servicio o aplicación) en uno o más de los EEs. Sin embargo, dado que los protocolos de la DM son agnósticos respecto de los contenidos o valores de los MOs, un MO de un segundo EE (o efectivamente de un entero árbol de gestión para este EE) pueden ser manejados como un MO (virtual) en el árbol de gestión del primer EE. En otras palabras, el segundo EE es gestionado por medio de un VMT concreto dentro del árbol de gestión del primer EE.

Considérese el caso en el que el primer EE es un “área protegida” y el segundo EE es un “área no protegida”. Disponiendo que haya un árbol de gestión único (en el área protegida) y construyendo un Árbol de Gestión Virtual dentro de este árbol que está enlazado con el otro EE (el área no protegida), solo se necesita establecer un canal de comunicación, configuración, etc. Todos los MOs del sistema operativo situados dentro del área no protegida estarían agrupados dentro de un VMT y se situarían dentro del árbol de gestión del área de seguridad y, a continuación, quedarían dirigidos hasta el agente de la DM del otro sistema operativo existente en el otro EE.

La forma de realización expuesta parte de la base de que hay un EE de confianza (TEE) desde el cual pueden ser gestionados otros EEs. En un ejemplo, un EE de confianza puede ser responsable de la gestión tanto de sí mismo como de un OS complejo. En otro supuesto, cada OS dispuesto en el terminal puede situarse por encima de algún software de virtualización, el cual podría él mismo ser responsable de la gestión de todos los OSs (o de todos los EEs) situados por encima de él.

Así mismo, se contemplan otras disposiciones, por ejemplo una disposición en la que el primer EE sea el OS principal del dispositivo, y el segundo EE sea un TEE aislado del OS principal, donde el árbol de gestión del EE de confianza sea un VMT situado dentro del árbol de gestión del OS principal. Dicha disposición presenta la ventaja de que evita la necesidad de implementar protocolos de comunicaciones complejos dentro del área de confianza, manteniéndola lo más sencilla y segura posible. Dado que los niveles de confianza en el TEE son más elevados que en el OS principal, el árbol de gestión del TEE puede, entonces, ser protegido de manera independiente y autenticado (por ejemplo mediante la firma digital del MOs) antes de ser transformado en un VMT y suministrado por el servidor de la DM del OS principal al agente de la DM del OS principal.

En las formas de realización precedentes, cada EE adicional puede ser gestionado como un VMT dentro del árbol de gestión principal. En este caso, el cliente de la DM existente en el EE principal recibiría los VMTs para otros EEs. Estos VMTs podrían ser almacenados en el árbol de gestión principal (y el MEE podría adoptar las acciones de gestión apropiadas dentro de los EEs gestionados) o podrían ser transferidos directamente a los clientes de la DM de los EEs relevantes para su procesamiento.

Si un servidor de la DM desea gestionar un EE concreto, el VMT asociado con el EE puede ser actualizado dentro del árbol de gestión principal, y el agente de la DM principal pasaría entonces ese VMT al EE relevante para su procesamiento o para su tratamiento con las funciones de gestión mismas.

Como resultado de lo expuesto, el árbol de gestión principal es accesible por un servidor de la DM y el cliente de la DM principal comunica directamente con el servidor. Esto da respuesta a los problemas de duplicación de códigos y de configuración identificados con anterioridad.

Los EEs adicionales tienen que ser gestionados. La invención facilita la gestión eficiente de estos entornos a través del marco de la DM existente. El uso del marco de la DM existente significa, así mismo, que la interfaz es familiar tanto al operador de la red como al usuario de los dispositivos.

REIVINDICACIONES

1.- Un terminal de telecomunicaciones móvil que incorpora una plataforma de ejecución que incluye un primer entorno de ejecución y un segundo entorno de ejecución, estando cada entorno de ejecución dispuesto para la ejecución de un agente de gestión de dispositivos respectivo y emitiendo cada agente, de acuerdo con las instrucciones procedentes de un servidor de gestión de dispositivos, unas acciones de gestión que actúan sobre una o más entidades de gestión respectivas ejecutadas dentro de uno o más de los entornos de ejecución;

en el que las entidades de gestión del segundo entorno de ejecución están agrupadas en una estructura de gestión, siendo la estructura de gestión una de las entidades de gestión situadas dentro del primer entorno de ejecución,

por medio de lo cual el servidor de gestión de dispositivos está autorizado para gestionar aplicaciones y / o servicios ejecutados dentro tanto de los primero como de los segundos entornos de ejecución.

2.- Un terminal de acuerdo con la reivindicación 1, en el que el primer entorno de ejecución es un entorno de ejecución protegido.

3.- Un terminal de acuerdo con la reivindicación 1, en el que el primer entorno de ejecución es el sistema operativo principal del terminal.

4.- Un terminal de acuerdo con cualquiera de las reivindicaciones 1 a 3, en el que el segundo entorno de ejecución es un entorno de ejecución protegido.

5.- Un terminal de acuerdo con una cualquiera de las reivindicaciones precedentes, en el que el servidor de gestión de dispositivos, en funcionamiento, da instrucciones a al menos uno de los agentes de gestión de dispositivos respectivo para suministrar una acciones de gestión a una o más entidades de gestión.

6.- Un terminal de acuerdo con una cualquiera de las reivindicaciones precedentes, que incluye así mismo un medio para la recepción de unas acciones de gestión que proceden de un autor de acciones de gestión, en el que el medio de recepción opera para suministrar las acciones de gestión recibidas al servidor de gestión de dispositivos.

7.- Un terminal de acuerdo con una cualquiera de las reivindicaciones precedentes, en el que el primer entorno de ejecución es un servidor de gestión de dispositivos apoderado del agente de gestión de dispositivos del segundo entorno de ejecución,

8.- Un terminal de acuerdo con una cualquiera de las reivindicaciones precedentes, en el que al menos uno de los entornos de ejecución es implementado en un elemento protegido basado en hardware.

9.- Un terminal de acuerdo con una cualquiera de las reivindicaciones precedentes, en el que al menos uno de los entornos de ejecución es implementado en una tarjeta inteligente extraíble.

10.- Un procedimiento para procesar unas acciones de gestión recibidas de un servidor de gestión de dispositivos por un terminal, que comprende:

la provisión de una plataforma de ejecución que presenta un primer entorno de ejecución y un segundo entorno de ejecución;

en el primer entorno de ejecución, la ejecución de un primer agente de gestión de dispositivos, emitiendo el primer agente, de acuerdo con unas instrucciones procedentes de un servidor de gestión de dispositivos, unas acciones de gestión que actúan sobre una o más entidades de gestión respectivas ejecutadas dentro del primer entorno de ejecución;

en el segundo entorno de ejecución, la ejecución de un segundo agente de gestión de dispositivos, emitiendo el segundo agente, de acuerdo con unas instrucciones procedentes de un servidor de gestión de dispositivos, unas acciones de gestión que actúan sobre una o más entidades de gestión respectivas ejecutadas dentro del segundo entorno de ejecución;

en el que las entidades de gestión del segundo entorno de ejecución están agrupadas en una estructura de gestión, siendo la estructura de gestión una de las entidades de gestión situadas dentro del primer entorno de ejecución.

11.- Un procedimiento de acuerdo con la reivindicación 10, en el que el primer entorno de ejecución es un entorno de ejecución protegido.

12.- Un procedimiento de acuerdo con la reivindicación 10, en el que el primer entorno de ejecución es el sistema operativo principal del terminal.

13.- Un procedimiento de acuerdo con una cualquiera de las reivindicaciones 10 a 12, en el que el segundo entorno de ejecución es un entorno de ejecución protegido.

14.- Un procedimiento de acuerdo con una cualquiera de las reivindicaciones 10 a 13, que incluye así mismo la emisión de unas instrucciones para suministrar unas acciones de gestión a una o más entidades de gestión, siendo las instrucciones recibidas desde el servidor de gestión de dispositivos, a al menos uno de los agentes de gestión de dispositivos respectivos.

15.- Un procedimiento de acuerdo con una cualquiera de las reivindicaciones 10 a 14, que incluye así mismo la recepción de unas acciones de gestión que proceden de un autor de acciones de gestión original, y el suministro de las acciones de gestión recibidas al servidor de gestión de dispositivos.

16.- Un procedimiento de acuerdo con una cualquiera de las reivindicaciones 10 a 15, en el que el primer entorno de ejecución es un entorno de gestión de dispositivos apoderado para el agente de gestión de dispositivos del segundo entorno de ejecución.