(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 406 694**

(51) Int. CI.:

G06F 1/00 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **24.10.2001 E 01989290 (0)**

(97) Fecha y número de publicación de la concesión europea: **17.04.2013 EP 1352308**

(54) Título: **Procedimiento y aparato para la gestión de la configuración en un dispositivo informático**

(30) Prioridad:

26.10.2000 US 698526

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
07.06.2013

(73) Titular/es:

QUALCOMM INCORPORATED (100.0%)
5775 MOREHOUSE DRIVE
SAN DIEGO, CA 92121-1714, US

(72) Inventor/es:

VASSILOVSKI, DAN y
TONG, HENRY

(74) Agente/Representante:

CARPINTERO LÓPEZ, Mario

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

Procedimiento y aparato para la gestión de la configuración en un dispositivo informático

Antecedentes de la invención

I. Campo de la invención

El procedimiento y el aparato para la gestión de configuración se refiere, en general, al campo de la gestión de software y, más concretamente, a un procedimiento y a un aparato para proporcionar la gestión de la configuración de software utilizada para un dispositivo informático general.

II. Descripción de la técnica relacionada

En los modernos sistemas informáticos a menudo es importante gestionar de manera eficaz una configuración de software que se incorpora dentro de un sistema informático. Dichos sistemas informáticos incluyen no solo las computadoras tradicionales que se encuentran en negocios y domicilios sino, así mismo, una amplia variedad de dispositivos electrónicos, incluyendo teléfonos inalámbricos, computadoras portátiles, asistentes personales digitales (PDAs), dispositivos electrónicos automovilísticos, etc. Dichos sistemas informáticos algunas veces emplean procedimientos para asegurar la compatibilidad del software verificando una versión del software actual con la de una versión más novedosa de software a ser cargada. Sin embargo, estos procedimientos no intentan impedir una actualización de un software existente, o la introducción de un nuevo software, bajo determinadas condiciones.

Un ejemplo de una necesidad de gestionar y controlar el tipo de versión de software que debe ser cargada en un dispositivo informático, se puede encontrar en aplicaciones de seguridad para dichos dispositivos informáticos. Por ejemplo, en una organización gubernamental en la que a cada persona se le otorga un dispositivo de comunicación inalámbrico, la organización podría quedar segregada en diferentes niveles de seguridad. Si una persona que presenta un nivel de seguridad inferior fuera a adquirir un dispositivo de comunicación inalámbrico perteneciente a una persona que presenta un nivel de seguridad superior, esa persona podría tratar de cargar el software en el dispositivo de comunicación inalámbrico para que pudiera acceder a la información que en otro caso no estaría disponible para él. En otro aspecto de este ejemplo, sería conveniente cargar solo software autenticado en un dispositivo de comunicación inalámbrico una vez que el dispositivo de comunicación inalámbrico ha sido otorgado a una persona que presenta un elevado nivel de seguridad. El software autenticado se refiere al software que ha sido distribuido por una fuente “de confianza”, y que no ha sido alterado.

De esta manera, se necesita un procedimiento y un aparato para llevar a cabo la gestión de la configuración y el control del software utilizado en un dispositivo informático.

Así mismo, se reclama la atención sobre el documento EP 0706275, el cual proporciona un aparato y un procedimiento para asegurar la distribución de software, las actualizaciones del software, y los datos de la configuración. La criptografía se utiliza para proteger el software o las actualizaciones de los datos enviados a los productos informáticos o periféricos que utilizan canales de distribución no seguros. Los contenidos de los datos no pueden ser leídos por cualquiera que obtenga los datos, y los datos no serán aceptados a menos que sean modificados y procedan de una fuente válida para dichos datos.

Así mismo, se reclama la atención sobre el documento EP 0997807, el cual describe un procedimiento que implica la provisión de claves públicas y secretas para cada subsistema. El subsistema determina una instancia de certificación, un organismo oficial, para certificar la pertenencia de la clave a un subsistema con un certificado. Cada subsistema recibe un certificado clave y un certificado procedente del organismo de certificación. Cada persona implicada en la producción y verificación y comprobación del software de producto firma al pie el software de producto y redirige la firma actual con la clave secreta junto con el propio certificado clave de él / ella. El organismo de certificación genera una lista de comprobadores para cada usuario y la firma. La computadora de destino acepta y comprueba hasta el final el software de producto, la lista encadenada de firmas y la lista de certificados clave de participantes y la lista de comprobadores.

Finalmente, se reclama la atención sobre el documento WO 9815082, el cual describe un subsistema que impide modificaciones no autorizadas del código de programa BIOS incorporado en dispositivos de memoria no volátil modificables, como por ejemplo la memoria flash. Un coprocesador criptográfico que contiene el dispositivo de memoria BIOS lleva a cabo la autentificación y la validación sobre la actualización BIOS en base a un protocolo de clave público / privado. La autenticación se lleva a cabo mediante la verificación de la firma digital incorporada en la actualización BIOS.

Sumario de la invención

De acuerdo con la presente invención, se proporcionan un procedimiento y un aparato para la gestión de la configuración de un dispositivo informático, de acuerdo con lo definido en las reivindicaciones 1 y 9. Formas de realización de la invención se proporcionan en las reivindicaciones dependientes.

El problema de llevar a cabo la gestión de la configuración y el control del software utilizado en un dispositivo informático se resuelve, en una forma de realización, mediante un procedimiento para la gestión de la configuración del software, que comprende las etapas de la provisión de un software disponible a una interfaz asociada con un dispositivo informático, a continuación la determinación acerca de si el software residente almacenado en un área de almacenamiento de aplicación asociada con el dispositivo informático ha sido o no autenticado. Si el software residente no ha sido autenticado, el software disponible es cargado en un dispositivo informático. Si el software residente ha sido autenticado, el software disponible es cargado solo si ha también autenticado.

En otra forma de realización, el problema de llevar a cabo la gestión de la configuración y el control del software utilizado en un dispositivo informático se resuelve mediante un aparato para la gestión de la configuración de software, que comprende una interfaz para la provisión de un software disponible al dispositivo informático y un dispositivo de almacenamiento para almacenar el software residente y los datos. El aparato comprende así mismo, un procesador para la ejecución de un conjunto de instrucciones informáticas para la determinación acerca de si el software residente está o no autenticado. El procesador carga el software disponible si el software residente no ha sido autenticado. Si el software residente ha sido autenticado, el software disponible es cargado solo si también ha sido autenticado.

Breve descripción de los dibujos

Las características distintivas, los objetivos y las ventajas de la presente invención se pondrán con mayor facilidad de manifiesto a partir de la descripción detallada desarrollada en las líneas que siguen tomada en combinación con los dibujos, en los que:

la FIG. 1 ilustra un dispositivo informático en un formato de diagrama de bloques funcional; y

la FIG. 2 es un diagrama de flujo que ilustra una forma de realización del procedimiento para la provisión de la gestión de la configuración en un dispositivo informático.

Descripción de la forma de realización preferente

Se presenta un procedimiento y un aparato para la gestión de la configuración en un dispositivo informático. Debe entenderse que el procedimiento y el aparato divulgados pueden ser aplicados a una diversidad de dispositivos informáticos, incluyendo computadoras portátiles y de escritorio, computadoras personales, asistentes digitales personales (PDAs), dispositivos de comunicación cableados o inalámbricos que ofrecen servicios de comunicación de voz y / o datos, por nombrar unos pocos. En general, el procedimiento y el procedimiento divulgados pueden ser aplicados a cualquier dispositivo electrónico que requiera que un software lleve a cabo una tarea que se pretenda.

La FIG. 1 ilustra un dispositivo **100** informático en un formato de diagrama de bloques funcional. En una forma de realización, el dispositivo **100** informático comprende un procesador **102**, una interfaz **104**, un dispositivo **112** de almacenamiento que comprende un área **106** de almacenamiento de la aplicación, un área **108** de almacenamiento programable, y un área **110** de almacenamiento permanente. Debe entenderse que son posibles otras configuraciones, y que el procedimiento y el aparato descritos en la presente memoria podrían ser implementados en un número indeterminado de posibles configuraciones.

De acuerdo con lo expuesto con anterioridad, el dispositivo **100** informático comprende un dispositivo electrónico el cual requiere un software para llevar a cabo su tarea pretendida. En una forma de realización, el dispositivo **100** informático comprende un dispositivo de datos inalámbrico, como por ejemplo un teléfono inalámbrico que incorpora unas capacidades de datos para llevar a cabo dichas tareas como planificaciones de gestión, acceso a Internet, envío y recepción de correos electrónicos, etc. El análisis desarrollado a continuación describirá el procedimiento y el aparato para la provisión de la gestión de la configuración en un dispositivo informático con respecto a dicho dispositivo de comunicación inalámbrico. Debe entenderse que el procedimiento y el aparato para la provisión de la gestión de la configuración en un dispositivo informático podrían, así mismo, ser aplicados a cualquier dispositivo informático que utilizara software para llevar a cabo su función pretendida.

El procesador **102** comprende un procesador digital para la ejecución de uno o más conjuntos de instrucciones de software ejecutables en un dispositivo **112** de almacenamiento. En una forma de realización, el procesador **102** comprende un microprocesador digital como por ejemplo uno de la familia de procesadores 80 x 86 de Intel Corporation de Santa Clara, California. En otra forma de realización, el procesador **102** comprende un procesador digital de la señal (DSP), como por ejemplo la serie TMS320 de Texas Instruments Incorporated de Dallas, Texas. En otra forma de realización, el procesador **102** comprende un ASIC personalizado. Otras configuraciones conocidas en la técnica pueden ser utilizadas como alternativa.

El dispositivo **100** informático es inicialmente provisto de unas instrucciones informáticas ejecutables para hacer posible que se produzcan determinadas actividades principales, por ejemplo, justo después de que el dispositivo **100** informático es puesto en marcha. Estas instrucciones informáticas ejecutables son designadas en la presente memoria como un núcleo. El núcleo puede llevar a cabo una diversidad de autopruebas emitiendo instrucciones informáticas ejecutables almacenadas ya sea en el área **106** de almacenamiento de aplicaciones en el área **108** de almacenamiento programable o el núcleo puede ejecutar su propia serie de autopruebas. Así mismo, el núcleo

puede iniciar otros programas de software como por ejemplo un sistema operativo, como por ejemplo el Windows CE, utilizado para albergar otros programas de software. El núcleo, así mismo, comprende unas instrucciones informáticas ejecutables para proporcionar la gestión de la configuración del software cuando es cargado dentro del dispositivo **100** informático.

El dispositivo **100** informático puede, en general, ejecutar uno o más programas de software, ya sea de manera simultánea o en secuencia unos con otros. Por ejemplo, un programa de correo informático y un navegador de Internet podrían ser ejecutados de forma simultánea por el procesador **102**. Otros ejemplos de software que podrían ser operados mediante el dispositivo **100** informático incluyen un software de procesamiento de texto, un software de hoja de cálculo, un software de comunicación, un software de encriptación, etc.

En una forma de realización, un usuario que desea añadir un software al dispositivo **100** informático suministra el software al dispositivo **100** informático utilizando la interfaz **104**. El software que debe ser cargado se designa en la presente memoria como el software disponible. La interfaz **104** comprende un aparato para hacer posible la comunicación entre el dispositivo **100** informático y un dispositivo electrónico externo, como por ejemplo un segundo dispositivo informático. La interfaz **104** comprende una unidad de disco, un puerto paralelo, o un puerto serie, o cualquier otra interfaz electrónica que haga posible que el software sea cargado en el dispositivo **100** informático. En otra forma de realización, la interfaz **104** comprende un sistema de comunicación inalámbrico para recibir el software a través de las ondas.

Las instrucciones son dadas al procesador **102**, ya sea de manera automática por la presencia del software disponible en la interfaz **104**, o por el usuario que instruya de manera explícita al procesador **102** utilizando un dispositivo de E / S, como por ejemplo un teclado numérico y un dispositivo de representación, para cargar el software disponible procedente de la interfaz **104** en el dispositivo **106** de almacenamiento.

El procesador **102**, después de recibir instrucciones para la carga del software disponible en la interfaz **104**, puede de manera temporal aceptar el software y almacenarlo en el área **108** de almacenamiento programable dentro del dispositivo **112** de almacenamiento. El dispositivo **112** de almacenamiento comprende una o más memorias electrónicas para el almacenamiento de programas de software ejecutables y los datos de soporte. Más en concreto, el dispositivo **108** de almacenamiento programable comprende una memoria de acceso aleatorio (RAM), una RAM flash, una memoria de solo lectura programable eléctricamente borrable (EEPROM), u otra memoria electrónica borrable que sea conocida en la técnica. Si el dispositivo **112** de almacenamiento comprende más de un dispositivo de almacenamiento, se podrían utilizar diversas combinaciones de procedimientos técnicos para almacenar la información relacionada con la operación del dispositivo **100** informático.

En una forma de realización, el dispositivo **112** de almacenamiento está dividido en dos o más áreas de almacenamiento, designadas en la FIG. 1 como el área **106** de almacenamiento de aplicaciones, el área **108** de almacenamiento programable y el área **110** de almacenamiento permanente. El área **106** de almacenamiento de aplicaciones almacena programas de software, generalmente de forma ejecutable y datos asociados. El área **108** de almacenamiento programable almacena la información sobre una base temporal. Por ejemplo, los datos generados por el software a partir del área **106** de almacenamiento de aplicaciones pueden generar datos que van a ser utilizados por un operador del dispositivo informático y podrían ser almacenados en el área de almacenamiento programable. El área de almacenamiento programable podría, así mismo, ser utilizada para almacenar el software disponible de forma temporal hasta que los diversos procedimientos de autenticación hubieran sido completados. El software disponible almacenado en el área **108** de almacenamiento programable puede, a continuación, ser borrado o desplazado al área **106** de almacenamiento de las aplicaciones dependiendo de los resultados de los procesos de autenticación. El área **110** de almacenamiento permanente comprende un área de dispositivo **112** de almacenamiento donde se almacena el núcleo. Este área del dispositivo **112** de almacenamiento en general no es susceptible de ser alterada por el procesador **102**, a diferencia del área **106** de almacenamiento de aplicaciones y del área **108** de almacenamiento programable. Así mismo, el área **110** de almacenamiento permanente almacena “una bandera de autenticación”, la cual se analizará más adelante, en una forma de realización.

Después de la recepción de instrucciones para cargar el software disponible, ya sea a partir de la interfaz **104** o almacenada en el área **108** de almacenamiento programable, el procesador **102** determina si el software residente que corresponde al software disponible ha sido o no autenticado, en una forma de realización. En otra forma de realización, el procesador **102** determina si el software residente no relacionado con el software disponible ha sido autenticado. Por ejemplo, el procesador **102** determinaría si un software de sistema operativo ha sido autenticado antes de la carga de una aplicación, como por ejemplo un programa de encriptación o un programa de procesamiento de texto. El software residente se define en la presente memoria como un software que está almacenado en el dispositivo **112** de almacenamiento y es capaz de ser ejecutado por el procesador **102**.

La autenticación es una técnica sobradamente conocida para la verificación de que el software procedente de una “fuente de confianza” no ha sido alterado. El software de autenticación implica la agregación de un código de autenticación alfanumérico al software en el cual una “clave privada” del destinatario, o código privado, se utiliza para generar un código de autenticación alfanumérico. Cuando el software es recibido por el destinatario, en este caso el dispositivo **100** informático, el software puede ser autenticado por el dispositivo **102** informático llevando a cabo un procedimiento de autenticación en el código de autenticación. En una forma de realización, el procedimiento

de autenticación comprende la ejecución de una verificación de redundancia cíclica (CRC). En otra forma de realización, el procedimiento de autenticación comprende la ejecución de algoritmo de partición de seguridad (SHA). Ambos métodos son sobradamente conocidos en la técnica. Por supuesto, pueden ser utilizados otros procedimientos conocidos para autenticar el software incorporado al dispositivo **100** informático.

El proceso de autenticación puede contar con la ayuda de una "bandera de autenticación". Una bandera de autenticación es una indicación de que al menos una pieza de software autenticado ha sido cargado en el dispositivo **100** informático. En una forma de realización, la bandera de autenticación comprende una indicación dispuesta en el área **110** de almacenamiento permanente. Por ejemplo, cuando el software es cargado en el dispositivo **100** informático es, en primer lugar, verificado por el procesador **102** para determinar si está autenticado o no. Si el procesador **102** determina que el software está autenticado, la bandera de autenticación se incluye en el área **110** de almacenamiento permanente por el procesador **102**. Una vez que la bandera de autenticación se ha establecido, normalmente no se puede restablecer. Por tanto, una vez que la pieza de software autenticado ha sido cargada en el dispositivo **100** informático, cualquier software adicional que deba ser cargado en el dispositivo **100** informático tendrá que ser autenticado. De no ser así, será rechazado, de acuerdo con lo expuesto a continuación.

En otra forma de realización, la bandera de autenticación comprende un "fusible" hardware. Un fusible hardware es un dispositivo sobradamente conocido el cual, en términos generales, comprende un conductor capaz de ser destruido con una corriente eléctrica. En el supuesto actual, si el procesador **102** determina que una pieza del software autenticado ha sido cargada en el dispositivo **100** informático, el procesador **102** envía una señal para "instalar" el fusible hardware, esto es, para destruir el conductor relacionado con el fusible. Cuando el procesador **102** se presenta con el software disponible que va a ser cargado en el dispositivo **100** informático, el fusible es verificado para determinar si ha sido fundido con anterioridad o se ha incorporado. Si se ha incorporado, ello indica que al menos una pieza del software autenticado ha sido cargada en el dispositivo **100** informático, y que solo el software autenticado puede ser cargado en dispositivo **100** informático. Este procedimiento de determinación del estado de la autenticación del dispositivo **102** informático es ventajoso en el sentido de que el dispositivo **102** no tiene que llevar a cabo un procedimiento de autenticación en el software residente cada vez que el software está disponible para ser cargado en el dispositivo **100** informático.

En cualquier caso, la bandera de autenticación se puede incorporar en un número indeterminado de formas diferentes. En una forma de realización, la bandera de autenticación se incorpora únicamente si el software seleccionado de antemano es cargado en el dispositivo **100** informático y el software seleccionado de antemano es autenticado. En otra forma de realización, el software seleccionado de antemano no tiene que ser autenticado con el fin de que el procesador **102** incluya la bandera de autenticación. En otra forma de realización, la bandera de autenticación puede incorporarse de forma manual, generalmente por un técnico de la fábrica. En este caso, el dispositivo **100** informático es fabricado únicamente con la finalidad de recibir el software autenticado. La bandera de autenticación puede incorporarse por un técnico generalmente conectando una computadora a la interfaz **104** y ejecutando un programa informático que incorpore la bandera de autenticación.

En una forma de realización, el procesador **102** lleva a cabo la autenticación del software correspondiente al software disponible. El software correspondiente se refiere a una versión de emisión del mismo software. Por ejemplo, el software correspondiente al Microsoft Word 7.0 de Microsoft comprende el Microsoft Word 6.0 de Microsoft, el Microsoft Word 5.0 de Microsoft así como cualquier versión anteriormente emitida por Microsoft anterior a la versión 7.0. Si el software residente no ha sido autenticado, el procesador **102** carga el software disponible desde, o bien el área **108** de almacenamiento programable o bien desde la interfaz **104**, llegado el caso, hasta el área **106** de almacenamiento de aplicaciones. Si el software residente está autenticado, entonces el procesador **102** determina si el software disponible está o no autenticado. Si el software disponible está también autenticado, el procesador **102** carga el software disponible en el área **106** de almacenamiento de aplicaciones. Si el software disponible no está autenticado, el procesador **102** rechaza el software disponible y no se carga en el dispositivo **100** informático.

En otra forma de realización, el procesador **102** lleva a cabo la autenticación en un software no relacionado con el software disponible. En esta forma de realización, el software no relacionado generalmente controla las funciones importantes del dispositivo **100** informático. Por ejemplo, el software no relacionado comprende un software de sistema operativo almacenado en el dispositivo **106** de almacenamiento de aplicaciones. El software del sistema operativo puede ser verificado para su autenticación antes de que cualquier software disponible sea cargado en el dispositivo **100** informático. Si el software no relacionado no ha sido autenticado, el procesador **102** procede a cargar el software disponible en el área **106** de almacenamiento de aplicaciones. Esta forma de realización puede ser utilizada si una versión anterior del software disponible no está almacenada en el dispositivo **106** de almacenamiento de aplicaciones, o puede ser utilizada con independencia de si la versión anterior del software disponible ha sido ya o no cargada en el dispositivo **100** informático.

Si el software no relacionado no está autenticado, el procesador **102** carga el software disponible en el área **106** de almacenamiento de aplicaciones. Si el software no relacionado está autenticado, entonces el procesador **102** determina si el software disponible está o no autenticado. Si el software disponible no está autenticado, el procesador **102** rechaza el software disponible, y no es cargado en el dispositivo **100** informático. Si el software

disponible está autenticado, entonces el procesador **102** carga el software disponible en el área **106** de almacenamiento de aplicaciones.

En otra forma de realización adicional, el procesador **102** verifica si existe una versión anterior del software disponible y, así mismo, verifica el software no relacionado con el software disponible. En esta forma de realización, la autenticación se lleva a cabo tanto en la versión anterior del software disponible si está ya cargada en el dispositivo **100** informático como en el software no relacionado. El procesador **102** a continuación determinará si carga o no el software disponible en base a los resultados de las autenticaciones. Por ejemplo, si ambos programas de software no están autenticados, el procesador **102** generalmente cargará el software disponible en el área **106** de almacenamiento de aplicaciones. Si ambos programas de software están autenticados, entonces el procesador **102** generalmente rechazará el software disponible y no será cargado en el dispositivo **100** informático. Si uno y otro de los programas de software están autenticados, entonces el procesador **102** puede o puede no cargar el software disponible en el dispositivo **100** informático, en base a un procedimiento definido de antemano. Por ejemplo, si el software del sistema operativo está autenticado, pero el software relacionado no está autenticado, entonces el software disponible no será cargado a menos que esté también autenticado. En esta forma de realización, podría ser utilizada una bandera de autenticación separada para indicar el estado de autenticación de cada programa de software.

La FIG. 2 es un diagrama de flujo que ilustra una forma de realización del procedimiento para la gestión de la configuración en un dispositivo informático. En la etapa 2**00**, el software que debe ser cargado en el dispositivo **100** informático es suministrado al dispositivo **100** informático a través de la interfaz **104**. Este software se designa en la presente memoria como software disponible.

En la etapa **202** el procesador **102** determina si el software residente almacenado en el dispositivo **106** de almacenamiento de aplicaciones ha sido autenticado, utilizando una o más de las técnicas descritas con anterioridad. Si el software residente no está autenticado, el procesador, a continuación, determina si el software disponible está o no autenticado, tal y como se muestra en la etapa **204**. De nuevo, el procesador **102** lleva a cabo la autenticación en el software disponible de acuerdo con lo descrito con anterioridad. Si el software disponible está autenticado, se incorpora una bandera de autenticación en la etapa **206**. La bandera de autenticación es una indicación de que el dispositivo **100** informático puede solo aceptar software autenticado. Después de que se ha incorporado la bandera de autenticación el software disponible cargado en el dispositivo **100** informático, tal y como se muestra en la etapa 208. Si el software disponible está autenticado es cargado en el dispositivo **100** informático sin la incorporación de la bandera de autenticación, tal y como se muestra en la etapa **210**.

Si el software residente ha sido autenticado por el procesador **102** en la etapa **202,** el software disponible es verificado con respecto a su autenticación en la etapa **212**. Si el software disponible no está autenticado el procesador **102** rechaza el software disponible tal y como se muestra en la etapa **214,** y el software disponible no es cargado en el dispositivo **100** de procesamiento. Si el software disponible está autenticado, entonces el procesador **102** carga el software disponible en el dispositivo **100** informático, tal y como se muestra en la etapa **216**.

La descripción anterior de las formas de realización precedentes se ofrece para hacer posible que cualquier persona experta en la materia lleve a la práctica o utilice la presente invención. Las diversas modificaciones a estas formas de realización resultarán sin dificultad evidentes a los expertos en la materia, y los principios genéricos definidos en la presente memoria pueden ser aplicados a otras formas de realización sin el uso de la facultad inventiva. Por tanto, la presente invención no pretende quedar limitada a las formas de realización mostradas en la presente memoria, sino que se debe conceder el alcance más amplio coherente con los principios y las características distintivas novedosas de la presente memoria.

REIVINDICACIONES

1.- Un procedimiento de gestión de la configuración en un dispositivo (100) informático, que comprende las etapas de:

proporcionar (200) un software disponible a dicho dispositivo (100) informático por medio de una interfaz (104);

determinar (202) si el software residente almacenado en un dispositivo (112) de almacenamiento, asociado con dicho dispositivo (100) informático, está o no autenticado; y

cargar dicho software disponible en dicho dispositivo (112) de almacenamiento si dicho software residente no ha sido autenticado con éxito.

2.- El procedimiento de la reivindicación 1, que comprende así mismo las etapas de:

determinar (212) si dicho software disponible está o no autenticado;

rechazar (214) dicho software disponible si dicho software residente está autenticado y dicho software disponible no está autenticado; y

cargar (216) dicho software disponible si dicho software residente está autenticado y dicho software disponible está autenticado.

3.- El procedimiento de la reivindicación 1, en el que la etapa de determinar si dicho software residente está o no autenticado comprende las etapas de:

determinar si la bandera de autenticación ha sido o no incorporada;

en el que dicho software residente es determinado como que está autenticado si dicha bandera de autenticación ha sido incorporada; en otro caso

dicho software residente es determinado como que no está autenticado.

4.- El procedimiento de la reivindicación 3, en el que dicha bandera de autenticación es incorporada cuando el software autenticado ha sido cargado en dicho dispositivo (100) informático.

5.- El procedimiento de la reivindicación 3, en el que dicha bandera de autenticación es incorporada por un técnico de servicio.

6.- El procedimiento de la reivindicación 1, en el que la etapa de determinar si dicho software residente está o no autenticado, comprende la etapa de realizar un procedimiento de autenticación directo sobre dicho software residente.

7.- El procedimiento de la reivindicación 6, en el que dicho procedimiento de autenticación directo comprende la realización de una verificación de redundancia cíclica.

8.- El procedimiento de la reivindicación 6, en el que dicho procedimiento de autenticación directo comprende la realización de un algoritmo de partición de seguridad.

9.- Un aparato para la realización de la gestión de la configuración en un dispositivo (100) informático, que comprende:

una interfaz (104) para proporcionar un software disponible a dicho dispositivo (100) informático;

un dispositivo (112) de almacenamiento para almacenar el software residente y un conjunto de instrucciones informáticas ejecutables para determinar si el software residente está o no autenticado;

un procesador (102) para la ejecución de dicho conjunto de instrucciones informáticas ejecutables y para la carga de dicho software disponible si dicho software residente no ha sido autenticado con éxito.

10.- El aparato de la reivindicación 9, en el que:

dicho conjunto de instrucciones informáticas ejecutables está, además, destinado a determinar si dicho software disponible está o no autenticado;

dicho procesador (102) está, además, destinado a rechazar dicho software disponible si dicho software residente ha sido autenticado y dicho software disponible no está autenticado; y

dicho procesador (102) está, además, destinado a la carga de dicho software disponible si dicho software residente está autenticado y dicho software disponible está autenticado.

11.- El aparato de la reivindicación 9, en el que:

dicho dispositivo (112) de almacenamiento está, además, destinado al almacenamiento de una bandera de autenticación para indicar el estado de autenticación de dicho dispositivo (100) informático; y

dicho procesador (102) está, además, destinado a la determinación de si dicho software residente está autenticado en base a dicha bandera de autenticación.

12.- El aparato de la reivindicación 11, en el que dicha bandera de autenticación es incorporada cuando el software autenticado está cargado en dicho dispositivo (100) informático.

13.- El aparato de la reivindicación 11, en el que dicha bandera de autenticación es incorporada por un técnico de servicio.

14.- El aparato de la reivindicación 9, en el que dicho procesador (102) está, además, destinado a la realización de un procedimiento de autenticación directo sobre dicho software residente para determinar si dicho software residente está o no autenticado.

15.- El aparato de la reivindicación 14, en el que dicho procedimiento de autenticación directo, comprende la realización de una verificación de redundancia cíclica.

16.- El aparato de la reivindicación 14, en el que dicho procedimiento de autenticación directo, comprende la realización de un algoritmo de partición de seguridad.

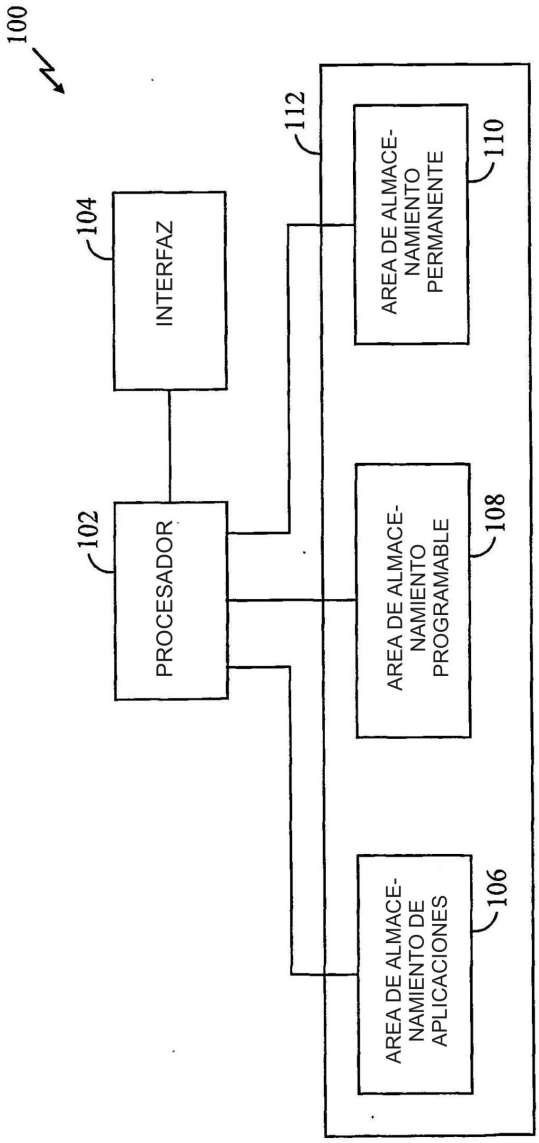
100
112
104
INTERFAZ
AREA DE ALMACE-NAMIENTO PERMANENTE
110
102
PROCESADOR
AREA DE ALMACE-NAMIENTO PROGRAMABLE
108
AREA DE ALMACE-NAMIENTO DE APLICACIONES
106

FIG. 1

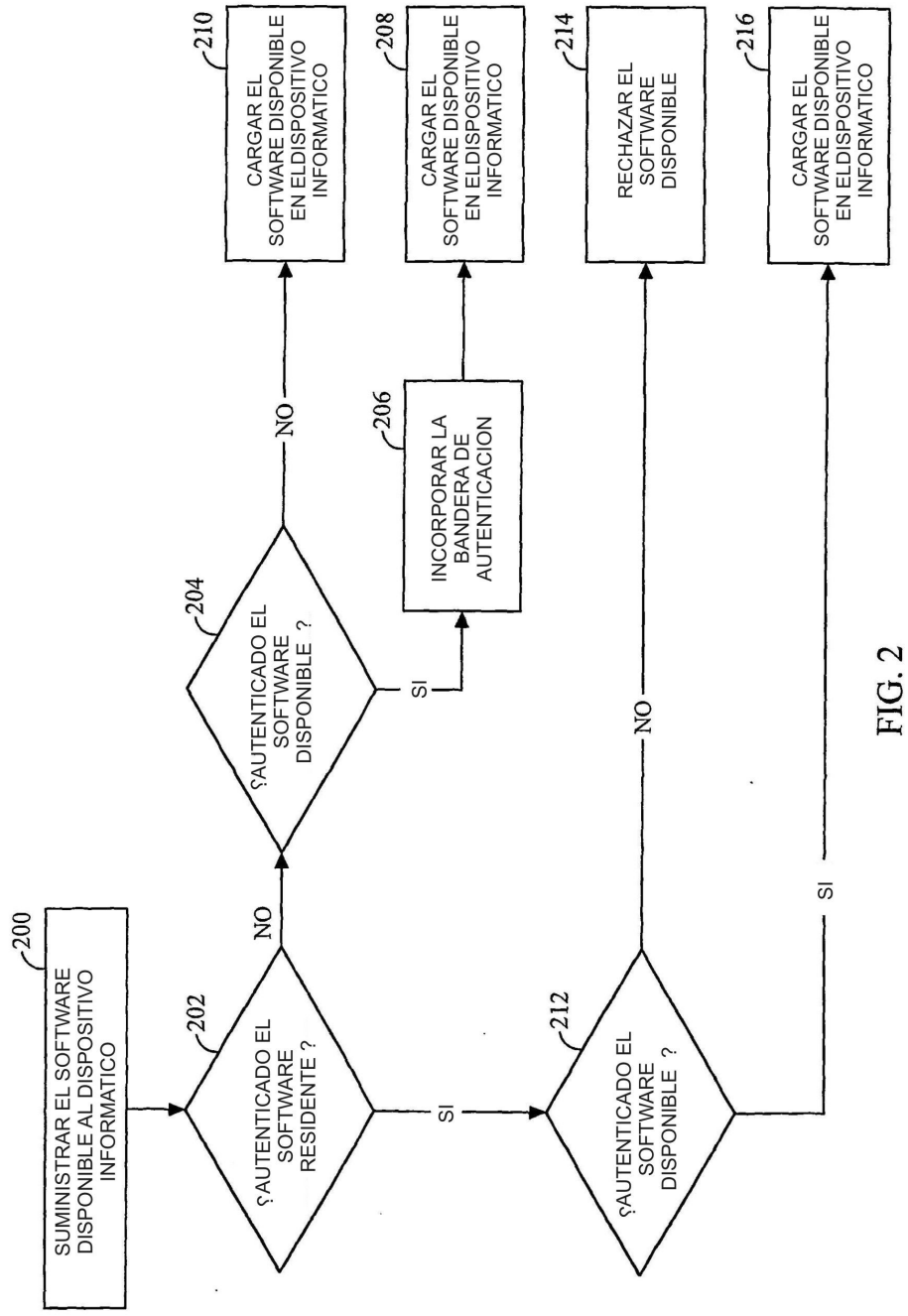
200
SUMINISTRAR EL SOFTWARE DISPONIBLE AL DISPOSITIVO INFORMATICO
202
¿AUTENTICADO EL SOFTWARE RESIDENTE ?
NO
SI
204
¿AUTENTICADO EL SOFTWARE DISPONIBLE ?
NO
SI
206
INCORPORAR LA BANDERA DE AUTENTICACION
208
CARGAR EL SOFTWARE DISPONIBLE EN EL DISPOSITIVO INFORMATICO
210
CARGAR EL SOFTWARE DISPONIBLE EN EL DISPOSITIVO INFORMATICO
212
¿AUTENTICADO EL SOFTWARE DISPONIBLE ?
NO
SI
214
RECHAZAR EL SOFTWARE DISPONIBLE
216
CARGAR EL SOFTWARE DISPONIBLE EN EL DISPOSITIVO INFORMATICO

FIG. 2