(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 415 832**

(51) Int. CI.:

G06F 9/445 (2006.01)
G06F 21/00 (2013.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **03.06.2010 E 10164806 (1)**

(97) Fecha y número de publicación de la concesión europea: **27.03.2013 EP 2393007**

(54) Título: **Dispositivo de procesamiento**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
29.07.2013

(73) Titular/es:

TELEFONAKTIEBOLAGET L M ERICSSON AB (PUBL) (100.0%)
164 83 Stockholm, SE

(72) Inventor/es:

SMEETS, BERNARD y
EKDAHL, PATRIK

(74) Agente/Representante:

DE ELZABURU MÁRQUEZ, Alberto

DESCRIPCIÓN

Dispositivo de procesamiento

CAMPO TÉCNICO

Se describe un dispositivo de procesamiento y un método correspondiente para llevar un dispositivo de procesamiento a un estado operativo predeterminado.

ANTECEDENTES

Los sistemas de procesamiento de datos tales como los ordenadores personales, los sistemas integrados como los teléfonos móviles u otros dispositivos móviles, y otros dispositivos de procesamiento de datos dependen de la ejecución de software correcto que no haya sido manipulado de manera no autorizada. La manipulación del software podría conducir a un comportamiento incorrecto del dispositivo o incluso a ruptura de las características de seguridad fundamentales del dispositivo. Por ello, es particularmente importante proteger el software central del dispositivo.

La operación de los sistemas de procesamiento de datos y similares puede verse perturbada mediante software malicioso tal como programas de virus y troyanos. Una forma de proteger tales dispositivos de usuario frente a estos tipos de amenazas consiste en desplegar programas de antivirus y de seguridad Internet tales como los ofrecidos por compañías como Symantec, F-Secure y E-set. Con el paso de los años, estas herramientas de protección han resultado ser muy eficaces para bloquear amenazas conocidas (y similares). Mediante el uso de tecnologías de Sistema de Detección de Intrusión en estas herramientas, es también posible impedir muchos otros ataques sobre los dispositivos de usuario. Otra alternativa de atacar el software malicioso consiste en mantener lo que se conoce como “ruta de acceso de software de confianza”. En este caso, la idea básica consiste en que todo el software que se ejecuta en un dispositivo sea auténtico (y con la esperanza de que no sea perjudicial). La autenticidad del software se entiende en el sentido de que tiene un arranque de seguridad que garantiza que el sistema (básico) que está cargado en el dispositivo del usuario es auténtico, y que el sistema tiene entonces que cargar solamente el software que es auténtico, lo que puede ser reforzado con el uso de signaturas digitales que se puede necesitar que cada software lleve a cabo. Un estándar industrial para realizar arranque de seguridad ha sido definido por el Trusted Computing Group (TCG), véase por ejemplo la “Especificación TCG, Visión General de la Arquitectura”, Specification, Revisión 1.4, Agosto de 2007.

Aún más, sigue existiendo el problema de que, a pesar de las medidas anteriores, pueden aún tener éxito algunos ataques y afectar al funcionamiento de un dispositivo de usuario.

El TCG ha desarrollado un mecanismo seguro conocido como atestación, mediante el que un sistema observador externo (servidor) puede interrogar el estado del motor de seguridad central, mencionado como Módulo de Plataforma de Confianza (TPM), por ejemplo como se describe en la “Especificación TCG, Visión General de la Arquitectura” (ibid.) y en la “Especificación Principal TPM Nivel 2 Versión 1.2, Revisión 103”. Este proceso se conoce como atestación remota, e incluye que el servidor reciba un valor firmado de estado de registro de TPM PCR. Esto permite al servidor remoto seguir el rastro de, por ejemplo, el software que se cargó en el dispositivo de usuario. Sin embargo, la atestación remota de la técnica anterior mencionada anteriormente, no proporciona una forma segura para que el servidor o cualquier sistema de gestión de dispositivo de usuario decida y ejecute correctamente un re-arranque (reinicio) del dispositivo de usuario en caso de que un dispositivo de usuario sea infectado por software malicioso.

El software de detección de virus y de IDS no puede impedir por completo que el software malicioso alcance un dispositivo de usuario. El uso de software firmado puede ser ejecutado para los componentes estándar de un sistema (como software de arranque y módulos de software de OS). Para controladores de dispositivos, un cumplimiento estricto es más problemático debido a que ello implica, por ejemplo, que los desarrolladores de tarjetas gráficas deben obtener sus controladores de dispositivo firmados por el proveedor del OS o por el proveedor del dispositivo de usuario. Para software de aplicación, la metodología de software firmado se considera con frecuencia que es demasiado restrictiva para los desarrolladores de la aplicación. Por lo tanto, no se usa con frecuencia una cadena de software de confianza (signaturas) y se usa en su lugar una interacción de usuario mediante la que se solicita al usuario que proporcione su aceptación de este software que va a ser instalado en el dispositivo. Tal propuesta se utiliza, por ejemplo, en el sistema Android para dispositivos móviles. De ese modo, incluso en presencia de soluciones de arranque seguro tal como la que define el TCG, sigue existiendo la necesidad de una protección mejorada frente al software malicioso.

La función de atestación remota según se ha descrito por TCG, puede ser usada por un sistema de gestión de dispositivo para observar el dispositivo y para concluir que el dispositivo está infectado. Sin embargo, esto implica que la parte confiable del dispositivo de usuario esté capacitada para observar su funcionamiento completo, es decir, esté capacitada para tomar la decisión de que está infectada. Sin embargo, si ocurre tal infección, ha sido el software de protección del dispositivo el que ha fallado realmente en cuanto a bloquear el software malicioso.

En términos de TCG, existe un problema adicional dado que el núcleo de los mecanismos de protección está construido en torno al TPM que es un módulo de hardware resistente a las manipulaciones que está capacitado para mantener secretos y variables de estado de forma segura. Sin embargo, el TPM es un dispositivo esclavo, es decir, que actúa cuando recibe instrucciones de que lo haga. Con ello, el cálculo realizado por el TPM es inducido por el software del dispositivo de usuario, es decir, en caso de una infección, el cálculo realizado por el TPM está inducido por una entidad infectada. En consecuencia, cuando llega una petición de atestación remota, el software malicioso puede poner de nuevo el dispositivo en un estado aparentemente correcto, ocultarse en sí mismo, e iniciar el proceso de petición de atestación. Cuando la respuesta de la atestación ha finalizado, el software malicioso puede tomar de nuevo el control. Mientras tanto, el sistema de gestión obtiene todavía las indicaciones procedentes del dispositivo de que todo está ok, aunque el sistema de gestión pueda tener indicación procedente de otras observaciones en el sentido de que hay algo erróneo en cuanto a las operaciones del dispositivo.

El documento US7360253 describe un método de estimulación de un estado operativo conocido en un ordenador. El ordenador incluye un circuito de vigilancia y ejecuta un sistema de monitorización. El circuito de vigilancia incluye un temporizador, y tras la expiración del temporizador, el ordenador es arrancado de nuevo a menos que el sistema de monitorización envíe un mensaje al circuito de vigilancia que provoque un reinicio del temporizador.

Sin embargo, sigue existiendo el problema de que la seguridad del método de la técnica anterior mencionado en lo que antecede dependa del sistema de monitorización. Con ello, si el sistema de monitorización es atacado, la seguridad del método puede verse comprometida.

Un método similar se conoce a partir del documento US 2006/143446.

SUMARIO

En la presente memoria se describe un dispositivo de procesamiento que comprende:

- un entorno de ejecución segura, que comprende medios para llevar el dispositivo de procesamiento a un estado operativo predeterminado; y un temporizador;
- una interfaz de comunicación para comunicación de datos entre el dispositivo de procesamiento y un sistema de gestión de dispositivo remoto, externo al dispositivo de procesamiento;

en donde el entorno de ejecución segura está configurado

- en respuesta a la expiración del temporizador, para llevar el dispositivo de procesamiento a dicho estado operativo predeterminado;
- en respuesta a una recepción, procedente del sistema de gestión de dispositivo remoto a través de dicha interfaz de comunicación, de una señal de activación, para reiniciar el temporizador.

Con ello, las realizaciones del dispositivo de procesamiento descritas en la presente memoria proporcionan un mecanismo eficiente, fácilmente implementable, para imponer que el dispositivo de procesamiento sea llevado a un estado operativo predeterminado, por ejemplo un estado que cause una nueva carga del software auténtico inicial, y de ese modo la reanudación del funcionamiento normal de un dispositivo de usuario infectado que está bajo el control de un sistema gestionado (tal como los teléfonos móviles en una red de operadores o los ordenadores de sobremesa/PCs en una red corporativa).

Con la provisión de un sistema de gestión de dispositivo remoto y un temporizador en un entorno seguro, de confianza, la seguridad del mecanismo de monitorización y de re-arranque no se basa exclusivamente en entidades que están incluidas en el dispositivo, y por tanto sujetas a ataques maliciosos.

Puesto que software que lleva a cabo la determinación de si el dispositivo está infectado reside en el sistema de gestión de dispositivo, la complejidad del software en el entorno de ejecución confiable puede mantenerse baja, facilitando de ese modo el mantenimiento de la confianza en el entorno de ejecución confiable.

El término “entorno de ejecución segura” según se utiliza en la presente memoria está previsto que comprenda cualquier medio adecuado para ejecutar un código de programa en el dispositivo de procesamiento, en donde el código de programa está protegido del resto del software ejecutado en el dispositivo de procesamiento con el fin de impedir que el otro software lea y/o modifique datos y/o el código de programa en el entorno de ejecución segura. El entorno de ejecución segura, a los efectos de la presente descripción, mencionado también como Entorno de Ejecución de Confianza (TEE), puede estar protegido frente a alteraciones mediante cualquier mecanismo de protección adecuado. El TEE puede estar implementado a modo de módulo de software, a modo de módulo de hardware, o como una combinación de los mismos. Por ejemplo, el TEE puede estar implementado como módulo de plataforma de confianza incrementada (TPM, véase por ejemplo la Especificación Principal TPM Nivel 2 Versión 1.2, Revisión 103), configurado también de modo que proporcione funcionalidad para imponer un re-arranque del dispositivo de procesamiento, para mantener un contador programable, donde el contador actúa en respuesta a la recepción de una señal de activación externa. Alternativamente, el TEE puede ser materializado como una

combinación de un TPM estándar y una arquitectura de hardware de seguridad adecuada tal como el hardware ARM TrustZone®, por ejemplo según se describe en el sitio web http://arm.com/products/processors/technologies/trustzone.php, u otra arquitectura de hardware adecuada. También alternativamente, el entorno de ejecución segura puede estar materializado como un ambiente seguro TrustZone configurado además para que incluya uno o más temporizadores y uno o más interruptores.

En general, el valor de temporizador del temporizador puede ser reiniciado a partir de cualquier valor adecuado, por ejemplo el mismo valor que para un reinicio previo del temporizador, o un nuevo valor establecido, es decir el reinicio del temporizador puede incluir el ajuste del temporizador a un nuevo valor. Se apreciará que la elección del valor del temporizador puede ser determinado mediante un número de factores. Por ejemplo, valores de temporizador más cortos dan como resultado un tráfico de datos incrementado, puesto que las señales activadoras tendrán que ser comunicadas y procesadas de manera más frecuente. Valores de temporizador más largos permiten más tiempo para que el sistema de gestión de dispositivo (DMS) detecte posibles irregularidades en el comportamiento del dispositivo de usuario; por otra parte, los valores de temporizador más grandes incrementan el período de tiempo durante el que un dispositivo de usuario infectado puede operar de una manera no autorizada sin que tenga que ejecutarse un re-arranque. En algunas realizaciones, el valor de temporizador puede ser elegido entre varias horas y varios días; sin embargo, se pueden elegir igualmente intervalos de tiempo más cortos y/o más largos. En algunas realizaciones, el DMS puede determinar un valor de temporizador adecuado para el siguiente intervalo de temporizador cuando envíe una señal activadora. Por ejemplo, los valores de temporizador pueden ser determinados en base a situaciones de amenaza conocida, al comportamiento previo del dispositivo de usuario, y/o a otros factores. El nuevo valor de temporizador determinado puede ser comunicado a continuación al dispositivo de usuario, por ejemplo como parte de la señal activadora. La señal activadora puede adoptar la forma de un comando go-ahead que puede incluir un valor de temporizador.

En algunas realizaciones, llevar al dispositivo de procesamiento a un estado operativo predeterminado comprende hacer que el dispositivo de procesamiento re-arranque. Por ello, en algunas realizaciones el TEE está configurado para ejecutar un arranque seguro e incluye interrupciones del temporizador inmutables.

El sistema de gestión de dispositivo remoto (DMS) puede estar configurado para llevar a cabo actualizaciones de software y/u otras operaciones de gestión de dispositivo con respecto al dispositivo de procesamiento. En algunas realizaciones, el DMS está configurado para recopilar información indicativa del estado operativo del dispositivo de procesamiento. En algunas realizaciones, el DMS puede estar configurado para recibir tal información desde el dispositivo de procesamiento, por ejemplo por medio de un mecanismo de atestación remoto adecuado. Por consiguiente, el dispositivo de procesamiento puede estar adaptado para transmitir, vía interfaz de comunicaciones, un mensaje indicativo del estado operativo al sistema de gestión de dispositivo remoto, por ejemplo en forma de mensajes de atestación remotos tal como respuestas de atestación remotas en respuesta a la recepción de peticiones de atestación remotas procedentes del DMS. Un mensaje indicativo del estado operativo del dispositivo de procesamiento puede incluir uno o más valores de uno o más registros predeterminados del dispositivo de procesamiento. Adicional o alternativamente, el DMS puede estar configurado para recibir la información indicativa del estado operativo del dispositivo de procesamiento en forma de observaciones de conducta, por ejemplo mediante observación del tráfico de datos entrante y/o saliente en la interfaz de comunicaciones. Por ejemplo, el DMS puede operar a modo de sistema de detección de intrusión de red (NIDS).

En algunas realizaciones el entorno de ejecución segura está configurado, por ejemplo programado adecuadamente, para llevar a cabo un reinicio en frío del dispositivo de procesamiento y cargar una imagen de software firmada digitalmente si el entorno de ejecución segura no recibe un mensaje predeterminado (mencionado también en lo que sigue como pasaje de “go-ahead”) procedente del DMS antes de un límite de tiempo establecido predeterminado. Si llega el pasaje, el temporizador es reiniciado y continúa el funcionamiento normal del dispositivo. Si llega un pasaje que no es correcto, entonces ocurre el reinicio en frío y el dispositivo re-arrancará y cargará la imagen de software firmada. La imagen de software firmada puede comprender código de programa adaptado para proporcionar funcionalidad de comunicación que permita al DMS comunicar con el dispositivo. En consecuencia, el DMS puede realizar una interrogación del dispositivo que permita que el DMS confirme que se ha producido un re-arranque y que la imagen de software firmada ha sido cargada. Con ello, se impide que el dispositivo simplemente ignore el comando de reinicio o que simule que hace el reinicio sin que el DMS detecte el fallo para realizar realmente un arranque.

A continuación, el DMS puede emprender acciones subsiguientes, tal como provocar que el dispositivo cargue otros módulos de software (desde el DMS o desde el almacenaje del propio dispositivo) y/o utilice una atestación remota para comprobar que se ha alcanzado adecuadamente el siguiente estado de operación antes de enviar comandos adicionales. De ese modo, el DMS puede restaurar el dispositivo de procesamiento y eliminar cualquier software malicioso que hubiera infectado el dispositivo de procesamiento.

El término dispositivo de procesamiento de datos se ha previsto que comprenda cualquier ordenador, tal como ordenador personal, equipo portátil de comunicaciones de radio, y otros dispositivos de procesamiento de datos manuales o portátiles. El término equipo portátil de comunicaciones de radio incluye todo el equipamiento tal como

teléfonos móviles, localizadores, comunicadores, organizadores electrónicos, teléfonos inteligentes, asistentes digitales personales (PDAs), ordenadores portátiles, ordenadores de sobremesa, o similares.

La presente invención se refiere a aspectos diferentes incluyendo el dispositivo de procesamiento descrito en lo que antecede y en lo que sigue, métodos, sistemas y productos correspondientes, produciendo cada uno de ellos uno o más de los beneficios y ventajas que se describen en relación con uno de los dispositivos de procesamiento anteriormente mencionados, y teniendo cada uno de ellos una o más realizaciones correspondientes a las realizaciones descritas en relación con uno de los dispositivos de procesamiento mencionados con anterioridad.

De manera más específica, de acuerdo con otro aspecto, se describe un sistema de gestión de dispositivo para controlar el funcionamiento de un dispositivo de procesamiento remoto externo al dispositivo de procesamiento, comprendiendo el dispositivo de procesamiento remoto un entorno de ejecución segura que comprende un temporizador y medios para llevar al dispositivo de procesamiento a un estado operativo predeterminado. Las realizaciones del sistema de gestión de dispositivo comprenden:

una interfaz de comunicaciones para comunicación de datos entre el sistema de gestión de dispositivo y el dispositivo de procesamiento remoto;

medios de procesamiento configurados para:

- determinar un estado operativo del dispositivo de procesamiento remoto
- en respuesta al estado operativo determinado, enviar una señal activadora al dispositivo de procesamiento a través de la interfaz de comunicaciones para provocar que el dispositivo de procesamiento reinicie el temporizador.

Según otro aspecto más, un sistema de comunicaciones puede comprender un dispositivo de procesamiento según se describe en la presente memoria, y un sistema de gestión de dispositivo descrito en la presente memoria.

Según otro aspecto adicional, se describe un método de control de operación de un dispositivo de procesamiento mediante un sistema de gestión de dispositivo remoto externo al dispositivo de procesamiento, comprendiendo el dispositivo de procesamiento en entorno de ejecución segura que comprende un temporizador y medios para llevar el dispositivo de procesamiento a un estado operativo predeterminado. Las realizaciones del método comprenden:

- en respuesta a la expiración del temporizador, llevar el dispositivo de procesamiento a dicho estado operativo predeterminado;
- en respuesta a una recepción, procedente del sistema de gestión de dispositivo remoto a través de una interfaz de comunicaciones del dispositivo de procesamiento, de una señal activadora, reiniciar el temporizador.

Según otro aspecto más, se describe en la presente memoria un entorno de ejecución segura para un dispositivo de procesamiento. Las realizaciones del entorno de ejecución segura comprenden un temporizador y medios para llevar el dispositivo de procesamiento a un estado operativo predeterminado; y están configurados para realizar las etapas del método descrito en la presente memoria.

BREVE DESCRIPCIÓN DE LOS DIBUJOS

Los aspectos anteriores y otros aspectos, resultarán evidentes y claros a partir de las realizaciones descritas en lo que sigue con referencia a los dibujos en los que:

La Figura 1 muestra un diagrama esquemático de bloques de un sistema para establecer un estado operativo conocido de un dispositivo de procesamiento de datos;
La Figura 2 ilustra esquemáticamente un ejemplo de un sistema de gestión de dispositivo y de un dispositivo de procesamiento;
La Figura 3 ilustra un ejemplo del flujo de mensaje entre un sistema de gestión de dispositivo, un entorno de ejecución normal y un entorno de ejecución de confianza con anterioridad a que expire un temporizador de reinicio y durante el reinicio de un dispositivo de procesamiento;
La Figura 4 ilustra con mayor detalle la comunicación de un ejemplo de comando de go-ahead;
La Figura 5 muestra un ejemplo de flujo de mensaje entre un sistema de gestión de dispositivo, un entorno de ejecución normal y un entorno de ejecución de confianza durante un proceso de recuperación.

DESCRIPCIÓN DETALLADA

La Figura 1 muestra un diagrama esquemático de bloques de un sistema para establecer un estado operativo conocido de un dispositivo de procesamiento de datos.

El sistema comprende un dispositivo de procesamiento 101 (mencionado también en lo que sigue como dispositivo de usuario o UD), tal como un teléfono móvil, un módem, un ordenador de sobremesa, un ordenador personal, un

PDA, o cualquier otro dispositivo de procesamiento operado por el usuario que esté gestionado y/o controlado por un sistema 102 de gestión de dispositivo (DMS). A este efecto, el dispositivo de procesamiento 101 está conectado por medio de una red 105 de comunicaciones al sistema 102 de gestión de dispositivo. En el ejemplo de la Figura 1, el DMS ha sido mostrado como una entidad simple, por ejemplo un nodo de red de la red 105 de comunicaciones, un ordenador servidor, y/o similar. Se apreciará, no obstante, que el DMS puede estar implementado por una pluralidad de entidades físicas, por ejemplo un conjunto corporativo de nodos, que implementen conjuntamente las funciones de DMS. El dispositivo de procesamiento 101 comprende un bloque 103 de hardware, un entorno 106 de ejecución normal (NEE) y un entorno 107 de ejecución de confianza (TEE), ambos implementados por el bloque 103 de hardware. El bloque de hardware puede comprender una unidad central de proceso (CPU), un sistema de memoria, un conjunto de funciones de re-arranque/reinicio, uno o más interruptores de hardware y/o temporizadores, una o más unidades de protección de memoria MMUs o MPUs, y/o componentes similares de hardware.

El entorno de ejecución normal (NEE) está configurado para ejecutar el sistema operativo (OS) del dispositivo de procesamiento y uno o más programas de aplicación. El entorno de ejecución de confianza (TEE) está configurado de modo que sea inmutable por el NEE, y está configurado para ejecutar un conjunto de componentes de software de confianza. El TEE tiene uno o más temporizadores 117 seguros, e interruptores que el software del NEE no puede modificar o influir. Un ejemplo de hardware de procesamiento que implementa un entorno de ejecución normal y de confianza es el sistema TrustZone de ARM. Alternativamente, el NEE y/o el TEE pueden estar implementados por medio de cualquier otra combinación adecuada de hardware y de software, por ejemplo mediante una unidad de protección de memoria adecuada. El dispositivo de procesamiento 101 comprende una interfaz 104 de comunicaciones que comprenden circuitos y/o dispositivos adecuados para permitir que el dispositivo de procesamiento comunique datos con el DMS a través de una red de comunicaciones alámbrica o inalámbrica, por ejemplo una red celular de telecomunicaciones, por ejemplo WCDMA GSM, o similar, una red de área local alámbrica o inalámbrica, una red de área amplia, Internet, etc., o una combinación de las mismas. En consecuencia, los ejemplos de interfaces de comunicaciones adecuadas incluyen una interfaz de RF, tal como la antena principal de un teléfono celular (no mostrado), u otra antena dentro del teléfono celular, tal como un transceptor Bluetooth, o similar. Otros ejemplos de interfaces adecuadas incluyen un módem por cable, un módem telefónico, un adaptador de Red Digital de Servicios Integrados (ISDN), un adaptador de Línea de Abonado Digital (DSL), un transceptor por satélite, un adaptador Ethernet, o similar. En algunas realizaciones, la comunicación entre el DMS y el UD puede ser llevada a cabo a través de la capa de señalización de una interfaz de radio. En otras realizaciones, la comunicación puede ser llevada a cabo vía Internet.

La Figura 2 ilustra esquemáticamente un ejemplo de un sistema 202 de gestión de dispositivo (DMS) y un dispositivo de procesamiento 201 (UD), por ejemplo el DMS y el dispositivo de procesamiento descritos en relación con la Figura 1.

El DMS 202 mantiene un registro para cada dispositivo o grupo de dispositivos gestionados por el DMS. En el ejemplo de la Figura 2, el DMS ha sido ilustrado de modo que mantiene tres registros 208a-c correspondientes a tres dispositivos o grupos respectivos de dispositivos, de los que solamente uno ha sido mostrado explícitamente en la Figura 2. Sin embargo, se apreciará que el número de registros mantenidos por un DMS depende del número de dispositivos o de grupos de dispositivos gestionados por el DMS, y que este número puede variar. Los registros 208a-c pueden estar almacenados en el DMS de cualquier forma adecuada, por ejemplo en un dispositivo de almacenamiento de datos adecuado tal como un disco duro. En el ejemplo de la Figura 2, los registros incluyen el registro 208a asociado al UD 201. El registro 208a comprende datos indicativos de la identidad del dispositivo (UDI), un indicador de OK del dispositivo (DOK), y una clave pública (PuUDK) asociada al dispositivo o grupo de dispositivos. Opcionalmente, el registro 208a puede comprender además el valor de un temporizador de reinicio programado (RBT), permitiendo así que los valores de temporizador específicos del dispositivo o que los valores uniformes de temporizador puedan cambiar con el tiempo. El UDI puede ser un ID de dispositivo que identifique unívocamente al dispositivo o grupo de dispositivos. La clave pública puede ser una clave pública de cualquier método adecuado criptográfico asimétrico que sea apropiado para asegurar autenticidad y/o ocultamiento. Un proceso de autenticación criptográfica adecuado puede ser cualquier proceso criptográfico adecuado para verificar la autenticidad de los datos, es decir, asegurar que los datos se originan de hecho desde la entidad esperada y que no se han falsificado o modificado.

El DMS tiene además almacenada en el mismo, por ejemplo en un entorno de confianza del DMA, una clave secreta de gestión de dispositivo SDMK. La SDMK puede ser una clave privada conocida solamente por el DMS y almacenada de modo seguro por el DMS. En el ejemplo de la Figura 2, el DMS mantiene solamente una única SDMK; sin embargo, en realizaciones alternativas, el DMS puede mantener, por ejemplo almacenadas como parte de los registros 208a-c, diferentes SDMKs asociadas a dispositivos o grupos de dispositivos respectivos. La SDMK puede ser una clave privada o cualquier sistema criptográfico adecuado para proteger la autenticidad de los mensajes, en comandos particulares, enviados por el DMS al UD. Alternativa o adicionalmente, los comandos de DMS al UD pueden estar protegidos mediante otros métodos de protección adecuados, por ejemplo los usados en OMA DM.

Según se ha descrito en lo que antecede, el UD comprende un entorno 207 de ejecución de confianza (TEE) y un

entorno 206 de ejecución normal (NEE). El TEE 207 está programado con una clave pública de gestión de dispositivo (PuDMK) correspondiente a la SDMK del DMS, es decir, tal que la SDMK y la PuDMK forman un par de claves pública-privada de un sistema criptográfico, por ejemplo un PKI. El TEE 207 está además programado con una clave secreta de dispositivo de usuario (SUDK) y con una identidad de dispositivo de usuario UDI. El TEE comprende además un temporizador de reinicio programado (RBT) y un par de claves de dispositivo de usuario privada-pública, es decir, una clave pública de dispositivo de usuario (PuUDK) y una clave privada de dispositivo de usuario (SUDK) correspondiente. El TEE constituye un entono de confianza, confiable por el DMS para que sea inalterable mediante por ejemplo el NEE.

El NEE 206 está configurado para ejecutar el software operativo normal, por ejemplo incluyendo un software de sistema operativo (OS) y de aplicación. El software operativo comprende una porción firmada, mencionada en lo que sigue también como el sistema base de dispositivo de usuario (UDBS), que puede ser reiniciado independientemente de otras porciones, si las hay, del software operativo, y que está configurado para permitir comunicación de datos con el DMS a través de la interfaz 104 de comunicaciones. El UDBS está firmado y puede ser verificado respecto a la clave pública de dispositivo de usuario PuUDK. Alternativamente, el UDBS puede ser una imagen de software separada, firmada, separada del software operativo normal, que puede ser arrancado independientemente del software operativo normal. Por ejemplo, el UDBS puede ser un código ROM incluido en el, o separado del, TEE. También alternativamente, la autenticidad del UDBS puede ser verificable por el TEE usando otro mecanismo criptográfico adecuado. El NEE comprende además un BootLoader (gestor de arranque) para controlar las fases iniciales del proceso de arranque y para cargar el UDBS en la memoria con anterioridad a la ejecución. Cuando han arrancado, a través del TEE tras un reinicio en frío (activado por la expiración del RBT), los servicios proporcionados por el UDBS constituyen servicios de confianza (desde la perspectiva del DMS). El UDBS proporciona funcionalidad para restaurar el software del UD a un estado que puede ser fiable. Dependiendo de la complejidad del software de UD y de la necesidad de recuperación, el UDBS puede llevar a cabo esta restauración por sí mismo o en cooperación con el DMS (por ejemplo, descarga de software original). El DMS puede interrogar el UD pidiendo una operación de atestación remota del estado del TEE que mantenga el rastro sobre el software que ha sido arrancado/iniciado.

La Figura 3 ilustra un ejemplo del flujo de mensaje entre el DMS 302, el NEE 306 y el TEE 307 antes de que expire el RBT y durante el reinicio del UD. Cada vez que el TEE recibe un comando “go-ahead” predeterminado desde el DMS, el TEE reinicia y opcionalmente ajusta el temporizador de reinicio. El comando 310 de “go-head” es enviado desde el DMS hasta el UD donde es recibido por el NEE y reenviado por el software del NEE hasta el TEE según se ha ilustrado mediante la flecha 311, provocando de ese modo que el TEE ajuste/reinicie el temporizador de reinicio. El TEE puede restablecer el temporizador de reinicio a partir de un valor de temporizador predeterminado, por ejemplo un valor almacenado en el TEE, o bien ajustar el temporizador de reinicio a un valor recibido como parte del comando de “go-ahead” y reiniciar el temporizador de reinicio a partir del valor de temporizador establecido.

El TEE arranca de ese modo el temporizador de reinicio y, si este temporizador de reinicio expira (es decir, si no se recibe ningún comando de “go-ahead” con anterioridad a que expire el temporizador, el TEE dispara un reinicio y re-arranque de hardware 312 del UD para cargar el UDBS. A este fin, el TEE envía una señal 313 de interrupción al NEE que provoca el re-arranque 312. En respuesta a la señal 313 de interrupción, el NEE puede enviar una notificación 314 al DMS informando al DMS del re-arranque.

Con ello, si el NEE falla o rechaza pasar un comando 310 de “go-ahead” al TEE antes de que el temporizador expire, el UD re-arrancará en el UDBS para proporcionar solamente servicios de confianza. Con el fin de evitar que el NEE u otra entidad externa no autorizada pase comandos de go-ahead erróneos o disruptivos al TEE, el comando 310 de go-ahead procedente del DMS está firmado con la SDMK que permite al TEE verificar el comando Go-ahead recibido frente a la PuDMK.

La Figura 4 ilustra con mayor detalle un ejemplo de la comunicación del comando go-ahead. El proceso es iniciado por el DMS 402 que envía un comando init 415 a través del NEE 406 al TEE 407. Por ejemplo, el DMS puede comprender un temporizador asociado a cada dispositivo de procesamiento gestionado por el sistema de gestión de dispositivo, y que tenga un valor de temporizador correspondiente al, por ejemplo suficientemente más corto que el, valor de temporizador del temporizador de re-arranque del TEE. En respuesta a este comando init 415, el TEE envía un nonce (vector de inicialización) 416 al DMS a través del NEE. El nonce (vector de inicialización) puede ser cualquier elemento de datos, por ejemplo un número, que se utiliza una sola vez (al menos el intervalo de tiempo entre una repetición deberá ser suficientemente largo). Para asegurar que un nonce (vector de inicialización) es utilizado una sola vez, éste puede ser una variable de tiempo, por ejemplo incluyendo una marca de tiempo adecuadamente minuciosa en su valor, o puede incluir un número aleatorio generado con bits aleatorios suficientes para asegurar una opción probabilísticamente insignificante de repetición de un valor generado previamente. Se apreciará que el proceso puede ser iniciado por el UD en vez del DMS, por ejemplo por el TEE que envía el nonce (vector de inicialización) y que solicita un comando go-ahead. Por ejemplo, el TEE puede ser activado para solicitar un comando go-ahead en un momento predeterminado antes de que expire el temporizador de reinicio. Cuando el proceso es iniciado por el DMS, el riesgo de denegación de ataques de servicio en el DMS se reduce.

En respuesta a la recepción del nonce (vector de inicialización), el DMS puede determinar si debe enviar realmente el comando go-ahead. Alternativamente, la determinación puede ser llevada a cabo con anterioridad al envío del comando init 415. La determinación puede estar basada en la información de sistema recibida, por ejemplo en respuesta a una petición de atestación remota. Alternativamente, el DMS puede observar el tráfico de red entrante y/o saliente del UD con el fin de identificar cualquier pauta inusual usando técnicas de Sistema de Detección de Intrusión de Red tales como las usadas en IDSs como Bro o Snort. Por ejemplo, el DMS puede verificar de forma continua o periódica la operación apropiada del dispositivo de procesamiento y mantener una banderola correspondiente (por ejemplo, la banderola DOK mostrada en la Figura 2) en el registro asociado al dispositivo de procesamiento. Cuando el DMS ha determinado que puede ser emitido un comando go-ahead, el DMS envía el comando go-ahead 410 actual, el cual puede incluir un comando que identifique el mensaje como comando de go-ahead y el nonce (vector de inicialización) 416 recibido anteriormente. El comando go-ahead puede incluir información adicional, por ejemplo un valor de temporizador al que deba el TEE ajustar su temporizador de reinicio. Algunos de, o todos, los contenidos del comando go-ahead están firmados con la SDMK. Cuando la interacción para tales comandos go-ahead es de estado en el sentido de que el comando 310 procedente del DMS para el TEE/UD contiene un nonce (vector de inicialización) que el TEE haya pasado anteriormente de forma segura al DMS, el riesgo de reproducción perjudicial de comandos se reduce. Tras la recepción del comando 410 desde el DMS a través del NEE, el TEE verifica la signatura en base a su PuDMK y compara el nonce (vector de inicialización) recibido con el nonce (vector de inicialización) 416 previamente enviado. Si ambas verificaciones tienen éxito, el TEE reinicia el temporizador de arranque, incluyendo opcionalmente el ajuste del temporizador a un nuevo valor, por ejemplo un valor recibido con el comando go-ahead.

Haciendo de nuevo referencia a la Figura 3, después de que el UDBS ha sido arrancado en la etapa 312, el DMS puede interactuar de forma segura con el UD y asegurar la reanudación de la operación normal con software auténtico. Un ejemplo del proceso de recuperación del UD después del re-arranque del UDBS ha sido ilustrado en la Figura 5, la cual muestra un ejemplo del flujo de mensaje entre el DMS 502, el NEE 506 y el TEE 507 durante el proceso de recuperación.

En la etapa 512, tras la recepción de una señal de reinicio procedente del TEE, el NEE re-arranca en el UDBS según se ha descrito en relación con la Figura 3. La información de estado mantenida en el TEE (y mantenida durante el re-arranque en el UDBS según se ha ilustrado mediante la etapa 521, por ejemplo en una situación en la que el TEE necesita conservar algunos valores de registro, por ejemplo con el fin de conservar información acerca de la causa del re-arranque), es actualizada después de que el UDBS ha iniciado el funcionamiento según se ha ilustrado mediante la etapa 522. Por ejemplo, en un sistema TCG, “Actualizar estado” puede incluir una actualización del Registro de Configuración de Plataforma (PCR).

Después de que el UDBS ha sido arrancado (por ejemplo, el UDBS puede estar configurado para contactar con el DMS con el fin de informar al DMS de que el UD está ejecutando el Sistema de Base), el DMS puede interactuar de forma segura con el UD y éste envía una petición 523 de atestación firmada al UD, la cual es recibida por el NEE que ejecuta el UDBS y la reenvía (524) al TEE. La petición de atestación puede incluir un nonce (vector de inicialización). Tras la recepción de una respuesta 525 desde el TEE, el NEE que ejecuta el UDBS envía una respuesta 526 firmada al DMS. La respuesta puede incluir el nonce (vector de inicialización) que fue recibido en la petición de atestación. Además, la respuesta puede incluir una o más variables de estado adecuadas, por ejemplo el PCR. En base a la respuesta 526, el DMS puede comprobar ahora que el arranque ha tenido éxito. Tras la determinación de éxito por parte del DMS de que el arranque ha tenido éxito, el DMS puede enviar uno o más comandos 527 de mantenimiento al UD, en caso de que el DMS determine que se está realizando una o más operaciones 528 de mantenimiento por parte del DMS, o provocar que el UD realice algunas operaciones de mantenimiento sobre sí mismo, con anterioridad a que el UD arranque su sistema operativo y reanude el funcionamiento normal (etapa 530). Como parte del proceso de mantenimiento, el TEE puede haber salvado información de estado con anterioridad al re-arranque. La información de estado puede ser reenviada por el TEE al NEE según se ha ilustrado mediante la flecha 531. El NEE puede transferir la información de estado al DMS y/o usarla en el mantenimiento 528 de prearranque. Puesto que el TPM es operado como esclavo, está consiguientemente controlado por un comando adecuado para actualizar el PCR (529), permitiendo con ello registrar que la operación de mantenimiento ha tenido lugar.

El proceso de la Figura 5 es por tanto un ejemplo de un proceso de recuperación de UD tras el arranque del UDBS, donde el DMS verifica que ha ocurrido un re-arranque apropiado del UD y donde se pueden realizar operaciones de mantenimiento con anterioridad a que se haya restablecido el funcionamiento normal.

De ese modo, en lo que antecede, se han descrito realizaciones de un sistema seguro para recuperación de dispositivo en el que uno o más dispositivos gestionados con una parte segura, son re-arrancados por medio de un temporizador local y de dependencia de pasaje procedente de un sistema de gestión remota. Aunque algunas de las realizaciones han sido descritas y mostradas en detalle, la invención no está restringida a las mismas, sino que puede ser materializada de otras formas dentro del alcance de la materia objeto definida en las reivindicaciones que siguen.

El método, el producto y el dispositivo descritos en la presente memoria pueden ser implementados por medio de hardware que comprenda varios elementos distintos, y por medio de un microprocesador programado adecuadamente. En las reivindicaciones de dispositivo que enumeran varios medios, algunos de esos medios pueden estar materializados por un solo y mismo elemento de hardware, por ejemplo un microprocesador programado adecuadamente, uno o más procesadores de señal digital, o similar. El mero hecho de que algunas medidas sean citadas en reivindicaciones dependientes mutuamente diferentes o sean descritas en realizaciones diferentes, no indica que no pueda usarse de manera ventajosa una combinación de estas medidas.

Se debe hacer hincapié en que el término “comprende/comprendiendo”, cuando se usa en la presente descripción, debe ser tomado en el sentido de que especifica la presencia de características mencionadas, números enteros, etapas o componentes, pero no excluye la presencia o la adición de una o más de otras características, números enteros, etapas, componentes o grupos de los mismos.

REIVINDICACIONES

1.- Un dispositivo de procesamiento (101; 201), que comprende:

- un entorno (107) de ejecución segura que comprende un temporizador (117) y medios para llevar el dispositivo de procesamiento a un estado operativo predeterminado;
en donde el entorno de ejecución segura está configurado para:

- en respuesta a la expiración del temporizador (117), llevar el dispositivo de procesamiento (101; 201) a dicho estado operativo predeterminado,
caracterizado porque el dispositivo de procesamiento comprende además:

- una interfaz (104) de comunicaciones para la comunicación de datos entre el dispositivo de procesamiento y un sistema (102; 202) de gestión de dispositivo remoto externo al dispositivo de procesamiento;
y porque el entorno de ejecución segura está configurado además para:
- en respuesta a una recepción, procedente del sistema (102; 202) de gestión de dispositivo remoto a través de dicha interfaz (104) de comunicaciones, de una señal activadora, reiniciar el temporizador.

2.- Un dispositivo de procesamiento según la reivindicación 1, en donde la señal activadora comprende un valor de temporizador, y en donde el entorno de ejecución segura está adaptado para reiniciar el temporizador a partir del valor de temporizador recibido.

3.- Un dispositivo de procesamiento según una cualquiera de las reivindicaciones anteriores, en donde el entorno de ejecución segura está adaptado para enviar un primer nonce (vector de inicialización) al sistema de gestión de dispositivo remoto, para extraer un segundo nonce (vector de inicialización) de la señal activadora recibida; para comparar el primer y el segundo nonces (vectores de inicialización); y, para reiniciar el temporizador solamente, si el primer y el segundo nonces (vectores de inicialización) son iguales.

4.- Un dispositivo de procesamiento según la reivindicación 3, en donde el entorno de ejecución segura está configurado para verificar la autenticidad del segundo nonce (vector de inicialización), y para reiniciar el temporizador solamente, si la autenticidad ha sido verificada con éxito.

5.- Un dispositivo de procesamiento según una cualquiera de las reivindicaciones anteriores, en donde el entorno de ejecución segura está configurado para llevar el dispositivo de procesamiento a dicho estado operativo predeterminado mediante el re-arranque del dispositivo de procesamiento en un estado predeterminado.

6.- Un dispositivo de procesamiento según la reivindicación 5, en donde el re-arranque comprende verificar la autenticidad de un componente de software básico para proporcionar un conjunto de funciones básicas de sistema, y cargar el componente de software básico condicionado a una verificación con éxito.

7.- Un dispositivo de procesamiento según la reivindicación 5 ó 6, en donde el dispositivo de procesamiento está configurado para enviar, después de un reinicio del dispositivo de procesamiento en el estado predeterminado, un mensaje al sistema de gestión de dispositivo indicativo del estado operativo del dispositivo de procesamiento.

8.- Un dispositivo de procesamiento, según la reivindicación 7, en donde enviar un mensaje al sistema de gestión de dispositivo indicativo del estado operativo del dispositivo de procesamiento comprende recibir una petición de atestación desde el sistema de gestión de dispositivo y responder a la petición de atestación recibida mediante comunicación de al menos un valor de una variable de estado indicativa del estado operativo del dispositivo de procesamiento mantenido por el entorno de ejecución segura.

9.- Un dispositivo de procesamiento según una cualquiera de las reivindicaciones anteriores, en donde el entorno de ejecución segura comprende un identificador que identifica el dispositivo de procesamiento, una clave pública asociada al sistema de gestión de dispositivo, el temporizador, y una clave criptográfica para verificar la autenticidad del estado operativo predeterminado.

10.- Un dispositivo de procesamiento según una cualquiera de las reivindicaciones anteriores, que comprende además un entorno de ejecución normal que tiene un nivel de seguridad más bajo que el entorno de ejecución segura; en donde el entorno de ejecución segura está asegurado frente a una alteración no autorizada por parte del entorno de ejecución normal.

11.- Un dispositivo de procesamiento según la reivindicación 10, en donde el entorno de ejecución normal comprende un sistema operativo y opcionalmente software de aplicación adicional para operar el dispositivo de procesamiento.

12.- Un dispositivo de procesamiento según una cualquiera de las reivindicaciones anteriores, configurado para proporcionar comunicación protegida criptográficamente entre el sistema de gestión de dispositivo y el entorno de ejecución segura.

13.- Un sistema (102; 202) de gestión de dispositivo para controlar el funcionamiento de un dispositivo (101; 201) de procesamiento remoto externo al sistema de gestión de dispositivo, comprendiendo el dispositivo de procesamiento remoto un entorno (107) de ejecución segura que comprende un temporizador (117) y medios para llevar el dispositivo de procesamiento a un estado operativo predeterminado; comprendiendo el sistema de gestión de dispositivo:

una interfaz de comunicaciones para comunicación de datos entre el sistema de gestión de dispositivo y el dispositivo de procesamiento remoto;
medios de procesamiento configurados para:

- determinar un estado operativo del dispositivo de procesamiento remoto;
- en respuesta al estado operativo determinado, enviar una señal activadora al dispositivo de procesamiento a través de la interfaz de comunicaciones para provocar que el dispositivo de procesamiento reinicie el temporizador.

14.- Un sistema de gestión de dispositivo según la reivindicación 13, configurado para observar y analizar tráfico de datos de uno o más dispositivos de procesamiento remoto con el fin de determinar uno o más parámetros indicativos de un funcionamiento normal de los uno o más dispositivos; y, condicionada a los uno o más parámetros determinados, enviar una señal predeterminada al uno o más dispositivos de procesamiento para provocar que el dispositivo de procesamiento reinicie el temporizador.

15.- Un sistema de comunicaciones que comprende un dispositivo de procesamiento según se ha definido en una cualquiera de las reivindicaciones 1 a 12, y un sistema de gestión de dispositivo según se ha definido en una cualquiera de las reivindicaciones 13 a 14.

16.- Un método de operar un dispositivo de procesamiento (101; 201) bajo el control de un sistema (102; 202) de gestión de dispositivo remoto externo al dispositivo de procesamiento, comprendiendo el dispositivo de procesamiento un entorno (107) de ejecución segura que comprende un temporizador (117) y medios para llevar el dispositivo de procesamiento a un estado operativo predeterminado; comprendiendo el método:

- en respuesta a la expiración del temporizador (117), llevar el dispositivo de procesamiento (101; 201) a dicho estado operativo predeterminado;
- en respuesta a una recepción, procedente del sistema (102; 202) de gestión de dispositivo remoto a través de una interfaz (104) de comunicaciones del dispositivo de procesamiento, de una señal activadora generada por el sistema de gestión de dispositivo remoto en respuesta a un estado operativo determinado del dispositivo de procesamiento, reiniciar el temporizador.

17.- Un producto de programa de ordenador adaptado para implementar un entorno de ejecución segura para un dispositivo de procesamiento, comprendiendo el entorno de ejecución segura un temporizador y medios para llevar el dispositivo de procesamiento a un estado operativo predeterminado; y configurado para ejecutar las etapas del método según la reivindicación 16.

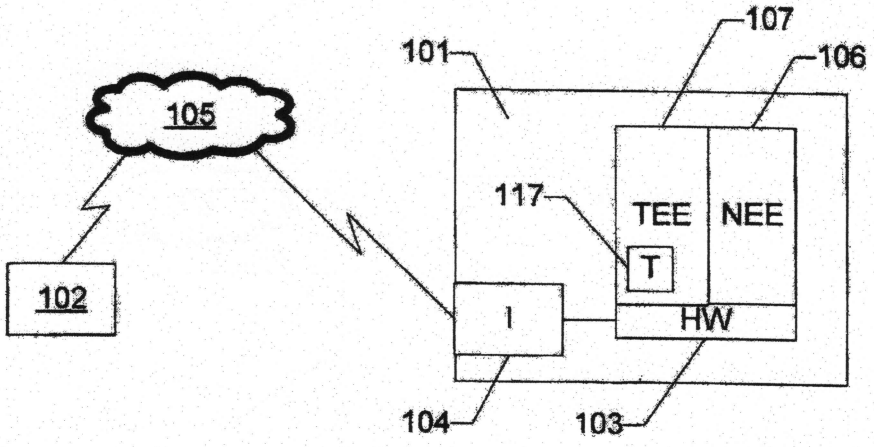
101
107
106
105
117
TEE
NEE
T
102
I
HW
104
103

Fig. 1

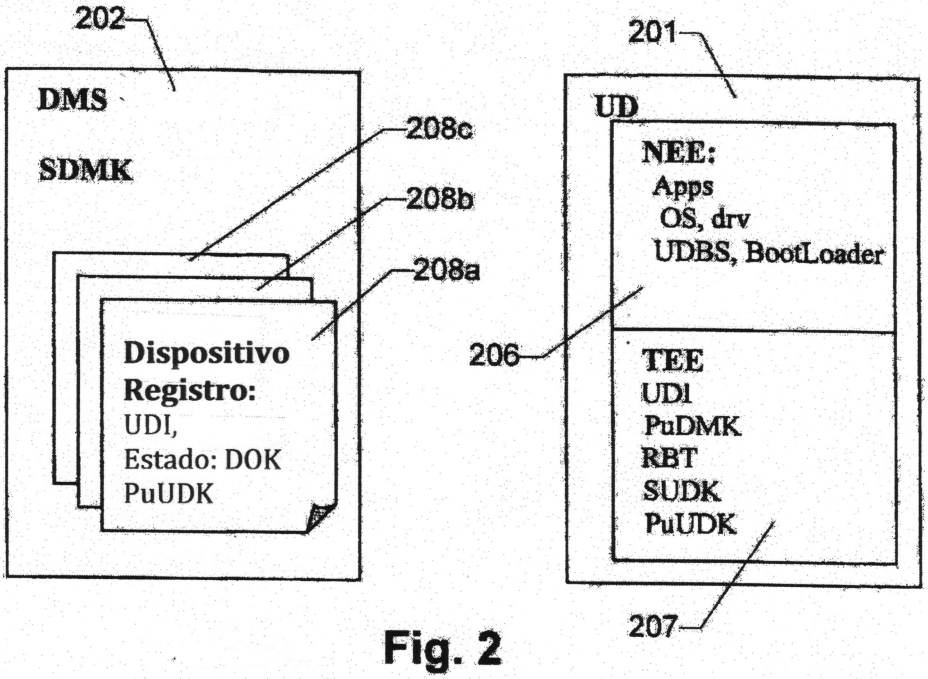
202
DMS
SDMK
208c
208b
208a
Dispositivo
Registro:
UDI,
Estado: DOK
PuUDK
201
UD
NEE:
Apps
OS, drv
UDBS, BootLoader
206
TEE
UDI
PuDMK
RBT
SUDK
PuUDK
207

Fig. 2

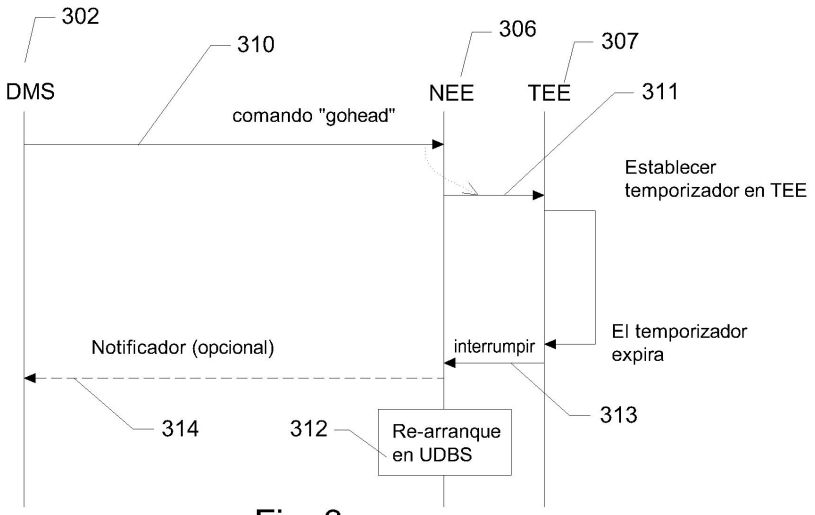
302
310
306
307
DMS
NEE
TEE
311
comando "gohead"
Establecer
temporizador en TEE
El temporizador
expira
Notificador (opcional)
interrumpir
313
314
312
Re-arranque
en UDBS

Fig. 3

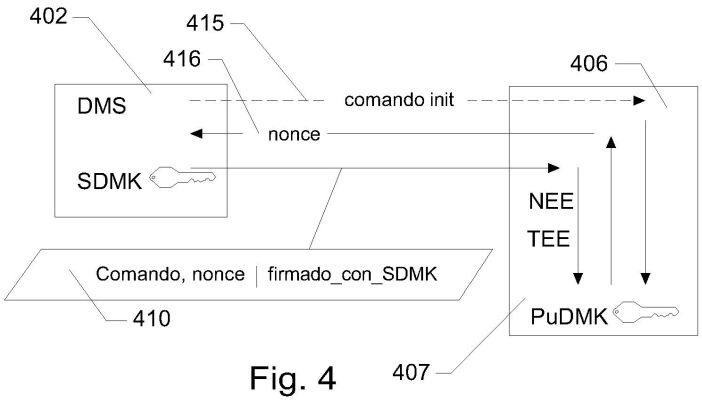
402
415
416
406
DMS
comando init
nonce
SDMK
NEE
TEE
Comando, nonce | firmado_con_SDMK
410
PuDMK
407

Fig. 4

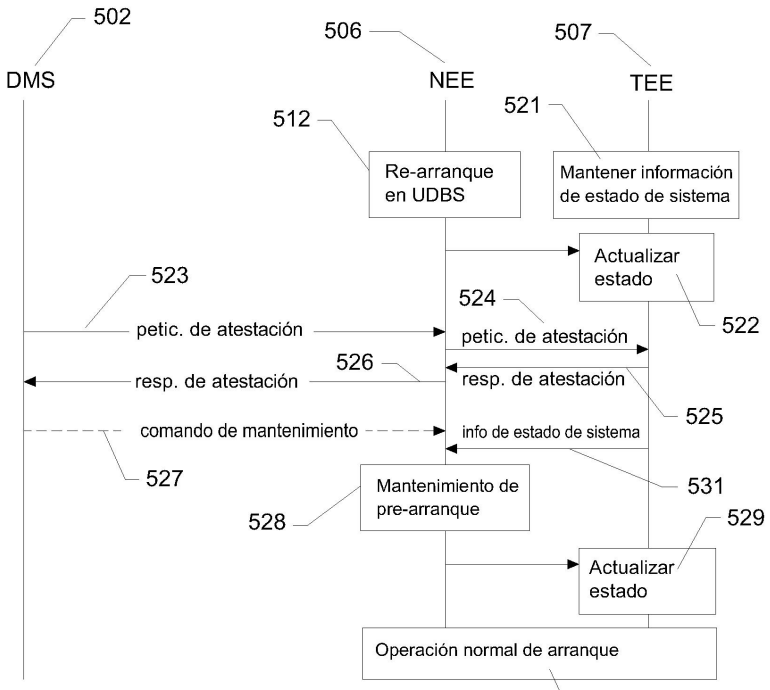
502
DMS
506
NEE
507
TEE
512
521
Re-arranque en UDBS
Mantener información de estado de sistema
Actualizar estado
522
523
524
petic. de atestación
petic. de atestación
526
resp. de atestación
resp. de atestación
525
comando de mantenimiento
info de estado de sistema
527
531
Mantenimiento de pre-arranque
528
529
Actualizar estado
Operación normal de arranque
530

Fig. 5