(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 381 355**

(51) Int. CI.:
G06F 21/02 (2006.01)
G06F 21/00 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **03742347 .2**
(96) Fecha de presentación: **27.06.2003**
(97) Número de publicación de la solicitud: **1518158**
(97) Fecha de publicación de la solicitud: **30.03.2005**

(54) Título: **Plataforma informática de confianza**

(30) Prioridad:
28.06.2002 US 185391

(45) Fecha de publicación de la mención BOPI:
25.05.2012

(45) Fecha de la publicación del folleto de la patente:
25.05.2012

(73) Titular/es:
INTEL CORPORATION
2200 MISSION COLLEGE BOULEVARD
SANTA CLARA, CA 95052, US

(72) Inventor/es:
WISEMAN, Willard y
GRAWROCK, David

(74) Agente/Representante:
Carpintero López, Mario

DESCRIPCIÓN

Plataforma informática de confianza

La presente invención versa en general acerca de aparatos, sistemas y procedimientos que proporcionan seguridad para plataformas de cálculo. Más en particular, la presente invención versa acerca de aparatos, sistemas y procedimientos usados para proporcionar autenticación de soporte físico y soporte lógico, como pueden darse en plataformas informáticas de confianza.

En un mundo crecientemente influido por la existencia de redes que conectan un amplio conjunto de recursos informáticos, nunca han sido más importantes los temas de la seguridad de los datos, la protección de la información y la privacidad de los usuarios. Típicamente, los ordenadores personales (PC) ofrecen una arquitectura abierta como estándar industrial que puede ser usado para construir una plataforma informática omnipresente. Sin embargo, la confianza en la plataforma no ha formado comúnmente parte de tales diseños. Tal como se usa en el presente documento, puede interpretarse que el término “plataforma” significa cualquier tipo de dispositivo, incluyendo soporte físico, soporte lógico o cualquier combinación de estos, cuya actividad se dirija según una pluralidad de instrucciones programadas.

Típicamente, las plataformas se ejecutan bajo el control de un sistema operativo (SO) cuando han de ejecutarse aplicaciones. Los sistemas operativos y los componentes previos al sistema operativo son complejos y requieren un procedimiento de carga (es decir, de “arranque”) para cargarlos en la memoria de la plataforma. La plataforma carga el SO cuando la plataforma pasa de un estado apagado o suspendido a un estado encendido, o cuando se aplica una señal de reposición a la línea de reposición de la plataforma. En el presente documento, la expresión “reposición de la plataforma” puede ser usada para referirse a cualquiera de estas condiciones. El código de inicialización de la plataforma incluye dos componentes: el bloque de arranque de inicialización de la plataforma (PIBB) y el código de inicialización de la plataforma principal (MPIC). Después de que ocurra una reposición de la plataforma, la unidad central de proceso (CPU) comienza la ejecución en una ubicación bien conocida y definida dentro del PIBB. Este código es intencionalmente pequeño, robusto y seguro. El PIBB ejecuta código para habilitar dispositivos en la plataforma necesarios para que se ejecute el código de inicialización de la plataforma principal. El PIBB pasa entonces el control de la plataforma al código de inicialización de la plataforma principal.

El código de inicialización de la plataforma principal lleva a cabo funciones necesarias para completar la inicialización de la plataforma. Tales funciones pueden incluir la inicialización de dispositivos integrados dentro de la plataforma y localizar e inicializar adaptadores opcionales acoplables o integrados (que tienen su propio código de inicialización de dispositivos). Después de esto, el código de inicialización de la plataforma principal localiza el cargador del SO y lo ejecuta. El cargador del SO, a su vez, carga el SO en memoria y comienza a ejecutar el SO. En este punto, se considera que la plataforma está en el estado actual del SO y bajo el control completo del SO cargado.

Siempre que una plataforma sin confianza carga un SO, pueden producirse violaciones de las directrices de seguridad sin tan siquiera conectar la plataforma a la red. Así, la informática de confianza está cobrando importancia en todos los aspectos de las operaciones de cálculo, incluso cuando tales operaciones se realicen aparte de una red.

El documento EP1085396 da a conocer una entidad informática que incluye una unidad autónoma autocontenida de confianza de proceso de datos que comprende un procesador que tiene un primer medio de proceso y un primer medio de memoria. La entidad también comprende una plataforma informática que tiene un medio de proceso principal y un área de memoria principal, junto con una pluralidad de recursos asociados físicos y lógicos, tales como dispositivos periféricos, incluyendo impresoras, módems, programas de aplicación, sistemas operativos y similares. La plataforma informática tiene una pluralidad de estados de operación diferentes, teniendo cada estado de operación un nivel diferente de seguridad y de fiabilidad. Estados seleccionados de los estados comprenden estados de confianza, en los que un usuario puede introducir información confidencial sensible con un alto grado de certeza de que la plataforma informática no se ha visto comprometida por influencias externas, como virus, piratas informáticos u ataques hostiles. Para entrar en un estado de confianza, se realizan automáticamente referencias al componente de confianza, y para salir de un estado de confianza debe hacerse referencia al componente de confianza. Al salir del estado de confianza, se borran de la plataforma informática todas las referencias al estado de confianza. Al entrar en el estado de confianza, se entra en el estado de una manera reproducible y conocida que tiene una configuración reproducible y conocida que es confirmada por el componente de confianza.

Según un aspecto de la presente invención, se proporciona un aparato según la reivindicación 1.

Según otro aspecto de la presente invención, se proporciona un procedimiento según la reivindicación 7.

Breve descripción de los dibujos

La FIG. 1 es un diagrama de bloques de un aparato, de un artículo que incluye un medio accesible por máquina y de un sistema según diversas realizaciones de la invención;

la FIG. 2 es un diagrama de bloques de un módulo de directrices según una realización de la invención; y las FIGURAS 3A y 3B son diagramas de flujo que ilustran un procedimiento de verificar la confianza en una plataforma según una realización de la invención.

Descripción detallada de las realizaciones

La confianza se establece cuando una primera entidad (por ejemplo, un programa que se ejecuta en nombre de una persona u organización) tiene base para creer que el estado, la configuración y las respuestas recibidas de una segunda entidad (por ejemplo, un ordenador personal) son precisamente las representadas para la primera entidad. La Alianza de Plataformas Informáticas de Confianza (TCPA) ha desarrollado un estándar para proporcionar a la industria un conjunto de condiciones operativas que den confianza en las plataformas y los entornos informáticos. Este estándar, "The TCPA Main Specification", versión 1.1a, de 12 de noviembre de 2001, puede encontrarse en la actualidad en www-trusted computing-org (para evitar hiperenlaces involuntarios, los puntos del precedente URL han sido sustituidos por guiones). Como parte integral de cada plataforma, la "TCPA Main Specification" define elementos del entorno informático que operan para proteger la información dentro de las comunicaciones informáticas comerciales y personales. Los servicios existentes de seguridad basados en soporte lógico son inadecuados para dar prueba de que una plataforma es de confianza. La "TCPA Main Specification" detalla mecanismos que, cuando son implementados en una plataforma, proporcionan mayor confianza y permiten mejoras de los servicios existentes, así como la provisión de nuevos servicios.

La "TCPA Main Specification" también define un conjunto de componentes del que se puede confiar en que opere como se espera. Cuando están integrados en una plataforma, estos componentes medirán de forma fiable información sobre el entorno en esa plataforma, e informarán de ella. Esta "comprobación de integridad" de los componentes complementa y mejora los servicios de seguridad basados solo en componentes lógicos. Los componentes incluyen un motor informático aislado en cuyos procesos se puede confiar porque no pueden ser alterados. Estos procesos de confianza incluyen una almacenamiento protegido, una firma digital y un intercambio de datos de infraestructura de clave pública (PKI).

El comportamiento propuesto para una dispositivo habilitado por la TCPA, un módulo de plataforma de confianza (TPM), es "informar" de la integridad de la plataforma, permitiendo que la plataforma arranque hasta el SO incluso con componentes sin confianza instalados. Esto permite que un recurso externo (por ejemplo, un servidor en una red) determine la fiabilidad de la plataforma, pero no impide el acceso a la plataforma por el usuario.

La FIG. 1 es un diagrama de bloques de un aparato, de un artículo que incluye un medio accesible por máquina y de un sistema según diversas realizaciones de la invención. En una realización de la invención, un aparato 100 para proporcionar confianza en una plataforma 102 puede incluir una raíz de confianza para el módulo 104 de medición (RTM) y un módulo 106, 106' de directrices de propiedades de seguridad de la plataforma. El RTM 104 establece la base de la confianza en la plataforma 102. Así, el usuario de la plataforma debe decidir en primer lugar confiar en el RTM 104 de la plataforma. Una vez que se ha adoptado esa decisión, puede usarse el aparato 100 descrito en el presente documento para proporcionar una base de la confianza en las porciones restantes del procedimiento de arranque.

Según se describe en el presente documento, se da por sentado que una entidad no autorizada no será capaz de modificar el PIBB 108, que puede ser el RTM 104. También puede darse por sentado que todos los demás componentes y/o módulos dentro de la plataforma 102 están sujetos a ataques o a modificación, intencional o no. Así, diversas realizaciones de la invención pueden actuar para evitar la carga del SO 110 (típicamente incluido en una memoria 111 u otro dispositivo de almacenamiento) dentro de la plataforma 102, y pueden alertar al usuario de la plataforma si ocurre una modificación no autorizada de los componentes de la plataforma.

La "TCPA Main Specification" define un conjunto de funciones de confianza y emplazamientos de almacenamiento blindados. Estas funciones y estos emplazamientos de almacenamiento están contenido en un módulo 112 de plataforma de confianza (TPM) que, típica, pero no necesariamente, está implementado como un dispositivo permanentemente conectado a la plataforma 102.

Ejemplos de emplazamientos de almacenamiento blindados incluyen registros 114 de integridad de datos (DIR), registros no volátiles que solo pueden ser modificados por el propietario de la plataforma y registros 116 de configuración de la plataforma (PCR) que contienen valores que miden la integridad de la plataforma 102. Parte de la "TCPA Main Specification" define la generación de una clave calculada de dianas y la puesta de los valores de clave calculada en un emplazamiento de almacenamiento blindado, posiblemente combinando los valores de clave calculada con valores almacenados previamente. Tales dianas pueden incluir código ejecutable, datos de configuración, un registro de información definida por la TCPA y otros elementos.

El módulo 106 de directrices de propiedades de seguridad de la plataforma, que incluye posiblemente información en forma de una tabla 118 de directrices, puede estar incluido en el PIBB 108. Típicamente, la tabla 118 de directrices contiene información que afecta a las operaciones de la plataforma durante el procedimiento de arranque.

Según se describe en el presente documento, uno de los DIR 114 es el DIR 120 de la tabla de directrices. El DIR 120 de la tabla de directrices (incluido en el TPM 112) contiene información puesta por el propietario de la plataforma, o por un agente autorizado, para validar el PIBB 108 y, por extensión, la tabla 118 de directrices. Así, se establece la confianza en el PIBB 108 y en el módulo 106, 106' de directrices midiendo y comparando con un valor cargado de antemano puesto en el DIR 120 de la tabla de directrices por una entidad autorizada de confianza (es decir, el módulo 106, 106' de directrices debe ser verificado). La tabla 118 de directrices contiene directrices a las que debe atenerse la plataforma 102 durante el procedimiento de inicialización/arranque.

La medición es la acción de obtener un valor que puede ser directamente asociado con la integridad de la entidad. Un ejemplo es calcular el valor de clave calculada de un gran flujo de bytes o, para valores pequeños, puede usarse directamente el propio valor. La verificación consiste en comparar el valor medido con un valor de confianza conocido. Así, tal como se define en el presente documento, "medir" significa reunir datos sobre un componente, introducir opcionalmente la información reunida en un registro (que puede estar en una ubicación sin confianza), crear opcionalmente una clave calculada de los valores de los datos y/o de los valores registrados, y almacenar los datos o los datos objeto de clave calculada en uno de los PCR 116. "Comparar mediciones" significa comparar valores en la tabla de directrices con los datos objeto de clave calculada o extendidos de un PCR 116 o del registro.

Tal como se ha hecho notar en lo que antecede, el módulo RTM 104 puede ser un PIBB 108 asociado con la plataforma 102, que incluye un punto 122 de entrada. Suponiendo que un procesador 124 dentro de la plataforma 102 esté acoplado con una línea 126 de reposición, el procesador 124 operará típicamente comenzando la ejecución en el punto 122 de entrada tras recibir una señal 128 de reposición por la línea 126 de reposición (es decir, una condición de reposición de la plataforma).

Un módulo 130 de comparación puede estar acoplado en comunicación y situado dentro del módulo RTM 104, con el módulo 106 de directrices de propiedades de seguridad de la plataforma y con diversas funciones internas 131 de medición. El módulo 130 de comparación puede operar evitando la transferencia de control al SO 110 y/o incluso impedir el resto del procedimiento de arranque si se viola una directriz D1-Dn incluida en el módulo 106 de directrices de propiedades de seguridad de la plataforma. Además, si, en cualquier momento durante la inicialización de la plataforma 102 un componente dentro de la plataforma 102 viola una directriz del módulo 106 de directrices de propiedades de seguridad de la plataforma, según la detección del módulo 130 de comparación, la plataforma 102 puede operar, por ejemplo, alertando al usuario de la plataforma (y/o posiblemente a otros dispositivos a través, por ejemplo, de una conexión de red) de que la plataforma 102 intentó inicializarse usando un componente inválido.

Así, el aparato 100 puede incluir un dispositivo 132 de alerto acoplado en comunicación con el procesador 124, posiblemente usando un módulo 134 del dispositivo de alerta. El dispositivo 132 de alerta puede ser accionado por el procesador 124 para proporcionar una señal 136 de alerta cuando se viola una directriz D1-Dn incluida en el módulo 106 de directrices de propiedades de seguridad de la plataforma. El dispositivo 132 de alerta puede ser un mecanismo de soporte físico usado para alertar al usuario de la plataforma que la plataforma no ha logrado completar la secuencia de arranque debido a la falta de conformidad de una o más directrices D1-Dn de seguridad definidas. La señal de alerta puede ser un simple tono audible o una secuencia de tonos, una luz o ráfagas de luz, pulsaciones táctiles, mensajería remota, etc. Además, pueden enviarse una alerta u otro mensaje 140, posiblemente usando el módulo 134 del dispositivo de alerta acoplado al módulo 130 de comparación, a otro dispositivo al otro lado de una red 142, normalmente por medio de una interfaz 144 de red. Después de accionar el dispositivo 132 de alerta, la plataforma 102 puede entrar en un estado que requiera una condición de reposición de la plataforma (por ejemplo, típicamente, una reposición del soporte físico, descrito en lo que antecede) para continuar.

El aparato 100 puede también tener una memoria 146 que incluya un MPIC 148 asociado con la plataforma 102. La memoria 146 puede estar acoplada en comunicación con la plataforma 102, y la plataforma 102 puede estar acoplada en comunicación con el módulo RTM 104.

Antes de transferir el control a la parte siguiente de la secuencia de inicialización de la plataforma, debe obtenerse autorización de la tabla 118 de directrices. La tabla 118 de directrices puede incluir valores no tratados de clave calculada, valores de PCR extendidos o identificadores de las credenciales de validación. Un identificador puede ser un puntero a una ubicación de memoria, un valor de índice o cualquier número único que pueda ser buscado.

Por último, antes de transferir el control de la plataforma 102 al cargador 150 del SO, el código 148 de inicialización de la plataforma principal compara la configuración global y la secuencia de carga de la plataforma 102 comprobando la tabla 118 de directrices para determinar que: existe un conjunto requerido de componentes contenido dentro de la plataforma 102, que la plataforma 102 no contiene componentes rechazados y/o que se ha cargado un conjunto de componentes en una secuencia particular. Así, la plataforma 102 puede incluir una memoria 152 u otro dispositivo de almacenamiento que incluyan la configuración 154 de la plataforma, así como una credencial 156 de aval de la plataforma y una credencial 158 de conformidad de la plataforma.

La TCPA también permite varios tipos de credenciales, incluyendo una credencial de aval, una credencial de plataforma y una credencial de validación. La credencial de aval proporciona seguridad de que la plataforma contiene un TPM válido. La credencial de plataforma proporciona seguridad de que el TPM está debidamente ligado a la plataforma. Y la credencial de validación proporciona seguridad de que un dispositivo o un código de

inicialización de dispositivos son del fabricante nombrado en la credencial. El módulo 106 de directrices de propiedades de seguridad de la plataforma (y/o la tabla 118 de directrices) puede también incluir una credencial de aval, una credencial de conformidad de la plataforma, validaciones de estas (por ejemplo, una clave calculada de las credenciales) si son externas al módulo 106 de directrices de propiedades de seguridad de la plataforma y/o un conjunto obligatorio de componentes en secuencia.

La plataforma 102 también puede incluir una memoria 160 u otro dispositivo de almacenamiento que incluya una o más configuraciones 162 de dispositivo asociadas con uno o más dispositivos DISP1-DISPn y sus dispositivos códigos 164 de inicialización de dispositivos CÓDIGO1-CÓDIGOn. Las memorias 111, 152 y 160 pueden ser contiguas y estar contenidas dentro de una sola memoria mayor 166, o las memorias 111, 152, 160 pueden existir como parte de componentes o dispositivos físicamente separados de la plataforma 102.

La FIG. 2 es un diagrama de bloques de un módulo 206 de directrices según una realización de la invención. Tal como se ha hecho notar en lo que antecede, la tabla 218 de directrices incluida en el módulo 206 de directrices puede ser usada para definir las propiedades de seguridad de la plataforma usando una o más directrices contenidas en la misma. Típicamente, la tabla 218 de directrices reside dentro del PIBB. Alternativamente, la tabla 218 de directrices puede residir fuera del PIBB (véase la ubicación del módulo 106' en la FIG. 1), pero su valor medido debe estar incluido con el del PIBB cuando se compara con el DIR de la tabla de directrices.

La tabla 218 de directrices puede incluir varias entradas, típicamente agrupadas en secciones 267 de directrices que definen las propiedades de seguridad de la plataforma, tales como: directrices 268 del código de inicialización de la plataforma, directrices 270 de configuración de la plataforma, directrices 272 de código de inicialización de dispositivos, directrices 274 de configuración de dispositivos opcionales o integrados, directrices 276 del cargador del SO, directrices 278 de configuración del cargador del SO y otras reglas y definiciones relacionadas con la seguridad. Cada una de las secciones 267 puede también incluir ninguno, algunos o todos los siguientes: valores 280 no tratados de directrices de clave calculada, valores extendidos 282 de directrices, identificadores 284 de credenciales de validación, valores que identifiquen la credencial 286 de aval de la plataforma, valores que identifiquen la credencial 288 de conformidad de la plataforma y/o valores que identifiquen las credenciales 290 de validación.

Típicamente, cada entrada incluye una bandera que indica la directriz requerida para esa sección. Por ejemplo, la sección puede contener solo valores no tratados de clave calculada que han de ser usados para verificar una directriz o puede contener solo identificador de las credenciales de validación que indique que para esa sección particular solo se permiten los componentes que tienen credenciales de validación.

La verificación de que un elemento/módulo del componente o la plataforma satisface las directrices definidas ocurre comparando mediciones del elemento/módulo con la debida entrada de la tabla de directrices. Puede haber múltiples entradas pertenecientes a un solo componente o módulo en la tabla 218 de directrices. Puede requerirse que ninguna, algunas o todas las entradas coincidan para que ese componente o módulo satisfaga una directriz definida. Por ejemplo, una directriz 274 para un componente requerido 292 puede incluir la comprobación del valor 280 no tratado de clave calculada, la comprobación de los valores extendidos 282 de clave calculada, la validación de al menos una de las credenciales 290 del componente y luego la comparación del valor 280 no tratado de clave calculada con los valores especificados dentro de la credencial 290. Si un componente 292 no logra satisfacer la directriz asociada 274, la entidad que comprobó el componente 292 puede transferir el control de la plataforma al módulo del dispositivo de alerta.

Con referencia de nuevo a la FIG. 1, es ahora fácil entender que una plataforma 102 puede incluir uno o más de los siguientes componentes: un procesador 124, código 194 de inicialización de la plataforma (dotado de un PIBB 108 y de un código 148 de inicialización de la plataforma principal) y diversos dispositivos, tales como dispositivos integrados y/u opcionales DISP1-DISPn dentro de la plataforma 102, que pueden contener sus propios códigos respectivos CÓDIGO1-CÓDIGOn de inicialización del dispositivo. Típicamente, la plataforma 102 también incluye un dispositivo que incluye o tiene la capacidad de acceder al cargador 150 del SO y un dispositivo que incluye o tiene la capacidad de acceder al SO 110.

Así, en otra realización de la invención, un sistema 196 puede incluir un procesador 124 acoplado con una memoria 198. La memoria 198 puede incluir un módulo RTM 104, un módulo 106 de directrices de propiedades de seguridad de la plataforma (capaz de estar acoplado en comunicación con la memoria 198) y un módulo 130 de comparación (capaz de estar acoplado en comunicación con la memoria 198). Así, la memoria 198 puede incluir un bloque de arranque de inicialización, tal como un PIBB 108. Típicamente, el módulo 130 de comparación opera impidiendo la transferencia del control al sistema operativo 110 o a otros componentes previos al SO (por ejemplo, deteniendo por completo el procedimiento de arranque) cuando se viola una directriz incluida en el módulo 106 de directrices de propiedades de seguridad de la plataforma. Esto puede ocurrir, por ejemplo, cuando falla la medición y la comparación (es decir, la verificación) el módulo 106 de directrices de seguridad de la plataforma con el valor en el DIR 120 de la tabla de directrices incluido en el TPM 112. En esta realización, el módulo 130 de comparación debería ser verificado antes de que haya confianza en él para efectuar comparaciones válidas.

Con referencia aún a la FIG. 1, el sistema 196 también puede incluir una línea 126 de reposición acoplada al procesador 124 en la que el procesador 124 ejecuta un punto 122 de entrada incluido en el RTM 104 cuando se aplica una señal 128 de reposición a la línea 126 de reposición para iniciar una condición de reposición de la plataforma. Por último, debería hacerse notar que el sistema 196 puede también incluir un dispositivo 132 de alerta acoplado en comunicación con el procesador 124, en el que el dispositivo 132 de alerta puede ser accionado por el procesador 124 para proporcionar una señal de alerta cuando se viola una directriz incluida en el módulo 106 de directrices de propiedades de seguridad de la plataforma verificada.

Con referencia ahora tanto a la FIG. 1 como a la 2, el aparato 100; el módulo RTM 104; los módulos 106, 106', 206 de directrices de propiedades de seguridad de la plataforma (incluyendo cada uno de los diversos elementos dentro de los mismos); el PIBB 108; los DIR 114; los PCR 116; las tablas 118, 218 de directrices; el procesador 124; el módulo 130 de comparación; las funciones internas 131 de medición; el dispositivo 132 de alerta; el módulo 134 del dispositivo de alerta; la interfaz 144 de red; y las memorias 111, 146, 152, 160, 166, 198 pueden ser caracterizados en el presente documento como "módulos". Tales módulos pueden incluir circuitería de soporte físico y/o un microprocesador y/o circuitos de memoria, módulos de programas de soporte lógico y/o soporte lógico inalterable y combinaciones de los mismos, según desee el arquitecto del aparato 100 y del sistema 196, y apropiados para realizaciones particulares de la invención.

Las aplicaciones que pueden incluir el aparato y el sistema novedosos de la presente invención incluyen circuitería electrónica usada en ordenadores de alta velocidad, circuitería de procesamiento de comunicaciones y señales, módems, módulos de procesador, procesadores integrados y módulos específicos de aplicación, incluyendo módulos multicapa y de chips múltiples. Tales aparatos y sistemas pueden, además, estar incluidos como subcomponentes dentro de una variedad de sistemas electrónicos, tales como televisores, teléfonos celulares, ordenadores personales, radios, vehículos y otros.

Las FIGURAS 3A y 3B son diagramas de flujo que ilustran un procedimiento de verificación de la confianza en una plataforma según una realización de la invención. El procedimiento 313 puede empezar en la FIG. 3A en el bloque 315 cuando un procesador u otro módulo dentro de la plataforma detecta una condición de reposición de la plataforma. El procesador puede entonces comenzar la ejecución del código del punto de entrada en el bloque 317.

El PIBB contiene su propio código para llevar a cabo mediciones (es decir, las funciones internas de medición) porque todos los demás componentes carecen de confianza en este momento. El PIBB, usando el código interno, se mide a sí mismo en el bloque 319 y verifica que satisface la directriz según el DIR de la tabla de directrices dentro del TPM en los bloques 321 y 323. Si la medición no satisface la directriz, típicamente el control se pasa entonces al módulo del dispositivo de alerta y/o al dispositivo de alerta, y el usuario de la plataforma es alertado en el bloque 325. Opcionalmente, el TPM puede ser inhabilitado para que la plataforma se comporte como una plataforma sin confianza, pero se permite que el procedimiento de arranque continúe. Si la medición satisface la directriz, entonces se puede tener confianza en la tabla de directrices, y el procedimiento 313 puede continuar con el bloque 327.

Diversas realizaciones de la invención dada a conocer en el presente documento implican el uso del PIBB para medir el código de inicialización de la plataforma principal en el bloque 327, y verifican que satisface la directriz en el bloque 329. Con referencia aún al bloque 327, si hay extensiones al código de inicialización de la plataforma principal, el PIBB también mide las extensiones y verifica que satisfacen la directriz. Si los resultados de la medición no satisfacen la directriz en el bloque 329, típicamente el control se pasa entonces al módulo del dispositivo de alerta y/o al dispositivo de alerta, y el usuario de la plataforma es alertado en el bloque 325.

Si la plataforma contiene una o varias credenciales de plataforma, conformidad o aval, son verificadas con las entradas respectivas dentro de la tabla de directrices en el bloque 333. Si las credenciales no se verifican, la plataforma no satisface la directriz. Si la medición no satisface la directriz en el bloque 335, el control es típicamente pasado entonces al módulo del dispositivo de alerta y/o al dispositivo de alerta, y el usuario de la plataforma es alertado en el bloque 325.

El código de inicialización de la plataforma principal puede ser usado para examinar la plataforma en busca de dispositivos opcionales o integrados y sus códigos de inicialización del dispositivo. Sin embargo, antes de transferir el control del código de inicialización de la plataforma principal a cualquier código de inicialización de dispositivos, el código de inicialización de la plataforma principal debería verificar que el dispositivo y su código de inicialización del dispositivo satisfacen la directriz en los bloques 337 y 339. Si la medición no satisface la directriz en el bloque 339, el control es típicamente pasado entonces al módulo del dispositivo de alerta y/o al dispositivo de alerta, y el usuario de la plataforma es alertado en el bloque 325.

Los códigos de inicialización de dispositivos pueden validar la configuración de sus dispositivos asociados. En este caso, el control puede ser transferido al código de inicialización de dispositivo en el bloque 341. Para cada dispositivo, si hay una entrada en la tabla de directrices relacionada con un dispositivo seleccionado, el código de inicialización del dispositivo asociado con ese dispositivo puede verificar que la configuración del dispositivo asociado satisface la directriz en el bloque 343, incluyendo cualquier componente oculto del dispositivo asociado. Si la medición no satisface la directriz en el bloque 345, el control es típicamente pasado entonces al módulo del dispositivo de alerta y/o al dispositivo de alerta, y el usuario de la plataforma es alertado en el bloque 325. Si se

determina en el bloque 347 que existen que otra entrada de la tabla de directrices y un código de inicialización del dispositivo asociado, el código puede ser medido entonces en el bloque 337 y los procedimientos esquematizados por los bloques 339, 341, 343, 345 y 347 pueden ser repetidos cualquier número de veces.

Después de que todos los códigos de inicialización de dispositivos han sido ejecutados y de que todos los dispositivos han sido inicializados, el procedimiento 313 puede continuar en la FIG. 3B en el bloque 349, en el que puede usarse el código de inicialización de la plataforma principal para reunir información relativa a la configuración de la plataforma y a verificar que satisface la directriz en el bloque 351. Si la medición no satisface la directriz en el bloque 351, el control es típicamente pasado entonces al módulo del dispositivo de alerta y/o al dispositivo de alerta, y el usuario de la plataforma es alertado en el bloque 325.

Tras la conclusión de todas las funciones del código de inicialización de la plataforma principal, el código de inicialización de la plataforma principal puede localizar el cargador del SO y verificar que el cargador del SO satisface la directriz en los bloques 353 y 355. Si la medición no satisface la directriz en el bloque 355, el control es típicamente pasado entonces al módulo del dispositivo de alerta y/o al dispositivo de alerta, y el usuario de la plataforma es alertado en el bloque 325.

Antes de transferir el control al cargador del SO, el código de inicialización de la plataforma principal puede verificar la tabla de directrices en busca de conjuntos requeridos, rechazados y/u obligatorios de componentes en secuencia en el bloque 357. La directriz puede requerir la presencia de componentes particulares; puede rechazar componentes particulares; o puede requerir una secuencia particular de componentes. Si no se satisface alguna de las condiciones requeridas, la plataforma no satisface la directriz en el bloque 359 y el control es típicamente pasado entonces al módulo del dispositivo de alerta y/o al dispositivo de alerta, y el usuario de la plataforma es alertado en el bloque 325.

Si la directriz es satisfecha en el bloque 359, el control es transferido al cargador del SO en el bloque 361. Si el cargador del SO permite opciones, el cargador del SO puede operar verificando que esas opciones satisfacen la directriz en los bloques 363 y 365. Si la medición no satisface la directriz en el bloque 365, el control es típicamente pasado entonces al módulo del dispositivo de alerta y/o al dispositivo de alerta, y el usuario de la plataforma es alertado en el bloque 325. Si la directriz es satisfecha en el bloque 365, entonces se permite que el cargador del SO cargue el SO y el control de la plataforma es transferido al SO en el bloque 369. En este punto finaliza el procedimiento 313.

En resumen, el procedimiento 313 puede incluir la detección de una condición de reposición de la plataforma, el comienzo de la ejecución en un punto de entrada dentro de una raíz de confianza para la medición (RTM), y la determinación de que el RTM es digno de confianza, lo que puede incluir determinar que un módulo de directrices de propiedades de seguridad de la plataforma asociado con el RTM es digno de confianza. Determinar que el módulo de directrices de propiedades de seguridad de la plataforma asociado con el RTM es digno de confianza puede incluir la medición de una tabla de directrices y la comparación de las mediciones con uno o más valores incluidos en un DIR (incluido en un TPM).

El procedimiento puede continuar con la determinación de que un código de inicialización principal asociado con una plataforma es digno de confianza, y con la transferencia del control al código de inicialización principal. Si no, el procedimiento puede operar determinando que un código de inicialización principal asociado con una plataforma no es digno de confianza, y puede abstenerse de transferir el control al código de inicialización principal. Además, el procedimiento puede operar absteniéndose de carga un sistema operativo asociado con la plataforma si se viola una directriz asociada con el RTM.

El procedimiento puede también incluir la determinación de que la configuración de una plataforma no viola una directriz asociada con el RTM, la determinación de que un dispositivo no viola una directriz asociada con el RTM, la determinación de que un código de inicialización de dispositivos asociado con el dispositivo no viola una directriz asociada con el RTM y la transferencia del control al código de inicialización del dispositivo.

El procedimiento puede incluir también la determinación de que un cargado de sistema operativo asociado con la plataforma no viole una directriz asociada con el RTM, la determinación de que está presente un grupo seleccionado de componentes y la transferencia del control a un cargador de sistema operativo asociado con la plataforma. El procedimiento también puede incluir la determinación de que no está presente un grupo seleccionado de componentes rechazados y la transferencia del control a un cargador de sistema operativo asociado con la plataforma.

Así, con referencia de nuevo a la FIG. 1, se entiende ahora fácilmente que otra realización de la invención puede incluir un artículo 199, tal como un ordenador, un sistema de memoria, un disco magnético u óptico, algún otro dispositivo de almacenamiento y/o cualquier tipo de dispositivo o de sistema electrónicos, que comprenda un medio 194 accesible por máquina (por ejemplo, una memoria que incluya un conductor eléctrico, óptico o electromagnético) que tenga datos asociados 108 (por ejemplo, instrucciones de programa de ordenador) que, cuando sean objeto de acceso, den como resultado que una máquina lleve a cabo acciones tales que comiencen la ejecución en un punto de entrada dentro de una raíz de confianza para la medición (RTM), determinando que un código de inicialización

principal asociado con una plataforma es digno de confianza y transfiriendo el control al código de inicialización principal y, si no, determinando que un código de inicialización principal asociado con una plataforma no es digno de confianza y absteniéndose de transferir el control al código de inicialización principal.

Otras acciones pueden incluir determinar que la configuración de una plataforma no viola una directriz asociada con el RTM, determinar que un cargador de sistema operativo asociado con la plataforma no viola una directriz asociada con el RTM, determinar que un grupo seleccionado de componentes está presente, y transferir el control a un cargador de sistema operativo asociado con la plataforma. De forma similar, determinar que no está presente un grupo seleccionado de componentes rechazados y transferir el control a un cargador de sistema operativo asociado con la plataforma también puede estar incluido dentro del alcance de tales actividades.

REIVINDICACIONES

1. Un aparato que comprende:

una plataforma (102) de cálculo que incluye:

una raíz de confianza para un módulo (104) de medición que comprende un bloque (108) de arranque de inicialización de la plataforma;
un procesador (124) para ejecutar instrucciones, incluido el código de inicialización de la plataforma, que incluye el bloque (108) de arranque de inicialización de la plataforma que comienza en un punto (122) de entrada dentro de la raíz de confianza para el módulo de medición y un código (148) de inicialización de la plataforma principal, ejecutando dicho bloque de arranque de inicialización de la plataforma código para habilitar dispositivos en la plataforma necesarios para que se ejecute el código de inicialización de la plataforma principal; y llevando a cabo dicho código de inicialización de la plataforma principal funciones necesarias para completar la inicialización de la plataforma de cálculo;
un cargador (150) de sistema operativo;
un módulo (112) de plataforma de confianza que incluye valores cargados de antemano almacenados en un emplazamiento (120) de almacenamiento blindado, estando relacionados dichos valores cargados de antemano con la integridad de la plataforma de cálculo;
un módulo (106) de directrices de propiedades de seguridad de la plataforma que incluye una tabla (118) de directrices que contiene información de directrices (D1 - Dn) que definen propiedades de seguridad de la plataforma a las que hay que atenerse durante la inicialización de la plataforma;
un módulo (130) de comparación acoplado en comunicación con la raíz de confianza para el módulo (104) de medición; y
en la que dicho bloque de arranque de inicialización de la plataforma y dicho módulo de directrices de propiedades de seguridad de la plataforma son para determinar si son dignos de confianza mediante la medición y la comparación con uno de dichos valores cargados de antemano de dicho módulo de plataforma de confianza usando código interno a dicho bloque de arranque de inicialización de la plataforma, en la que la medición es la acción de obtener un valor que pueda ser directamente asociado con la integridad de una entidad, y en la que el módulo de comparación verifica acto seguido que el valor medido coincide con uno de dichos valores cargados de antemano del módulo (112) de programa de confianza y, si no, impide el resto del procedimiento de arranque, permitiendo, de lo contrario, que la ejecución continúe
con el bloque de arranque de inicialización de la plataforma para medir y verificar si la información de las directrices relativa al código de inicialización de la plataforma principal satisface una correspondiente directriz localizada en el módulo de plataforma de confianza y, si no, abstenerse de transferir el control a dicho código de inicialización principal, y, en caso afirmativo, permitir la ejecución del código de inicialización de la plataforma principal para medir y verificar si dispositivos adicionales (DISP1 a DISPn) acoplados a la plataforma satisfacen la información de las directrices y, en caso afirmativo, permitir la ejecución del código de inicialización de la plataforma principal y verificar si el cargador del sistema operativo satisface la información de las directrices y, en caso afirmativo, permitir que el procesador cargue un sistema operativo (110) y, si no, abstenerse de cargar un sistema operativo; y en la que el sistema operativo, si se carga, ha de ser ejecutado por el procesador.

2. El aparato de la reivindicación 1 en el que el bloque de arranque de inicialización incluye un punto de entrada capaz de ser ejecutado por el procesador tras la recepción de una señal (128) de reposición en una línea (126) de reposición acoplada al procesador para iniciar una condición de reposición de la plataforma.

3. El aparato de la reivindicación 1 que, además, comprende:

punteros a credenciales (156, 158) de la plataforma incluidas en la tabla (118) de directrices.

4. El aparato de la reivindicación 1 en el que la información de las directrices define un conjunto obligatorio de componentes en secuencia incluidos en la plataforma.

5. El aparato de cualquier reivindicación precedente que, además, comprende:

un dispositivo (132) de alerta operable para proporcionar una señal (136) de alerta cuando se viola la información de las directrices incluida en la tabla de directrices.

6. Un procedimiento en un aparato que comprende una plataforma (102) de cálculo que incluye un procesador (124), un cargador (150) de sistema operativo, un módulo (112) de plataforma de confianza que incluye valores cargados de antemano almacenados en un emplazamiento (120) de almacenamiento blindado, estando relacionados dichos valores cargados de antemano con la integridad de la plataforma de cálculo, una raíz de confianza para un módulo (104) de medición que comprende un bloque (108) de arranque de inicialización de la plataforma, un módulo (106) de directrices de propiedades de seguridad de la plataforma que incluye una tabla (118) de directrices que contiene información de directrices (D1 - Dn) que definen propiedades de

seguridad de la plataforma a las que hay que atenerse durante la inicialización de la plataforma, un módulo (130) de comparación acoplado en comunicación con la raíz de confianza para el módulo (104) de medición, comprendiendo el procedimiento las etapas de

que dicho procesador (124) ejecute instrucciones, incluido el código de inicialización de la plataforma, que tiene dicho bloque (108) de arranque de inicialización de la plataforma y un código (148) de inicialización de la plataforma principal, comenzando dicha ejecución en un punto (122) de entrada dentro de dicha raíz de confianza para el módulo de medición, ejecutando dicho bloque de arranque de inicialización de la plataforma código para habilitar dispositivos en la plataforma necesarios para que se ejecute el código de inicialización de la plataforma principal, y llevando a cabo dicho código de inicialización de la plataforma principal funciones necesarias para completar la inicialización de la plataforma de cálculo,

determinando si dicho bloque de arranque de inicialización de la plataforma y dicho módulo de directrices de propiedades de seguridad de la plataforma son dignos de confianza mediante la medición y la comparación con uno de dichos valores cargados de antemano de dicho módulo de plataforma de confianza usando código interno a dicho bloque de arranque de inicialización de la plataforma, mediante lo cual son verificados dicho bloque de arranque de inicialización de la plataforma y dicho módulo de directrices de propiedades de seguridad de la plataforma, en el que la medición es la acción de obtener un valor que pueda ser directamente asociado con la integridad de una entidad y,

si dicho bloque de arranque de inicialización de la plataforma y dicho módulo de directrices de propiedades de seguridad de la plataforma no son verificados, se detenga la ejecución y, en caso contrario,

medir y verificar, usando dicho bloque de arranque de inicialización de la plataforma, si la información de las directrices relativa al código de inicialización de la plataforma principal satisface una correspondiente directriz localizada en el módulo de plataforma de confianza y, si no, impedir el resto del procedimiento de arranque y, en caso afirmativo, permitir la ejecución del código de inicialización de la plataforma principal para medir y verificar si dispositivos adicionales (DISP1 a DISPn) acoplados a la plataforma satisfacen la información de las directrices y, en caso afirmativo, permitir la ejecución del código de inicialización de la plataforma principal para medir y verificar si el cargador del sistema operativo satisface la información de las directrices y, en caso afirmativo, permitir que el procesador cargue un sistema operativo (110) y, si no, abstenerse de cargar un sistema operativo; y en el que el sistema operativo, si se carga, ha de ser ejecutado por el procesador.

7. El procedimiento de la reivindicación 6 que, además, comprende:

detectar una condición de reposición de la plataforma.

8. Un artículo que comprende un medio accesible por máquina que tiene datos asociados en el que los datos, cuando son objeto de acceso, dan como resultado que una máquina lleve a cabo un procedimiento según cualquiera de las reivindicaciones 6 y 7.

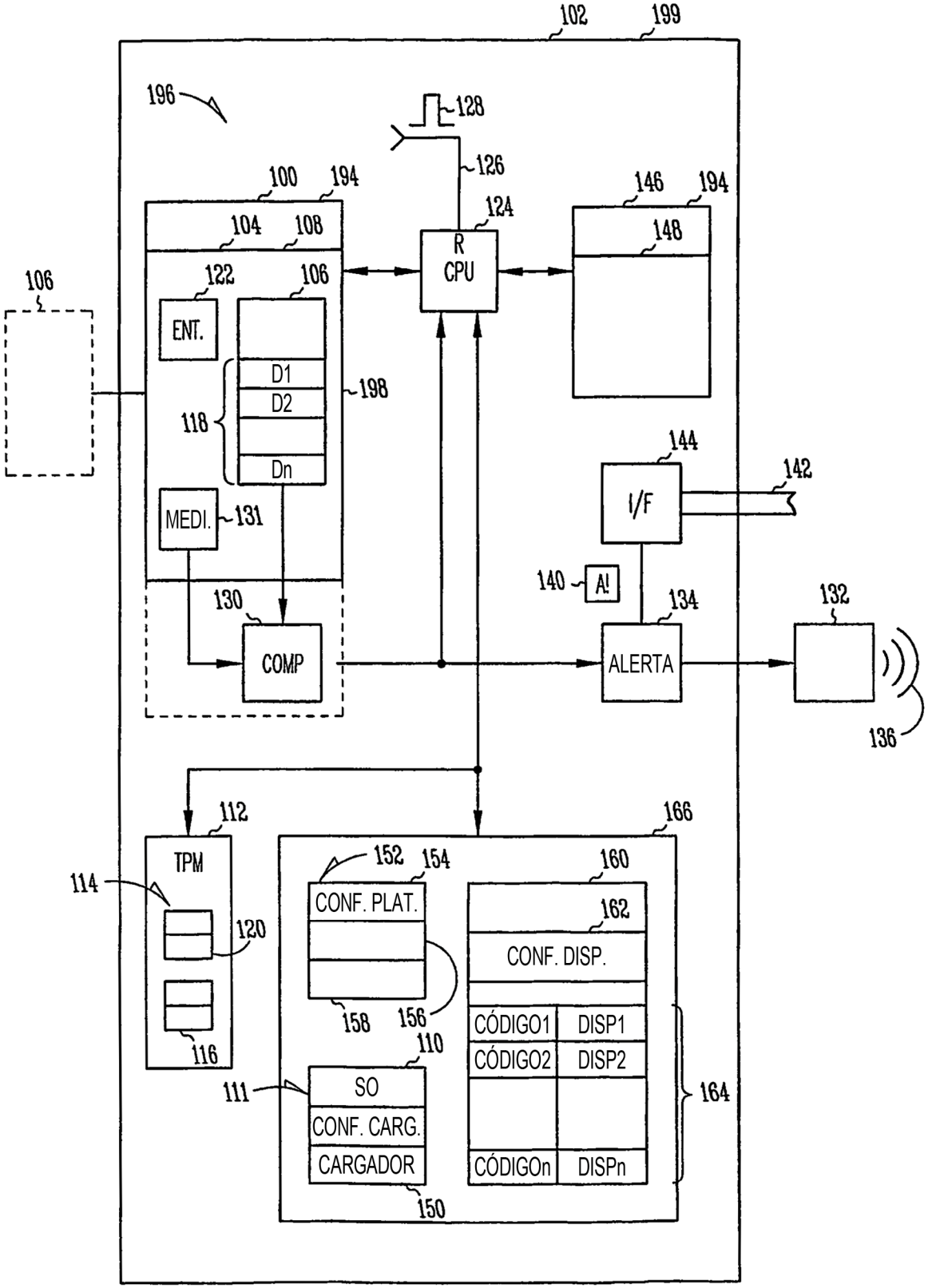
102
199
196
128
126
100
194
146
194
104
108
124
148
R
CPU
106
122
106
ENT.
D1
D2
198
118
Dn
144
142
I/F
MEDI.
131
140
A!
130
134
132
COMP
ALERTA
136
112
166
TPM
152
154
160
114
CONF. PLAT.
162
CONF. DISP.
120
158
156
CÓDIGO1
DISP1
116
110
CÓDIGO2
DISP2
111
SO
164
CONF. CARG.
CÓDIGOn
DISPn
CARGADOR
150

Fig. 1

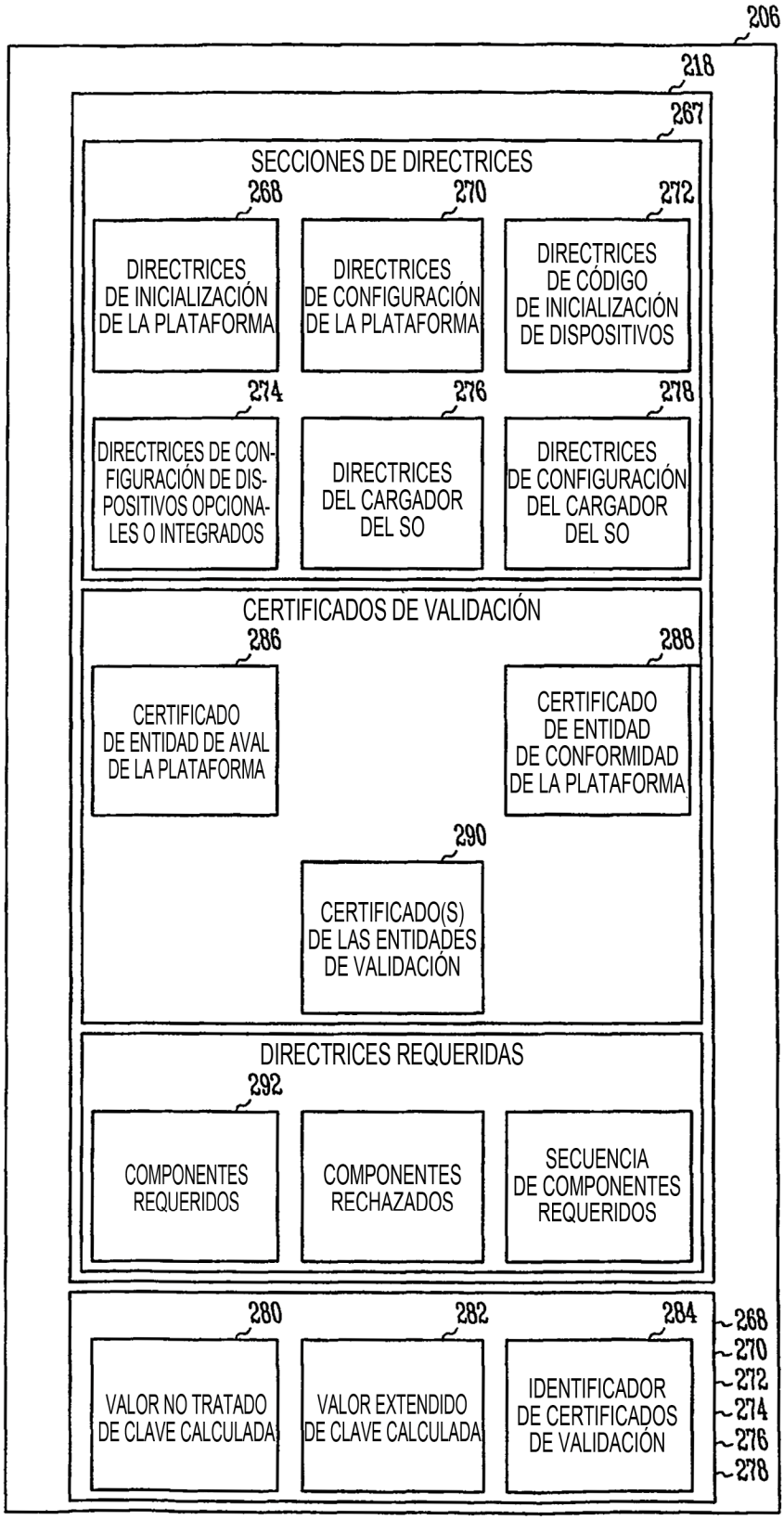
206
218
267
SECCIONES DE DIRECTRICES
268
DIRECTRICES DE INICIALIZACIÓN DE LA PLATAFORMA
270
DIRECTRICES DE CONFIGURACIÓN DE LA PLATAFORMA
272
DIRECTRICES DE CÓDIGO DE INICIALIZACIÓN DE DISPOSITIVOS
274
DIRECTRICES DE CONFIGURACIÓN DE DISPOSITIVOS OPCIONALES O INTEGRADOS
276
DIRECTRICES DEL CARGADOR DEL SO
278
DIRECTRICES DE CONFIGURACIÓN DEL CARGADOR DEL SO
CERTIFICADOS DE VALIDACIÓN
286
CERTIFICADO DE ENTIDAD DE AVAL DE LA PLATAFORMA
288
CERTIFICADO DE ENTIDAD DE CONFORMIDAD DE LA PLATAFORMA
290
CERTIFICADO(S) DE LAS ENTIDADES DE VALIDACIÓN
DIRECTRICES REQUERIDAS
292
COMPONENTES REQUERIDOS
COMPONENTES RECHAZADOS
SECUENCIA DE COMPONENTES REQUERIDOS
280
VALOR NO TRATADO DE CLAVE CALCULADA
282
VALOR EXTENDIDO DE CLAVE CALCULADA
284
IDENTIFICADOR DE CERTIFICADOS DE VALIDACIÓN
268
270
272
274
276
278

Fig. 2

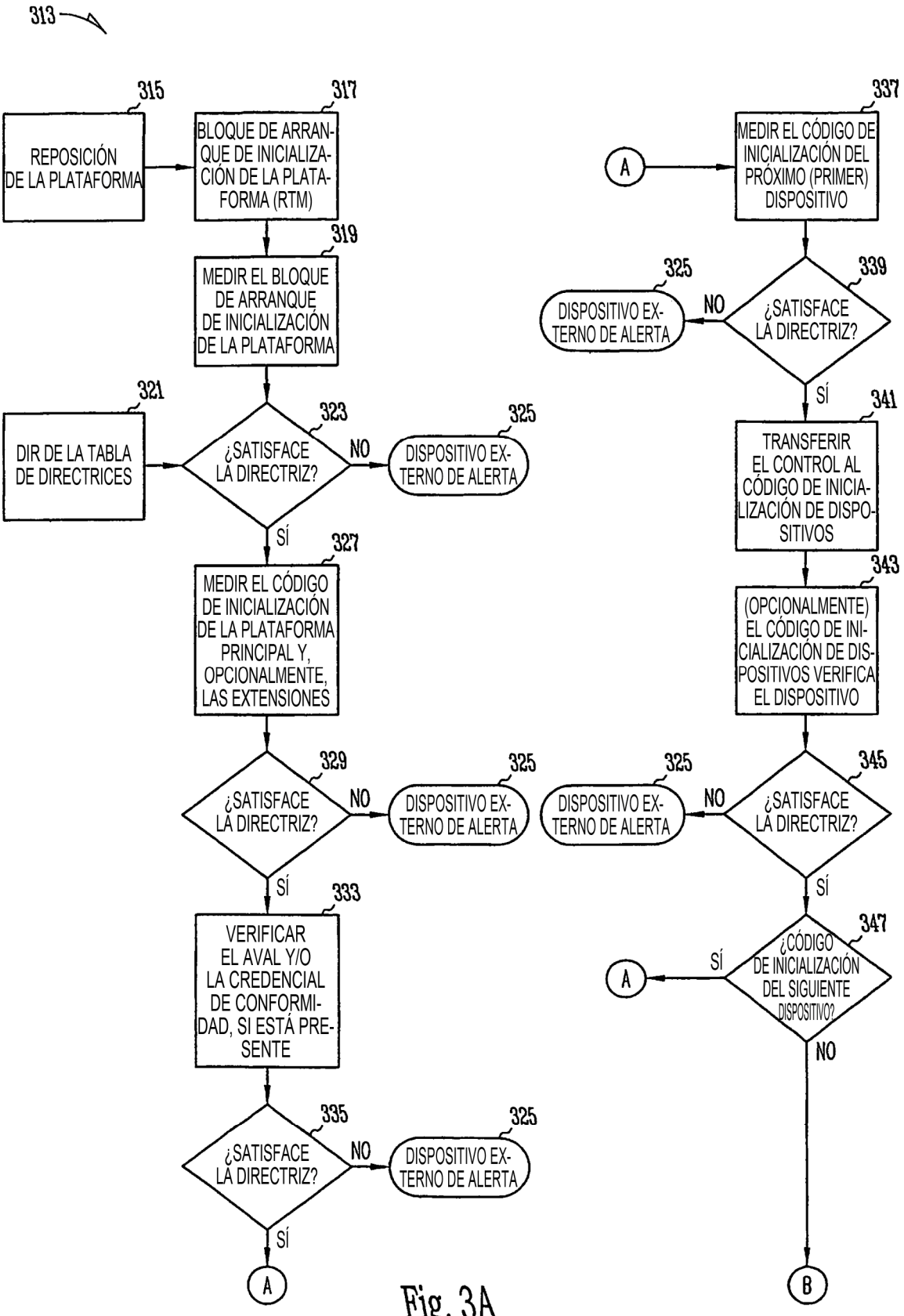
313
315
REPOSICIÓN DE LA PLATAFORMA
317
BLOQUE DE ARRANQUE DE INICIALIZACIÓN DE LA PLATAFORMA (RTM)
319
MEDIR EL BLOQUE DE ARRANQUE DE INICIALIZACIÓN DE LA PLATAFORMA
321
DIR DE LA TABLA DE DIRECTRICES
323
¿SATISFACE LA DIRECTRIZ?
NO
325
DISPOSITIVO EXTERNO DE ALERTA
SÍ
327
MEDIR EL CÓDIGO DE INICIALIZACIÓN DE LA PLATAFORMA PRINCIPAL Y, OPCIONALMENTE, LAS EXTENSIONES
329
¿SATISFACE LA DIRECTRIZ?
NO
325
DISPOSITIVO EXTERNO DE ALERTA
SÍ
333
VERIFICAR EL AVAL Y/O LA CREDENCIAL DE CONFORMIDAD, SI ESTÁ PRESENTE
335
¿SATISFACE LA DIRECTRIZ?
NO
325
DISPOSITIVO EXTERNO DE ALERTA
SÍ
A
A
337
MEDIR EL CÓDIGO DE INICIALIZACIÓN DEL PRÓXIMO (PRIMER) DISPOSITIVO
339
¿SATISFACE LA DIRECTRIZ?
NO
325
DISPOSITIVO EXTERNO DE ALERTA
SÍ
341
TRANSFERIR EL CONTROL AL CÓDIGO DE INICIALIZACIÓN DE DISPOSITIVOS
343
(OPCIONALMENTE) EL CÓDIGO DE INICIALIZACIÓN DE DISPOSITIVOS VERIFICA EL DISPOSITIVO
345
¿SATISFACE LA DIRECTRIZ?
NO
325
DISPOSITIVO EXTERNO DE ALERTA
SÍ
347
¿CÓDIGO DE INICIALIZACIÓN DEL SIGUIENTE DISPOSITIVO?
SÍ
A
NO
B

Fig. 3A

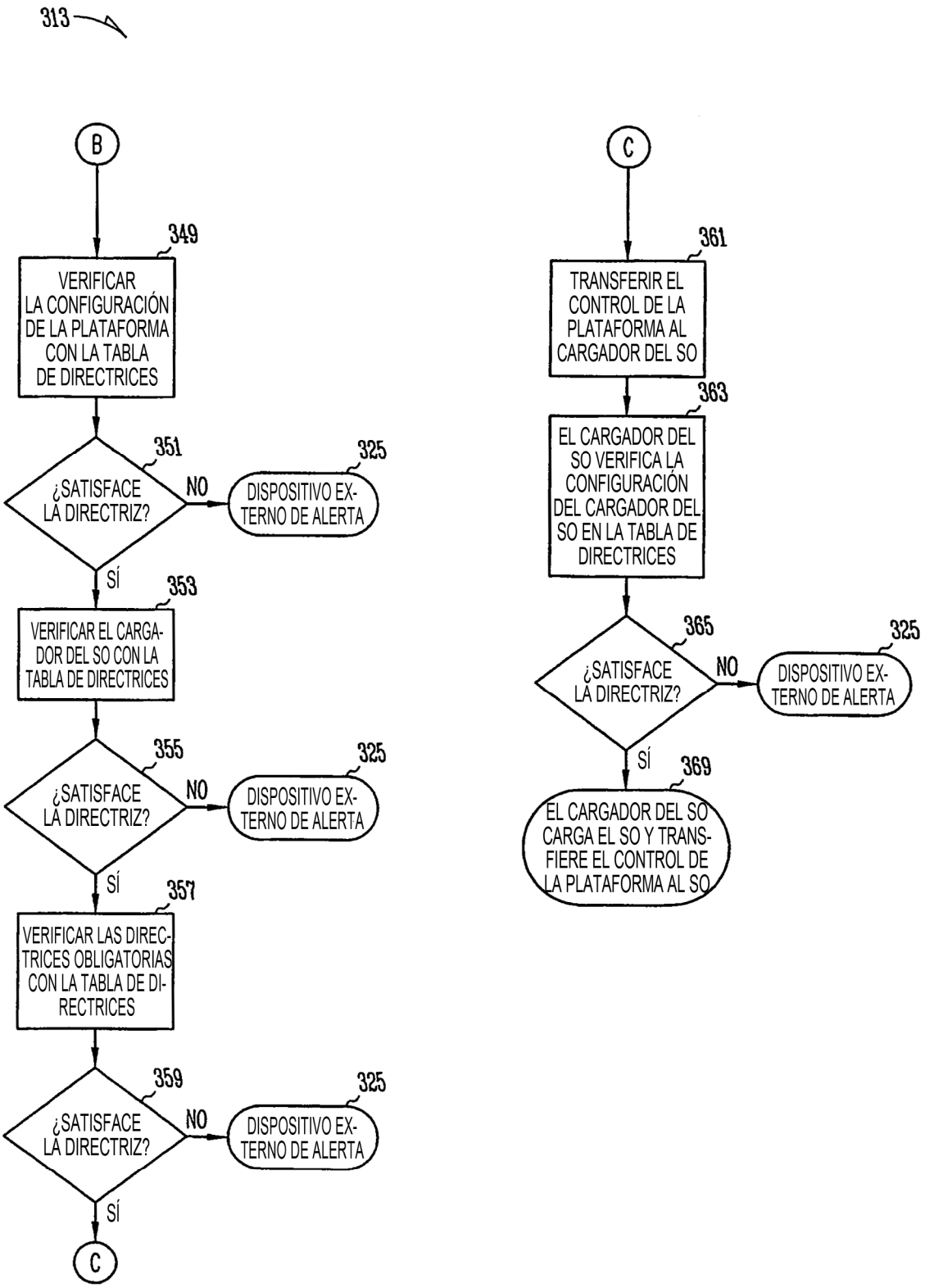
313
B
349
VERIFICAR LA CONFIGURACIÓN DE LA PLATAFORMA CON LA TABLA DE DIRECTRICES
351
¿SATISFACE LA DIRECTRIZ?
NO
325
DISPOSITIVO EXTERNO DE ALERTA
SÍ
353
VERIFICAR EL CARGADOR DEL SO CON LA TABLA DE DIRECTRICES
355
¿SATISFACE LA DIRECTRIZ?
NO
325
DISPOSITIVO EXTERNO DE ALERTA
SÍ
357
VERIFICAR LAS DIRECTRICES OBLIGATORIAS CON LA TABLA DE DIRECTRICES
359
¿SATISFACE LA DIRECTRIZ?
NO
325
DISPOSITIVO EXTERNO DE ALERTA
SÍ
C
C
361
TRANSFERIR EL CONTROL DE LA PLATAFORMA AL CARGADOR DEL SO
363
EL CARGADOR DEL SO VERIFICA LA CONFIGURACIÓN DEL CARGADOR DEL SO EN LA TABLA DE DIRECTRICES
365
¿SATISFACE LA DIRECTRIZ?
NO
325
DISPOSITIVO EXTERNO DE ALERTA
SÍ
369
EL CARGADOR DEL SO CARGA EL SO Y TRANSFIERE EL CONTROL DE LA PLATAFORMA AL SO

Fig. 3B