(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 392 440**

(51) Int. CI.:

G06F 21/00 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **05757249 .7**

(96) Fecha de presentación: **03.06.2005**

(97) Número de publicación de la solicitud: **1759261**

(97) Fecha de publicación de la solicitud: **07.03.2007**

(54) Título: **Procedimiento y aparato para proporcionar una virtualización segura de un módulo de plataforma de confianza**

(30) Prioridad:

24.06.2004 US 876994

(45) Fecha de publicación de la mención BOPI:

10.12.2012

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

10.12.2012

(73) Titular/es:

INTEL CORPORATION (100.0%)
(A DELAWARE CORPORATION) 2200 MISSION COLLEGE BOULEVARD
SANTA CLARA, CA 95052, US

(72) Inventor/es:

SCARLATA, VINCENT y
ROZAS, CARLOS

(74) Agente/Representante:

CARPINTERO LÓPEZ, Mario

DESCRIPCIÓN

Procedimiento y aparato para proporcionar una virtualización segura de un módulo de plataforma de confianza

Campo de la invención

La presente divulgación versa en general acerca del campo del procesamiento de datos y, más en particular, acerca de un procedimiento y de aparatos relacionados para proporcionar una virtualización segura de un módulo de plataforma de confianza.

Antecedentes

Un sistema de procesamiento convencional puede incluir recursos de soporte físico, tal como una unidad central de proceso (CPU) y una memoria de acceso aleatorio (RAM), así como recursos de soporte lógico, tal como un sistema operativo (SO) y uno o más programas o aplicaciones de usuario final. Normalmente, una aplicación se desarrolla para ser ejecutada en un SO particular. Cuando se arranca un sistema de ordenador típico convencional, carga el SO antes de cargar los programas o aplicaciones de usuario final. Normalmente, el SO hace de intermediario entre las aplicaciones de soporte lógico y el soporte físico en un sistema de procesamiento.

Además de RAM y una o más CPU, un sistema de procesamiento puede incluir un módulo de plataforma de confianza (TPM). Un TPM es un componente de soporte físico que reside dentro de un sistema de procesamiento y proporciona diversos dispositivos y servicios para mejorar la seguridad del sistema de procesamiento. Por ejemplo, puede usarse un TPM para proteger datos y para certificar la configuración de una plataforma. Los subcomponentes de un TPM pueden incluir un motor de ejecución y memoria o almacenamiento seguro no volátil (NV). La memoria segura NV se usa para almacenar información sensible, tal como claves de cifrado, y el motor de ejecución protege la información sensible según las normas de seguridad que han de ser implementadas por el TPM.

Puede implementarse un TPM según especificaciones tales como la Versión 1.2 de TPM del Trusted Computing Group (TCG), fechada el 2 de octubre de 2003 (en lo sucesivo, “especificación TPM”), que incluye partes como Principios de diseño, Estructuras TMP e Instrucciones TPM. La especificación TPM está publicada por el TCG es está disponible en Internet en www.trustedcomputinggroup.pro/home.

En general, un TPM compatible con TCG proporciona servicios de seguridad tales como certificación de la identidad y/o la integridad de la plataforma con base en las características de la plataforma. Las características de la plataforma normalmente consideradas por un TPM incluyen componentes de soporte físico de la plataforma tales como el o los procesadores y el conjunto de chips, así como el soporte lógico que reside en la plataforma, tal como el soporte lógico inalterable y el SO. Un TPM también puede soportar la auditoría y el registro de la procesos de soporte lógico, así como la verificación de la integridad de arranque de la plataforma, la integridad de los ficheros y la licencia de uso del soporte lógico. Por lo tanto, puede decirse que un TPM proporciona una raíz de confianza para una plataforma. En consecuencia, un tercero puede implementar normas de seguridad que requieran que los sistemas solicitantes proporcionen una certificación de la plataforma basada en TPM. Por ejemplo, el tercero puede configurar un servidor para que deniegue las peticiones de los clientes, a no ser que esos clientes estén acompañados de una certificación válida, procedente de los sistemas clientes, de la plataforma basada en TPM.

Sin embargo, cuando un sistema de procesamiento convencional usa un TPM, ese sistema de procesamiento puede ser capaz de soportar únicamente un único entorno de soporte lógico en un momento dado.

Recientemente, la Intel Corporation empezó a desarrollar tecnología para proporcionar múltiples entornos independientes de soporte lógico dentro de un solo sistema de procesamiento. Por ejemplo, la tecnología desarrollada por Intel Corporation incluye características para particionar y gestionar los recursos de soporte físico de un sistema de procesamiento de una manera que permita que múltiples SO se ejecuten en la misma máquina de forma concurrente, operando cada SO sustancialmente como si estuviere en su propia máquina física independiente. En un sistema de procesamiento de ese tipo, cada SO puede operar dentro de un entorno de soporte lógico sustancialmente independiente. Tales entornos independientes pueden denominarse particiones o máquinas virtuales (VM). En la publicación de solicitud estadounidense nº 20020194482 se da a conocer una plataforma anfitriona de cálculo que proporciona uno o más entornos de cálculo e incluye un dispositivo de confianza dispuesto formando una métrica de integridad individual a cada entorno de cálculo. Se proporciona la métrica de integridad a un usuario en respuesta a una interrogación de integridad, firmada para su autenticación usando una clave de firma mantenida por el dispositivo de confianza. El usuario puede verificar que la métrica firmada de integridad corresponde al entorno de cálculo esperado.

Breve descripción de los dibujos

Las características y las ventajas de la presente invención se harán evidentes a partir de las reivindicaciones adjuntas, de la siguiente descripción detalladas de una o más realizaciones ejemplares y de las correspondientes figuras, en las cuales:

la FIG. 1 es un diagrama de bloques que representa un entorno adecuado de procesamiento de datos en el cual pueden implementarse ciertos aspectos de una realización ejemplar de la presente invención;
la FIG. 2 es un diagrama de bloques que representa una arquitectura adecuada de máquina virtual según una realización ejemplar de la presente invención;
la FIG. 3 es un diagrama de flujo que ilustra un procedimiento para proporcionar un TPM virtual según una realización de la presente invención; y
la FIG. 4 es un diagrama de flujo que ilustra un procedimiento para utilizar un TPM virtual según una realización de la presente invención.

Descripción detallada

Un TPM virtual (vTPM) es un dispositivo lógico que proporciona una funcionalidad similar a la de un TPM. La presente divulgación describe una o más realizaciones ejemplares de sistemas, procedimientos y aparatos para proporcionar TPM virtuales.

La FIG. 1 es un diagrama de bloques que representa un entorno 12 adecuado de procesamiento de datos en el cual pueden implementarse ciertos aspectos de una realización ejemplar de la presente invención. El entorno 12 de procesamiento de datos incluye un sistema 20 de procesamiento que incluye uno o más procesadores o unidades centrales 22 de proceso (CPU) acopladas en comunicación con diversos componentes adicionales a través de uno o más buses 24 de sistema u otras vías o medios de comunicación.

Tal como se usan en el presente documento, se pretende que las expresiones “sistema de procesamiento” y “sistema de procesamiento de datos” abarquen en líneas generales una sola máquina o un sistema de máquinas o dispositivos acoplados de forma comunicativa que operan conjuntamente. Sistemas de procesamiento ejemplares incluyen, sin limitación, sistemas de cálculo distribuidos, superordenadores, sistemas de cálculo de alto rendimiento, agrupamientos informáticos, ordenadores centrales, miniordenadores, sistemas cliente-servidor, ordenadores personales, estaciones de trabajo, servidores, ordenadores de bolsillo, ordenadores portátiles, tableros, teléfonos, agendas electrónicas (PDA), dispositivos de mano, dispositivos de entretenimiento tales como dispositivos de audio y/o vídeo y otros dispositivos para procesar o transmitir información.

El sistema 20 de procesamiento puede ser controlado, al menos en parte, por medio de indicaciones de dispositivos convencionales de entrada, tales como teclados, ratones, etc., y/o por directrices recibidas de otra máquina, interacción con un entorno de realidad virtual (VR), información biométrica de retorno u otras fuentes o señales de entrada. El sistema 20 de procesamiento puede utilizar una o más conexiones con uno o más sistemas 76, 78 de procesamiento de datos remotos, tal como a través de un controlador de red, un módem u otro acoplamiento comunicativo. Los sistemas de procesamiento pueden estar interconectados por medio de una red física y/o lógica 80, tal como una red de área local (LAN), una red de área amplia (WAN), una intranet, Internet, etc. Las comunicaciones que implican a la red 80 pueden utilizar diversas portadoras y protocolos cableados y/o inalámbricos de corto alcance o de largo alcance, incluyendo radiofrecuencia (RF), satélites, microondas, 802.11 del Instituto de Ingenieros Eléctricos y Electrónicos (IEEE), Bluetooth, ópticos, infrarrojos, cables, láser, etc.

Dentro del sistema 20 de procesamiento, el procesador 22 puede estar acoplado en comunicación con uno o más dispositivos de almacenamiento de datos volátiles o no volátiles, tales como memoria 26 de acceso aleatorio (RAM), memoria de solo lectura (ROM), dispositivos de almacenamiento masivo, como discos duros de electrónica de dispositivos integrada (IDE) y/u otros dispositivos o medios, tales como disquetes, almacenamiento óptico, cintas, memoria flash, tarjetas de memoria, discos de vídeo digital, almacenamiento biológico, etc. Para los fines de esta divulgación, el término “ROM” puede ser usado en general para referirse a dispositivos de memoria no volátil, tal como ROM programable borrable (EPROM), ROM programable borrable eléctricamente (EEPROM), ROM flash, memoria flash, etc. El procesador 22 también puede estar acoplado en comunicación con componentes adicionales, tales como controladores de vídeo, controladores de interfaz para sistemas informáticos pequeños (SCSI), controladores de red, controladores de bus serie universal (USB), dispositivos de entrada tales como un teclado y un ratón, etc. El sistema 20 de procesamiento también puede incluir uno o más puentes o concentradores 27, tales como un concentrador controlador de memoria, un concentrador, controlador de entrada/salida (I/O), un puente raíz PCI, etc., para acoplar en comunicación diversos componentes del sistema.

Algunos componentes tales como, por ejemplo, un controlador de red, pueden implementarse como tarjetas adaptadoras con interfaces, como un conector PCI, para comunicarse con un bus PCI. En una realización, uno o más dispositivos pueden implementarse como controladores integrados usando componentes tales como dispositivos o matrices lógicos programables o no programables, circuitos integrados para aplicaciones específicas (ASIC), ordenadores integrados, tarjetas inteligentes y similares.

Tal como se ilustra, el sistema 20 de procesamiento también incluye un TPM 30 acoplado comunicativamente con el procesador 24. El TPM 30 también puede denominarse TPM físico o TPM 30 de soporte físico (hwTPM). En una realización, el TPM 30 se implementa como un dispositivo integrado que reside en una placa base del sistema o placa principal del sistema 20 de procesamiento. El TPM 30 incluye varios dispositivos de almacenamiento, incluyendo registros volátiles 32 de configuración de la plataforma (PCR) y sesiones de autorización, así como

registros persistentes 36 de integridad de datos (DIR), resúmenes de autorizaciones y almacenamiento persistente de uso general. Cada uno de estos dispositivos puede tener una correspondiente estructura de datos en memoria.

La invención puede describirse por referencia a datos asociados o en conjunción con los mismos, incluyendo instrucciones, funciones, procedimientos, estructuras de datos, programas de aplicación, etc., los cuales, cuando son objeto de acceso por parte de una máquina, dan como resultado que la máquina lleve a cabo tareas o en la definición de tipos abstractos de datos o de contextos de soporte físico de bajo nivel. Los datos pueden almacenarse en un almacenamiento de datos volátil o no volátil.

Por ejemplo, la RAM 26 puede incluir una o más colecciones o grupos de instrucciones para proporcionar una virtualización segura de un TPM. En la realización ejemplar, esas instrucciones pueden implementar un servicio 104 de TPM seguro, que puede residir parcial o completamente dentro de un monitor 106 de máquina virtual (VMM) (véase la FIG. 2). El sistema 20 de procesamiento puede cargar el VMM 106 en la RAM 26 en el momento del arranque para soportar una o más máquinas virtuales dentro del sistema 20 de procesamiento. El sistema 20 de procesamiento puede cargar las instrucciones que implementan el VMM 106 desde la ROM y/o, por ejemplo, desde uno o más dispositivos locales o remotos de almacenamiento masivo. Si se usa cualquier instrucción adicional para soportar la virtualización segura de un TPM, esas instrucciones también pueden ser cargadas desde la ROM y/o, por ejemplo, desde uno o más dispositivos locales o remotos de almacenamiento masivo.

La FIG. 2 es un diagrama de bloques que representa una arquitectura ejemplar de máquina virtual que implica un VMM 106 dentro de un sistema 20 de procesamiento. En el nivel más bajo están el TPM 30 y otros componentes de soporte físico, tales como el procesador 24, el concentrador 27, etc. (ilustrados individualmente en la FIG. 1; identificados colectivamente como procesador y conjunto 23 de chips en la FIG. 2). En operación, el sistema 20 de procesamiento también incluye el VMM 106, implementado mediante la ejecución de componentes de soporte lógico o de soporte lógico inalterable, tales como un micronúcleo 100 y un SO 102 de servicio. El micronúcleo 100 puede incluir un pequeño núcleo de instrucciones para tareas de gestión del sistema tales como programación de instrucciones. El SO 102 de servicio puede incluir controladores de dispositivos y soporte lógico de virtualización de entornos para crear y mantener máquinas virtuales.

En la realización ejemplar, el VMM 106 también incluye un servicio 104 de TPM virtual para crear y mantener vTPM. El servicio 104 de TPM virtual también puede dotar a las máquinas virtuales de acceso a respectivos vTPM. Aunque los módulos de soporte lógico tales como el servicio 104 de TPM virtual residen dentro del VMM 106 en la realización ejemplar, en realizaciones alternativas esos módulos pueden residir en el soporte lógico inalterable o en cualquier otro entorno protegido.

Pueden proporcionarse servicios de TPM virtual para una amplia variedad de arquitecturas de VMM. En algunas realizaciones, no es necesario integrar un servicio de TPM virtual en un VMM. Además, en algunas realizaciones, el servicio de TPM virtual puede no ser parte en absoluto de un VMM.

En la realización ejemplar, el servicio 104 de TPM virtual reside en la memoria protegida del anfitrión. Por ejemplo, el sistema 20 de procesamiento puede usar tecnología tal como la descrita en las patentes estadounidenses n^{os} 6.507.904, 6.633.963 y 6.678.825 (transferidas todas a Intel Corporation) para cargar el servicio 104 de TPM en un área aislada de memoria que está protegida por el soporte físico, y ejecutar el servicio 104 de TPM desde la misma. En la realización ejemplar, la memoria protegida garantiza que el soporte lógico/las instrucciones puedan ejecutarse sin interferencia ni observación. En realizaciones alternativas, pueden usarse otras técnicas para proporcionar memoria protegida. Por ejemplo, un entorno puede incluir un modo de gestión del sistema (SMM) que proporcione memoria protegida, o podría crearse un entorno de ejecución protegida usando un compilador de soporte lógico resistente a la manipulación. También pueden residir en la memoria protegida otros componentes (por ejemplo, el VMM 106, el micronúcleo 100, los TPM virtuales 120A y 120B, etc.).

En la realización ejemplar, el VMM 106 soporta múltiples máquinas virtuales 110A y 110B, cada una de las cuales ejecuta su propio SO huésped independiente, y su propia pila de soporte lógico independiente de la confianza o su propia pila 108A, 108B de soporte lógico TCG (TSS). En la realización ejemplar, las TSS 108A y 108B se atienen a los estándares de TCG.

Tal como se describe con mayor detalle en lo que sigue, el servicio 104 de TPM virtual puede usar el TPM 30 para proporcionar TMP virtuales 120A y 120B distintos para las máquinas virtuales 110A y 110B, respectivamente.

Las flechas en negrita de la FIG. 2 representan eventos de virtualización (VE). Por ejemplo, la flecha 112 representa un VE que implica la transferencia de control desde la VM 110A al SO 102 de servicio. La flecha 114 representa un VE desencadenado cuando la VM 110A intenta acceder a un TPM. Tal como se ilustra, el servicio 104 de TPM virtual intercepta el VE para procesar el evento por referencia al vTPM 120A, según se indica por medio de la flecha 116. En la realización ejemplar, aunque la VM 110A puede no estar al tanto de ningún otro TPM que el vTPM 120A, el servicio 104 de TPM virtual puede usar el hwTPM 30 para soportar el vTPM 120A.

En la realización ejemplar, cada vTPM tiene sus propias estructuras de TPM, incluyendo una clave de aprobación (EK), una clave raíz de almacenamiento (SRK), una credencial de aprobación (credencial de la EK), una jerarquía de

claves de usuario, registros de configuración de plataforma (PCR), contadores monótonos, almacenamiento persistente interno, registros de integridad de datos (DIR), etc. Con referencia de nuevo a la FIG. 1, tal como se indica en las equivalencias de la esquina inferior derecha, las claves de almacenamiento se ilustran como óvalos sin relleno alguno, las claves de certificación de identidad (AIK) se ilustran como óvalos rellenos con líneas horizontales y las claves de firma se ilustran como óvalos rellenos con un patrón de puntos. Además, los óvalos en negrita representan claves que están ligadas a los PCR 32 del TPM 30. Las líneas entre claves indican relaciones madre/hija entre las claves. Por ejemplo, esas líneas indican que la SRK 50 es una clave madre para ciertas claves de soporte físico dentro del TPM 30, así como para ciertas claves virtuales dentro de cada vTPM. Las credenciales se representan mediante paralelogramos.

Las claves virtuales y otras estructuras u objetos dentro de un vTPM pueden tener la misma estructura que las claves u objetos de un TPM de soporte físico, pero los objetos virtuales dentro de un TPM virtual no son meras referencias a los objetos estándar dentro del TPM 30, tales como la EK 52, la SRK 50 y los PCR 32. En vez de ello, tal como se describe con mayor detalle en lo que sigue, cada TPM virtual recibe sus propios objetos diferenciados, tales como una EK virtual (vEK) 64, una SRK virtual (vSRK) 66, PCR virtuales (vPCR) 92 y DIR virtuales (vDIR) 94. Esos objetos virtuales pueden basarse o derivarse de los objetos del TPM de soporte físico. Por ejemplo, en la realización ejemplar, las SRK virtuales y las EK virtuales son hijas de la SRK de soporte físico o, en el caso de vTPM anidados, de una SRK virtual basada en último término en la SRK de soporte físico. Permitiendo que las claves del vTPM tengan su raíz en vSRK, este modelo permite el anidamiento de los vTPM.

Los objetos de TPM virtual tales como la vEK 64, la vSRK 66 y los vPCR 92 pueden, a su vez, servir de base para objetos virtuales adicionales dentro del vTPM 120A, tales como las claves virtuales 68 de firma (vSig), AIK virtuales 70 (vAIK) y claves virtuales 72 de almacenamiento/cifrado (vEnc). En la realización ejemplar, cada vTPM proporciona todas las funciones proporcionadas por un TPM de soporte físico (hwTPM), con las mismas interfaces de programación de aplicaciones (API). Cada vTPM 120A proporciona así características emuladas de TPM físico. Por ejemplo, el vTPM 120A puede incluir sus propios vDIR 94, vPCR 92, vAIK 70, etc. En consecuencia, el SO huésped de cada VM puede ser completamente ignorante de que el correspondiente vTPM no es un hwTPM. Por lo tanto, las VM pueden usar código de SO preexistentes. Además, según la realización ejemplar, puede configurarse un sistema de procesamiento con un hwTPM convencional para proporcionar vTPM sin requerir ninguna modificación al hwTPM.

Los PCR virtuales como los vPCR 92 no tienen las limitaciones de recursos de los hwTPM, sino que, en vez de ello, pueden tener un número configurable de PCR disponible para ellos. En la realización ejemplar, se almacenan vPCR 92 en el espacio de memoria del vTPM 120A, y el vTPM 120A emula las operaciones de PCR estándar, tales como operaciones de lectura y ampliación, en los vPCR 92.

En la realización ejemplar, el vTPM 120A usa soporte lógico para proporcionar contadores simulados persistentes monótonos. El número de contadores puede ser sustancialmente ilimitado. En la realización ejemplar, el vTPM 120A proporciona al menos los cuatro contadores esperados de los hwTPM. Los contadores del vTPM pueden no requerir ningún enlace directo con los contadores del TPM de soporte físico.

La arquitectura de la máquina virtual puede utilizar el TPM de soporte físico para proteger las claves virtuales y los datos relacionados. En una realización, las jerarquías de claves de la vTPM y los datos relacionados están protegidos dentro de un hwTPM estándar. Por ejemplo, las claves del TPM virtual pueden estar almacenadas en el TPM de soporte físico, y no ser liberadas nunca de él, a no ser que los datos sean cifrados primero por el vTPM 120A, según se describe en lo que sigue. En consecuencia, si un TPM virtual se ve comprometido, es posible que las porciones públicas de las claves del vTPM asociadas se vean sujetas a un uso no autorizado, pero solo mientras dure la situación comprometida. En la realización ejemplar, todas las claves permanecerán dentro del TPM de soporte físico y, por lo tanto, las claves privadas no pueden ser robadas ni usadas una vez que la situación comprometida haya finalizado.

Un sistema de procesamiento según la presente invención también puede proporcionar una arquitectura de protocolos de certificación que permita que los vTPM proporcionen servicios de certificación de TPM convencional. Pueden participar plenamente en el procedimiento de certificación interrogadores remotos que no sean conscientes en modo alguno de los TPM virtuales. Además, los interrogadores remotos conscientes del vTPM pueden ser capaces, sin protocolos adicionales, de distinguir los hwTPM de los vTPM y pueden entonces decidir si confiar o no en una plataforma que albergue un vTPM.

En la realización ejemplar, cuando un TPM virtual (vTPM) no está operativo, las estructuras de datos persistentes para ese vTPM se almacenan en disco y quedan selladas en los PCR de servicio del vTPM con la SRK madre. Así, el TPM 30 protege la vTPM incluso cuando la vTPM no se ejecuta.

En la realización ejemplar, el vTPM 120A es capaz de proporcionar de forma transparente funcionalidad de TPM tanto de sí mismo como del hwTPM en una única sesión de autorización de usuario. El vTPM 120A logra este objetivo manteniendo sesiones de autorización separadas tanto con el usuario como con el hwTPM. Es decir, el usuario creará una sesión de autorización con el vTPM 120A como si el vTPM fuese un hwTPM. Con base en esta sesión, el vTPM 120A puede completar la totalidad de las mismas verificaciones de autorización que realización un

hwTPM. Si el vTPM 120A puede proporcionar directamente la función solicitada, el vTPM 120A puede simplemente actualizar los valores de uso único para la lesión y responder. Si el vTPM 120A precisa que el TPM de soporte físico proporcione el servicio, el vTPM 120A creará una sesión de autorización o reutilizará una sesión existente de autorización con el hwTPM para realizar la solicitud. Una vez que vTPM 120A ha acabado de usar el hwTPM, el vTPM 120A puede actualizar los valores de uso único en la sesión del usuario y responder.

La FIG. 3 es un diagrama de flujo que ilustra un procedimiento para proporcionar un TPM virtual según una realización de la presente invención. El procedimiento de la FIG. se inicio después de que el TPM 30 se haya activado en el sistema 20 de procesamiento, de tal modo que, como un TPM convencional, el TPM 30 incluye una SRK 50, una EK 52 y credenciales estándar, tales como una Credencial EK 54, según se ilustra en la FIG. 1. En los bloques 210-214, el VMM 106 lleva a cabo varias operaciones para inicializar el servicio 104 de TPM virtual, en preparación para el soporte de TPM virtuales. Por ejemplo, en el bloque 210, el VMM 106 crea una AIK denominada clave certificadora (CK) 56. El VMM 106 puede usar un procedimiento estándar para crear las AIK para crear la CK 56. El servicio 104 de TPM virtual puede usar subsiguientemente la CK 56 cuanto certifique claves de aprobación virtual tales como la vEK 64. En el bloque 212, el servicio 104 de TPM virtual obtiene de un tercero o de un tercero de confianza (TTP), tal como una autoridad 76 de certificación de privacidad (CA), una credencial 58 para la CK 56. La credencial 58 de la CK está firmada por la CA 76 de privacidad y responde de la CK 56, lo que indica que la CK 56 está protegida por un TPM válido.

En el bloque 214, el VMM 106 crea una AIK denominada clave 57 de enlace (BK). La BK 57 puede ser usada más tarde para proteger los datos del vTPM cuando esos datos sean liberados del servicio 104 del vTPM. Por ejemplo, en la realización ejemplar, el vTPM 120A conserva los datos persistentes de forma similar a como el hwTPM almacena las claves y los registros persistentes. Sin embargo, para proteger contra la liberación de los datos, el vTPM 120A enlaza a la BK 57 lo que sigue: blobs de claves encapsulados por la vEK 64, blobs de claves encapsulados por la vSRK 66, datos de autorización para la vEK 64, datos de autorización para la vSRK 66, los vDIR 94 y blobs de claves encapsulados para claves persistentes que están cargadas.

Para el vTPM 120A, el equivalente lógico de los controladores de bus para implementar la localidad es el VMM 106. Así, el vTPM 120A operará en cualquier localidad en la que el VMM 106 instruya que lo haga. El VMM 106 puede usar cualquier técnica apropiada para cambiar la localidad actual del vTPM 120A según sea necesario.

Una vez que el VMM 106 haya inicializado el servicio 104 de TPM virtual, el servicio 104 de TPM virtual puede crear TPM virtuales cuando se le pida.

En la realización ejemplar, una vez inicializado, cada TPM virtual es capaz de operar y de soportar funciones tradicionales tales como la certificación, como si el TPM virtual fuese un TPM de soporte físico. Para permitir que el TPM virtual opere de esta manera, se dota al TPM virtual del mismo tipo de credenciales que se espera que tenga un TPM de soporte físico. Por ejemplo, tal como se describe con mayor detalle en lo que sigue, en una realización, para cada nuevo vTPM, el servicio 104 de TPM virtual crea u obtiene una nueva vEK, una nueva SRK virtual (vSRK) y credenciales para la vEK. Las credenciales de la vEK indican que la vEK está almacenada de manera segura según las especificaciones de un TPM. Además, el proveedor de soporte lógico del TPM virtual puede proporcionar una credencial de plataforma y una credencial de conformidad.

En la realización ejemplar, los bloques 216-222 representan operaciones para inicializar un TPM virtual para una máquina virtual. Por ejemplo, en respuesta a una solicitud de creación de la máquina virtual 110A, el servicio 104 de TPM virtual puede usar el TPM 30 para crear una clave de almacenamiento denominada vEK 64, tal como se indica en el bloque 216. Posteriormente, el servicio 104 de TPM virtual puede usar el TPM 30 para enlazar la vEK 64 con los valores de los PCR para el servicio 104 de TPM virtual y el entorno de arranque en los que reside el servicio 104 de TPM virtual. En el vTPM 120A también pueden crearse y almacenarse datos de autorización inicial para la vEK 64.

En el bloque 218, el servicio 104 de TPM virtual uses la CK 56 para certificar la vEK 64. Por ejemplo, el servicio 104 de TPM virtual puede usar la función TPM_CertifyKey del TPM 30 para certificar la vEK 64 y obtener información de certificación, tal como una estructura TPM_CERTIFY_INFO, para la vEK 64. En la realización ejemplar, esta información de certificación para la vEK 64 está firmada por la CK 56, y contiene la información de los PCR con la que está enlazada la vEK 64 (por ejemplo, información para los PCR 32). Este procedimiento puede garantizar que la vEK 64 esté almacenada en un TPM de soporte físico que esté autorizado por la CA 76 de privacidad. En la realización ejemplar, dado que la CA 76 de privacidad ha firmado la credencial 58 de la CK, se confiará en la certificación por parte de la CK 56 de los enlaces PCR de la vEK 64 como si la CA 76 de privacidad hubiese indicado que la vEK 64 está en un hwTPM que se considere bueno según los estándares TCG.

En el bloque 220, el servicio 104 de TPM virtual puede transmitir una solicitud de credenciales de la EK del vTPM a un tercero o un TTP denominado CA 78 de virtualización. Esa solicitud de credenciales puede incluir credenciales 58 de la CK y la información de certificación para la vEK 64 firmada por la CK 56.

La CA 78 de virtualización puede ser una autoridad certificadora en la que confía la CA de privacidad. Puede verse la CA 78 de virtualización, en general, como otro fabricante de TPM. En la realización ejemplar, la CA 78 de

virtualización es consciente del vTPM y es capaz de diferenciar entornos de TPM virtual autorizados o “seguros” de entornos de TPM virtual no autorizados o “inseguros”. En una realización, la CA 78 de virtualización es la única entidad fuera del sistema 20 de procesamiento que debe ser consciente de la existencia de la virtualización del TPM para una virtualización efectiva del TPM.

Una vez que la CA 78 de virtualización evalúa las credenciales 58 de la CK y la información de certificación para la vEK 64, incluyendo los enlaces de los PCR, si se aprueba la solicitud, la CA 78 de virtualización devolverá una credencial firmada 60 de la vEK al sistema 20 de procesamiento. En la realización ejemplar, la credencial 60 de la vEK incluye un campo modelo con datos que indican que la vEK 64 está asociada con un TPM virtual que se ejecuta en un entorno identificable. En el bloque 222 el servicio 104 de TPM virtual puede recibir la credencial firmada 60 de la vEK.

El procedimiento anterior puede establecer, por ello, la siguiente cadena de confianza: la credencial 58 de la CK es una credencial firmada por la CA 76 de privacidad para indicar que la CK 56 es una AIK legítima dentro de un TPM legítimo. La información de certificación para la vEK 64 indica que, según la CK 56, la vEK 64 es una clave enlazada con un conjunto particular de PCR y albergada en el mismo TPM legítimo. Dado que la CA 76 de privacidad creó las credenciales 58 de la CK, la CA 78 de virtualización confía en la información de certificación para la vEK 64 creada por la CK 56. Si la CA 78 de virtualización aprueba el entorno del vTPM al que está enlazada la EK, estará dispuesta, por lo tanto, a producir una credencial de aprobación para la vEK 64 para indicar que la vEK 64 representa a un TPM válido. Además, en la credencial 60 de la vEK, la CA 78 de virtualización puede incluir información de modelo para indicar que este TPM es virtual y puede ser objeto de confianza a discreción del interrogador remoto durante la certificación.

Los bloques 224-226 representan operaciones adicionales para inicializar el vTPM. En una realización, para llevar a cabo estas operaciones, el servicio 104 de TPM virtual usa funciones estándar para inicializar el vTPM 120A, como si el vTPM 120A fuese un hwTPM. Por ejemplo, el servicio 104 de TPM virtual puede efectuar una llamada a TPM_Get_PUBEK para obtener la porción pública de la vEK 64, y puede efectuar una llamada a TPM_TakeOwnership para crear la vSRK 66, tal como se representa en los bloques 224 y 226, respectivamente. En la realización ejemplar, el servicio 104 de TPM virtual enlaza la vSRK a los mismos PCR que la vEK 64 (es decir, los PCR 32). El servicio 104 de TPM virtual puede proporcionar las autorizaciones al vTPM 120A de una forma cifrada con la porción pública de la vEK 64. Estas autorizaciones pueden ser entonces descifradas por el vTPM 120A usando la vEK 64. En la realización ejemplar, se usa la clave vEK 64 preexistente para descifrar las autorizaciones, dado que no son TPM_BOUND_DATA (datos ligados a TPM).

En la realización ejemplar, los datos de autorización para la vEK 64 cambian de los almacenados en el vTPM 120A durante la creación de la vEK 64 a los proporcionados en la llamada a TPM_TakeOwnership.

La VM 110A puede usar entonces el vTPM 120A como si el vTPM 120A fue un hwTPM, tal como se representa en el bloque 228 y según se describe con mayor detalle en lo que sigue en relación con la FIG. 4. Tal como se muestra en el bloque 240, el servicio 104 de TPM virtual puede determinar entonces si se está creando una nueva VM que requiera un nuevo vTPM. En caso afirmativo, el procedimiento puede volver al bloque 216, llevándose a cabo operaciones para instanciar el nuevo vTPM según se ha descrito en lo que antecede, por ejemplo, creándose una nueva vEK para la nueva VM, etc. Si no se está creando una nueva VM, el servicio 104 de TPM virtual puede seguir usando el TPM 30 para proporcionar el vTPM 120A para la VM 110A.

La FIG. 4 es un diagrama de flujo que ilustra una realización ejemplar de un procedimiento para utilizar un TPM virtual, tal como el vTPM 120A. El procedimiento ilustrado proporciona más detalle en cuanto a algunas de las operaciones resumidas en el bloque 228 de la FIG. 3. Por ejemplo, los bloques 310-314 representan operaciones para crear una vAIK para la VM 110A, en las que la VM 110A usa el vTPM 120A como si el vTPM 120A fuese un hwTPM. El TPM virtual 120A puede crear una vAIK 70 en el TPM 30, y puede crear los documentos normales que un TPM de soporte físico crearía normalmente para una AIK.

Por ejemplo, en el bloque 310, la VM 110A crea una vAIK en el vTPM 120A realizando una llamada a TPM_MakeIdentity. En respuesta a esa llamada, el vTPM 120A da al TPM 30 la instrucción de que cree una nueva clave TCG_SIGNING_KEY dentro del TPM 30. Esa clave de firma, que servirá de nueva clave certificación de identidad virtual, tal como en representa en la FIG. 1 como vAIK 70. Así, desde la perspectiva del hwTPM, una AIK virtual puede no ser del tipo “AIK,” sino que puede ser una clave de firma. Sin embargo, para el mundo exterior al hwTPM, la AIK virtual puede servir de clave de tipo “AIK” y parecer serlo.

El vTPM 120A y la TSS 108A crean entonces el campo TCG_IDENTITY_CONTENTS para la vAIK 70. La TSS 108A puede ejecutar entonces TSS_CollateIdentityRequest para crear una TCG_IDENTITY_REQ. Esta llamada puede realizarse de la forma habitual, salvo que la credencial de la EK usada será la credencial 60 de la vEK, en vez de una credencial de la EK para un hwTPM.

Tal como se representa en el bloque 312, la TSS 108A que se ejecuta dentro de la VM 110A puede enviar entonces a la CA 76 de privacidad esa solicitud, que incluye documentos tales como la vAIK 70 y las credenciales 60 de la vEK. La CA 76 de privacidad examinará los documentos. Además, la CA 76 de privacidad puede no estar al tanto de

la virtualización del TPM y puede confiar en la credencial 60 de aprobación de la vEK procedente de la CA 78 de virtualización como lo haría con las credenciales de cualquier otro fabricante de TPM. Después de verificar los documentos, la CA 76 de privacidad creará una nueva credencial 62 de identidad para la vAIK 70, firmará esa credencial y la enviará al sistema 20 de procesamiento. En consecuencia, la TSS 108A puede recibir la credencial 62 de la vAIK procedente de la CA 76 de privacidad, tal como se muestra en el bloque 314.

A continuación, los bloques 320-324 representan operaciones ejemplares para la gestión de solicitudes de certificación. En el bloque 320, la vTPM 120A determina si una instrucción recibida requiere certificación en cuanto a la fiabilidad de la VM 110A. Cuando se recibe una solicitud de ese tipo, la TSS 108A puede usar el vTPM 120A para citar los vPCR 92, y puede usar la vAIK 70 para firmar la cita de los PCR, tal como se muestra en el bloque 322. Tal como se indica en el bloque 324, cuando una entidad remota interroga a la VM 110A, la TSS 108A puede transmitir la credencial 62 de la vAIK a la entidad remota como si la vAIK 70 fuese un hwTPM.

Según una realización, si el interrogador es consciente del vTPM, será capaz de mirar la información de modelo, descubrir que el TPM usado por la VM 110A es un vTPM, y decidir si debe o no confiarse en la plataforma subyacente. La información de modelo puede identificar de forma única la configuración de la plataforma subyacente.

Si el interrogador confía en la plataforma subyacente, el interrogador conocerá que la CA 76 de privacidad pretende lo siguiente: el vTPM tiene su raíz en un TPM de soporte físico, el vTPM solo está disponible para su uso en el TPM de soporte físico. Si el interrogador no confía en la configuración particular del TPM, el interrogador puede elegir rechazar la transacción. Además, si el interrogador es una aplicación preexistente no consciente de los vTPM, el interrogador será capaz de usar protocolos TPM estándar para concluir la certificación basándose simplemente en una determinación de confianza para la firma de la CA 76 de privacidad.

De manera similar, el vTPM 120A puede proporcionar todas las demás funcionalidades para una VM que un TPM convencional de soporte físico puede proporcionar para un sistema monolítico.

La realización o las realizaciones dadas a conocer permiten, así, que múltiples VM usen la funcionalidad de un TPM sin requerir múltiples TPM dedicados de soporte físico, sin requerir la modificación del soporte lógico dentro de una VM y sin requerir modificación a las entidades remotas que interactúan con un sistema como el presente. Según la presente divulgación, un TPM virtual puede medir el SO y las aplicaciones en una VM para proporcionar certificación a entidades remotas. Además, un TPM virtual puede certificar el estado de una máquina virtual para un interrogador del TPM de soporte físico, aunque el TPM de soporte físico y el interrogador puedan utilizar únicamente la funcionalidad descrita en las especificaciones actuales de un TPM, tal como la Especificación de diseño, Versión 1.2 de TPM a la que se hizo referencia en lo que antecede. El SO huésped en una máquina virtual puede seguir inconsciente de que se esté compartiendo un TPM de soporte físico, y no se requieren relaciones de confianza entre las VM dentro de un sistema.

Tal como se ilustra en la FIG. 1, para cada vTPM pueden crearse cero o más vSig 68, cero o más vAIK 70 y cero o más vEnc 72. Tal como se ha descrito en lo que antecede, en una realización pueden crearse y almacenarse en el hwTPM claves virtuales tales como las vSig 68, las vEnc 72, etc. En consecuencia, un vTPM puede almacenar y crear sus propias claves de tal manera que una situación comprometida de un TPM virtual no comprometa permanentemente las claves que se almacenaron en el vTPM.

Alternativamente, para una flexibilidad y/o un rendimiento mayores, las claves virtuales pueden ser creadas y usadas por el soporte lógico del vTPM. Por ejemplo, las claves virtuales pueden no ser almacenadas en el hwTPM ni ser directamente protegidas por el mismo. Las claves privadas pertenecientes al TPM virtual o generadas por el mismo pueden no ser objeto de operación por parte del TMP de soporte físico, porque el TMP de soporte físico puede no usar esas claves privadas para llevar a cabo operaciones criptográficas. En vez de ello, el TPM virtual puede usar el procesador anfitrión y un soporte lógico criptográfico para llevar a cabo operaciones criptográficas con sus claves privadas. Para hacer esto, el servicio de TPM virtual puede almacenar sus claves privadas en memoria protegida del anfitrión. Sin embargo, aunque la clave privada no esté en uso, el servicio de TPM virtual puede usar características del TPM de soporte físico para encapsular la clave en su configuración de soporte lógico.

Estas opciones pueden permitir que el vTPM cifre, descifre, firme y verifique objetos en el soporte lógico del vTPM con un rendimiento mucho mayor que el que puede ser proporcionado por un TPM de soporte físico. Por ello, estas opciones pueden resultar preferibles para el cifrado masivo o su uso, por ejemplo, en entornos servidores sensibles al rendimiento. Sin embargo, una solución de compromiso para un mayor rendimiento es que las claves virtuales puedan verse permanentemente comprometidas si un vTPM se ve comprometido.

En vista de los principios y de las realizaciones ejemplares descritos e ilustrados en el presente documento, se reconocerá que las realizaciones ilustradas pueden modificarse en disposición y detalle sin apartarse de tales principios. Por ejemplo, se han descrito TPM virtuales en conexión con máquinas virtuales, pero las realizaciones alternativas también incluyen los vTPM usados en conexión con otros tipos de subdivisiones del sistema, tales como particiones dentro de un servidor o un grupo de servidores que compartan un TPM de soporte físico. Por ejemplo, pueden usarse TPM virtuales en un sistema de cuatro procesadores que esté particionado en dos sistemas lógicos

de dos procesadores. Las enseñanzas del presente documento también podrían ser usadas para proporcionar un TPM lógico a uno o más coprocesadores de servicio, o a uno o más tipos distintos de elementos independientes de procesamiento en una plataforma de soporte físico.

Además, las realizaciones alternativas incluyen servicios de vTPM que no emulan un TPM de soporte físico, pero que sí amplían y/o amplifican las capacidades de un TPM de soporte físico (por ejemplo, proporcionando más PCR, más almacenamiento, etc.). Las realizaciones alternativas también incluyen un servicio de TPM virtual que se ejecute sobre un SO seguro, sobre un entorno gestionado de tiempo de ejecución (MRTE), en un procesador o coprocesador de servicio, en un modo de gestión del sistema (SMM) de una plataforma, etc.

Además, la exposición anterior se ha centrado en realizaciones particulares, pero se contemplan otras configuraciones. En particular, aunque en el presente documento se usen expresiones tales como “en una realización”, “en otra realización” o similares, estas frases están concebidas para hacer referencia en general a posibilidades de realización, y no se pretende que limiten la invención a configuraciones de realizaciones particulares. Tal como se usan en el presente documento, estas expresiones pueden hacer referencia a realizaciones iguales o distintas que sean combinables en otras realizaciones.

De forma similar, aunque se han descrito procedimientos ejemplares en relación con operaciones particulares llevadas en cabo en una secuencia particular, podrían aplicarse numerosas modificaciones a esos procedimientos para derivar numerosas realizaciones alternativas de la presente invención. Por ejemplo, realizaciones alternativas pueden incluir procedimientos que usen un número menor que la totalidad de las operaciones dadas a conocer, procedimientos que usen operaciones adicionales, procedimientos que usen las mismas operaciones en una secuencia diferente, y procedimientos en los que las operaciones individuales dadas a conocer en el presente documento se combinen, se subdividan o se alteren de otro modo.

Realizaciones alternativas de la invención incluyen también instrucciones de codificación de medios accesibles por máquina para llevar a cabo las operaciones de la invención. Tales realizaciones también pueden ser denominadas productos de programa. Tales medios accesibles por máquina pueden incluir, sin limitación, medios de almacenamiento tales como disquetes, discos duros, CD-ROM, ROM y RAM; así como medios de comunicaciones tales como antenas, cables, fibras ópticas, microondas, ondas de radio y otros soportes electromagnéticos u ópticos. En consecuencia, pueden distribuirse instrucciones y otros datos en entornos de transmisión o redes en forma de paquetes, datos en serie, datos en paralelo, señales, propagadas, etc., y pueden ser usados en un entorno distribuido y almacenados local y/o remotamente para su acceso por máquinas de un solo procesador o de múltiples procesadores.

También debería entenderse que los componentes de soporte físico y de soporte lógico representados en el presente documento representan elementos funcionales que están autocontenidos razonablemente, de modo que cada uno puede ser diseñado, construido o actualizado de forma sustancialmente independiente de los demás. En realizaciones alternativas, muchos de los componentes pueden ser implementados como soporte físico, soporte lógico o combinaciones de soporte físico y soporte lógico para proporcionar la funcionalidad descrita e ilustrada en el presente documento.

En vista de la amplia variedad de permutaciones útiles que pueden derivarse fácilmente a partir de las realizaciones ejemplares descritas en el presente documento, se pretende que esta descripción detallada sea únicamente ilustrativo, y no debería interpretarse que limite el alcance de la invención. Por lo tanto, lo que se reivindica como la invención son todas las implementaciones que se encuentren dentro del alcance de las reivindicaciones siguientes y todos los equivalentes de tales implementaciones.

REIVINDICACIONES

1. Un procedimiento de operación de un sistema (20) de procesamiento que comprende un procesador (22) y un módulo físico (30) de plataforma de confianza acoplado en comunicación con el procesador, comprendiendo el procedimiento:

a) ejecutar una máquina virtual (110) en el procesador;
b) ejecutar en el procesador un servicio (104) que usa el módulo físico de plataforma de confianza para crear para la máquina virtual un módulo virtual (120) de plataforma de confianza en una memoria protegida del sistema (20) de procesamiento que tiene registros (92) de configuración de la plataforma virtual en un espacio de memoria del módulo virtual de plataforma de confianza;
c) almacenar una clave (68, 70, 72) para el módulo virtual de plataforma de confianza en el módulo físico de plataforma de confianza;
d) operar el módulo virtual de plataforma de confianza para proporcionar a la máquina virtual características emuladas del módulo de plataforma de confianza basadas en valores almacenados en los registros de configuración de la plataforma virtual en el espacio de memoria del módulo virtual de plataforma de confianza y la clave almacenada en el módulo físico de plataforma de confianza.

2. Un procedimiento según la reivindicación 1 que, además, comprende:

emular la operación de los registros de configuración de registros estándar de configuración de plataforma usando los registros (92) de configuración de la plataforma virtual.

3. Un procedimiento según la reivindicación 1 en el que la operación de utilización del módulo virtual (120A:120B) de plataforma de confianza para proporcionar características de un módulo físico (30) de plataforma de confianza comprende:

usar el módulo virtual (120A:120B) de plataforma de confianza para emular un módulo físico (30) de plataforma de confianza de soporte físico para la máquina virtual (110A:110B) en el sistema (20) de procesamiento.

4. Un procedimiento según la reivindicación 3 en el que el módulo virtual (120A:120B) de plataforma de confianza comprende un primer módulo virtual (120A) de plataforma de confianza y la máquina virtual comprende una primera máquina virtual (110A:110B), comprendiendo el procedimiento, además:

crear un segundo módulo virtual (120B) de plataforma de confianza en el sistema (20) de procesamiento;
almacenar una clave para el segundo módulo virtual (120B) de plataforma de confianza en el módulo físico (30) de plataforma de confianza; y
emular un módulo físico de plataforma de confianza para la segunda máquina virtual usando el segundo módulo virtual (120B) de plataforma de confianza.

5. Un procedimiento según la reivindicación 1 en el que la operación de almacenamiento de una clave para el módulo virtual (120A:120B) de plataforma de confianza en el módulo físico de plataforma de confianza comprende almacenar al menos una clave seleccionada del grupo que consiste en:

una clave (52) de aprobación para el dispositivo virtual (120A:120B) de confianza; y
una clave raíz (50) de almacenamiento para el módulo virtual (120A:120B) de plataforma de confianza.

6. Un procedimiento según la reivindicación 1 que, además, comprende:

generar una clave (52) de aprobación para el módulo virtual (120A:120B) de plataforma de confianza, estando ligada la clave (52) de aprobación a un entorno para la máquina virtual (110A: 110B).

7. Un procedimiento según la reivindicación 6 que, además, comprende:

transmitir información de certificación para la clave (52) de aprobación a una autoridad de certificación; y
obtener una credencial de autorización de la autoridad de certificación.

8. Un procedimiento según la reivindicación 6 que, además, comprende:

transmitir información de certificación para la clave (52) de aprobación a una autoridad (78) de certificación de virtualización;
obtener una credencial de autorización para el módulo virtual (120A:120B) de plataforma de confianza de la autoridad (78) de certificación de virtualización;
transmitir la credencial de aprobación a una autoridad (76) de certificación de privacidad; y
recibir una credencial de identidad de la autoridad (76) de certificación de privacidad.

9. Un procedimiento según la reivindicación 1 en el que la operación de uso del módulo virtual (120A:120B) de plataforma de confianza para proporcionar características emuladas del módulo (30) de plataforma de confianza comprende:

obtener, de una autoridad (76) de certificación de privacidad, una credencial de identidad para una clave virtual (70) de certificación de la identidad asociada con una máquina virtual (110A:110B); y
transmitir la credencial de identidad a un interrogador.

10. Un aparato que comprende:

un medio accesible por máquina e instrucciones codificadas en el medio accesible por máquina en el que las instrucciones, cuando son ejecutadas por un sistema de procesamiento con un módulo físico (30) de plataforma de confianza, hacen que el sistema (20) de procesamiento lleve a cabo operaciones que comprenden:

a) ejecutar una máquina virtual (110) en el procesador;
b) ejecutar en el procesador un servicio (104) que usa el módulo físico de plataforma de confianza para crear para la máquina virtual un módulo virtual (120) de plataforma de confianza en una memoria protegida del sistema (20) de procesamiento que tiene registros (92) de configuración de la plataforma virtual en un espacio de memoria del módulo virtual de plataforma de confianza;
c) almacenar una clave (68, 70, 72) para el módulo virtual de plataforma de confianza en el módulo físico de plataforma de confianza;
d) operar el módulo virtual de plataforma de confianza para proporcionar a la máquina virtual características emuladas del módulo de plataforma de confianza basadas en valores almacenados en los registros de configuración de la plataforma virtual en el espacio de memoria del módulo virtual de plataforma de confianza y la clave almacenada en el módulo físico de plataforma de confianza.

11. Un aparato según la reivindicación 10 en el que el módulo virtual (120A:120B) de plataforma de confianza comprende un primer módulo virtual (120A) de plataforma de confianza, y las operaciones llevadas a cabo por las instrucciones comprenden, además:

crear un segundo módulo virtual (120B) de plataforma de confianza en el sistema (20) de procesamiento; y
almacenar una clave para el segundo módulo virtual (120B) de plataforma de confianza en el módulo físico (30) de plataforma de confianza.

12. Un aparato según la reivindicación 10 en el que la operación de uso del módulo virtual (120A:120B) de plataforma de confianza para proporcionar características emuladas del módulo físico (30) de plataforma de confianza comprende:

obtener, de una autoridad (76) de certificación de privacidad, una credencial de identidad para una clave virtual (70) de certificación de la identidad; y
transmitir la credencial de identidad a un interrogador.

13. Un aparato según la reivindicación 10 en el que la operación de uso del módulo virtual (120A:120B) de plataforma de confianza para proporcionar características emuladas del módulo (30) de plataforma de confianza comprende:

usar el módulo virtual (120A:120B) de plataforma de confianza para emular un módulo físico (30) de plataforma de confianza para la máquina virtual (110A:110B) en el sistema (20) de procesamiento.

14. Un sistema (20) de procesamiento que comprende:

un procesador (22);
un módulo físico (30) de plataforma de confianza acoplado en comunicación con el procesador (24);
un medio accesible por máquina acoplado en comunicación con el procesador; e
instrucciones para llevar a cabo operaciones que comprenden:

a) ejecutar una máquina virtual (110) en el procesador;
b) ejecutar en el procesador un servicio (104) que usa el módulo físico de plataforma de confianza para crear para la máquina virtual un módulo virtual (120) de plataforma de confianza en una memoria protegida del sistema (20) de procesamiento que tiene registros (92) de configuración de la plataforma virtual en un espacio de memoria del módulo virtual de plataforma de confianza;
c) almacenar una clave (68, 70, 72) para el módulo virtual de plataforma de confianza en el módulo físico de plataforma de confianza;
d) operar el módulo virtual de plataforma de confianza para proporcionar a la máquina virtual características emuladas del módulo de plataforma de confianza basadas en valores almacenados en los registros de configuración de la plataforma virtual en el espacio de memoria del módulo virtual de plataforma de confianza y la clave almacenada en el módulo físico de plataforma de confianza.

15. Un aparato según la reivindicación 14 en el que:

el sistema (20) de procesamiento comprende procesadores múltiples en uno o más servidores; y la operación de uso del módulo virtual (120A:120B) de plataforma de confianza para proporcionar características emuladas de plataforma de confianza comprende:

proporcionar un primer módulo virtual (120A) de plataforma de confianza a una primera partición en el sistema (20) de procesamiento y proporcionar un segundo módulo virtual (120B) de plataforma de confianza a una segunda partición en el sistema (20) de procesamiento.

16. Un aparato según la reivindicación 14 en el que la operación de uso del módulo virtual (120A:120B) de plataforma de confianza para proporcionar características emuladas del módulo de plataforma de confianza comprende:

proporcionar un módulo lógico de plataforma de confianza a uno o más coprocesadores de servicio.

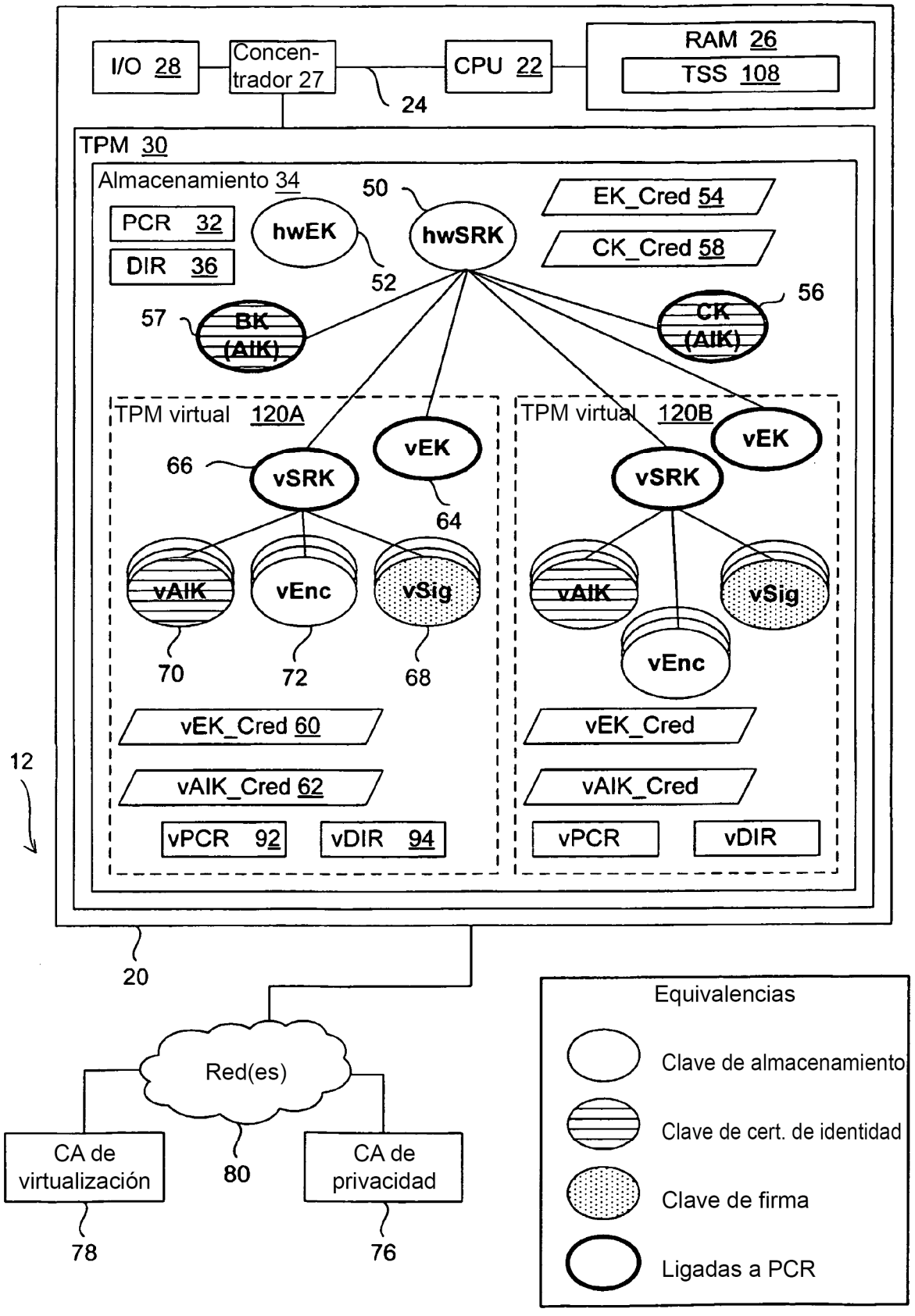
I/O 28
Concen-trador 27
24
CPU 22
RAM 26
TSS 108
TPM 30
Almacenamiento 34
PCR 32
DIR 36
hwEK
50
hwSRK
52
EK_Cred 54
CK_Cred 58
56
57
BK (AIK)
CK (AIK)
TPM virtual 120A
TPM virtual 120B
66
vSRK
vEK
64
vAIK
vEnc
vSig
70
72
68
vEK_Cred 60
vAIK_Cred 62
vPCR 92
vDIR 94
vEK_Cred
vAIK_Cred
vPCR
vDIR
12
20
Red(es)
80
CA de virtualización
78
CA de privacidad
76
Equivalencias
Clave de almacenamiento
Clave de cert. de identidad
Clave de firma
Ligadas a PCR

FIG. 1

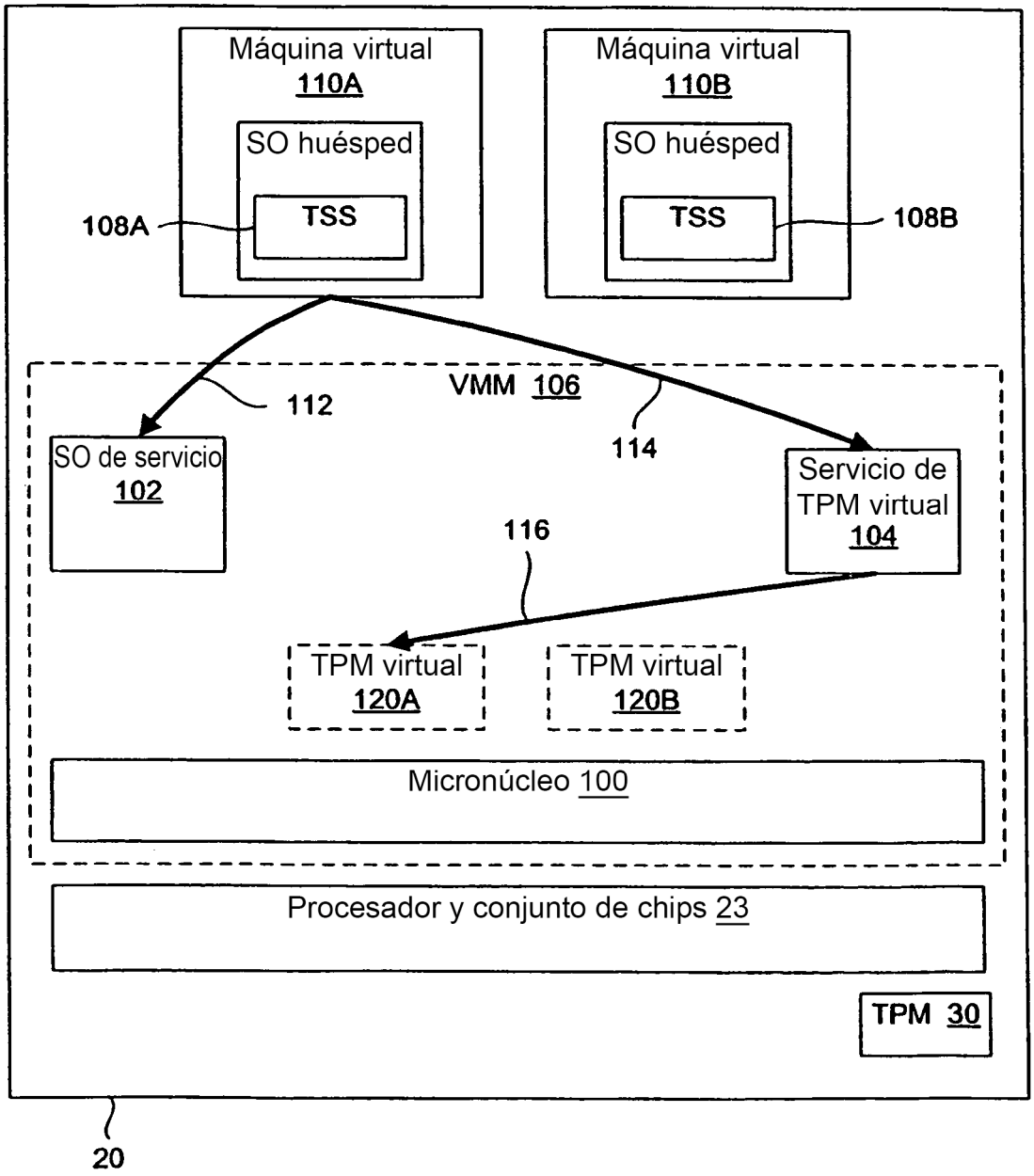
Máquina virtual
110A
SO huésped
TSS
108A
Máquina virtual
110B
SO huésped
TSS
108B
VMM 106
112
114
SO de servicio
102
Servicio de
TPM virtual
104
116
TPM virtual
120A
TPM virtual
120B
Micronúcleo 100
Procesador y conjunto de chips 23
TPM 30
20

FIG. 2

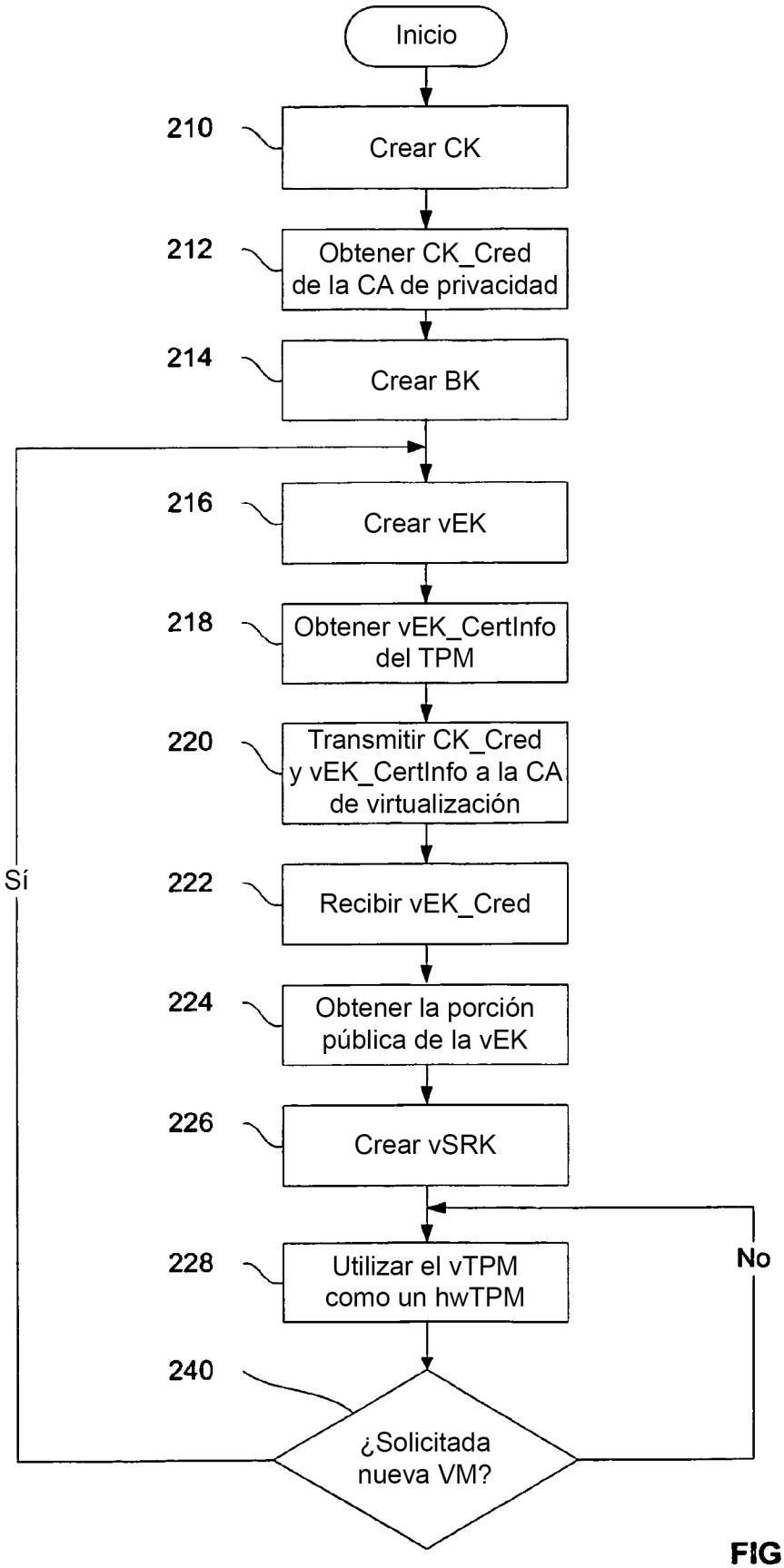
Inicio
210
Crear CK
212
Obtener CK_Cred de la CA de privacidad
214
Crear BK
216
Crear vEK
218
Obtener vEK_CertInfo del TPM
220
Transmitir CK_Cred y vEK_CertInfo a la CA de virtualización
222
Recibir vEK_Cred
224
Obtener la porción pública de la vEK
226
Crear vSRK
228
Utilizar el vTPM como un hwTPM
240
¿Solicitada nueva VM?
Sí
No

FIG. 3

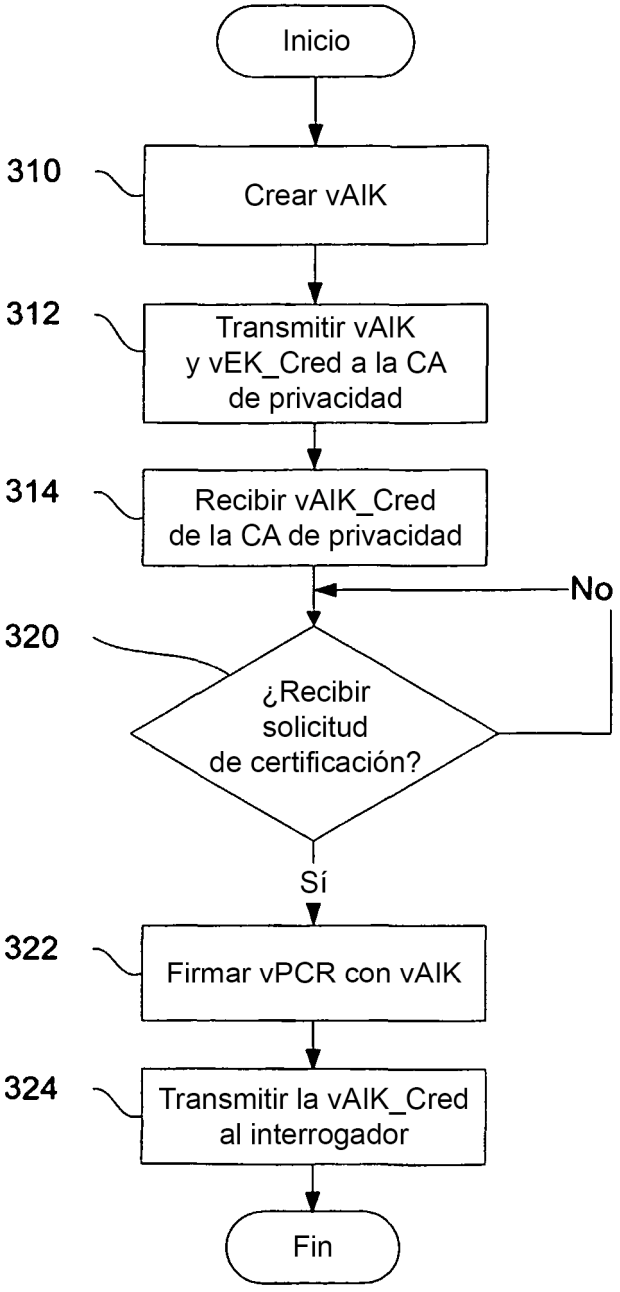
Inicio
310
Crear vAIK
312
Transmitir vAIK y vEK_Cred a la CA de privacidad
314
Recibir vAIK_Cred de la CA de privacidad
No
320
¿Recibir solicitud de certificación?
Sí
322
Firmar vPCR con vAIK
324
Transmitir la vAIK_Cred al interrogador
Fin

FIG. 4