(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 692 900**

(51) Int. CI.:

G06F 15/16 (2006.01)
G06F 9/44 (2008.01)
G06F 21/57 (2013.01)
G06F 21/00 (2013.01)
H04L 9/32 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **04.12.2012 PCT/US2012/067662**

(87) Fecha y número de publicación internacional: **20.06.2013 WO13090045**

(96) Fecha de presentación y número de la solicitud europea: **04.12.2012 E 12858587 (4)**

(97) Fecha y número de publicación de la concesión europea: **25.07.2018 EP 2791817**

(54) Título: **Certificación criptográfica de entornos de ejecución alojados seguros**

(30) Prioridad:

12.12.2011 US 201113323465

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
05.12.2018

(73) Titular/es:

MICROSOFT TECHNOLOGY LICENSING, LLC (100.0%)
One Microsoft Way
Redmond, WA 98052, US

(72) Inventor/es:

BAUMANN, ANDREW A.;
HUNT, GALEN C. y
PEINADO, MARCUS

(74) Agente/Representante:

ELZABURU, S.L.P

DESCRIPCIÓN

Certificación criptográfica de entornos de ejecución alojados seguros

Antecedentes

En un entorno informático convencional, el usuario controla el acceso físico a los sistemas informáticos del usuario. El usuario confía, hasta cierto punto, en el hardware y el software en sus centros de datos. Esta confianza, combinada con el control físico de los dispositivos, proporciona al usuario un cierto grado de confianza en que sus sistemas informáticos son seguros.

En un entorno informático alojado (hosted, en inglés), el usuario típicamente no tiene control físico sobre los sistemas informáticos utilizados para ejecutar las aplicaciones del usuario. El usuario, además de confiar en el hardware y software que se ejecuta en el entorno informático alojado, no tiene elección, excepto confiar en que el proveedor informático alojado no manipule o espíe el código y los datos del usuario. El usuario también confía en el proveedor informático alojado para proporcionar una seguridad física suficiente para evitar que personas no autorizadas extraigan los discos duros o manipulen el sistema. Y los usuarios depositan su confianza en el proveedor informático alojado para evitar la manipulación o el robo de sus datos por parte de terceros. Un proveedor informático alojado puede incurrir, por lo tanto, en una cierta cantidad de responsabilidad, en la forma de garantías y similares, para animar a los usuarios a ejecutar su software en el entorno informático alojado por el proveedor.

El documento US 2011/302415 A1 da a conocer un método para hacer seguras máquinas virtuales de clientes en una nube de múltiples usuarios. Se proporciona un primer disco virtual para una primera máquina virtual y se proporciona un segundo disco virtual para una segunda máquina virtual. Cada disco virtual comprende uno o más archivos de datos que contienen una imagen de disco (o parte de ella) para el disco virtual de cada máquina virtual. Los archivos de imagen del disco virtual son almacenados en un almacén de datos en forma cifrada, y se accede a los mismos a través de uno de los adaptadores de bus de anfitrión (HBA – Host Bus Adapter, en inglés) sobre la red. Se deberá obtener una clave de cifrado del cliente o del tercero de confianza del cliente antes de que las máquinas virtuales puedan ser operadas (realizar operaciones de entrada / salida) en los datos almacenados en los discos virtuales. Se debe reconocer que los datos descifrados son almacenados en memoria y puestos a disposición de las máquinas virtuales, pero seguirán siendo inaccesibles por el administrador.

Breve resumen

Este resumen se proporciona para introducir conceptos simplificados de la presente invención, que se describen con más detalle más adelante en la Descripción Detallada. Este resumen no pretende identificar características esenciales del objetivo reivindicado, ni está destinado a su utilización en la determinación del alcance del objeto reivindicado.

Las realizaciones de la presente invención permiten un servicio de alojamiento (hosting, en inglés) de aplicaciones para certificar de manera criptográfica que proporciona un entorno de ejecución seguro que es resistente al espionaje y a la manipulación de manera que incluye, por ejemplo, solo el código y los datos de confianza del usuario. Para atender una solicitud del sistema del cliente para establecer un entorno de ejecución seguro, se crea una instancia de área protegida de la memoria mediante un procesador con seguridad habilitada. El sistema informático alojado pasa por un protocolo de autenticación para proporcionar hechos verificables acerca del procesador con seguridad habilitada y el software y los datos en el entorno de ejecución seguro, tal como el fabricante y el modelo del procesador con seguridad habilitada y la identidad del distribuidor o código del software. Tras la finalización con éxito del protocolo de autenticación, se establece un canal de comunicación protegido criptográficamente entre el sistema del cliente y el entorno de ejecución seguro, y se ejecutan una o más aplicaciones dentro del entorno de ejecución seguro.

El servicio de alojamiento de la aplicación puede utilizar diversos certificados de confianza, incluidos los certificados de una autoridad confiable y uno o más intermediarios, para establecer una cadena de confianza del procesador con seguridad habilitada a la autoridad de confianza Estos certificados de confianza pueden ser utilizados colectivamente en el protocolo de autenticación para certificar la seguridad del procesador con seguridad habilitada. La aplicación del servicio de alojamiento puede ser auditada para verificar que los procesadores habilitados con seguridad del servicio de alojamiento de la aplicación son hechos seguros físicamente y no han sido manipulados. El auditor puede proporcionar un certificado de auditoría que puede ser utilizado como parte del protocolo de autenticación. Alternativamente, el auditor puede hacer que los resultados de la auditoría estén disponibles de otras maneras (por ejemplo, publicarlos en internet). El servicio de alojamiento de la aplicación puede utilizar (en el protocolo de autenticación) credenciales criptográficas para el procesador, producidas por el fabricante del hardware, que avala la integridad y el correcto funcionamiento del procesador con seguridad habilitada.

Breve descripción de los dibujos

La Descripción Detallada se expone haciendo referencia a las figuras adjuntas. En las figuras, el dígito o dígitos más a la izquierda de un número de referencia identifican la figura en la que aparece por primera vez el número de

referencia. La utilización de los mismos números de referencia en diferentes figuras indica elementos similares o idénticos.

La figura 1 es un diagrama esquemático de un sistema a modo de ejemplo que se puede utilizar para proporcionar un entorno de ejecución seguro.

La figura 2 es un diagrama de bloques de un sistema informático a modo de ejemplo que se puede utilizar para proporcionar un servidor de alojamiento de la aplicación según las realizaciones.

La figura 3 es un diagrama de bloques de un sistema informático a modo de ejemplo que se puede utilizar para proporcionar un sistema cliente de acuerdo con las realizaciones.

La figura 4 es un diagrama de flujo que muestra un proceso a modo de ejemplo para crear una instancia de un entorno de ejecución seguro.

La figura 5 es un diagrama de flujo que muestra un proceso a modo de ejemplo para verificar el establecimiento de un entorno de ejecución seguro.

La figura 6 muestra un entorno para la migración de un área protegida de la memoria de acuerdo con las realizaciones.

La figura 7 es un diagrama de flujo que muestra un proceso a modo de ejemplo para migrar un entorno de ejecución seguro.

La figura 8 es un diagrama de flujo que muestra un proceso a modo de ejemplo para recrear un entorno de ejecución seguro.

Descripción detallada

Descripción general

Tal como se explicó anteriormente, un usuario deposita un cierto grado de confianza en un proveedor informático alojado convencional para ejecutar de manera segura las aplicaciones del usuario y salvaguardar los datos del usuario. Las realizaciones de la presente Descripción Detallada permiten que el servicio informático alojado proporcione una certificación criptográfica de que el entorno de ejecución del usuario es resistente tanto a la manipulación como al espionaje, y de que el entorno de ejecución del usuario se establece con el contenido que el cliente solicita y sin código o datos no confiables. Proporcionar un entorno de ejecución seguro que esté libre de espionaje y manipulación puede, por sí solo, permitir que un proveedor informático alojado infalible configure el entorno de ejecución con código no confiable que pueda espiar o manipular el código del usuario y los datos desde dentro. Y el simple hecho de proporcionar un entorno de ejecución sin nada excepto el código y los datos de confianza del usuario puede, por sí solo, permitir que el proveedor alojado o un tercero manipulen o analicen el contenido del entorno de ejecución desde fuera del entorno de ejecución. Pero las realizaciones de la presente invención permiten que un proveedor informático alojado certifique criptográficamente que proporciona un entorno de ejecución seguro que es resistente al espionaje y manipulación externos y que no incluye códigos y datos no confiables.

Los sistemas informáticos de acuerdo con las realizaciones incluyen un procesador con seguridad habilitada configurado para crear, para un sistema cliente (tal como un dispositivo informático controlado por un usuario o consumidor informático alojado), un entorno informático seguro que incluye un área protegida de la memoria. El código y los datos seleccionados por el sistema cliente son almacenados en un área protegida de la memoria y se puede acceder al código almacenado en el área protegida de la memoria, pero es inaccesible para todos los códigos que se ejecutan fuera del área protegida de la memoria. Este último incluye el código que se ejecuta en otras áreas protegidas de la memoria que puedan existir. El código en el entorno de ejecución seguro puede ser elegido por el sistema cliente, por el proveedor de servicios, por terceros o por una combinación de todos ellos. Por ejemplo, el sistema cliente podría elegir ejecutar solo su código de aplicación (incluidas las librerías de soporte) en el entorno de ejecución seguro. La ejecución de este código está protegida de todos los demás códigos del ordenador.

Los hilos pueden pasar del código de ejecución fuera del área protegida de la memoria al código de ejecución dentro del área protegida de la memoria solo a través de funciones de puerta de entrada específicas mediadas por el procesador con seguridad habilitada. Del mismo modo, los hilos pasan de un código en ejecución dentro del área protegida de la memoria al código en ejecución fuera del área protegida de la memoria a través de funciones específicas de la puerta de salida por medio del procesador con seguridad habilitada. El código que se ejecuta en el área protegida de la memoria no tiene privilegios especiales, excepto la capacidad de acceder al código y a los datos en el área protegida de la memoria. Por ejemplo, el código que se ejecuta en el área protegida de la memoria no necesita ser ejecutado en el modo de kernel o en el modo privilegiado del procesador, ni tampoco necesita acceso a instrucciones, tal como instrucciones de E/S, a las que solo se puede acceder desde el modo de kernel del procesador o modo privilegiado. El área de la memoria protegida mediante hardware es llevada a un estado inicial

conocido y, a continuación, cargada con un módulo de cargador y uno o más parámetros especificados por el sistema cliente del usuario para establecer un estado de activación solicitado del área protegida de la memoria.

El entorno de ejecución confiable proporciona un mecanismo por el cual el código de confianza del usuario que es ejecutado dentro del área protegida de la memoria certifica al sistema cliente que se está ejecutando dentro de un entorno de ejecución seguro. El procesador con seguridad habilitada ejecuta un protocolo de autenticación, que implica proporcionar al sistema cliente una certificación de que se ha establecido un entorno de ejecución seguro y de que, en un estado de activación inicial del entorno de ejecución seguro, solo se ejecuta el software identificado (de manera explícita o implícita) en una solicitud del usuario cliente. El protocolo de autenticación puede involucrar al cliente o a otras partes. El propósito del protocolo de autenticación es verificar criptográficamente el sistema cliente (u otro sistema) que el entorno de ejecución seguro tiene propiedades particulares. Estas propiedades pueden incluir, en varios ejemplos no limitativos:

1. El fabricante y modelo del procesador con seguridad habilitada.

2. El código y los datos con los que se inició el entorno de ejecución seguro.

3. El proveedor de software y otra información sobre el código y los datos con los que se inició el entorno de ejecución seguro. Por ejemplo,

a. el software fue escrito por (y firmado por) un desarrollador / distribuidor concreto de software

b. el software es una versión particular con parches de seguridad de una fecha en particular. En diversas realizaciones no limitativas, el proveedor de software firma certificados que contienen resúmenes, tal como autenticadores criptográficos de los módulos de software relevantes.

Ejemplos no limitativos de protocolos de autenticación incluyen:

- Direct Anonymous Attestation (referencia: E. Brickell, J. Camenish, L. Chen. Autenticación anónima directa. En las actas de la 11ª conferencia ACM sobre seguridad de los ordenadores y en las comunicaciones (ACM conference on computer and communications security). Páginas 132 a 145, 2004.

- Protocolos de clave pública estándar que incluyen certificados de autenticación firmados con la clave privada del procesador con seguridad habilitada.

A continuación, se describen diversas realizaciones de un protocolo de autenticación. Las realizaciones no se limitan a las siguientes realizaciones, y el protocolo de autenticación descrito a continuación puede incluir una funcionalidad adicional, tal como con cadenas de confianza basadas en una o más autoridades de certificación de confianza, sin apartarse del alcance de la presente Descripción Detallada. Una vez que se crea una instancia del área protegida de la memoria con el estado de activación solicitado, el procesador con seguridad habilitada produce un identificador que identifica el estado de activación inicial de activación de la memoria protegida mediante hardware, y almacena el identificador en una ubicación accesible solo para el procesador con seguridad habilitada. El identificador puede incluir un resumen, tal como un autenticador criptográfico (hash, en inglés), del estado de activación del área protegida de la memoria. El identificador puede incluir una clave pública que el procesador de seguridad utilizó para descifrar los contenidos colocados en el área protegida de la memoria en el estado de activación. El identificador puede ser algún otro identificador que identifique el estado de activación.

El módulo de cargador es ejecutado, y hace que el procesador con seguridad habilitada cree un certificado de autenticación firmado mediante una clave privada del procesador con seguridad habilitada. El certificado de autenticación firmado es transmitido al sistema cliente y, por lo tanto, permite al sistema cliente verificar, utilizando una clave pública conocida del procesador con seguridad habilitada que se corresponde con la clave privada del procesador con seguridad habilitada, que el certificado de autenticación está firmado por el procesador con seguridad habilitada. El certificado de autenticación firmado permite asimismo al sistema cliente verificar que el sistema cliente se comunica con un módulo de cargador que se ejecuta en un área protegida de la memoria creada por el procesador con seguridad habilitada. Por lo tanto, se forma una relación de confianza entre el sistema cliente y el procesador con seguridad habilitada. Una cadena de confianza que incluye certificados adicionales de una autoridad de confianza, y posiblemente uno o más intermediarios, puede ser utilizada en las realizaciones para establecer la relación de confianza.

El certificado de autenticación incluye el identificador del estado de activación del área protegida de la memoria. El sistema cliente compara el identificador con un identificador conocido del estado de activación solicitado para determinar que el estado de activación del área protegida de la memoria es el estado de activación solicitado, incluido el módulo de cargador y uno o más parámetros. Debido a que el certificado de autenticación con el identificador está firmado / cifrado con la clave privada del procesador con seguridad habilitada, y debido a que se establece una relación de confianza entre el sistema cliente y el procesador con seguridad habilitada, el sistema cliente puede confiar en el identificador para determinar que el estado de activación del área protegida de la memoria es el estado de activación solicitado.

Por lo tanto, las realizaciones proporcionan al sistema cliente la verificación de que el proveedor de servicios informáticos alojado establece un entorno de ejecución de seguridad frente a la manipulación y el espionaje, y que en el entorno de ejecución seguro se crea una instancia con el estado de activación solicitado. El certificado de autenticación firmado proporciona al sistema cliente la verificación de que el entorno de ejecución seguro está establecido. Y el identificador proporciona al sistema cliente la verificación de que en el entorno de ejecución seguro se crea una instancia con el estado de activación solicitado. El sistema cliente, a continuación, utiliza el entorno de ejecución seguro para cargar y ejecutar las aplicaciones solicitadas.

Si bien el procesador con seguridad habilitada puede resistir ataques físicos ocasionales, puede ser vulnerable a la manipulación física. El sistema informático alojado está configurado, asimismo, en diversas realizaciones, para certificar al sistema cliente que el procesador con seguridad habilitada es físicamente seguro, por ejemplo, en una realización el sistema informático alojado está configurado para transmitir un certificado de auditor, firmado por una clave privada de la entidad auditora, declarando que el procesador con seguridad habilitada no ha sido manipulado físicamente durante un período de tiempo específico. El personal de la entidad auditora puede monitorizar periódicamente o de manera continua el servicio informático alojado para determinar que los procesadores con seguridad habilitada están intactos físicamente. Por lo tanto, el certificado del auditor proporciona al sistema cliente grados adicionales de confianza en el entorno de ejecución seguro. En otra realización, el sistema cliente presenta el certificado del procesador con seguridad habilitada directamente a un sistema informático de la entidad auditora que solicita la verificación de la seguridad física del procesador. El sistema informático de la entidad auditora responde con un certificado que verifica que el procesador con seguridad habilitada no ha sido manipulado físicamente.

El servicio de alojamiento de la aplicación de acuerdo con varias realizaciones descritas en este documento solo ejecuta código en el entorno de ejecución seguro que ha sido seleccionado por el sistema cliente. Una entidad asociada con el sistema cliente puede escribir todo el software que se ejecuta dentro del entorno de ejecución seguro, o bien la entidad puede subcontratar porciones del software a proveedores de software en los que la entidad confía. En un ejemplo no limitativo, el sistema cliente puede seleccionar una aplicación de un proveedor de software de aplicación confiable y un sistema operativo de la librería de un proveedor confiable de sistemas operativos. La entidad asociada con el sistema cliente se considera el distribuidor de software para las porciones del software creadas directamente por la entidad. Los distribuidores de software pueden proporcionar certificados para binarios firmados verificando que los archivos binarios de software son ciertamente los proporcionados por los distribuidores de software respectivamente, y que los binarios no han sido alterados.

Con estas divisiones de responsabilidad, el servicio de alojamiento de la aplicación actúa como un intermediario, pero en realidad no certifica la integridad de todos los componentes del sistema. El distribuidor de procesadores con seguridad habilitada certifica el entorno de ejecución seguro. La entidad auditora certifica la seguridad física del entorno de ejecución seguro. Los proveedores de software certifican el software que se ejecuta en el entorno de ejecución seguro. El servicio de alojamiento de la aplicación puede realizar algunas, ninguna o todas estas funciones en diversas realizaciones. En las realizaciones, el proveedor del servicio de alojamiento de la aplicación mantiene la disponibilidad de la instalación informática, lo que incluye proporcionar la instalación informática, la alimentación y la conectividad de la red, y otras entidades, tales como los proveedores de hardware, los proveedores de software y entidades auditoras, proporcionan otros diversos aspectos de la seguridad de las aplicaciones que están alojadas.

Ejemplos de servicios de alojamiento de la aplicación incluyen instalaciones de alojamiento de Internet, proveedores de informática en la nube, centros de datos corporativos subcontratados, centros de datos corporativos operados por contrato y redes de distribución de contenido.

Los procesos, sistemas y dispositivos descritos en este documento pueden ser implementados de varias maneras. A continuación, se proporcionan implementaciones a modo de ejemplo haciendo referencia a las siguientes figuras.

Entorno a modo de ejemplo para proporcionar un entorno de ejecución seguro

La figura 1 es un diagrama esquemático de un sistema 100 a modo de ejemplo que puede ser utilizado para proporcionar un entorno de ejecución seguro. Los aspectos del sistema 100 pueden ser implementados en varios tipos de dispositivos informáticos adecuados que pueden implementar un sistema informático de alojamiento de la aplicación, un sistema informático cliente, etc. El dispositivo o dispositivos informáticos adecuados pueden incluir, o formar parte de, uno o más ordenadores personales, servidores, parques de servidores, centros de datos, ordenadores de propósito especial, ordenadores de tableta, consolas de juegos, teléfonos inteligentes, combinaciones de estos o cualquier otro dispositivo o dispositivos informáticos capaces de almacenar y ejecutar todo o parte de un entorno de ejecución seguro.

Un servicio de alojamiento de la aplicación 102 incluye una memoria 104 y un procesador con seguridad habilitada 106. La memoria 104 incluye un sistema operativo (OS – Operating System, en inglés) anfitrión 108 y un módulo de configuración 110. Aunque el módulo de configuración 110 se muestra en la figura 1 para estar separado del OS anfitrión 108, el módulo de configuración 110 puede ser un componente del OS anfitrión 108. Asimismo, el servicio de alojamiento de la aplicación 102 puede incluir múltiples procesadores, incluidos varios procesadores de seguridad, tales como el procesador con seguridad habilitada 106. El OS anfitrión 108 y/o el módulo de

configuración 110 pueden ser ejecutados en el procesador con seguridad habilitada 106, o en uno o más de los otros procesadores no mostrados en la figura 1.

El sistema 100 realiza diversas funciones, tales como, entre otras, una o más de las siguientes: (a) inicializar entornos de ejecución seguros con código y datos; (b) recibir solicitudes de cliente para vincular una instancia de un entorno de ejecución seguro a un sistema cliente y configurarlo para ejecutar el software del cliente; (c) vincular una instancia de un entorno de ejecución seguro a un cliente y configurar el entorno de ejecución seguro para ejecutar el software del cliente; (d) proporcionar al cliente una especificación certificada del software que se ejecutará dentro del entorno de ejecución seguro. Estas diversas funciones pueden ser realizadas en diferentes órdenes, dependiendo de las realizaciones específicas. Además, las realizaciones específicas pueden combinar algunas de las funciones.

En una realización, el servicio de alojamiento puede realizar la función (b) antes de realizar otras de las funciones mencionadas anteriormente. Cuando se recibe la solicitud de un cliente, el servicio de alojamiento inicializa un entorno de ejecución seguro (acción a). El servicio de alojamiento puede incluir un código y/o datos (por ejemplo, parámetros) suministrados en la solicitud del cliente en la inicialización. Por lo tanto, la vinculación (acción c) se puede realizar implícitamente como parte de la acción (b). Alternativamente, el servicio de alojamiento puede inicializar el entorno de ejecución seguro (acción a) con código y datos genéricos (no específicos para el cliente) y vincular el entorno de ejecución seguro a un cliente (acción c) en una etapa separada.

En otra realización, el servicio de alojamiento inicializa uno o más entornos de ejecución seguros (acción a) con código y datos genéricos. Estos código y datos genéricos podrían proporcionar un entorno de tiempo de ejecución genérico para aplicaciones arbitrarias. Cuando se recibe una solicitud de cliente (acción b), el servicio de alojamiento selecciona uno de los entornos de ejecución seguros inicializados anteriormente y lo vincula al cliente (acción c) enviándole el código o los datos de la solicitud del cliente.

Las acciones (c) y (d) se pueden combinar. Por ejemplo, las variantes de los protocolos de intercambio de claves autenticadas pueden ejecutar un protocolo de autenticación. El protocolo de autenticación proporciona al cliente propiedades verificables acerca del software y los datos del entorno de ejecución seguro (acción d) y establece una clave criptográfica compartida entre el entorno de ejecución seguro y el cliente (acción c).

El siguiente ejemplo es una descripción detallada de una clase de realizaciones. El módulo de configuración 110 recibe una solicitud del sistema cliente 112, a través de la red 114, para establecer un entorno de ejecución seguro en el servicio de alojamiento 102 de la aplicación. La red 114 puede ser la Internet pública, o algún otro tipo de red de conexión por cable o inalámbrica. Las realizaciones no se limitan a ningún tipo o tipo de redes. La solicitud está acompañada de una indicación de un módulo de cargador 116 y de uno o más parámetros 118. La indicación del módulo de cargador 116 puede ser un identificador para el módulo de cargador 116, o puede ser un binario de aplicación del propio módulo de cargador 116, o algún otro indicador. En realizaciones en las que la identificación del módulo de cargador 116 es un identificador, puede ser un identificador uniforme de recursos (URI – Uniform Resource Identifier, en inglés), como un localizador uniforme de recursos (URL – Uniform Resource Locator, en inglés), que identifica el módulo de cargador 116 y posiblemente una ubicación en la que se puede encontrar el módulo de cargador 116.

El módulo de configuración 110 hace que, en respuesta a la recepción de la solicitud, el procesador con seguridad habilitada 106 cree una instancia de un área protegida de la memoria 120, que es un área de la memoria protegida mediante hardware, dentro de la memoria 104. El módulo de configuración 110 proporciona el procesador con seguridad habilitada 106 con punteros hacia el módulo de cargador 116 y los parámetros 118, e instruye al procesador con seguridad habilitada 106 para llevar el área protegida de la memoria 120 a un estado inicial conocido (tal como todas las direcciones de memoria dentro del área protegida de la memoria 120 y todos los registros apropiados dentro del procesador con seguridad habilitada 106 puesto a cero, o a algún otro estado inicial bien conocido, y para cargar el módulo de cargador 116 y los parámetros 118 en el área protegida de la memoria 120, después de llevar el área protegida de la memoria 120 al estado inicial bien conocido. La creación de una instancia del área protegida de la memoria 120 primero en el estado inicial bien conocido y a continuación la carga con el módulo de cargador 116 y los parámetros 118 representa un estado de activación solicitado del área protegida de la memoria 120. En otras palabras, representa el estado del entorno de ejecución seguro que el dispositivo cliente especifica en su solicitud para configurar un entorno de ejecución seguro.

La combinación del área protegida de la memoria 120 y la ejecución del código en la misma por parte del procesador con seguridad habilitada 106 representa el entorno de ejecución seguro. Aunque el área protegida de la memoria 120 se muestra como parte de un área de memoria contigua que también incluye el OS anfitrión 108 y el módulo de configuración 110, el área protegida de la memoria 120 puede formar parte, en realizaciones alternativas, de un área de memoria separada, tal como un área de memoria en el mismo circuito integrado que el procesador con seguridad habilitada 106 que aísla físicamente el área protegida de la memoria 120 del resto del servicio de alojamiento de la aplicación 102.

El procesador con seguridad habilitada 106 puede estar configurado para cifrar y descifrar todos los datos escritos y leídos, respectivamente, desde el área protegida de la memoria 120, para evitar el espionaje externo en el área protegida de la memoria 120. El procesador con seguridad habilitada 106 puede estar configurado asimismo para

producir resúmenes criptográficos, u otros resúmenes, de los datos escritos en el área protegida de la memoria 120 para verificar, tras la lectura del contenido del área protegida de la memoria 120, que los contenidos no han sido alterados.

Como parte del proceso de creación de instancia, el procesador con seguridad habilitada 106 produce un identificador 122 que identifica el estado de activación del área protegida de la memoria 120. El identificador puede ser, en diversas realizaciones, un resumen, tal como una autenticador criptográfico, de los contenidos del área protegida de la memoria 120 en el estado de activación. El identificador puede ser una clave pública correspondiente a una clave privada que se utilizó para firmar el software almacenado en el área protegida de la memoria 120. El estado de activación incluye el módulo de cargador 116, los parámetros 118 y cualquier otro código o datos situados en el área protegida de la memoria 120 tras la creación de la instancia. El identificador 122 puede ser almacenado en una ubicación que sea accesible solo para el procesador con seguridad habilitada 106, tal como en un registro o ubicación de la memoria dentro del procesador con seguridad habilitada 106 que no sea accesible, excepto por el procesador con seguridad habilitada. 106, o quizás cifrado en un área de la memoria 104. En realizaciones en las que el identificador es un autenticador criptográfico del contenido del área protegida de la memoria 104 en el estado de activación, el procesador con seguridad habilitada produce el autenticador criptográfico utilizando una función de creador de autenticador criptográfico, tal como el algoritmo de resumen de mensaje, Message-Digest, MD5, algoritmos de creación de autenticador criptográfico seguro, Secure Hash Algorithms, SHA-0, SHA-1, SHA-2, u otra función de autenticador criptográfico.

Tras la creación de una instancia de área protegida de la memoria 120 con el módulo de cargador 116 y los parámetros 118, el módulo de configuración 110 instruye al procesador con seguridad habilitada 106 para que ejecute el módulo de cargador 116, por ejemplo, a través de una función o puerta de entrada que utiliza el procesador con seguridad habilitada 106 para permitir que el entorno de ejecución seguro reciba comunicaciones fuera del entorno de ejecución seguro. Una instancia del módulo de cargador 116 es ejecutada en el procesador con seguridad habilitada y hace que el procesador cree un certificado de autenticación 124 firmado mediante una clave privada 126 del procesador con seguridad habilitada (SEP – Security-Enabled Processor, en inglés). La clave privada del SEP 126 está almacenada de manera permanente en el procesador con seguridad habilitada 106 de manera que solo sea accesible para el procesador con seguridad habilitada 106. Por lo tanto, mientras el procesador con seguridad habilitada 106 esté físicamente intacto, una entidad que reciba el certificado de autenticación 124 puede tener un alto grado de confianza de que el certificado de autenticación 124 firmado está firmado por el procesador con seguridad habilitada 106.

El certificado de autenticación 124 puede incluir, entre otras cosas, el identificador 122. El módulo de cargador 116 transmite a continuación el certificado de autenticación al sistema cliente 112, a través de una función de salida o puerta de salida empleada por el procesador con seguridad habilitada para permitir al entorno de ejecución seguro comunicarse con el mundo exterior. De manera alternativa, el identificador 122 puede ser cifrado con la clave privada del SEP 126 y transmitido al sistema cliente 112 de manera separada del certificado de autenticación 124 (que también estaría firmado / cifrado utilizando la clave privada del SEP 126.

Tras la recepción del certificado de autenticación 124, el sistema cliente 112 lo descifra utilizando una clave pública del SEP 128 que se corresponde con la clave privada del SEP 126, del procesador con seguridad habilitada. A continuación, se describe el medio por el cual el sistema cliente 112 obtiene la clave pública del SEP 128.

El sistema cliente 112 compara el identificador 122 contenido en el certificado de autenticación 124 descifrado con un identificador conocido 130 del estado de activación solicitado del entorno de ejecución seguro. Una determinación de que el identificador conocido 130 coincide con el identificador 122 proporciona al sistema cliente 112 un alto grado de confianza de que el estado de activación real del área protegida de la memoria 120 coincide con el estado de activación solicitado del área protegida de la memoria 120. En diversos ejemplos no limitativos, la verificación con éxito del identificador 122 proporciona al sistema cliente 112 la confianza de que el área protegida de la memoria 120 incluye el módulo de cargador 116, los parámetros 118, cualquier otro código o datos implícita o explícitamente especificados en la solicitud para establecer un entorno de ejecución seguro, y nada más. Tal como se indicó anteriormente, el certificado de autenticación 124 está firmado / cifrado mediante la utilización de la clave privada del SEP a la que solo puede acceder el procesador con seguridad habilitada 106. El certificado de autenticación 124 incluye el identificador 122 del estado de activación del área protegida de la memoria 120, y el identificador 122 es producido por el procesador con seguridad habilitada 106 y puede almacenarse de manera segura de manera que el identificador 122 sea accesible solo para el procesador con seguridad habilitada 106.

Debido a que el módulo de cargador 116 u otro código (tal como un código malicioso cargado subrepticiamente dentro del área protegida de la memoria 120) no puede acceder a la clave privada del SEP 126, el módulo de cargador 116 u otro código no puede alterar el identificador 122 sin alterar también el certificado de autenticación 124 e invalidar la firma del procesador con seguridad habilitada 106. Por lo tanto, si se utiliza correctamente la clave pública del SEP 128 para verificar que el certificado de autenticación 124 está correctamente firmado con la clave privada del SEP 126, y verificando con éxito que el identificador 122 que contiene coincide con el identificador conocido 130, el sistema cliente 112 puede tienen un alto grado de confianza de que se comunica con un entorno de ejecución seguro cuya instancia fue creada con el estado de activación solicitado.

Para conseguir este alto grado de confianza, el sistema cliente 112 forma una relación de confianza con el procesador con seguridad habilitada 106. El simple hecho de poseer la clave pública del SEP 128 puede ser insuficiente para establecer que el procesador con seguridad habilitada 106 es un verdadero procesador con seguridad habilitada que está correctamente configurado para proporcionar un entorno de ejecución seguro en el servicio de alojamiento de la aplicación 102. Por lo tanto, se proporciona una cadena de confianza para garantizar la autenticidad del procesador con seguridad habilitada 106.

El módulo de cargador 116, o el módulo de configuración 110, pueden transmitir uno o más certificados de confianza, tal como un certificado de autoridad de confianza (TA – Trusted Authority, en inglés) 132 y, posiblemente, uno o más certificados intermedios 134. El certificado de TA 132 se firma con una clave privada de una autoridad confiable 136. El certificado de TA 132 identifica el procesador con seguridad habilitada 106, o posiblemente uno o más intermedios, y proporciona la clave pública del procesador con seguridad habilitada 106 (es decir, la clave pública del SEP 128), o claves públicas de la autoridad intermedia directamente debajo de ella. El sistema cliente 112 puede obtener la clave pública 138 de la autoridad de confianza (TA) y utilizarla para descifrar el certificado 132 de TA y, a continuación, obtener la clave pública publicada en el mismo. Todos los certificados intermedios 134 son descifrados, y las claves públicas de todos los intermediarios subyacentes son extraídas de los certificados intermedios 134. En última instancia, el sistema cliente 112 puede obtener, ya sea a partir del certificado de TA 132 o de uno de los certificados intermedios 134, la clave pública del SEP 128.

Este proceso crea una cadena de confianza desde la autoridad de confianza 136 al procesador con seguridad habilitada 106. Esencialmente, la autoridad de confianza responde por el intermediario más inmediato, los intermediarios responden por cualquier intermediario de nivel inferior y, en última instancia, uno de los intermediarios (o la autoridad de confianza 136 si no hay intermediarios) responde por el procesador con seguridad habilitada 106 y proporciona la clave pública de SEP 128. Al seguir la cadena de confianza de esta manera, el sistema cliente 112 puede establecer una relación de confianza con el procesador con seguridad habilitada 106

La autoridad de confianza 136 puede ser el fabricante del hardware que fabricó el procesador con seguridad habilitada 106. Alternativamente, la autoridad de confianza 136 puede ser alguna otra entidad que proporcione garantías de que un intermediario, que puede ser el fabricante del hardware, es de confianza.

En las mismas o diferentes realizaciones, el módulo de configuración 110 está configurado además para transmitir, al sistema cliente 112, un certificado de auditoría 140, firmado mediante una clave privada de una entidad auditora, lo que indica que el procesador con seguridad habilitada no ha sido manipulado. En realizaciones iguales o alternativas, el sistema cliente 112 proporciona a la entidad auditora una identidad del procesador con seguridad habilitada 106 (que puede estar incluida en el certificado de autenticación) y solicita que la entidad auditora proporcione al sistema cliente 112 el certificado de auditoría 140. La entidad auditora puede emplear uno o varios mecanismos para verificar la seguridad física del procesador con seguridad habilitada. Por ejemplo, el personal de la entidad auditora puede visitar periódicamente el centro o los centros de datos que albergan el servicio de alojamiento de la aplicación 102, inspeccionar físicamente los dispositivos informáticos, y verificar que el procesador con seguridad habilitada 106 no esté comprometido físicamente, no ha sido manipulado, y por lo demás está intacto. En otras realizaciones, el personal de la entidad auditora puede monitorizar de manera continua el centro o los centros de datos que albergan el servicio de alojamiento de la aplicación 102 utilizando circuitos cerrados, o el personal de la entidad auditora puede realizar inspecciones aleatorias de dispositivos informáticos elegidos al azar dentro del centro o los centros de datos que albergan el servicio de alojamiento de la aplicación 102. Dependiendo de los procesos de auditoría empleados, la entidad auditora puede ofrecer diferentes niveles de certificación de seguridad física para satisfacer las necesidades comerciales de diversos clientes. En diversas realizaciones, el certificado de auditoría 140 puede formar parte de la cadena de confianza descrita anteriormente. Alternativamente, el certificado de auditoría puede ser un certificado independiente (quizás respaldado por su propia cadena de confianza) utilizado por el sistema cliente 112 para verificar además que las instalaciones proporcionadas por el servicio de alojamiento de la aplicación 102 son seguras.

Una vez el sistema cliente 112 verifica que el certificado de autenticación 124 esté debidamente firmado por el procesador con seguridad habilitada 106 y que el identificador 122 contenido en el mismo coincide con el identificador 130 conocido (y posiblemente después de verificar la cadena de confianza a través del certificado de TA 132 y el certificado o los certificados intermedios 134 y cualquier otro certificado (tal como el certificado de auditoría 140), el sistema cliente 112 y el módulo de cargador 116 pueden establecer un canal de comunicación cifrado. En una realización, para establecer un canal de comunicación cifrado, el sistema cliente 112 produce una clave de sesión, cifra la clave de sesión con la clave pública del SEP 128 y transmite la clave de sesión cifrada al módulo de cargador 116. El módulo de cargador 116 recibe la clave de sesión (por ejemplo, a través de una función o puerta de entrada del procesador con seguridad habilitada 106). El módulo de cargador 116 hace que el procesador con seguridad habilitada 106 descifre la clave de sesión utilizando la clave privada del SEP 126, y el módulo de cargador 116 establece comunicaciones con el sistema cliente 112 utilizando la clave de sesión descifrada. El sistema cliente 112 y el módulo de cargador 116 utilizan la clave de sesión para proteger criptográficamente las comunicaciones entre ellos.

El protocolo de autenticación descrito anteriormente puede protegerse de varios ataques de repetición de estado utilizando varios métodos, tales como los descritos en las patentes de EE.UU. Nº 7.421.579, a nombre de England et

al. el 2 de septiembre de 2008 y titulada "Multiplexing a secure counter to implement second level secure counters"; Patente de EE.UU. Nº 7.065.607, a nombre de England et al. el 20 de junio de 2006 y titulada "System and Method for implementing a counter"; y tales como los descritos en "Memoir: Practical State Continuity for Protected Modules", por Bryan Parno, Jacob R. Lorch, John R. Douceur, James Mickens y Jonathan M. Mc-Cune, y publicado en las actas del IEEE Symposium on Security and Privacy, IEEE, mayo de 2011.

El sistema cliente 112 instruye al módulo de cargador 116 para que cargue y ejecute una aplicación 142. El módulo de cargador 116 carga y ejecuta a continuación la aplicación 142 en el área protegida de la memoria 120. Alternativamente, la aplicación 142 está identificada previamente por los parámetros 118 y es cargada por el módulo de cargador 116 una vez establecido el canal cifrado. En otras realizaciones adicionales, los parámetros 118 incluyen un binario de aplicación de la aplicación 142, y el módulo de cargador 116 recibe una orden a través del canal cifrado para ejecutar la aplicación 142. En otras realizaciones, la aplicación 142 se carga como parte del estado de activación del área protegida de la memoria 120. En otras realizaciones, la aplicación 142 se carga a través de la Red 114 desde un proveedor de aplicaciones. Otras variaciones son posibles sin apartarse del alcance de la presente invención.

La aplicación 142 puede incluir un subsistema del sistema operativo (a veces denominado "OS de librería"), tal como se describe en la solicitud de patente de EE.UU. Nº 12/834.895, presentada el 13 de julio de 2010 y titulada "ULTRA-LOW COST SANDBOXING FOR APPLICATION APPLIANCES". El subsistema del sistema operativo proporciona diversos elementos del sistema operativo dentro del proceso de la aplicación. El subsistema del sistema operativo también utiliza un pequeño subconjunto de interfaces de programación de aplicaciones (API – Application Programming Interfaces, en inglés) para comunicarse con un sistema operativo anfitrión, a través de una capa de adaptación de plataforma del sistema operativo (PAL – Platform Adaptation Layer, en inglés), a fin de proporcionar a la aplicación 141 servicios informáticos básicos.

En cualquier caso, la carga y ejecución de la aplicación 142 especificada por el sistema cliente 112 en el entorno de ejecución seguro puede ser el objetivo final del protocolo de autenticación descrito anteriormente. El protocolo de autenticación proporciona a un usuario asociado con el sistema cliente 112 un alto grado de confianza de que la aplicación 142 se ejecuta dentro de un entorno de ejecución seguro que está libre de espionaje y manipulación desde el exterior, y que está cargado sin ningún contenido no confiable.

Sistema informático a modo de ejemplo para proporcionar un servicio de alojamiento de la aplicación

La figura 2 es un diagrama de bloques de un sistema informático 200 a modo de ejemplo que se puede utilizar para proporcionar un servicio de alojamiento de la aplicación de acuerdo con las realizaciones. El sistema informático 200 puede configurarse como cualquier dispositivo informático adecuado capaz de implementar un servicio de alojamiento de la aplicación. De acuerdo con diversos ejemplos no limitativos, dispositivos informáticos adecuados pueden incluir ordenadores personales (PC – Personal Computers, en inglés), servidores, parques de servidores, centros de datos, ordenadores de propósito especial, ordenadores de tableta, consolas de juegos, teléfonos inteligentes, combinaciones de estos dispositivos informáticos o de cualquier otro capaces de almacenar y ejecutar toda o una parte de un servicio de alojamiento de la aplicación.

En una configuración a modo de ejemplo, el sistema informático 200 comprende uno o más procesadores 202 y la memoria 204. Los procesadores 202 incluyen uno o más procesadores con seguridad habilitada que son iguales o similares a los del procesador con seguridad habilitada 106. Los procesadores 202 pueden incluir uno o más procesadores de propósito general o de propósito especial distintos de un procesador con seguridad habilitada. El sistema informático 200 también puede contener una conexión o conexiones de comunicación 206 que permiten comunicaciones con diversos sistemas adicionales. El sistema informático 200 puede incluir asimismo uno o más dispositivos de entrada 208, tales como un teclado, un ratón, un lápiz, un dispositivo de entrada de voz, un dispositivo de entrada táctil, etc., y uno o más dispositivos de salida 210, tales como una pantalla, altavoces, una impresora, etc., acoplados en comunicación al procesador o procesadores 202 y a la memoria 204.

La memoria 204 puede almacenar instrucciones de programa que pueden ser cargadas y ejecutadas en el procesador o los procesadores 202, así como datos generados durante la ejecución y/o utilización en conjunto con estos programas. En el ejemplo ilustrado, la memoria 204 almacena un sistema operativo 212, que proporciona la funcionalidad básica del sistema informático 200 y, entre otras cosas, proporciona el funcionamiento de los otros programas y módulos del sistema informático 200. El sistema operativo 212 puede ser igual o similar al OS anfitrión 108.

La memoria 204 incluye un módulo de configuración 214, que puede ser igual o similar al módulo de configuración 110. La memoria 204 incluye un área protegida de la memoria 216, establecida por el procesador con seguridad habilitada. El área protegida de la memoria 216 puede ser igual o similar al área protegida de la memoria 120.

La memoria 204 incluye un módulo de cargador 218, que puede ser igual o similar al módulo de cargador 116. El módulo de cargador 218 puede ser cargado en el área protegida de la memoria 216 a petición de un sistema cliente. La memoria 204 incluye un certificado de TA 220 y uno o más certificados intermedios 222, que pueden ser iguales o similares al certificado de TA 132 y al certificado o los certificados intermedios 134, respectivamente.

La memoria 204 incluye un certificado de auditoría 224, que puede ser igual o similar al certificado de auditoría 140. La memoria 204 incluye un módulo de persistencia 226, que puede ser igual o similar al módulo de persistencia 614.

Sistema informático a modo de ejemplo para proporcionar un sistema cliente

La figura 3 es un diagrama de bloques de un sistema informático 300 a modo de ejemplo que se puede utilizar para proporcionar un sistema cliente de acuerdo con las realizaciones. El sistema informático 300 puede configurarse como cualquier dispositivo informático adecuado capaz de implementar un sistema cliente. De acuerdo con diversos ejemplos no limitativos, dispositivos informáticos adecuados pueden incluir ordenadores personales (PC), servidores, parques de servidores, centros de datos, ordenadores de propósito especial, ordenadores de tableta, consolas de juegos, teléfonos inteligentes, combinaciones de estos dispositivos informáticos o de cualquier otro capaces de almacenar y ejecutar toda o una parte de un sistema cliente.

En una configuración a modo de ejemplo, el sistema informático 300 comprende uno o más procesadores 302 y la memoria 304. El sistema informático 300 también puede contener una conexión o conexiones de comunicación 306 que permiten las comunicaciones con diversos sistemas. El sistema informático 300 puede incluir asimismo uno o más dispositivos de entrada 308, tales como un teclado, un ratón, un lápiz, un dispositivo de entrada de voz, un dispositivo de entrada táctil, etc., y uno o más dispositivos de salida 310, tales como una pantalla, altavoces, una impresora, etc. acoplados en comunicación al procesador o procesadores 302 y a la memoria 304.

La memoria 304 puede almacenar instrucciones de programa que se pueden cargar y ejecutar en los procesadores 302, así como datos generados durante la ejecución y/o utilización de estos programas. En el ejemplo ilustrado, la memoria 304 almacena un sistema operativo 312, que proporciona la funcionalidad básica del sistema informático 300 y, entre otras cosas, proporciona el funcionamiento de los otros programas y módulos del sistema informático 300.

La memoria 204 incluye un módulo de establecimiento 314 configurado para transmitir una solicitud a un servicio de alojamiento de la aplicación, tal como el servicio de alojamiento de la aplicación 102, para establecer un entorno de ejecución seguro dentro del servicio de alojamiento de la aplicación. La solicitud incluye una indicación de un estado de activación solicitado del entorno de ejecución seguro, tal como un módulo de cargador 316 y uno o más parámetros que deben estar cargados en el entorno de ejecución seguro.

El módulo de verificación 318 está configurado para recibir, desde una instancia del módulo de cargador 316 ejecutado en un área protegida de la memoria del servicio de alojamiento de la aplicación, un certificado de autenticación cifrado. El certificado de autenticación cifrado se cifra / firma con una clave privada de un procesador con seguridad habilitada del servicio de alojamiento de la aplicación. El módulo de verificación 318 está configurado, en varias realizaciones, para descifrar el certificado de autenticación utilizando una clave pública 320 del SEP del procesador con seguridad habilitada. El descifrado con éxito del certificado de autenticación con la clave pública 320 del SEP indica que el certificado de autenticación fue cifrado / firmado por el procesador con seguridad habilitada. El módulo de verificación 318 está configurado, en diversas realizaciones, para recibir uno o más certificados de confianza, tales como un certificado de autoridad de confianza y uno o más certificados intermedios, para el establecimiento de una cadena de confianza entre la autoridad de confianza y el procesador con seguridad habilitada, tal como se describe en otra parte, dentro de esta Descripción Detallada. Los uno o más certificados de confianza pueden responder colectivamente por la identidad del procesador con seguridad habilitada y/o para indicar que el procesador con seguridad habilitada es seguro.

El módulo de verificación 318 está configurado, en diversas realizaciones, como parte de, o además del, establecimiento de la cadena de confianza, para recibir un certificado de auditoría firmado mediante una clave privada de una entidad auditora, lo que indica que el procesador con seguridad habilitada no está comprometido físicamente. El certificado de auditoría puede ser proporcionado por el servicio de alojamiento de la aplicación, o por alguna otra entidad.

El módulo de verificación 318 está configurado, en diversas realizaciones, como parte de, o además del establecimiento de la cadena de confianza, para recibir un certificado de procesador, tal como el de un fabricante del procesador con seguridad habilitada, que indica que el procesador con seguridad habilitada es seguro.

Tras establecer con éxito una cadena de confianza y verificar que cualquier otro certificado, tal como el certificado de auditoría y/o el certificado del procesador, son válidos (por ejemplo, descifrando dichos certificados mediante las claves públicas de sus emisores), el módulo de verificación 318 acepta que el procesador con seguridad habilitada es un procesador legítimo con seguridad habilitada.

El módulo de verificación 318 está configurado para extraer un identificador del certificado de autenticación y compararlo con el identificador 322 conocido. El identificador 322 conocido representa el estado de activación solicitado del entorno de ejecución seguro, tal como se identifica en la solicitud transmitida en el módulo de establecimiento. El módulo de establecimiento 314 está configurado para establecer, en respuesta a la verificación por parte del módulo de verificación 318, que se verifica la legitimidad del procesador con seguridad habilitada y que el resumen coincide con el identificador 322 conocido del estado de activación solicitado, una conexión cifrada

ejecutándose la instancia del módulo de cargador en el entorno de ejecución seguro. El identificador 322 conocido puede incluir un resumen, tal como un autenticador criptográfico, del estado de activación solicitado del área protegida de la memoria. El identificador 322 conocido puede incluir una clave pública que coincide con una clave privada que se utilizó para firmar los contenidos colocados en el área protegida de la memoria en el estado de activación solicitado. El identificador 322 conocido puede ser algún otro identificador que identifique el estado de activación inicial. En algunas realizaciones, el módulo de establecimiento 314 produce una clave de sesión para la conexión cifrada, cifra la clave de sesión mediante la clave pública 320 del SEP del procesador con seguridad habilitada, y transmite la clave de sesión cifrada a la instancia del módulo de cargador que se ejecuta en el entorno de ejecución seguro del servicio de alojamiento de la aplicación. La conexión cifrada utiliza la clave de sesión para enviar y recibir datos hacia y desde el entorno de ejecución seguro. Otras realizaciones de establecimiento de una conexión cifrada son posibles sin apartarse del alcance de esta presente Descripción Detallada.

El módulo de establecimiento 314 instruye a la instalación del módulo de cargador que se ejecuta en el entorno de ejecución segura para cargar una Aplicación 324 para ejecuciones dentro del entorno de ejecución seguro. Ni la aplicación 324 ni el módulo de cargador deben estar incluidos en el sistema informático 300. Más bien, el módulo de establecimiento 314 puede indicar al módulo de cargador que descargue la aplicación 324 desde otra ubicación, por ejemplo, proporcionando un URI o URL para la aplicación 324. Los uno o más parámetros proporcionados por el módulo de establecimiento 314 en la solicitud enviada al servicio de alojamiento de la aplicación pueden identificar la aplicación 324 para su ejecución dentro del entorno de ejecución segura. Los parámetros pueden incluir un URI, una URL u otro identificador de la aplicación 324. Alternativamente, los parámetros pueden incluir un binario de aplicación para la aplicación 324 que se carga directamente en el entorno de ejecución seguro en el momento de la creación de instancias.

La memoria 304 puede incluir asimismo un módulo 326 de persistencia del lado del cliente configurado para realizar una o más funciones asociadas con la persistencia del entorno de ejecución seguro tal como, por ejemplo, para migrar el entorno de ejecución seguro entre ordenadores en un servicio de alojamiento de la aplicación, o para recrear el entorno de ejecución seguro en el mismo ordenador en el servicio de alojamiento de la aplicación, tal como se describe con más detalle con respecto a las figuras 6 a 8. Dichas funciones de persistencia del lado del cliente incluyen recibir una clave de persistencia como parte de una migración de un entorno de ejecución seguro, descifrar la clave de persistencia con una clave privada del sistema informático 300, y transmitir la clave de persistencia sin cifrar a un módulo de persistencia, tal como el módulo de persistencia 614, que reside en un ordenador de migración de un servicio de alojamiento de la aplicación, tal como el ordenador de migración 604-

Operaciones a modo de ejemplo para crear una instancia de un entorno de ejecución seguro

La figura 4 es un diagrama de flujo que muestra un proceso 400 a modo de ejemplo realizado por un servicio de alojamiento de la aplicación para crear instancias de un entorno de ejecución seguro. En 402, un módulo de configuración, tal como el módulo de configuración 110, recibe una solicitud de un sistema cliente para establecer un entorno de ejecución seguro en un servicio de alojamiento de la aplicación, tal como el servicio de alojamiento de la aplicación 102. La solicitud incluye una indicación de un módulo de cargador, tal como el módulo de cargador 116, y uno o más parámetros, tales como los parámetros 118. La indicación del módulo de cargador puede ser un URI o una URL (u otro tipo de identificador) para el módulo de carga, o puede ser un binario de aplicación del módulo de cargador, el paquete de aplicaciones, etc. Los parámetros pueden indicar una aplicación solicitada para ser ejecutada en el entorno de ejecución seguro. Los parámetros pueden ser un binario de aplicación de la aplicación que se solicita que se ejecute en el entorno de ejecución seguro. Los parámetros pueden ser algún otro parámetro que el sistema cliente solicita que se coloque en un área protegida de la memoria del entorno de ejecución seguro. En diversas realizaciones, los parámetros pueden ser omitidos de la solicitud.

En 404, el sistema operativo anfitrión coloca el módulo de cargador y los parámetros en un área a proteger de la memoria.

En 406, el módulo de configuración instruye a un procesador con seguridad habilitada (SEP) del servicio de alojamiento de la aplicación, tal como el procesador con seguridad habilitada 106, para configurar, en respuesta a la solicitud, un área protegida de la memoria que incluye el módulo de cargador y uno más parámetros identificados por la solicitud.

En 408, el procesador con seguridad habilitada establece un área protegida de la memoria poniendo el área de memoria que incluye el módulo de cargador y los parámetros en un estado protegido. El área protegida de la memoria se coloca en un estado inicial bien conocido. El estado inicial bien conocido puede ser todas las celdas de memoria del área protegida de la memoria, y todos los registros del procesador están escritos en cero, en uno, o en algún otro valor o patrón de valores predeterminado. Tal como se describe en otro lugar dentro de esta Descripción Detallada, los datos almacenados en el área protegida de la memoria son inaccesibles para el código almacenado y ejecutado fuera del área protegida de la memoria una vez que el procesador con seguridad habilitada coloca el área protegida de la memoria en el estado inicial conocido. Es el procesador con seguridad habilitada el que gobierna este acceso.

En 410, el módulo de configuración le indica al módulo de cargador que se ejecute dentro del área protegida de la memoria. El módulo de configuración puede ser capaz de pasar instrucciones al módulo de cargador a través de una puerta de entrada o función proporcionada por el procesador con seguridad habilitada que permite que el entorno de ejecución seguro reciba la comunicación del entorno de ejecución externo.

En 412, el procesador con seguridad habilitada produce un identificador del contenido del área protegida de la memoria. El identificador puede ser, en diversas realizaciones, un resumen (tal como un autenticador criptográfico) del contenido del área protegida de la memoria en el estado de activación. El identificador puede ser una clave pública que coincida con una clave privada utilizada para firmar el software almacenado en el área protegida de la memoria. En el punto en el que se crea el identificador, el contenido del área protegida de la memoria incluye el módulo de cargador y uno o más parámetros incluidos en la solicitud, pero ningún otro dato o código. Por lo tanto, el contenido del área protegida de la memoria representa el estado de activación solicitado implícita o explícitamente identificado por la solicitud. En las realizaciones en las que el identificador es un resumen, el resumen se puede producir utilizando una de varias funciones de creación de autenticador criptográfico u otras funciones criptográficas similares.

En 414, el procesador con seguridad habilitada almacena el identificador de una manera que es accesible solo para el procesador con seguridad habilitada. Por ejemplo, el procesador con seguridad habilitada puede almacenar el identificador en un registro seguro del procesador con seguridad habilitada. El procesador con seguridad habilitada puede almacenar el identificador cifrado en una ubicación de la memoria. Pero, en cualquier caso, el identificador se almacena de una manera que lo hace accesible solo para el procesador con seguridad habilitada. El identificador puede ser creado por instrucciones del módulo de cargador. En realizaciones alternativas, el identificador se puede crear tras la creación de una instancia del área protegida de la memoria sin instrucciones desde el módulo de cargador.

En 416, una instancia del módulo de cargador ejecutada en el entorno de ejecución seguro le indica al procesador con seguridad habilitada que produzca un certificado de autenticación que incluya el identificador y esté firmado mediante una clave privada del procesador con seguridad habilitada. La clave privada del procesador con seguridad habilitada se almacena de manera segura en el procesador con seguridad habilitada de una manera que es accesible solo para el procesador con seguridad habilitada. El certificado de autenticación puede incluir otra información además del identificador, tal como una marca de tiempo, los uno o más parámetros, u otros datos.

En 418, el procesador con seguridad habilitada cifra / firma el certificado de autenticación utilizando la clave privada del procesador con seguridad habilitada y proporciona el certificado de autenticación firmado a la ejecución del módulo de cargador en el entorno de ejecución seguro.

En 420, el módulo de cargador proporciona al sistema cliente la certificación de que el entorno de ejecución seguro se establece en un estado de activación inicial para eliminar únicamente el software identificado mediante la solicitud del sistema cliente. La certificación puede incluir un certificado de autenticación firmado. El módulo de cargador puede transmitir el certificado de autenticación a través de una puerta de salida o una función del procesador con seguridad habilitada que permite que el entorno de ejecución seguro se comunique con el código fuera del entorno de ejecución seguro.

En 422, el módulo de cargador y/o el servicio de alojamiento de la aplicación transmiten uno o más certificados de confianza, tal como el certificado de TA 132 y los certificados intermedios 134 que responden colectivamente de la identidad del procesador con seguridad habilitada y/o indican que el procesador con seguridad habilitada es seguro. Esto puede incluir asimismo un certificado de auditoría, firmado mediante una clave privada de una entidad auditora, que indica que el procesador con seguridad habilitada está físicamente intacto. Esto puede incluir un certificado de procesador de un fabricante del procesador con seguridad habilitada que indica que el procesador con seguridad habilitada es seguro. En realizaciones alternativas, el certificado de auditoría y/o el certificado del procesador se entregan por separado al sistema cliente, tal como directamente desde la entidad auditora, un fabricante de hardware o un tercero. En un ejemplo no limitativo, el certificado de autenticación puede incluir un URI que identifica dónde puede recuperar el sistema cliente el certificado de auditoría.

En 424, el módulo de cargador recibe un mensaje de autorización del sistema cliente.

En 426, el módulo de cargador obtiene uno o más componentes de la aplicación para ser ejecutados en el entorno de ejecución seguro. La obtención de uno o más componentes de la aplicación puede incluir la recuperación de uno o más componentes de la aplicación de un almacenamiento persistente del servicio de alojamiento de la aplicación, desde una ubicación remota (tal como a través de un URI identificado en los parámetros del estado de activación inicial o el mensaje de autorización, o en alguna otra ubicación). La obtención de uno o más componentes de la aplicación puede incluir la recuperación de uno o más componentes de la aplicación del sistema cliente, tal como a través de un canal de comunicación protegido criptográficamente.

Los uno o más componentes de la aplicación son seleccionados por el sistema cliente, ya sea mediante la transmisión de un URI, URL, otro identificador o un binario de la aplicación, un paquete de aplicación o una imagen del sistema de archivos. La transmisión del URI, la URL, otro identificador, el binario de la aplicación, el paquete de

aplicación, la imagen del sistema de archivos, etc., se puede realizar a través de la solicitud recibida en 402, en el mensaje de autorización recibido en 424, o recibido de alguna otra forma. Por ejemplo, a través de una conexión de comunicación segura establecida entre el módulo de cargador y el canal del sistema cliente (utilizando, por ejemplo, el protocolo de capa de conexión segura (SSL – Secure Socket Layer, en inglés) u otro protocolo).

En diversas realizaciones no limitativas, el sistema cliente proporciona al módulo de cargador una clave de cifrado. En estas realizaciones, obtener uno o más componentes de la aplicación puede incluir descifrar uno o más componentes utilizando la clave de cifrado (recibida a través de un canal de comunicación seguro). En diversas realizaciones, la clave de cifrado puede ser transportada sin cifrar a través de un canal de comunicación seguro. En otras realizaciones, la clave de cifrado se puede cifrar mediante la clave pública del procesador con seguridad habilitada y se puede descifrar mediante el procesador con seguridad habilitada en nombre del módulo de cargador. En diversas realizaciones, obtener los uno o más componentes de la aplicación en 426 puede ocurrir en una secuencia diferente de la que se muestra en la figura 4 sin apartarse del alcance de la presente invención. En un ejemplo no limitativo de dichas realizaciones alternativas, los uno o más componentes de la aplicación pueden haberse obtenido y cargado en el área protegida de la memoria como parte del estado de activación inicial. En 428, el módulo de cargador hace que la aplicación con seguridad habilitada ejecute uno o más componentes de aplicación dentro del área protegida de la memoria.

Operaciones a modo de ejemplo para verificar un establecimiento de entorno de ejecución seguro

La figura 5 es un diagrama de flujo que muestra un proceso a modo de ejemplo 500 para verificar el establecimiento de un entorno de ejecución seguro. En 502, un sistema cliente, tal como el sistema cliente 112, transmite una solicitud a un servicio de alojamiento de la aplicación, tal como el servicio de alojamiento de la aplicación 102, para establecer un entorno de ejecución seguro. La solicitud incluye una indicación de un estado de activación solicitado del entorno de ejecución seguro, tal como un módulo de cargador solicitado y uno o más parámetros para ser introducidos en un área protegida de la memoria del entorno de ejecución seguro.

En 504, el sistema cliente recibe, desde una posición del módulo de cargador que se ejecuta en un área protegida de la memoria del servicio de alojamiento de la aplicación, una certificación, tal como un certificado de autenticación, de que el entorno de ejecución seguro está establecido para ejecutar en el estado de activación solo el software identificado por la solicitud. El certificado de autenticación incluye un identificador. La recepción del certificado de autenticación indica que el servicio de alojamiento de la aplicación pretende haber establecido un entorno de ejecución seguro. El identificador identifica el contenido de un área protegida de la memoria del entorno de ejecución seguro en su creación de instancia. El identificador puede ser, en diversas realizaciones, un resumen, como un autenticador criptográfico, del contenido del área protegida de la memoria en el estado de activación. El identificador puede ser una clave pública que coincida con una clave privada utilizada para firmar el software almacenado en el área protegida de la memoria.

En 506, el sistema cliente recibe uno o más certificados de confianza, tal como el certificado de asistencia técnica 132 y/o los certificados intermedios 134. Tal como se describe en otro lugar dentro de esta Descripción Detallada, los uno o más certificados de confianza establecen de manera verificable y colectiva una cadena de confianza entre una autoridad confiable y el procesador con seguridad habilitada del servicio de alojamiento de la aplicación para indicar que el procesador con seguridad habilitada es seguro.

En 508, el sistema cliente recibe un certificado de auditoría, firmado mediante una clave privada de una entidad auditora, lo que indica que el procesador con seguridad habilitada no está comprometido físicamente. La entidad auditora inspecciona periódicamente los procesadores con seguridad habilitada del servicio de alojamiento de la aplicación, tal como se describe en otra parte dentro de esta Descripción Detallada.

En 510, el sistema cliente recibe un certificado de procesador de un fabricante del procesador con seguridad habilitada que indica que el procesador con seguridad habilitada es seguro. El certificado del procesador puede ser uno de los certificados de confianza recibidos en 506. Alternativamente, el procesador certificado puede ser recibido por separado del fabricante del hardware del procesador con seguridad habilitada, o de un tercero, garantizando la seguridad y el correcto funcionamiento del procesador con seguridad habilitada.

En 512, el sistema cliente verifica que los diversos certificados recibidos en 506, 508 y 510 son correctos, por ejemplo, verificando su autenticidad utilizando las claves públicas de los distintos emisores. Si uno o más de los certificados no son válidos, entonces el sistema cliente puede rechazar el entorno de ejecución seguro como no válido.

En 514, el sistema cliente obtiene una clave pública del procesador con seguridad habilitada. El sistema cliente puede obtener la clave pública de uno de los certificados de confianza recibidos en 506. Alternativamente, el sistema cliente puede tener previamente almacenada la clave pública del procesador con seguridad habilitada.

En 516, el sistema cliente verifica el certificado de autenticación utilizando la clave pública conocida de un procesador de seguridad cifrado del servicio de alojamiento de la aplicación. La clave pública conocida corresponde

a una clave privada del procesador con seguridad habilitada. El descifrado con éxito con la clave pública indica, por lo tanto, que el certificado de autenticación es verificable a partir del procesador con seguridad habilitada.

En 518, el sistema cliente extrae el identificador del certificado de autenticación descifrado. Y en 520, el sistema cliente compara el identificador con un valor esperado de un identificador conocido del estado de activación solicitado del entorno de ejecución seguro. Una coincidencia con éxito indica que el estado de activación del entorno de ejecución seguro cuya instancia fue creada por el procesador con seguridad habilitada del servicio de alojamiento de la aplicación es como se especifica en la solicitud transmitida en 502.

En 522, el sistema cliente determina si los identificadores coinciden. Si los identificadores no coinciden, entonces el sistema cliente rechaza el entorno de ejecución seguro por no tener el estado de activación solicitado. Los identificadores que no coinciden indican que el estado de activación real del entorno de ejecución seguro tiene menos, más o diferente código y datos diferentes o diferentes del estado de activación solicitado. Una coincidencia con éxito de los identificadores, junto con la verificación de que la autenticación y los certificados de confianza son válidos, permite que el sistema cliente tenga un alto grado de confianza de que se ha establecido un entorno de ejecución seguro sin código no confiable, tal como por ejemplo el entorno de ejecución seguro se establece solo con código y datos en los que el sistema cliente confía.

En 524, el sistema cliente autoriza la ejecución del módulo de cargador en el área protegida de la memoria para ejecutar uno o más componentes de la aplicación dentro del entorno de ejecución seguro. En las realizaciones, la autorización del módulo de cargador puede incluir la transmisión de un indicador de uno o más componentes de la aplicación que se ejecutarán en un entorno de ejecución seguro. El indicador puede ser un URI, una URL, otro identificador, un binario de la aplicación, un paquete de la aplicación o una imagen del sistema de archivos de los uno o más componentes de la aplicación que se ejecutarán. En varias realizaciones, la transmisión del indicador puede formar parte de la transmisión de la solicitud en 502. En otras realizaciones, la transmisión del indicador puede utilizar un mensaje separado (tal como, por ejemplo, un mensaje enviado a través de una conexión segura establecida utilizando SSL u otro protocolo), o un mensaje transmitido en algún momento anterior para "preparar" uno o más componentes de la aplicación que se ejecutarán en el entorno de ejecución seguro. El sistema cliente puede generar y transmitir al módulo de cargador una clave de cifrado que se utilizará para descifrar los diversos mensajes y/o el indicador.

Entorno a modo de ejemplo para la persistencia de un entorno de ejecución Seguro

En la informática alojada convencional, la migración o la recreación de un cliente alojado es manejada por un monitor de máquina virtual. En la migración informática alojada de manera convencional, un monitor de máquina virtual anfitrión analiza el estado de la ejecución, copia todas las páginas de memoria, escribe las páginas de memoria en un disco o las transfiere a través de una red, y comienza la ejecución en la misma o en una máquina diferente. Pero debido a que el código y los datos almacenados dentro de un área protegida de la memoria de un entorno de ejecución seguro de acuerdo con las realizaciones de la presente invención son inaccesibles para el código que se ejecuta fuera del área protegida de la memoria, un sistema operativo anfitrión no puede inspeccionar el estado de ejecución o copia la información del estado a un disco para migrar a otra máquina. En su lugar, el código que se ejecuta dentro del área protegida de la memoria maneja varios aspectos de los procesos de recreación y migración.

La figura 6 muestra un entorno para la migración de un área protegida de la memoria de acuerdo con realizaciones. El entorno 600 incluye un ordenador anfitrión 602 y un ordenador de migración 604. Se establece un entorno de ejecución seguro, que incluye un área protegida de la memoria 606 y un procesador con seguridad habilitada 608, en el ordenador anfitrión 602. Se crea una instancia del área protegida de la memoria 606 de una manera que se describe en otra parte dentro de esta Descripción Detallada, en particular en las descripciones de las figuras 1 a 5. El área protegida de la memoria 606 incluye un módulo de cargador 610 y una aplicación 612 que se ejecuta dentro del entorno de ejecución seguro. El área protegida de la memoria 606 también incluye un módulo de persistencia 614, que puede ser un subcomponente del módulo de cargador 610 o un subcomponente de la aplicación 612, que incluye un subcomponente de un subcomponente del sistema operativo de librería de la aplicación 612.

El OS del anfitrión 616 determina que es necesario mantener el entorno de ejecución seguro. Persistir en el entorno de ejecución seguro puede ser con el propósito de migrar el entorno de ejecución seguro desde el ordenador anfitrión 602 a el ordenador de migración 604. Alternativamente, la persistencia del entorno de ejecución seguro puede ser para recrear la ejecución en el ordenador anfitrión 602. En cualquier caso, el OS anfitrión 616 está configurado para llamar a una puerta de entrada o función proporcionada por el procesador con seguridad habilitada 608 que permite que el sistema operativo anfitrión 616 indique al entorno de ejecución seguro que persista en su estado de ejecución actual a persistente almacenamiento.

El módulo de persistencia 614 recibe la instrucción de persistencia a través de la puerta de entrada y, como respuesta, crea un punto de control cifrado 618. Para conseguir esto, el módulo de persistencia 614 detiene la ejecución del módulo de cargador 610 y la aplicación 612 (incluido, para ejemplo, hacer que los subprocesos se detengan, y escribe los registros del procesador en la memoria protegida. En ese momento, solo un hilo, el hilo de suspensión del módulo de persistencia 614, se puede dejar en ejecución. Las diversas páginas de memoria se

enumeran y almacenan, junto con los registros del procesador, como información del estado 620. El contenido del área protegida de la memoria 606, incluida la aplicación 612 y la información del estado 620, se almacena como el punto de control cifrado 618 en el almacenamiento persistente 622. El punto de control cifrado 618 se cifra mediante una clave de persistencia generada por el módulo de persistencia 614. El módulo de persistencia 614 cifra la clave de persistencia utilizando una clave pública 624 del sistema cliente 626. Alternativamente, la clave de persistencia se cifra utilizando una clave pública del procesador con seguridad habilitada para la migración 634, o una clave pública del procesador con seguridad habilitada 608. La clave de persistencia cifrada se almacena como clave de persistencia sellada 628 en el almacenamiento persistente 622.

En realizaciones que utilizan la persistencia del estado de ejecución para migrar la ejecución al ordenador de migración 604, un sistema operativo de migración 630 del ordenador de migración 604 causa el establecimiento de un área de protegida de la memoria de migración 632. En realizaciones que utilizan la persistencia del estado de ejecución para recrear la ejecución en el ordenador anfitrión 602 en una nueva área protegida de la memoria (debido, por ejemplo, a un reinicio del ordenador anfitrión 602 o por otro motivo), el OS anfitrión 616 causa el establecimiento de una nueva área protegida de la memoria en el ordenador anfitrión 602. Se crea una instancia del área protegida de la memoria de migración 632, o la nueva área protegida de la memoria que se debe establecer en el ordenador anfitrión 602, de una manera que se describe en otro lugar dentro de esta Descripción Detallada, en particular en las descripciones de las figuras 1 a 5

En realizaciones en las que la persistencia del estado de ejecución tiene el propósito de migrarlo al ordenador de migración 604, el OS del anfitrión de migración 630 llama a una puerta de entrada o función del procesador de migración con seguridad habilitada 634 para hacer que el módulo de cargador 610 inicie o ejecute el módulo de persistencia 614 dentro del área protegida de la memoria de migración 632. El módulo de persistencia 614 copia la clave de persistencia sellada 628 en el área protegida de la memoria de migración 632 y transmite la clave de persistencia sellada 628 al sistema cliente 626.El sistema cliente 626 descifra la clave de persistencia sellada 628 utilizando la clave privada del sistema cliente 626 y la transmite de nuevo al módulo de persistencia 614 a través de la conexión cifrada establecida durante la inicialización del entorno de ejecución seguro en el ordenador de migración 604. Alternativamente, en realizaciones que cifran la clave de persistencia mediante la clave pública del procesador de migración con seguridad habilitada 634, la clave de persistencia sellada es desactivada utilizando la clave privada del procesador de migración con seguridad habilitada 634.

En las realizaciones que utilizan la persistencia del estado de ejecución con el fin de recrear la ejecución en el ordenador anfitrión 602, el OS anfitrión 616 llama a una puerta de entrada o función del procesador con seguridad habilitada 608 para causar que el módulo de cargador 610 inicie o ejecute el módulo de persistencia 614 dentro de un área protegida de la memoria 606 y recién recreada, la unidad de persistencia 614 copia la clave de persistencia sellada 628 en el área protegida de la memoria 606 recién recreada y transmite la clave de persistencia sellada 628 al sistema cliente 626. El sistema cliente 626 descifra la clave de persistencia sellada 628 utilizando la clave privada del sistema cliente 626 y la transmite al módulo de persistencia 614 a través de la conexión cifrada establecida durante la inicialización del entorno de ejecución seguro en el ordenador de migración 604. Alternativamente, en las realizaciones que cifran la clave de persistencia mediante la clave pública del procesador con seguridad habilitada 608, la clave de persistencia sellada es desactivada utilizando la clave privada del procesador con seguridad habilitada 608.

El módulo de persistencia 614 copia el punto de control cifrado 618 en el área protegida de la memoria de migración 632 o en el área protegida de la memoria 606 recién recreada y utiliza la clave de persistencia no sellada para descifrar el punto de control cifrado 618. El módulo de persistencia 614 utiliza la información del estado 620 del punto de control cifrado 618 para volver a llenar las páginas de memoria asociadas con los subprocesos en ejecución desde el módulo de cargador 610 y la aplicación 612, y para volver a llenar los registros en el procesador de migración con seguridad habilitada 634 o el procesador con seguridad habilitada 608. De este modo, en diversas realizaciones, la ejecución del entorno de ejecución seguro en el ordenador anfitrión 602 se migra al ordenador de migración 604 o se vuelve a crear en el ordenador anfitrión 602.

En diversas realizaciones, el entorno de ejecución seguro en el ordenador de migración 604 se puede implementar antes de que comiencen los procesos de migración, tal como al mismo tiempo que se inicializa el entorno de ejecución seguro en el ordenador anfitrión 602. El módulo de persistencia 614 en el área protegida de la memoria de migración 632 puede rellenarse previamente con la clave privada del sistema cliente 626 para permitirle descifrar la clave de persistencia sellada 628 sin transmitirla al sistema cliente 626 para su desactivación. En algunas realizaciones, en lugar de utilizar la clave pública del sistema cliente 626 para cifrar la clave de persistencia, la clave de persistencia sellada 628 se cifra mediante una clave pública del procesador de migración con seguridad habilitada 634 para que pueda ser descifrada utilizando la clave privada del procesador de migración con seguridad habilitada 634.

Operaciones a modo de ejemplo para migrar un entorno de ejecución seguro

La figura 7 es un diagrama de flujo que muestra un proceso 700 a modo de ejemplo para migrar un entorno de ejecución seguro. En 702, un módulo de cargador o un módulo de persistencia que se ejecuta en un entorno de

ejecución seguro recibe una orden, a través de una puerta de entrada, para migrar a un ordenador de migración, tal como el ordenador de migración 604.

En 704, un módulo de persistencia, tal como el módulo de persistencia 614, genera una clave de persistencia. La clave de persistencia se utiliza para cifrar un punto de control del entorno de ejecución seguro.

En 706, el módulo de persistencia cifra la clave de persistencia. En realizaciones, el módulo de persistencia cifra la clave de persistencia utilizando una clave pública de un sistema cliente, tal como el sistema cliente 626. En realizaciones alternativas, en las que se conoce la identidad del ordenador principal de migración, el módulo de persistencia cifra la clave de persistencia utilizando una clave pública de un procesador con seguridad habilitada del ordenador de migración.

En 708, el módulo de persistencia escribe la clave de persistencia cifrada en el almacenamiento persistente. Alternativamente, el módulo de persistencia transmite la clave de persistencia al sistema cliente o a un entorno de ejecución seguro preestablecido en el ordenador de migración.

En 710, el módulo de persistencia detiene la ejecución de los procesos y subprocesos que se ejecutan en el entorno de ejecución seguro y escribe la información del estado en el área protegida de la memoria.

En 712, el módulo de persistencia cifra el contenido del área protegida de la memoria utilizando la clave de persistencia para generar un punto de control. El contenido del área protegida de la memoria incluye la información de estado, tal como los archivos de página y los datos de registro asociados con el entorno de ejecución seguro.

En 714, el punto de control cifrado se almacena en un almacenamiento persistente, tal como en una unidad de disco duro del servicio de alojamiento de la aplicación o en algún otro almacenamiento persistente. Alternativamente, el punto de control cifrado se carga directamente en un área protegida de la memoria preestablecida del ordenador de migración, tal como a través de un canal de comunicación cifrado hasta el área protegida de la memoria del ordenador de migración.

En 716, el área protegida de la memoria es inicializada en el ordenador de migración. El sistema operativo anfitrión del ordenador de migración hace que el módulo de cargador en el área protegida de la memoria del ordenador de migración cargue y ejecute el módulo de persistencia dentro del entorno de ejecución seguro del ordenador de migración.

En 718, el módulo de persistencia que se ejecuta dentro de un entorno de ejecución seguro del ordenador de migración transmite la clave de persistencia cifrada al sistema cliente. En realizaciones alternativas, en las que la clave de persistencia está cifrada utilizando la clave pública del procesador con seguridad habilitada del ordenador de migración, la clave de persistencia no se transmite al sistema cliente; por el contrario, el módulo de persistencia solicita que el procesador con seguridad habilitada descifre la clave de persistencia. En otra realización alternativa, en la que el entorno de ejecución seguro está preestablecido en el ordenador de migración, el entorno de ejecución seguro preestablecido en el ordenador de migración ya puede tener la clave privada del sistema cliente, obviando la necesidad de transmitir la clave de persistencia cifrada al sistema del cliente. En 720, el entorno de ejecución seguro en el ordenador de migración recibe la clave de persistencia no cifrada.

En 722, el módulo de persistencia descifra el punto de control cifrado utilizando la clave de persistencia, y carga la información de estado en el punto de control en los archivos de la página y los registros del nuevo entorno de ejecución seguro para restaurar el estado de ejecución, y el proceso de migración finaliza.

Operaciones a modo de ejemplo para recrear un entorno de ejecución seguro

La figura 8 es un diagrama de flujo que muestra un proceso a modo de ejemplo para recrear un entorno de ejecución seguro. En 802, un módulo de cargador o un módulo de persistencia ejecutado en un entorno de ejecución seguro recibe una orden, a través de una puerta de entrada, para persistir el estado actual del entorno de ejecución seguro para recrear el estado de ejecución en un nuevo entorno de ejecución seguro (tal como en el mismo ordenador anfitrión o en otro diferente).

En 804, un módulo de persistencia genera una clave de persistencia. La clave de persistencia se utiliza para cifrar un punto de control del entorno de ejecución seguro, tal como se describe más detalladamente a continuación.

En 806, el módulo de persistencia cifra la clave de persistencia. En realizaciones, el módulo de persistencia cifra la clave de persistencia utilizando una clave pública de un sistema cliente, tal como el sistema cliente 626. En realizaciones alternativas, el módulo de persistencia cifra la clave de persistencia utilizando una clave pública de un procesador con seguridad habilitada del ordenador anfitrión.

En 808, el módulo de persistencia escribe la clave de persistencia cifrada en el almacenamiento persistente. Alternativamente, el módulo de persistencia transmite la clave de persistencia al sistema cliente, o a un entorno de ejecución seguro preestablecido en el ordenador anfitrión, tal como a través de un canal de comunicación seguro hasta el área protegida de la memoria recién creada del entorno de ejecución seguro preestablecido.

En 810, el módulo de persistencia detiene la ejecución del entorno de ejecución seguro y escribe la información del estado en el área protegida de la memoria. La información del estado puede incluir las páginas de memoria virtual y el contexto de registro asociado con el entorno de ejecución seguro. En 812, el módulo de persistencia cifra la información del estado utilizando la clave de persistencia para generar un punto de control.

En 814, el punto de control cifrado se almacena en un almacenamiento persistente, tal como una unidad de disco duro del servicio de alojamiento de la aplicación o en algún otro almacenamiento persistente. Alternativamente, el punto de control cifrado se carga directamente en un área protegida de la memoria recién establecida, tal como por ejemplo a través de un canal de comunicación hasta el área protegida de la memoria de nueva creación.

En 816, una nueva área protegida de la memoria es inicializada en el ordenador anfitrión. En 818, el sistema operativo anfitrión del ordenador anfitrión coloca el módulo de cargador y uno o más parámetros en el área de memoria a proteger.

En 820, el módulo de persistencia que se ejecuta en el entorno de ejecución seguro recién creado del ordenador anfitrión lee la clave de persistencia sellada del almacenamiento persistente.

En 822, el módulo de persistencia en el entorno de ejecución seguro recién creado desactiva la clave de persistencia. En realizaciones en las que la clave de persistencia está cifrada utilizando la clave pública del procesador con seguridad habilitada del ordenador anfitrión, el módulo de persistencia solicita que el procesador de seguridad descifre la clave de persistencia. En otras realizaciones en las que el entorno de ejecución seguro está preestablecido en el ordenador anfitrión, la clave privada del procesador con seguridad habilitada del ordenador anfitrión se utiliza para desactivar la clave de persistencia.

En 824, el módulo de persistencia lee el punto de control cifrado del almacenamiento persistente. En 826, el módulo de persistencia descifra el punto de control cifrado utilizando la clave de persistencia, y carga la información del estado en el punto de verificación en la memoria virtual y el contexto de registros del nuevo entorno de ejecución seguro, para restaurar el estado de ejecución, y el proceso de recreación finaliza.

Las figuras 4, 5, 7 y 8 representan gráficas de flujo que muestran procesos a modo de ejemplo de acuerdo con diversas realizaciones. Las operaciones de estos procesos se ilustran en bloques individuales y se resumen con referencia a esos bloques. Estos procesos se ilustran como gráficas de flujo lógico, cada operación de los cuales puede representar un conjunto de operaciones que se pueden implementar en hardware, software o una combinación de los mismos. En el contexto del software, las operaciones representan instrucciones ejecutables por ordenador almacenadas en uno o más medios de almacenamiento en ordenador que, cuando son ejecutadas por uno o más procesadores, permiten que uno o más procesadores realicen las operaciones enumeradas. En general, las instrucciones ejecutables por ordenador incluyen rutinas, programas, objetos, módulos, componentes, estructuras de datos y similares que realizan funciones particulares o implementan tipos de datos abstractos particulares. El orden en que se describen las operaciones no se debe interpretar como una limitación, y cualquier número de las operaciones descritas puede ser combinado en cualquier orden, separar en operaciones secundarias y/o realizar en paralelo para implementar el proceso. Los procesos de acuerdo con diversas realizaciones de la presente invención pueden incluir solo algunas o todas las operaciones representadas en el gráfico de flujo lógico.

Medios legibles por ordenador

Dependiendo de la configuración y del tipo de dispositivo informático utilizado, las memorias 204 y 304 de los sistemas informáticos 200 y 300 en las figuras 2 y 3, respectivamente, pueden incluir una memoria volátil (tal como una memoria de acceso aleatorio (RAM – Random Access Memory, en inglés)) y/o una memoria no volátil (tal como una memoria de solo lectura (ROM – Read Only Memory, en inglés), una memoria rápida, etc.). Las memorias 204 y 304 pueden incluir asimismo un almacenamiento extraíble adicional y/o un almacenamiento no extraíble que incluye, entre otros, una memoria rápida, un almacenamiento magnético, un almacenamiento óptico y/o un almacenamiento en cinta, que puede proporcionar almacenamiento no volátil de instrucciones legibles por ordenador, estructuras de datos, módulos de programa y otros datos para los sistemas informáticos 200 y 300.

Las memorias 204 y 304 son ejemplos de medios legibles por ordenador. Los medios legibles por ordenador, incluyen al menos dos tipos de medios legibles por ordenador, a saber, medios de almacenamiento informático y medios de comunicaciones.

Los medios de almacenamiento informáticos incluyen medios volátiles y no volátiles, extraíbles y no extraíbles implementados en cualquier proceso o tecnología para el almacenamiento de información, tal como instrucciones legibles por ordenador, estructuras de datos, módulos de programa u otros datos. Los medios de almacenamiento informáticos incluyen, pero no están limitados a, una memoria de cambio de fase (PRAM – Phase change RAM, en inglés), una memoria estática de acceso aleatorio (SRAM – Static RAM, en inglés), una memoria dinámica de acceso aleatorio (DRAM – Dynamic RAM, en inglés), otros tipos de memoria de acceso aleatorio (RAM), una memoria de solo lectura (ROM), una memoria de solo lectura programable y borrable eléctricamente (EEPROM – Electrically Erasable Programmable Read-Only Memory, en inglés), una memoria rápida u otra tecnología de memoria, un disco compacto de solo lectura (CD-ROM – Compact Disc-ROM, en inglés), discos versátiles digitales

(DVD – Digital Versatile Disks, en inglés) u otro almacenamiento óptico, casetes magnéticos, cinta magnética, almacenamiento en disco magnético u otros dispositivos de almacenamiento magnético, o cualquier otro medio que no sea de transmisión que se pueda utilizar para almacenar información para el acceso por parte de un dispositivo informático.

Por el contrario, los medios de comunicación pueden incluir instrucciones legibles por ordenador, estructuras de datos, módulos de programa u otros datos en una señal de datos modulada, tal como una onda portadora u otro mecanismo de transmisión. Tal como se define en la presente memoria, los medios de almacenamiento informático no incluyen medios de comunicación.

Conclusión

Aunque la invención utiliza un lenguaje que es específico para las características estructurales y/o actos metodológicos, la invención no se limita a las características o actos específicos descritos. Más bien, las características y los actos específicos se describen como formas ilustrativas de implementación de la invención.

REIVINDICACIONES

1. Un método que comprende:

establecer, a petición de un sistema cliente (112), mediante un procesador con seguridad habilitada (106) de un sistema informático, un área de la memoria protegida mediante hardware dentro de una memoria del sistema informático, estando configurado el procesador habilitado con seguridad para mediar, a través de una o más funciones de puerta, el acceso al área de la memoria protegida mediante hardware mediante todo el código que se ejecuta fuera del área de la memoria protegida mediante hardware;

dar instrucciones al procesador con seguridad habilitada, en base, al menos, a una solicitud de un sistema cliente, para incluir, en un estado inicial, el software y los datos identificados por la solicitud del sistema cliente en el área de la memoria protegida mediante hardware;

dar instrucciones a una parte del software identificado por la solicitud del sistema cliente que se incluye en el área de la memoria protegida mediante hardware para ejecutar, la porción del software configurado, tras la ejecución, para hacer que el procesador con seguridad habilitada genere una certificación criptográfica de todo el contenido del área de la memoria protegida mediante hardware en el estado inicial;

recibir la certificación criptográfica del procesador con seguridad habilitada, incluyendo, al menos una parte de la certificación criptográfica, una autenticación creada por el procesador con seguridad habilitada utilizando una clave privada del procesador con seguridad habilitada; y

proporcionar la certificación criptográfica al sistema cliente (112), siendo la certificación criptográfica utilizable por el sistema cliente, en base a una comparación de al menos la porción de la certificación criptográfica con una indicación criptográfica conocida del Software y datos identificados en la solicitud en el estado inicial, para determinar que el contenido del área de la memoria protegida mediante hardware incluye, en el estado inicial, solo el software y los datos identificados en la solicitud, siendo la certificación utilizable por el sistema cliente, en base, al menos, en una clave pública asociada con el procesador con seguridad habilitada, para determinar que la certificación criptográfica de todos los contenidos del área de la memoria protegida mediante hardware en el estado inicial fueron creados por el procesador con seguridad habilitada.

2. El método de la reivindicación 1, en el que la certificación criptográfica incluye un autenticador criptográfico o un resumen de todos los contenidos del área de la memoria protegida mediante hardware en el estado inicial.

3. El método de la reivindicación 1 o la reivindicación 2, en el que los datos identificados en la solicitud del sistema cliente incluyen uno o más parámetros identificados por el sistema cliente, y en el que el sistema cliente puede utilizar la certificación criptográfica para determinar que el estado inicial no incluye ningún parámetro distinto de los uno o más parámetros.

4. El método de cualquier reivindicación precedente, que comprende además proporcionar, al sistema cliente, un certificado de auditoría, firmado por otra clave privada de una entidad auditora, indicando el certificado de auditoría que el procesador con seguridad habilitada está físicamente intacto.

5. El método de cualquier reivindicación precedente, en el que la autenticación incluye uno o más certificados de confianza, incluyendo un certificado de confianza de una autoridad confiable, uno o más certificados de confianza colectivamente utilizables por el sistema cliente para determinar que el procesador con seguridad habilitada es de un tipo que media el acceso al área de la memoria protegida mediante hardware por parte de todo el código que se ejecuta fuera del área de la memoria protegida mediante hardware y que cifra todo el contenido del área de la memoria protegida mediante hardware.

6. El método de cualquier reivindicación precedente, en el que la autenticación incluye un certificado de procesador de un fabricante del procesador con seguridad habilitada, el certificado del procesador que indica que el procesador con seguridad habilitada es de un tipo que media el acceso al área de la memoria protegida mediante hardware por parte de todo el código que se ejecuta fuera del área de la memoria protegida mediante hardware.

7. Medios legibles por ordenador, que comprenden una pluralidad de instrucciones de programación que son ejecutables por parte de uno o más procesadores para hacer que un sistema informático:

transmita una solicitud a un servicio de alojamiento de la aplicación, la solicitud de un procesador con seguridad habilitada del servicio de alojamiento de la aplicación para establecer un área de la memoria protegida mediante hardware del servicio de alojamiento de la aplicación, identificando la solicitud el software y los datos que se incluirán en el área de la memoria protegida mediante hardware (216) en un estado inicial, estando configurado el procesador con seguridad habilitada para mediar el acceso al área de la memoria protegida mediante hardware (216) por parte de todo el código que se ejecuta fuera del área protegida de la memoria (216), estando configurado el procesador con seguridad habilitada para cifrar todo el contenido del área de la memoria protegida mediante hardware, una porción del software para ser incluida en área de la memoria protegida mediante hardware y

ejecutable para hacer que el procesador con seguridad habilitada genere una certificación criptográfica de todos los contenidos del área de la memoria protegida mediante hardware en el estado inicial;

reciba la certificación criptográfica del servicio de alojamiento de la aplicación (102), incluyendo la certificación criptográfica, al menos una autenticación creada por el procesador con seguridad habilitada mediante una clave privada del procesador con seguridad habilitada;

determine, en base, al menos, a una comparación de al menos una parte de la certificación criptográfica con una indicación criptográfica conocida del software y a los datos en el estado inicial, que solo el software y los datos identificados por la solicitud están incluidos en el área de la memoria protegida mediante hardware en el estado inicial; y

determine, en base, al menos, a la autenticación y a una clave pública del procesador con seguridad habilitada, que la certificación criptográfica de todos los contenidos del área de la memoria protegida mediante hardware en el estado inicial está generada por el procesador con seguridad habilitada.

8. El medio legible por ordenador de la reivindicación 7, en el que la pluralidad de instrucciones de programación es ejecutable para hacer que el sistema informático reciba del servicio de alojamiento de la aplicación la certificación criptográfica de que el procesador con seguridad habilitada es físicamente seguro.

9. El medio legible por ordenador de la reivindicación 7 o la reivindicación 8, en el que la pluralidad de instrucciones de programación es además ejecutable para hacer que el sistema informático indique al servicio de alojamiento de la aplicación que cargue uno o más componentes de la aplicación en el área de la memoria protegida mediante hardware, siendo los uno o más componentes de la aplicación diferentes del software que se identifica mediante la solicitud y que está incluido en el área de la memoria protegida mediante hardware en el estado inicial.

10. El medio legible por ordenador de cualquiera de las reivindicaciones 7 a 9, en el que el identificador incluye al menos un autenticador criptográfico de los contenidos del área de la memoria protegida mediante hardware en el estado inicial.

11. Un sistema informático que comprende:

una memoria (104);

uno o más procesadores, incluido un procesador con seguridad habilitada (106) configurado para establecer un área de la memoria protegida mediante hardware (216) en la memoria (106), en el que el procesador con seguridad habilitada está configurado para mediar el acceso al área de la memoria protegida mediante hardware (216) mediante todo el código que se ejecuta en el sistema informático fuera del área protegida de la memoria (216), estando configurado el procesador con seguridad habilitada para cifrar todos los contenidos del área de la memoria protegida mediante hardware; y

uno o más módulos (214) almacenados en la memoria y ejecutables mediante uno o más procesadores (202) para:

recibir (402) una solicitud de un sistema cliente para establecer el área de la memoria protegida mediante hardware, incluyendo la solicitud una indicación del software y los datos que deben estar cargados en el área de la memoria protegida mediante hardware en un estado inicial;

causar (406), al menos parcialmente en respuesta a la solicitud, que el procesador con seguridad habilitada (106) cree una instancia del área de la memoria protegida mediante hardware (216) e incluya en el área de la memoria protegida mediante hardware el software y los datos en el estado inicial;

causar que una instancia de un módulo de cargador (116) ejecute el entorno para ejecutar, estando el módulo de cargador configurado, tras la ejecución, para transmitir al sistema cliente la certificación criptográfica, firmada por una clave privada del procesador con seguridad habilitada (106), que incluye un indicador que puede utilizar el sistema cliente, en base a una comparación del indicador con un indicador conocido del software y datos en el estado inicial, que el estado de activación del área protegida de la memoria (216) incluye solo el software y los datos indicados por la solicitud en el estado inicial, siendo la certificación criptográfica adicional utilizada por el sistema cliente, en base, al menos a una clave pública del procesador con seguridad habilitada, para determinar que el procesador con seguridad habilitada generó el indicador.

12. El sistema informático de la reivindicación 11, en el que la clave de privacidad del procesador con seguridad habilitada se almacena en el procesador con seguridad habilitada de manera que sea accesible para el procesador con seguridad habilitada, pero no para ningún otro componente del sistema informático.

13. El sistema informático de la reivindicación 11, en el que los uno o más módulos son ejecutables además por uno o más procesadores para recibir una clave de cifrado cifrada mediante una clave pública del procesador con seguridad habilitada que corresponde a la clave privada del procesador con seguridad habilitada, y para obtener,

utilizando la clave de cifrado, uno o más componentes de la aplicación que se ejecutarán en el área de la memoria protegida mediante hardware.

14. El sistema informático de la reivindicación 11, en el que el indicador incluye un resumen de todos los contenidos del área de la memoria protegida mediante hardware en el estado inicial y una clave pública correspondiente a la clave privada que fue utilizada para firmar la certificación criptográfica.

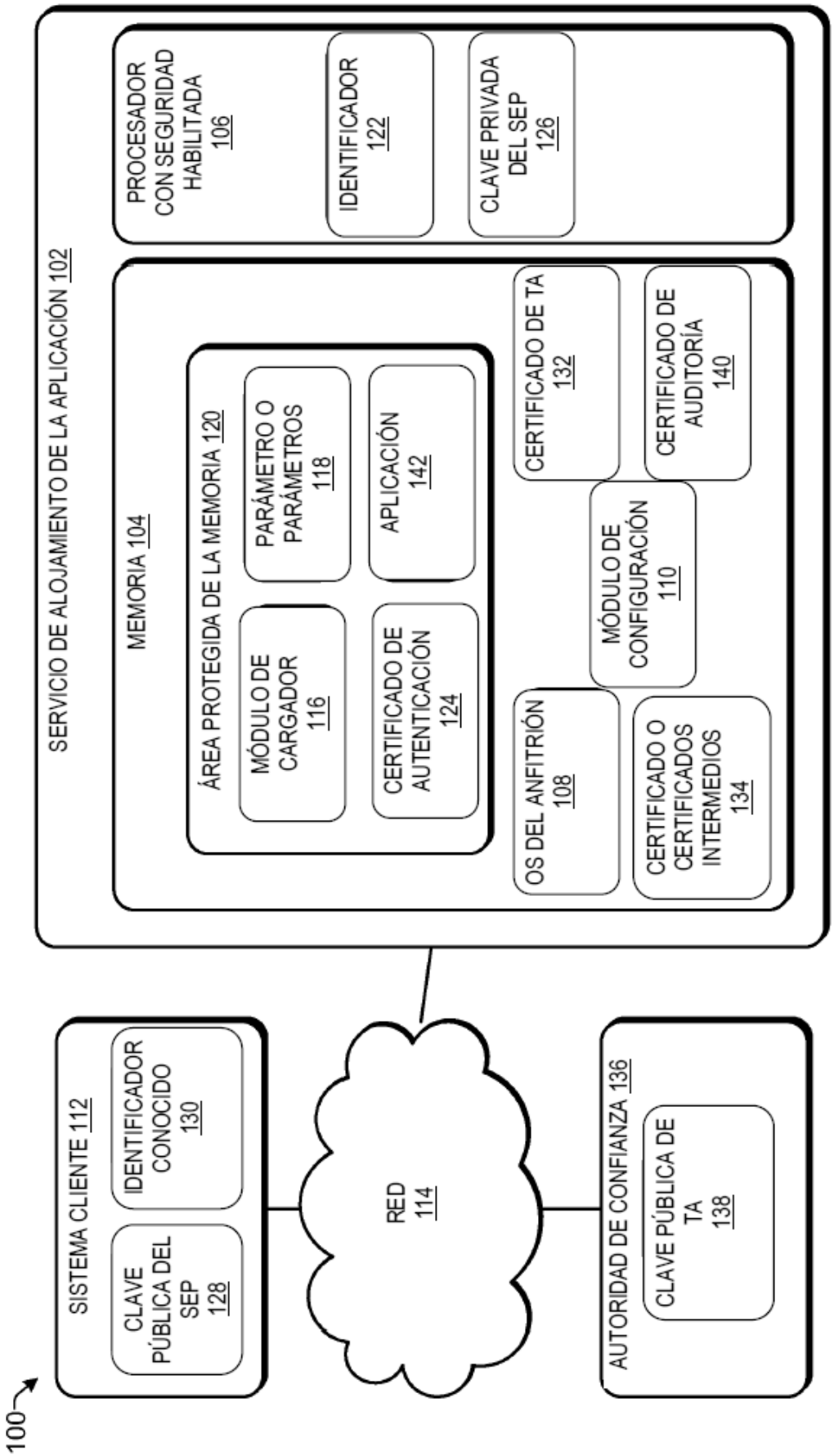
100
SISTEMA CLIENTE 112
CLAVE PÚBLICA DEL SEP 128
IDENTIFICADOR CONOCIDO 130
RED 114
AUTORIDAD DE CONFIANZA 136
CLAVE PÚBLICA DE TA 138
SERVICIO DE ALOJAMIENTO DE LA APLICACIÓN 102
PROCESADOR CON SEGURIDAD HABILITADA 106
IDENTIFICADOR 122
CLAVE PRIVADA DEL SEP 126
MEMORIA 104
ÁREA PROTEGIDA DE LA MEMORIA 120
MÓDULO DE CARGADOR 116
PARÁMETRO O PARÁMETROS 118
CERTIFICADO DE AUTENTICACIÓN 124
APLICACIÓN 142
CERTIFICADO DE TA 132
CERTIFICADO DE AUDITORÍA 140
MÓDULO DE CONFIGURACIÓN 110
OS DEL ANFITRIÓN 108
CERTIFICADO O CERTIFICADOS INTERMEDIOS 134

FIG. 1

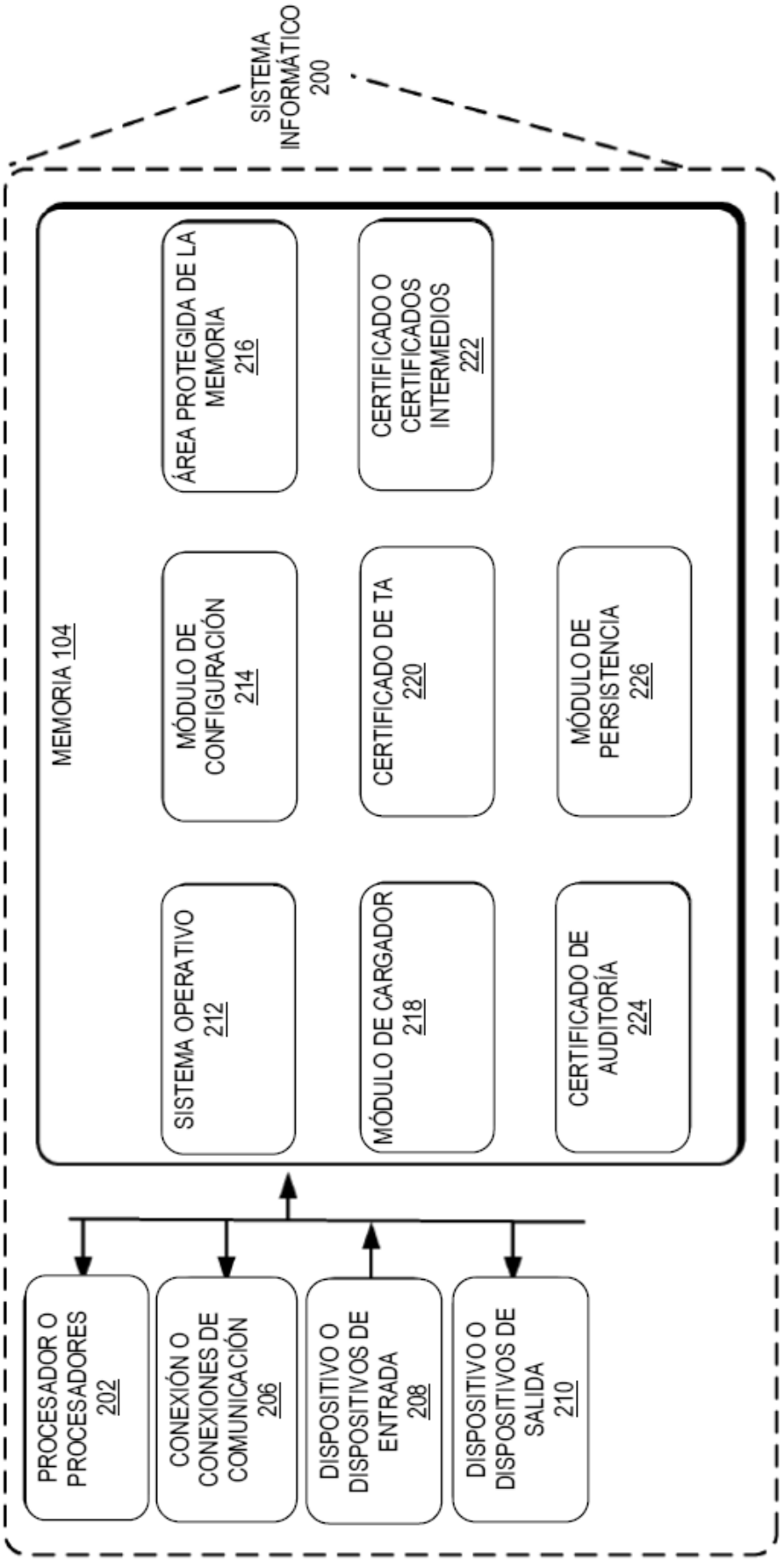
SISTEMA INFORMÁTICO 200
MEMORIA 104
ÁREA PROTEGIDA DE LA MEMORIA 216
CERTIFICADO O CERTIFICADOS INTERMEDIOS 222
MÓDULO DE CONFIGURACIÓN 214
CERTIFICADO DE TA 220
MÓDULO DE PERSISTENCIA 226
SISTEMA OPERATIVO 212
MÓDULO DE CARGADOR 218
CERTIFICADO DE AUDITORÍA 224
PROCESADOR O PROCESADORES 202
CONEXIÓN O CONEXIONES DE COMUNICACIÓN 206
DISPOSITIVO O DISPOSITIVOS DE ENTRADA 208
DISPOSITIVO O DISPOSITIVOS DE SALIDA 210

FIG. 2

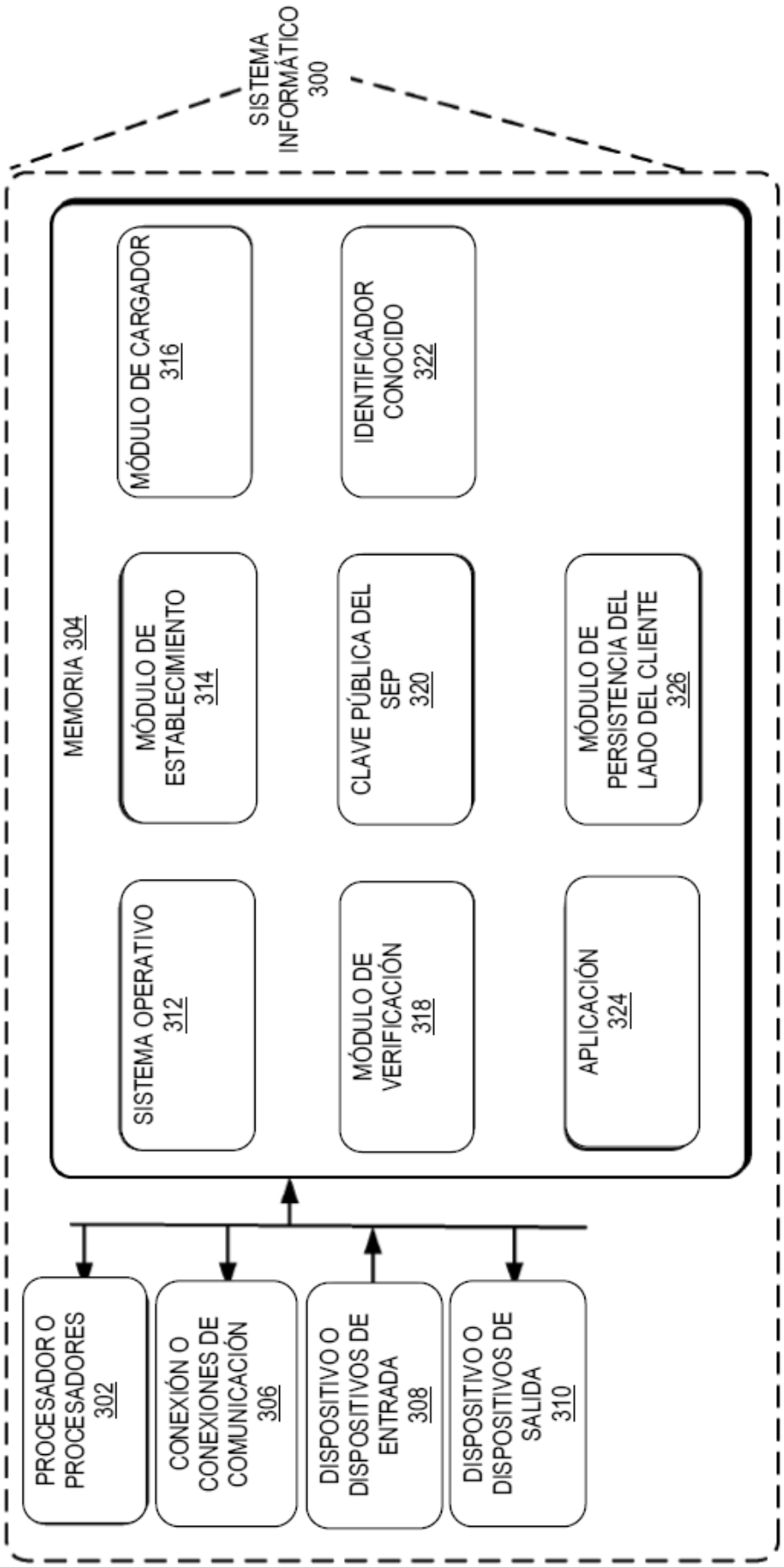
SISTEMA INFORMÁTICO 300
MEMORIA 304
MÓDULO DE CARGADOR 316
IDENTIFICADOR CONOCIDO 322
MÓDULO DE ESTABLECIMIENTO 314
CLAVE PÚBLICA DEL SEP 320
MÓDULO DE PERSISTENCIA DEL LADO DEL CLIENTE 326
SISTEMA OPERATIVO 312
MÓDULO DE VERIFICACIÓN 318
APLICACIÓN 324
PROCESADOR O PROCESADORES 302
CONEXIÓN O CONEXIONES DE COMUNICACIÓN 306
DISPOSITIVO O DISPOSITIVOS DE ENTRADA 308
DISPOSITIVO O DISPOSITIVOS DE SALIDA 310

FIG. 3

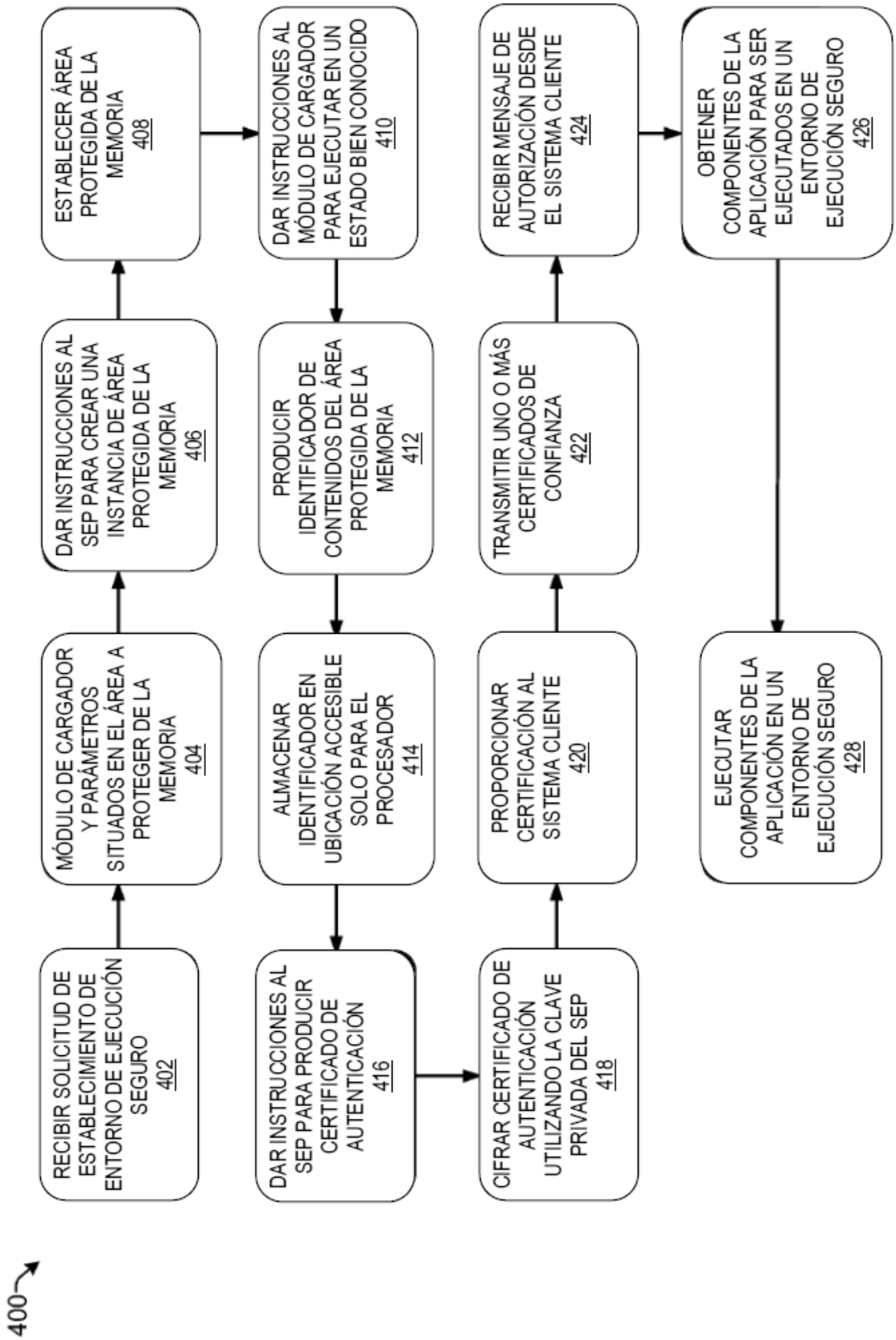
400
RECIBIR SOLICITUD DE ESTABLECIMIENTO DE ENTORNO DE EJECUCIÓN SEGURO 402
MÓDULO DE CARGADOR Y PARÁMETROS SITUADOS EN EL ÁREA A PROTEGER DE LA MEMORIA 404
DAR INSTRUCCIONES AL SEP PARA CREAR UNA INSTANCIA DE ÁREA PROTEGIDA DE LA MEMORIA 406
ESTABLECER ÁREA PROTEGIDA DE LA MEMORIA 408
DAR INSTRUCCIONES AL MÓDULO DE CARGADOR PARA EJECUTAR EN UN ESTADO BIEN CONOCIDO 410
PRODUCIR IDENTIFICADOR DE CONTENIDOS DEL ÁREA PROTEGIDA DE LA MEMORIA 412
ALMACENAR IDENTIFICADOR EN UBICACIÓN ACCESIBLE SOLO PARA EL PROCESADOR 414
DAR INSTRUCCIONES AL SEP PARA PRODUCIR CERTIFICADO DE AUTENTICACIÓN 416
CIFRAR CERTIFICADO DE AUTENTICACIÓN UTILIZANDO LA CLAVE PRIVADA DEL SEP 418
PROPORCIONAR CERTIFICACIÓN AL SISTEMA CLIENTE 420
TRANSMITIR UNO O MÁS CERTIFICADOS DE CONFIANZA 422
RECIBIR MENSAJE DE AUTORIZACIÓN DESDE EL SISTEMA CLIENTE 424
OBTENER COMPONENTES DE LA APLICACIÓN PARA SER EJECUTADOS EN UN ENTORNO DE EJECUCIÓN SEGURO 426
EJECUTAR COMPONENTES DE LA APLICACIÓN EN UN ENTORNO DE EJECUCIÓN SEGURO 428

FIG. 4

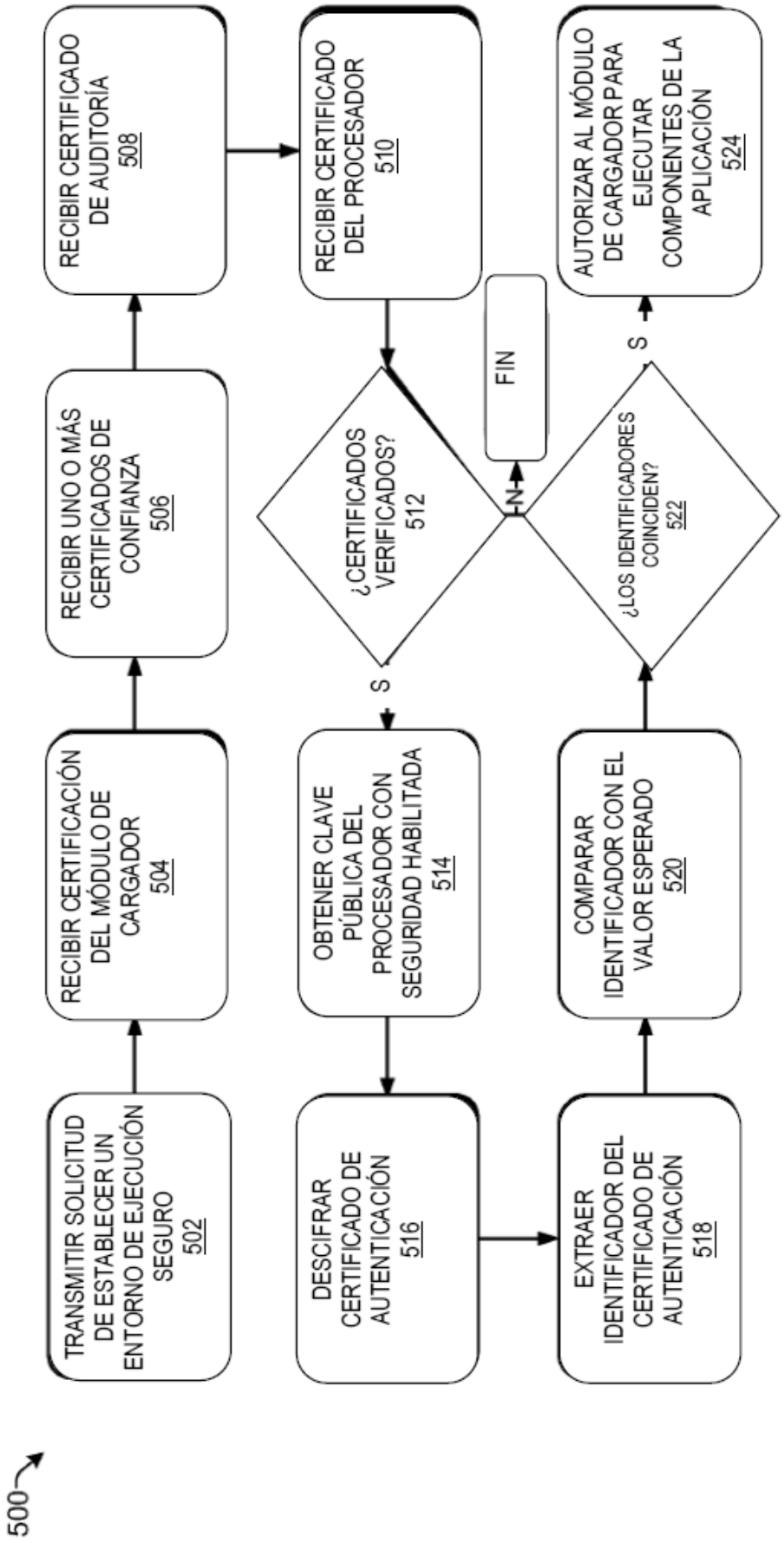
500
TRANSMITIR SOLICITUD DE ESTABLECER UN ENTORNO DE EJECUCIÓN SEGURO 502
RECIBIR CERTIFICACIÓN DEL MÓDULO DE CARGADOR 504
RECIBIR UNO O MÁS CERTIFICADOS DE CONFIANZA 506
RECIBIR CERTIFICADO DE AUDITORÍA 508
RECIBIR CERTIFICADO DEL PROCESADOR 510
¿CERTIFICADOS VERIFICADOS? 512
S
N
FIN
OBTENER CLAVE PÚBLICA DEL PROCESADOR CON SEGURIDAD HABILITADA 514
DESCIFRAR CERTIFICADO DE AUTENTICACIÓN 516
EXTRAER IDENTIFICADOR DEL CERTIFICADO DE AUTENTICACIÓN 518
COMPARAR IDENTIFICADOR CON EL VALOR ESPERADO 520
¿LOS IDENTIFICADORES COINCIDEN? 522
S
AUTORIZAR AL MÓDULO DE CARGADOR PARA EJECUTAR COMPONENTES DE LA APLICACIÓN 524

FIG. 5

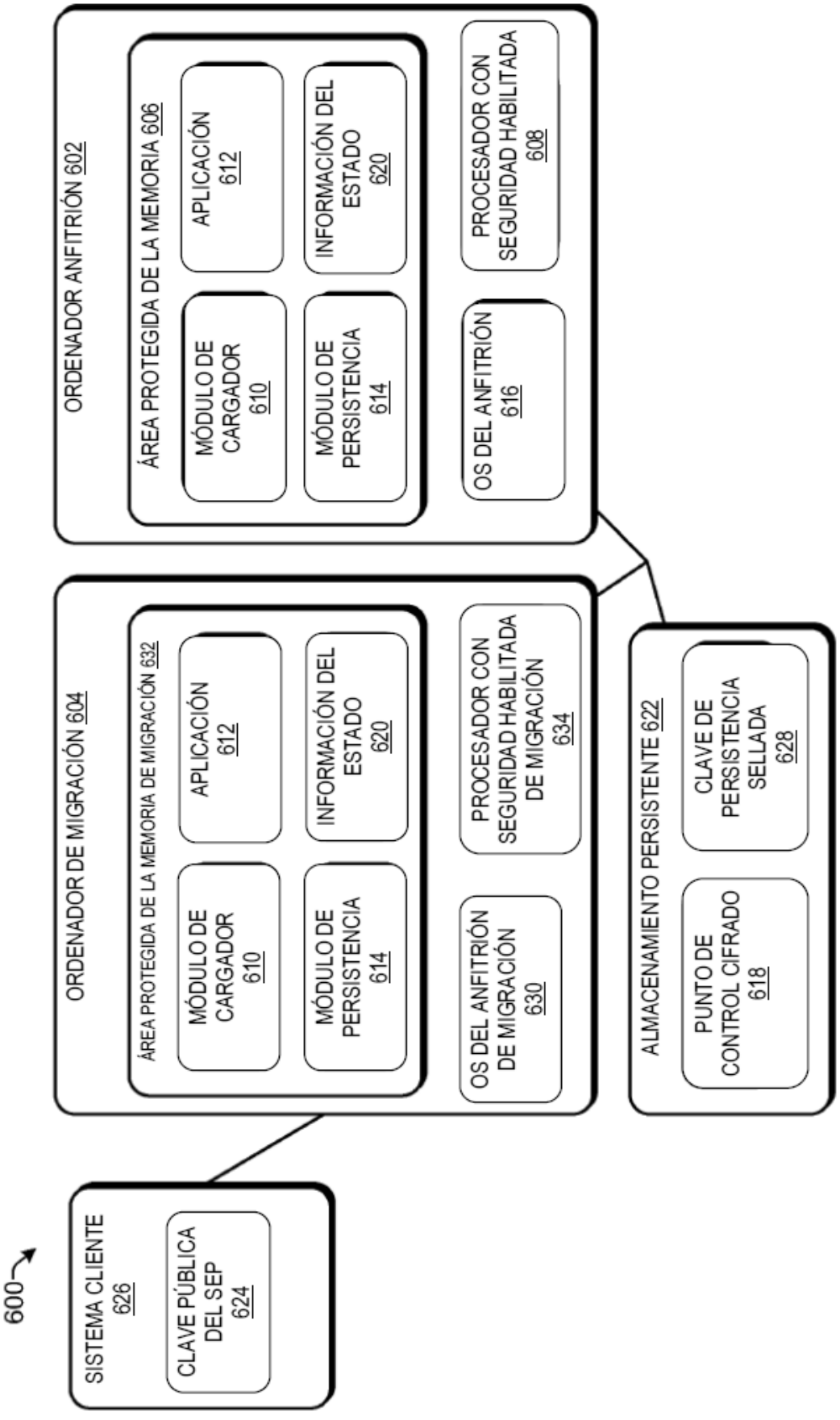
600
SISTEMA CLIENTE 626
CLAVE PÚBLICA DEL SEP 624
ORDENADOR DE MIGRACIÓN 604
ÁREA PROTEGIDA DE LA MEMORIA DE MIGRACIÓN 632
MÓDULO DE CARGADOR 610
APLICACIÓN 612
MÓDULO DE PERSISTENCIA 614
INFORMACIÓN DEL ESTADO 620
OS DEL ANFITRIÓN DE MIGRACIÓN 630
PROCESADOR CON SEGURIDAD HABILITADA DE MIGRACIÓN 634
ORDENADOR ANFITRIÓN 602
ÁREA PROTEGIDA DE LA MEMORIA 606
MÓDULO DE CARGADOR 610
APLICACIÓN 612
MÓDULO DE PERSISTENCIA 614
INFORMACIÓN DEL ESTADO 620
OS DEL ANFITRIÓN 616
PROCESADOR CON SEGURIDAD HABILITADA 608
ALMACENAMIENTO PERSISTENTE 622
PUNTO DE CONTROL CIFRADO 618
CLAVE DE PERSISTENCIA SELLADA 628

FIG. 6

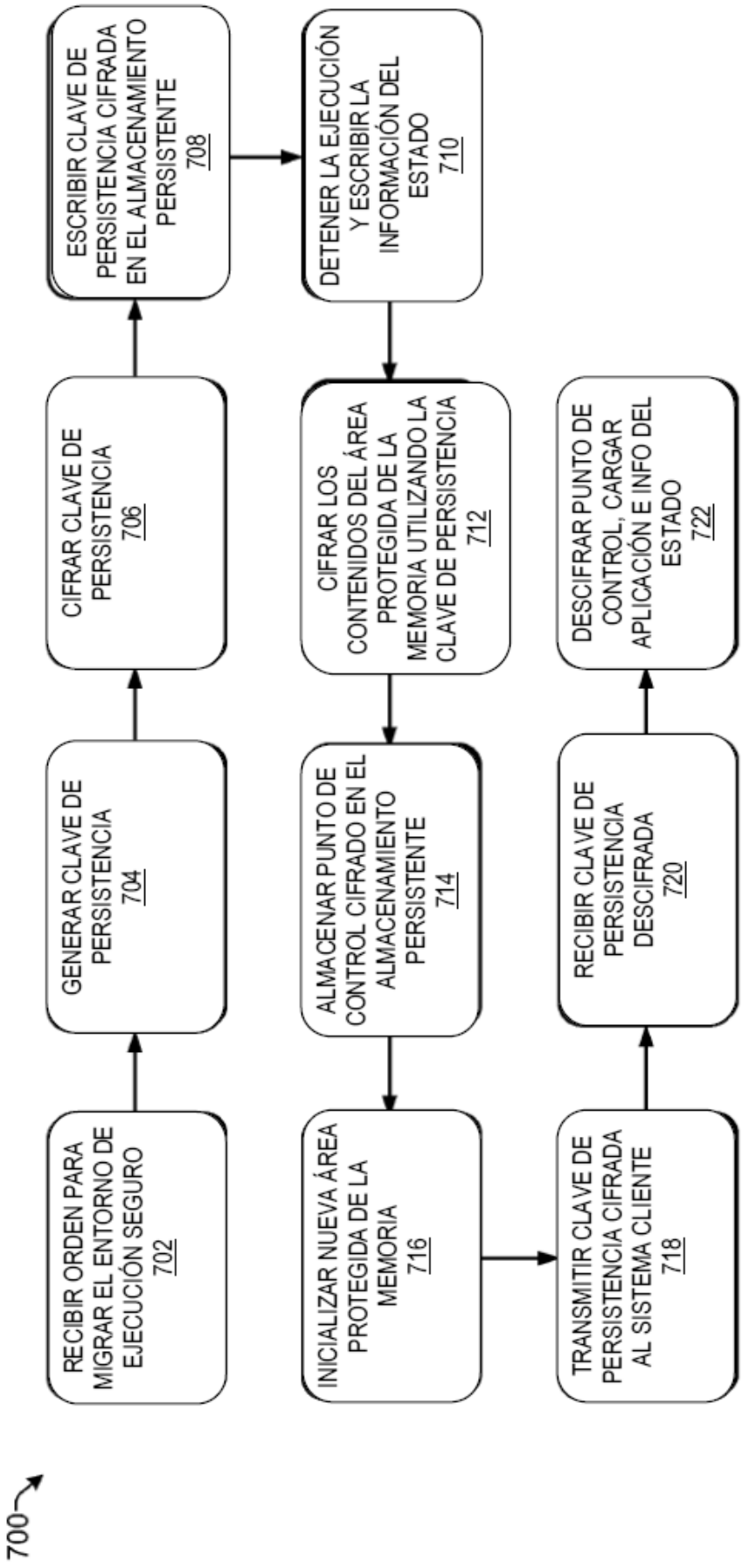
700
RECIBIR ORDEN PARA MIGRAR EL ENTORNO DE EJECUCIÓN SEGURO 702
GENERAR CLAVE DE PERSISTENCIA 704
CIFRAR CLAVE DE PERSISTENCIA 706
ESCRIBIR CLAVE DE PERSISTENCIA CIFRADA EN EL ALMACENAMIENTO PERSISTENTE 708
DETENER LA EJECUCIÓN Y ESCRIBIR LA INFORMACIÓN DEL ESTADO 710
CIFRAR LOS CONTENIDOS DEL ÁREA PROTEGIDA DE LA MEMORIA UTILIZANDO LA CLAVE DE PERSISTENCIA 712
ALMACENAR PUNTO DE CONTROL CIFRADO EN EL ALMACENAMIENTO PERSISTENTE 714
INICIALIZAR NUEVA ÁREA PROTEGIDA DE LA MEMORIA 716
TRANSMITIR CLAVE DE PERSISTENCIA CIFRADA AL SISTEMA CLIENTE 718
RECIBIR CLAVE DE PERSISTENCIA DESCIFRADA 720
DESCIFRAR PUNTO DE CONTROL, CARGAR APLICACIÓN E INFO DEL ESTADO 722

FIG. 7

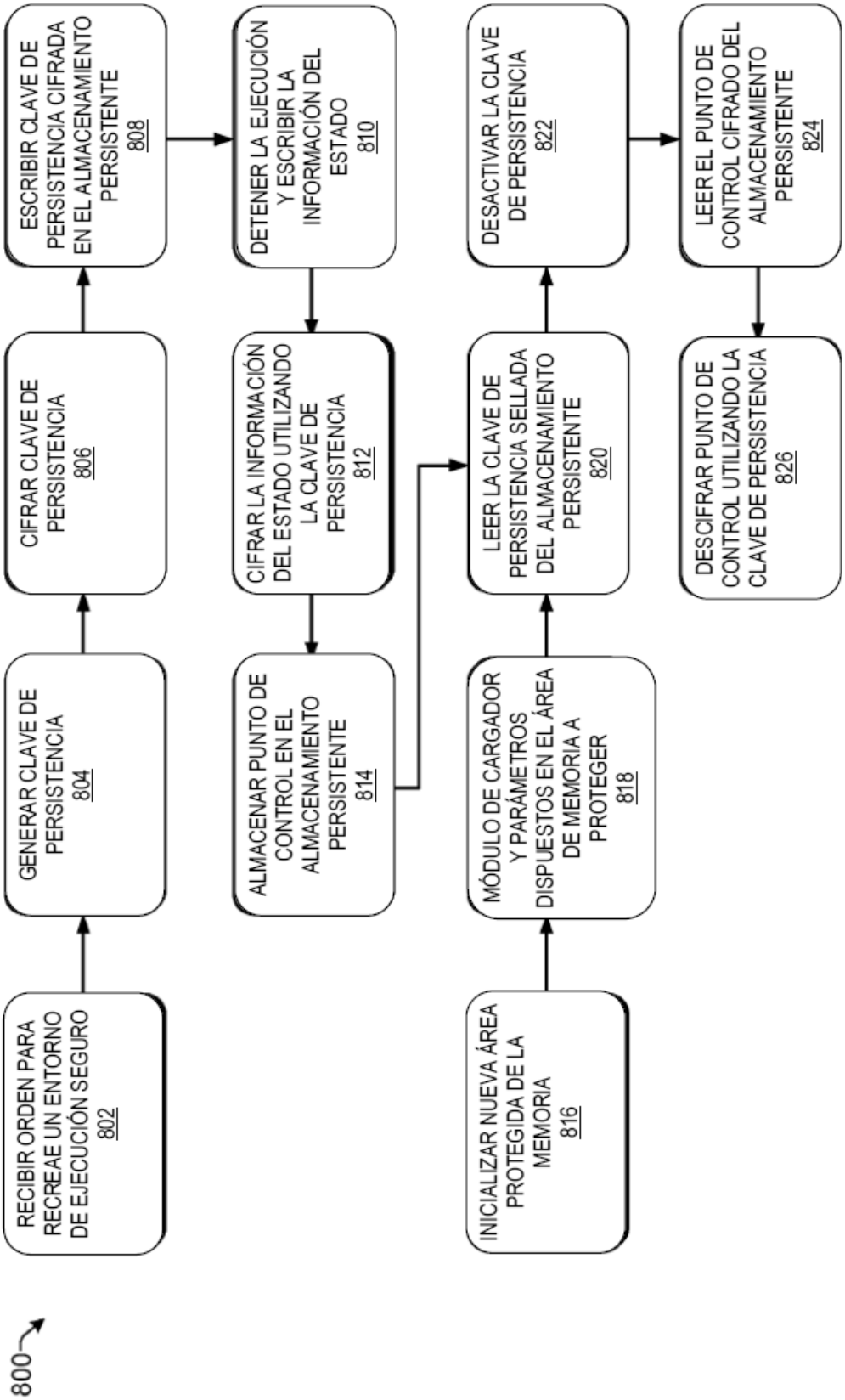
800
RECIBIR ORDEN PARA RECREAE UN ENTORNO DE EJECUCIÓN SEGURO 802
GENERAR CLAVE DE PERSISTENCIA 804
CIFRAR CLAVE DE PERSISTENCIA 806
ESCRIBIR CLAVE DE PERSISTENCIA CIFRADA EN EL ALMACENAMIENTO PERSISTENTE 808
DETENER LA EJECUCIÓN Y ESCRIBIR LA INFORMACIÓN DEL ESTADO 810
CIFRAR LA INFORMACIÓN DEL ESTADO UTILIZANDO LA CLAVE DE PERSISTENCIA 812
ALMACENAR PUNTO DE CONTROL EN EL ALMACENAMIENTO PERSISTENTE 814
INICIALIZAR NUEVA ÁREA PROTEGIDA DE LA MEMORIA 816
MÓDULO DE CARGADOR Y PARÁMETROS DISPUESTOS EN EL ÁREA DE MEMORIA A PROTEGER 818
LEER LA CLAVE DE PERSISTENCIA SELLADA DEL ALMACENAMIENTO PERSISTENTE 820
DESACTIVAR LA CLAVE DE PERSISTENCIA 822
LEER EL PUNTO DE CONTROL CIFRADO DEL ALMACENAMIENTO PERSISTENTE 824
DESCIFRAR PUNTO DE CONTROL UTILIZANDO LA CLAVE DE PERSISTENCIA 826

FIG. 8