(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 773 950**

(51) Int. CI.:

G06F 21/52 (2013.01)
G06F 21/84 (2013.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **18.09.2013 E 13185013 (3)**

(97) Fecha y número de publicación de la concesión europea: **01.01.2020 EP 2711859**

(54) Título: **Sistema informático asegurado con autenticación asíncrona**

(30) Prioridad:

19.09.2012 US 201261702763 P
13.08.2013 US 201313965256

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
15.07.2020

(73) Titular/es:

WINBOND ELECTRONICS CORP. (100.0%)
No. 8, Keya 1st Road, Daya District
Taichung City 428, TW

(72) Inventor/es:

HERSHMAN, ZIV;
TEPER, VALERY y
ALON, MOSHE

(74) Agente/Representante:

CARVAJAL Y URQUIJO, Isabel

DESCRIPCIÓN

Sistema informático asegurado con autenticación asíncrona

Campo de la invención

La presente invención se refiere, generalmente, a sistema informáticos, y particularmente a métodos y sistemas para una ejecución segura de programas almacenados en dispositivos externos.

Antecedentes

En los sistemas informáticos asegurados, un dispositivo informático asegurado se comunica, a menudo, con uno o más dispositivos externos. Normalmente, un dispositivo externo comprende al menos un dispositivo de memoria que almacena instrucciones de programa que van a ejecutarse por un núcleo de procesamiento dentro del dispositivo informático. En casos en los que el enlace de comunicación entre el dispositivo informático y los dispositivos externos no es seguro, a menudo, se requiere que el dispositivo informático asegurado valide la integridad y autenticidad de los datos recibidos mediante el enlace. La validación de autenticidad significa que un dispositivo de recepción (por ejemplo, un dispositivo informático asegurado) pueda verificar que los datos se enviaron desde una fuente legítima (por ejemplo, un dispositivo de memoria autorizado). La integridad significa que los datos no fueron alternados antes de introducirse al dispositivo de recepción. En la siguiente descripción, y en las reivindicaciones, el término “autenticación” se refiere, en conjunto, a técnicas que validan o bien la autenticidad de los datos o la integridad de los datos o ambas.

Los métodos para la autenticación de código y datos almacenados en un dispositivo externo al entorno informático se conocen en la técnica. Por ejemplo, la publicación de solicitud de patente estadounidense 2010/0070779 describe un método para proteger la integridad de datos cifrados por un algoritmo de cifrado que proporciona al menos un estado intermedio previsto para ser idéntico en su cifrado y en su descifrado, se muestrea este estado intermedio durante el cifrado para generar una firma. La divulgación se aplica, más específicamente, a la protección de la privacidad y de la integridad (o autenticidad) del contenido de una memoria externa a un circuito integrado considerado como seguro.

La patente estadounidense 8.108.941 describe un procesador, conectado a una memoria no volátil que almacena una primera información de autenticación de memoria para la autenticación de la memoria no volátil. El procesador incluye una unidad de funcionamiento configurada para realizar una operación que utiliza información almacenada en la memoria no volátil, una memoria de autenticación formada de manera solidaria con la unidad de funcionamiento, y almacenar segunda información de autenticación de memoria para la autenticación de la memoria no volátil, una unidad de adquisición de información de autenticación configurada para adquirir la primera información de autenticación de memoria procedente de la memoria no volátil, una unidad de autenticación de memoria configurada para comparar la primera información de autenticación de memoria y la segunda información de autenticación de memoria para autenticar la memoria no volátil, y una unidad de control de acceso de memoria configurada para permitir el acceso a la memoria no volátil cuando la unidad de autenticación de memoria realiza una autenticación satisfactoria.

La patente estadounidense 8.140.824, describe un producto de programa informático que comprende un medio usable por ordenador que tiene un programa legible por ordenador para la autenticación de código, tal como un código de arranque. Un motor de direccionamiento de memoria puede emplearse para seleccionar una parte de una memoria, en función de un valor de etapa, como primer valor resumen de entrada. El valor de etapa permite la condensación acumulativa no conmutativa de una pluralidad de partes de memoria con un segundo valor resumen de entrada, tal como un valor resumen anterior que se ha rotado hacia la izquierda. Un circuito autenticador puede emplearse para realizar una condensación después de la parte de memoria y el segundo valor resumen de entrada. Entonces, puede emplearse un circuito de comparación para comparar una salida del circuito autenticador con el valor esperado.

Gong L DK12SPEC PDF / JAVA-TM-Security-Architecture PDF: “Java security architecture (JDK1.2) Version 1.0” proporciona la plataforma Java (principalmente a través de JDK) como una plataforma segura, preparada para construirse en la que ejecutar aplicaciones permitidas por Java de forma segura.

El documento US 2010/016965A1 se refiere a un método implementado por ordenador para la verificación del autor y la autorización del código de objeto. En una realización, el código de objeto de programa se enlaza con una pluralidad de bloques de datos para crear un código de objeto enlazado y un archivo MAP. A continuación, se realiza la verificación del autor ejecutando una pluralidad de comparaciones entre el código de objeto enlazado y el archivo MAP. En otra realización, un procedimiento de firma digital se realiza en el código de objeto enlazado creando un bloque de datos de firma. Entonces, el bloque de datos de firma se encripta y se escribe en el código de objeto enlazado para crear un código de objeto de firma digital. En otra realización, un programa de aplicación incluido en el código de objeto enlazado genera un paquete de datos. El paquete de datos se compara entonces con un paquete de datos de firma anteriormente generado procedente del código de objeto enlazado para determinar si el código de objeto enlazado se autoriza.

El documento US2007/133437 A da a conocer un sistema para permitir una aplicación controlada de indicaciones derivada sobre quién está hablando relacionada con la actividad de participantes en una conferencia de comunicaciones con múltiples participantes en directo o emisiones grabadas. El sistema incluye un primer nodo que hospeda un conmutador de conexión de conferencia, software o una combinación de los mismos, que presenta múltiples canales de entrada de conferencia; un segundo nodo que presenta acceso de datos a al menos un puerto de señal de salida del conmutador de conexión de conferencia, software, o una combinación de los mismos, y una aplicación de software distribuida por completo al nodo primero o segundo, o en partes a los nodos primero y segundo. La aplicación se usa para aplicar las indicaciones sobre quién está hablando para emitir comunicaciones, archivos de datos, o flujos de datos, reenviados a uno de, una parte seleccionada de, o una combinación de, los participantes de la conferencia, terceros no participantes, y una o más instalaciones de almacenamiento.

El documento US 2005/123135A1 da a conocer un sistema de video seguro para un adaptador de visualización de gráficos que incluye un módulo para desencriptar una señal de contenido procedente de un reproductor de medios u otra fuente de contenido seguro. El adaptador puede proporcionarse como un componente de un sistema de gráficos de ordenador, o en un dispositivo con fines específico autónomo. El adaptador puede incluir otras características para impedir el uso no autorizado de contenido protegido, por ejemplo, autenticar la fuente de una señal de contenido antes de proporcionar una señal de video o audio de salida, encriptar la señal de video de salida, responder a órdenes para renovar o anular conjuntos de clave criptográfica, e integrar información de seguimiento forense en una señal de audio o video.

Sumario

Una realización de la presente invención proporciona un dispositivo informático que incluye un puente de entrada, un puente de salida, un núcleo de procesamiento, y lógica de autenticación. El puente de entrada se acopla para recibir una secuencia de elementos de datos para su uso mediante el dispositivo al ejecutar un programa. El núcleo de procesamiento se acopla para recibir los elementos de datos procedentes del puente de entrada y ejecutar el programa para provocar que el puente de salida emita una señal en respuesta a un elemento de datos dado en la secuencia, y la lógica de autenticación se acopla para recibir y autenticar los elementos de datos al tiempo que el núcleo de procesamiento ejecuta el programa, y para inhibir la emisión de la señal por el puente de salida hasta que el elemento de datos dado se haya autenticado.

En algunas realizaciones, los elementos de datos incluyen instrucciones de programa y el elemento de datos dado incluye una instrucción de salida, y el núcleo de procesamiento está configurado para ejecutar el programa ejecutando las instrucciones de programa, incluyendo la instrucción de salida. En otras realizaciones, la lógica de autenticación está configurada para autenticar los elementos de datos de manera asíncrona con la ejecución del programa mediante el núcleo de procesamiento. En todavía otras realizaciones, la lógica de autenticación está configurada para autenticar el elemento de datos dado después de haber usado el elemento de datos para ejecutar el programa mediante el núcleo de procesamiento, y para retrasar la emisión de la señal por el puente de salida hasta que la autenticación del elemento de datos dado se haya completado.

En una realización, la lógica de autenticación está configurada para autenticar los elementos de datos calculando una o más firmas digitales de los elementos de datos y comparando las firmas calculadas con firmas originales respectivas recibidas por el dispositivo por medio del puente de entrada. En otra realización, la lógica de autenticación está configurada para generar una señal de alerta si al menos una de las firmas calculadas no coincide con la firma original respectiva. En todavía otra realización, el puente de entrada está configurado para recibir los elementos de datos recibiendo bloques de elementos de datos primero y segundo, y recibir el segundo bloque se permite solo tras la autenticación de todos los elementos de datos del primer bloque usando la lógica de autenticación.

Adicionalmente, se proporciona, según una realización de la presente invención, un método que incluye, recibir en un dispositivo informático por medio de un puente de entrada una secuencia de elementos de datos para su uso al ejecutar un programa mediante un núcleo de procesamiento del dispositivo, ejecutar el programa mediante el núcleo de procesamiento para provocar la emisión de una señal del dispositivo en respuesta a un elemento de datos dado en la secuencia, y autenticar los elementos de datos usando la lógica de autenticación al tiempo que el núcleo de procesamiento ejecuta el programa, e inhibir la emisión de la señal hasta que el elemento de datos dado se haya autenticado.

Adicionalmente, se proporciona, según una realización de la presente invención, un sistema informático que incluye, un dispositivo externo y un dispositivo informático. El dispositivo externo está configurado para proporcionar una secuencia de elementos de datos, y el dispositivo informático incluye, además, un puente de entrada, un puente de salida, un núcleo de procesamiento, y lógica de autenticación. El puente de entrada se acopla para recibir desde el dispositivo externo la secuencia de elementos de datos para su uso mediante el dispositivo informático al ejecutar un programa. El núcleo de procesamiento se acopla para recibir los elementos de datos desde el puente de entrada y ejecutar el programa para provocar que el puente de salida emita una señal en respuesta a un elemento de datos dado en la secuencia, y la lógica de autenticación se acopla para recibir y autenticar los elementos de datos al tiempo que el núcleo de procesamiento ejecuta el programa, y para inhibir la emisión de la señal por el puente de salida hasta que el elemento de datos dado se haya autenticado.

La presente invención se comprenderá de manera más completa a partir de la siguiente descripción detallada de las realizaciones de la misma, tomadas junto con los dibujos, en los que:

Breve descripción de los dibujos

La figura 1 es un diagrama de bloques que ilustra esquemáticamente un sistema informático asegurado, según una realización de la presente invención;

la figura 2 es un diagrama de bloques que muestra esquemáticamente detalles del sistema informático asegurado de la figura 1, según una realización de la presente invención;

la figura 3 es un diagrama que muestra una máquina de estados de seguridad, según una realización de la presente invención; y

la figura 4 es un diagrama de flujo que ilustra esquemáticamente un método para la autenticación en un dispositivo informático asegurado, según una realización de la presente invención.

Descripción detallada de realizaciones

Resumen

A menudo, se requiere que los sistemas informáticos asegurados que aceptan datos (también denominados mensaje) procedentes de una fuente externa, validen la integridad y autenticidad de los datos antes de usarlos internamente. Las realizaciones de la invención presentadas a continuación usan firmas digitales para la autenticación de datos. Una firma digital comprende, normalmente, una cadena de bits que se almacena con los datos o se genera en tiempo real en el lado emisor (por ejemplo, un dispositivo de memoria) y se envía al receptor (por ejemplo, un dispositivo informático asegurado) junto con los datos para la autenticación. El receptor calcula una firma de los datos recibidos y compara la firma calculada con la firma original del emisor. Si las firmas coinciden, el receptor puede asumir que los datos son auténticos y que no se alteraron por un tercero no autorizado.

En muchos casos, la generación y validación de firmas se basa en el mensaje de datos y en una clave secreta. Normalmente, los algoritmos que generan firmas se diseñan de manera que no resulta factible que un tercero no autorizado genere firmas válidas sin un conocimiento completo de la clave secreta. Adicionalmente, cualquier cambio al mensaje de datos (es decir, la ruptura de la integridad de los datos) da como resultado un fallo de verificación de firma en el lado del receptor.

Se conocen diversos métodos en la técnica para la generación y validación de firmas usando claves secretas. Por ejemplo, un emisor puede generar una firma usando una clave privada, mientras que el receptor valida la firma usando una clave pública. Como otro ejemplo, tanto el emisor como el receptor pueden compartir una clave común que se mantiene en secreto entre los mismos. Los métodos para intercambio de clave entre un receptor y un emisor se conocen en la técnica. Tras validar una firma que corresponde a determinados datos (asumiendo que el secretismo de la clave no se ha incumplido), el dispositivo informático asegurado puede procesar de manera válida los datos recibidos. Por ejemplo, cuando los datos comprenden instrucciones de programa informático, el dispositivo informático puede ejecutar de manera segura el programa autenticado sin correr el riesgo de exponer información asegurada.

En cuanto a seguridad, las instrucciones de programa no autenticadas y otros elementos de datos que afectan al procesamiento en el interior del dispositivo informático pueden clasificarse en dos categorías con los fines de las realizaciones de la presente invención. El procesamiento de elementos de datos no autenticados de la primera categoría no expone ninguna información asegurada, y los elementos de datos en esta categoría se denominan, por tanto, instrucciones o elementos de datos neutros. Por otro lado, el procesamiento de elementos de datos no autenticados de la segunda categoría puede provocar la exposición de información asegurada o secreta directa o indirectamente. Los elementos de datos de la segunda categoría también pueden denominarse en el presente documento instrucciones de salida.

Las realizaciones de la presente invención que se describen en el presente documento proporcionan una mejora de los métodos y sistemas para la autenticación en un dispositivo informático asegurado. En una realización a modo de ejemplo, un núcleo de procesamiento en un dispositivo informático recibe instrucciones de programa para su ejecución desde un dispositivo externo, tal como una memoria, por medio de un puente de entrada. Las instrucciones se firman con una firma digital. Parte de las instrucciones (es decir, las instrucciones de salida) pueden provocar que el núcleo de procesamiento emita información por medio de un puente de salida. Los términos “puente de entrada” y “puente de salida” se usan de manera general en el presente documento para referirse a todas y cada una de las conexiones a través de las que el dispositivo informático puede recibir o transmitir señales, respectivamente. En la siguiente descripción y en las reivindicaciones, el término “señales” se refiere a cualquier canal que transporta información dentro o fuera del dispositivo, o ya sea por medio de una conexión de señal física o no. Ejemplos de canales de señal no físicos incluyen señales que pueden recogerse en ataques de canal lateral, tales como patrones de tensión en líneas de alimentación, cambios en emisión electromagnética e información asegurada que puede verse expuesta por un atacante que realiza operaciones de reseteo condicionales.

Las instrucciones recibidas a través del puente de entrada se autentican mediante lógica de autenticación específica dentro del dispositivo informático. La autenticación puede llevarse a cabo en paralelo con la ejecución mediante el núcleo de procesamiento de al menos partes del programa. Cuando el núcleo de procesamiento encuentra una instrucción de salida que todavía no se ha autenticado, la lógica de autenticación inhibe el puente de salida, y retrasa la emisión real de señales hasta que la instrucción de salida actual y todas las instrucciones que la anteceden se autentican. Por tanto, el rendimiento se maximiza evitando retrasos innecesarios de ejecución al tiempo que se espera la autenticación, al tiempo que se impide una exposición accidental de la información secreta.

En una realización, el dispositivo externo comprende un dispositivo de memoria no asegurado. Se comparte de manera seleccionada la capacidad de memoria para almacenar firmas que corresponden a bloques de datos de memoria. El dispositivo informático recibe datos y firma o firmas respectivas del dispositivo de memoria y autentica los bloques firmados. Los datos recibidos pueden almacenarse en una memoria caché antes de o al mismo tiempo que se ejecutan por el núcleo de procesamiento, y la reobtención de los datos del dispositivo externo se produce tras una situación de error de memoria caché. En lugar de funcionar en un ciclo de autenticado-obtención de único bloque, el dispositivo informático funciona en un modo en el que múltiples firmas se calculan, almacenan, y verifican tras la obtención de múltiples bloques de datos. Este modo de funcionamiento mejora la eficacia del dispositivo informático.

En otra realización, el dispositivo externo comprende un dispositivo de memoria asegurado, equipado con un motor de firma. El dispositivo externo asegurado comparte una clave secreta con el dispositivo informático y puede generar, mantener y enviar firmas de datos al dispositivo informático. Las firmas de datos pueden generarse calculando un resumen del mensaje con respecto a uno o más elementos de datos (por ejemplo, basados en bloque) y/o señales de direccionamiento y/o control suministradas con respecto a la interfaz del dispositivo. Una clave secreta puede usarse como una semilla para generar una secuencia seudoaleatoria que va a mezclarse con el resumen del mensaje. Alternativamente, el resumen del mensaje puede encriptarse con una clave secreta adecuada para generar la firma.

Alternativas de planificación para enviar firmas de datos al dispositivo informático incluyen: enviar de manera exhaustiva (es decir, tan pronto como se generan las firmas), periódicamente, previa solicitud, o según cualquier otro método de planificación, tal como combinar múltiples métodos de planificación para funcionar en paralelo. El dispositivo informático recibe datos y firmas respectivas del dispositivo de memoria y autentica los datos usando las firmas. De manera similar a las realizaciones que usan dispositivos de memoria externa no asegurados, los datos recibidos pueden almacenarse en una memoria caché antes de o en paralelo a su ejecución mediante el núcleo de procesamiento, y la reobtención de datos desde el dispositivo externo se produce tras una situación de error de memoria caché.

Descripción del sistema

La figura 1 es un diagrama de bloques que ilustra esquemáticamente un sistema 20 informático asegurado, según una realización de la presente invención. En el ejemplo de la figura 1, un dispositivo 24 informático asegurado se comunica con un dispositivo 26 externo asegurado y con un dispositivo 28 externo no asegurado. Cada uno de los dispositivos 26 y 28 comprende una memoria 32A o 32B respectiva que almacena datos en unidades básicas denominadas elementos de datos (que, alternativamente, pueden denominarse bloques de datos). Las firmas digitales que se calculan con respecto a los elementos de datos en el dispositivo 28 se almacenan en la memoria 32B. El dispositivo 26 asegurado puede almacenar de manera similar las firmas (no se muestra en la figura) calculadas con respecto a elementos de datos en la memoria 32A. Alternativa o adicionalmente, el dispositivo 26 puede generar firmas sobre la marcha con respecto a señales tales como señales de control, de dirección y/o de datos, que se comunican con el dispositivo 24 informático tal como se describe adicionalmente a continuación.

En la siguiente descripción y en las reivindicaciones, el término “elementos de datos” puede referirse a datos almacenados en un dispositivo de memoria (por ejemplo, el dispositivo 26 o 28) y/o a señales de datos, direccionamiento, y/o control que se comunican entre un dispositivo de memoria asegurado (por ejemplo, el dispositivo 26) y un dispositivo informático (por ejemplo, el dispositivo 24). Un elemento de datos almacenado puede comprender, por ejemplo, una instrucción de programa o información textual. Adicional o alternativamente, un elemento de datos almacenado puede comprender un grupo de instrucciones de programa y/o información textual.

El dispositivo 24 informático puede procesar elementos de datos enviados por el dispositivo 26 o 28 por medio de una interfaz 36A o 36B respectiva. El dispositivo 24 recibe las instrucciones por medio de un puente 44 de entrada y ejecuta el programa respectivo.

En algunas realizaciones, cada uno de los dispositivos 26 o 28 externos almacena uno o más elementos de datos y una o más firmas digitales en la memoria 36A o 36B respectiva. En algunas realizaciones, las firmas en el dispositivo 26 y 28 externo se calculan previamente y se almacenan. Las firmas pueden calcularse con respecto al conjunto completo de elementos de datos o con respecto a un subconjunto de los mismos. Por ejemplo, una firma puede calcularse para firmar un grupo de elementos de datos que comprenden una subrutina de un programa informático. Adicional o alternativamente, las firmas pueden calcularse con respecto a bloques de múltiples elementos de datos de un tamaño adecuado. En algunas realizaciones, todos los elementos de datos se firman usando una única clave.

En realizaciones alternativas, sin embargo, los subconjuntos de elementos de datos pueden firmarse usando diferentes claves.

Las claves para calcular las firmas pueden programarse o, de otro modo, almacenarse en el dispositivo 24 informático y/o en el dispositivo 26 externo asegurado mediante diversos medios que se conocen en la técnica, tal como (pero no limitados a) usar una memoria no volátil (NVM), NVM programable una sola vez (OTP), quema de fusibles eléctrica, o función física impredecible (PUF, también denominada función física inclonable). Adicionalmente, el dispositivo 26 externo asegurado puede emparejarse con el dispositivo 24 informático asegurado programando cada uno de los dispositivos 24 y 26 con una clave 42 compartida respectiva adecuada en un entorno seguro, o aplicando métodos de intercambio de clave tal como se conocen en la técnica.

El dispositivo 26 comprende, además, un motor 40 de firma que puede generar (sobre la marcha) una firma con respecto a instrucciones de programa, señales de direccionamiento, de control y/o de datos que pasan a través de la interfaz 36A al tiempo que se comunican con el dispositivo 24 asegurado. Alternativa o adicionalmente, el motor 40 de firma calcula una o más firmas con respecto a elementos de datos que se almacenan en la memoria 32A. Las firmas generadas mediante el motor 40 pueden almacenarse localmente en la memoria 32A y enviarse al dispositivo 24 informático previa solicitud o usando cualquier otro método de planificación adecuado.

En algunas realizaciones, parte de o todos los elementos de datos almacenados en los dispositivos 26 y 28 externos se encriptan. En tales realizaciones, el motor 40 de firma puede comprender, además, un cifrado de encriptado, y el dispositivo 24 puede comprender, además, un cifrado de desencriptado. El cifrado de desencriptado está dotado de una clave adecuada para desencriptar los elementos de datos encriptados antes de su ejecución por un núcleo 48 de procesamiento (descrito a continuación).

El puente 44 de entrada sirve como una interfaz de comunicación bidireccional con los dispositivos 26 y 28 externos y pasa los elementos de datos que recibe a un núcleo 48 de procesamiento. El núcleo 48 de procesamiento comprende, normalmente, la CPU principal del sistema 20 asegurado, posiblemente, procesadores adicionales, y control maestro de bus para coordinar la parte interna del núcleo y las actividades de I/O.

Un motor 56 de firma en el dispositivo 24 calcula las firmas con respecto a elementos de datos recibidos (y/u otras señales de datos, direccionamiento, y/o control) para validar la autenticidad de los elementos de datos. Cuando la validación falla, el dispositivo 24 toma las medidas adecuadas para impedir la filtración o exposición de información secreta. La estructura y funcionalidad del dispositivo 24 informático se describen a continuación en detalle con referencia a la figura 2.

En algunas realizaciones, antes de calcular una firma mediante el motor 56 o 40 de firma, los datos que van a firmarse se rellenan hasta una longitud que se ajusta a un tamaño de entrada adecuado tal como se especifica por el esquema de cálculo de firma en uso.

La figura 2 es un diagrama de bloques que muestra esquemáticamente detalles del sistema 20 informático asegurado, según una realización de la presente invención. En la figura 2, el dispositivo 24 informático asegurado se comunica con un dispositivo externo que está representado por un módulo denominado entradas 30 de sistema asegurado. Las entradas 30 de sistema asegurado pueden comprender, por ejemplo, el dispositivo 26 o 28 externo de la figura 1, un dispositivo de memoria, o cualquier otra fuente adecuada de elementos de datos y firmas respectivas. En la siguiente descripción, los términos “entradas de sistema asegurado” y “dispositivo externo” pueden usarse de manera intercambiable.

El dispositivo 24 genera señales de direccionamiento y de control que se enrutan por medio del puente 44 de entrada con el fin de acceder a los datos almacenados en la memoria del dispositivo externo. El núcleo 48 de procesamiento genera señales de direccionamiento y de control que se enrutan por medio del puente 44 de entrada para leer elementos de datos tales como instrucciones de programa procedentes del dispositivo externo. El puente 44 de entrada acepta y suministra los elementos de datos al núcleo 48 de procesamiento para su ejecución. En algunas realizaciones, los elementos de datos se incluyen en una memoria caché en una memoria 50 caché local antes de (o al mismo tiempo que) el suministro al núcleo de procesamiento.

Los elementos de datos recibidos también se introducen en la lógica 52 de control de autenticación y en el motor 56 de firma. La lógica 52 y el motor 56 pueden funcionar de manera simultánea y de manera asíncrona con respecto al núcleo 48. Adicionalmente, la lógica 52 de autenticación lee la firma original de los elementos de datos tal como se almacena o genera en el dispositivo externo, generando señales de direccionamiento y de control adecuadas que se enrutan por medio del puente 44 de entrada al dispositivo externo. Alternativamente, estas firmas pueden transportarse mediante las entradas 30 al puente 44 de entrada automáticamente junto con los datos. Al usar los elementos de datos recibidos y una clave respectiva, el motor 56 calcula una firma de los elementos de datos y envía la firma a la lógica 52 de autenticación para su validación. La lógica 52 de autenticación valida la autenticidad e integridad de los elementos de datos recibidos buscando una coincidencia entre la firma calculada por el motor 56 y la firma original. En algunas realizaciones, el motor 56 de firma calcula múltiples firmas (por ejemplo, firmas de múltiples elementos de datos en un bloque de datos) y almacena las firmas en una memoria 58 intermedia de firma. En tales realizaciones, la lógica 52 de autenticación puede validar todas las firmas pendientes en la memoria

intermedia antes de permitir que el puente 44 de entrada introduzca elementos de datos (o bloques) posteriores. Un método alternativo para validación de firma se describe adicionalmente a continuación.

Un puente 60 de salida conecta el núcleo 48 de procesamiento a salidas 64 de sistema asegurado, también denominadas canal de salida. Las salidas 64 de sistema asegurado incluyen cualquier espacio de direccionamiento al que una operación de lectura o escritura por el núcleo 48 de procesamiento puede exponer información asegurada, directa o indirectamente, así como cualquier otro tipo de receptor que puede recibir señales desde el puente 60 de salida. El dispositivo 24 puede configurar estáticamente el espacio de direccionamiento que corresponde con las salidas 64 de sistema asegurado. Adicional o alternativamente, el espacio de direccionamiento o partes del mismo pueden cambiar dinámicamente según variaciones en el estado y la configuración del sistema 20 asegurado.

En la siguiente descripción y en las reivindicaciones, un elemento de datos o un programa instrucción cuya ejecución dé como resultado la generación de una señal en el puente 60 de salida (que puede recibirse o enviarse mediante las salidas 64) se denomina instrucción de salida. En algunas realizaciones, el núcleo 48 de procesamiento señaliza a la lógica 52 de autenticación una señal de SOLICITUD DE SALIDA cuando se ejecuta una instrucción de salida. Simultáneamente, cuando se permite, la respuesta del puente 60 de salida a una instrucción de salida se denomina emitir una señal. Ejemplos de instrucciones de salida cuya ejecución puede exponer información asegurada a las salidas 64 del sistema asegurado incluyen:

• Escribir a una memoria no volátil (NVM), y/o a una memoria programable una sola vez (OTP) memoria.

• Escribir a una interfaz externa, tal como otro chip en el sistema, un dispositivo de memoria, o señales con fines generales de I/O (GPIO).

• Acceder a bits de bloqueo, modos de prueba, configuración de reloj, y registros de reseteo.

• Acceder a registros de control y/o de configuración de módulos de acelerador de seguridad (es decir, módulos que realizan funciones de seguridad tales como computar valores de AES, SHA1, SHA256, RSA, o ECC) que pueden exponer información y claves secretas a un atacante usando técnicas de ataque de canal lateral, tales como análisis de potencia o análisis de interferencia electromagnética (EMI).

El puente 44 de entrada sirve de árbitro entre la lógica 52 de control de autenticación y el núcleo 48 de procesamiento. Por defecto, el núcleo 48 de procesamiento obtiene una prioridad más elevada para obtener los elementos de datos del dispositivo (30) externo. Cuando se solicita, sin embargo (por ejemplo, cuando se encuentra en estado de autenticación tal como se muestra en la siguiente figura 3), la lógica 52 de autenticación puede detener al puente 44 de entrada para que deje de obtener elementos de datos, o bloques de elementos de datos posteriores, activando una señal de DETENCIÓN DE ENTRADA DE NÚCLEO, y tomar el control del puente 44 de entrada con el fin de leer firmas almacenadas o generadas externamente. En algunas realizaciones, se inhibe la entrada de bloques de datos posteriores hasta que todos los elementos de datos en bloques de datos anteriormente obtenidos se autentican. Adicionalmente, la lógica 52 de autenticación puede detener el puente 60 de salida y, por tanto, inhibir cualquier acceso a las salidas 64 aseguradas, activando una señal de DETENCIÓN DE SALIDAS. La funcionalidad del dispositivo 24, y específicamente el uso de estas funciones de “DETENCIÓN” para impedir la exposición de datos secretos, se describe adicionalmente con referencia a la siguiente figura 3.

Mientras que las técnicas de validación de firma descritas anteriormente comparan firmas computadas por el motor 56 de firma con firmas recibidas por medio del puente 44 de entrada, en realizaciones alternativas, la validación de firma puede realizarse basándose en la comparación del resumen condensado de los mensajes. En ocasiones, los algoritmos para calcular las firmas hacen uso de funciones de condensación y encriptado.

En una realización a modo de ejemplo, en la que el dispositivo 24 informático se comunica con el dispositivo 26 asegurado, una firma correspondiente a determinados datos comprende un resumen del mensaje calculado con respecto a esos datos usando una función de condensación. El resumen del mensaje puede calcularse con respecto a uno o más elementos de datos y/o señales de control, de dirección y/o de datos suministradas con respecto a la interfaz 36A. El resumen del mensaje puede calcularse sobre la marcha y actualizarse mediante ambos dispositivos 24 y 26. El dispositivo 26 externo asegurado puede programar y enviar las firmas de resumen del mensaje al dispositivo 24 informático asegurado de manera exhaustiva, periódica, o previa solicitud realizada por el dispositivo 24 informático asegurado. Tras la recepción de un resumen del mensaje actualizado, la lógica 52 de control de autenticación puede comparar el resumen del mensaje calculado por el dispositivo 26 con un resumen del mensaje calculado de manera interna con respecto a los datos recibidos por el motor 56 de firma y verificar la autenticidad de los datos firmados. La clave 42 secreta, que se comparte entre los dispositivos 24 y 26, puede usarse como una semilla para generar una secuencia seudoaleatoria que va a mezclarse con el resumen de los datos del mensaje.

En realizaciones alternativas, en lugar de mezclar el resumen del mensaje con una secuencia que depende de una clave secreta, un algoritmo de encriptado encripta el resumen del mensaje usando una clave secreta para generar la firma. El receptor (por ejemplo, el dispositivo 24 informático asegurado) recibe los datos y la firma y desencripta la firma usando una clave respectiva para cubrir el resumen sin encriptar original del mensaje, así como recalcula el propio resumen del mensaje con respecto al mensaje recibido. Si los resúmenes de los mensajes original y

recalculado coinciden, puede asumirse que los datos son auténticos. Ejemplos de funciones de encriptado y condensación incluyen, por ejemplo, el algoritmo de condensación seguro (SHA) SHA-1, y el algoritmo de encriptado avanzado (AES).

La configuración del dispositivo 24 informático y los dispositivos 26 y 28 externos en las figuras 1 y 2 es una configuración a modo de ejemplo, que se elige únicamente por motivos de claridad conceptual. En realizaciones alternativas, también puede usarse cualquier configuración adecuada. Los diferentes elementos del dispositivo 24 informático y los dispositivos 26 y 28 externos pueden implementarse usando cualquier hardware adecuado, tal como en un circuito integrado de aplicación específica (ASIC) o una matriz de puerta programable en el campo (FPGA). En algunas realizaciones, algunos elementos del dispositivo informático y los dispositivos externos pueden implementarse usando software, o usando una combinación de elementos de hardware y software. Por ejemplo, en la presente realización, el motor 56 de firma y la lógica 52 de autenticación pueden implementarse como módulos de hardware específicos. Como otro ejemplo, los cálculos de firma, así como las funciones de encriptado/desencriptado pueden implementarse en hardware dentro de motores 56 y 40 de firma, en software que va a ejecutarse mediante el núcleo 48 de procesamiento, o en una combinación de hardware y software.

Normalmente, el núcleo 48 de procesamiento en el dispositivo 24 informático comprende al menos un procesador informático de uso general, que se programa en software para llevar a cabo las funciones descritas en el presente documento. El software puede descargarse al dispositivo informático en formato electrónico, con respecto a una red, por ejemplo, o, alternativa o adicionalmente, puede proporcionarse y/o almacenarse en medios tangibles no transitorios, tales como memorias electrónicas, ópticas o magnéticas.

La figura 3 es un diagrama que muestra una máquina de estados de seguridad, según una realización de la presente invención. Algunos aspectos de seguridad y modos de funcionamiento del dispositivo 24 se derivan de los tres estados de la máquina de estados y reglas de transición definidas entre los estados. En un estado 80 asegurado, un elemento de datos o instrucción que se ejecuta en ese momento, así como todos los elementos de datos ejecutados anteriormente recibidos por medio del puente 44 de entrada, ya se han validado como auténticos por la lógica 52 de autenticación. El estado 80 asegurado es el único estado (de los tres estados) en el que se permite que el dispositivo 24 acceda a las salidas 64 de sistema asegurado. Al tiempo que en el estado 80, también se permite que el dispositivo 24 reciba elementos de datos por medio del puente 44 de entrada. Tras recibir los elementos de datos, la máquina de estados cambia a un estado 84 no asegurado.

Mientras que en el estado 84 no asegurado, la autenticidad de al menos parte de cualquier elemento de datos recibido nuevo todavía no se ha validado, y no se permite que el dispositivo 24 acceda a las salidas 64 de sistema asegurado. En caso de que el núcleo 48 de procesamiento reciba una instrucción de salida, el acceso real al canal de salida se retrasa (es decir, la emisión de la señal por el puente 60 de salida se retrasa) hasta que la instrucción de salida se autentica. Mientras que en el estado 84 no asegurado, sin embargo, el núcleo 48 de procesamiento puede continuar procesando elementos de datos neutros que no solicitan el acceso a las salidas 64 de sistema asegurado, incluso si estos elementos de datos neutros todavía no se han autenticado.

La transición del estado 84 no asegurado a un estado 88 de autenticación se produce después de que la lógica 52 de autenticación reciba una señal de SOLICITUD DE AUTENTICACIÓN. Cuando se encuentra en el estado 88 de autenticación, la lógica 52 de autenticación impide que el puente 44 de entrada reciba elementos de datos y tome el control del puente de entrada para leer las firmas originales procedentes del dispositivo (30) externo. La lógica 52 de autenticación compara las firmas originales con las firmas calculadas mediante el motor 56 de firma para autenticar los datos. Tal como se comentó anteriormente, la lógica 52 de autenticación puede autenticar de manera asíncrona los elementos de datos mientras que el núcleo 48 de procesamiento está ejecutando (posiblemente otros) elementos de datos.

Diversos activadores pueden generar una señal de SOLICITUD DE AUTENTICACIÓN que haga que la máquina de estados cambie al estado 88 de autenticación. Algunos activadores a modo de ejemplo se proporcionan a continuación en el presente documento:

• Activación de la señal de SOLICITUD DE SALIDA cuando el núcleo 48 de procesamiento intenta obtener acceso a las salidas 64 de sistema asegurado y el dispositivo no se encuentra en un estado 80 asegurado.

• Activación de la señal de SOLICITUD DE SALIDA periódicamente, o después de un tiempo inactivo predefinido desde que se visitó por última vez el estado 88 de autenticación.

• Cuando un espacio de memoria ubicado para las firmas pendientes de verificación se llena. Una realización a modo de ejemplo con una memoria no asegurada, que verifica múltiples firmas pendientes, se describe adicionalmente a continuación.

• Cuando el puente 44 de entrada no está ocupado por elementos de datos de suministro, y, por tanto, la lógica 52 de autenticación puede recuperar las firmas almacenadas en entradas 30 de sistema de entrada aseguradas por medio del puente de entrada.

Cuando los elementos de datos se validan como auténticos en el estado 88, la máquina de estados cambia de

nuevo al estado 80 asegurado. De otro modo, la autenticación ha fallado y la lógica 52 de autenticación genera una señal de alerta.

El dispositivo 24 puede tomar diversas mediciones en respuesta a una señal de alerta con el fin de mantener un alto nivel de seguridad. Acciones a modo de ejemplo que puede realizar el dispositivo 24 en respuesta a una señal de alerta incluyen:

• Resetear el entorno seguro.

• Borrar datos secretos tales como claves secretas.

• Forzar el dispositivo 24 para que finalice de manera permanente todas las operaciones, tales como procesado/autenticación de elementos de datos, y detener, adicionalmente, los puentes de entrada y salida.

• El nivel de respuesta puede depender del número de situaciones de fallo de autenticación. Por ejemplo, el dispositivo 24 asegurado puede reiniciar el funcionamiento tras reconocer un número predefinido de situaciones de fallo de autenticación, y responder de manera más agresiva, por ejemplo, retrasando información asegurada o finalizando todas las actividades si se produce un fallo de autenticación adicional.

Ahora va a describirse una realización a modo de ejemplo del sistema 20 asegurado, en la que el dispositivo externo comprende un dispositivo 28 de memoria no asegurado, tal como un dispositivo de almacenamiento no volátil comercialmente disponible. En el presente ejemplo, el dispositivo de memoria almacena elementos de datos que comprenden instrucciones de programa informático (y posiblemente datos relacionados), que van a ejecutarse por el dispositivo 24 informático asegurado. El dispositivo 28 puede ubicar cualquier acto para compartir adecuado de la capacidad de almacenamiento para almacenar firmas. Por ejemplo, el 75% de la capacidad de almacenamiento puede usarse para usar datos y el 25% para almacenar firmas. Las firmas pueden calcularse (fuera del dispositivo de memoria) con respecto a bloques de elementos de datos. Por ejemplo, cada bloque de memoria de 256-bit puede firmarse con una firma de 64-bit.

En este ejemplo se asume que el dispositivo 24 asegurado está equipado con una memoria 50 caché que tiene un tamaño de línea de memoria caché de 256 bits. Los elementos de datos leídos por medio del puente 44 de entrada se almacenan en la memoria caché antes o en paralelo a su suministro para su procesamiento por el núcleo 48 de procesamiento. En una situación de error de memoria caché, el dispositivo 24 informático obtiene nuevos elementos de datos en la memoria caché. La ejecución de las instrucciones de programa mediante el núcleo 48 de procesamiento y el cálculo de firmas por el motor 56 de firma para cada bloque de 256-bit puede llevarse a cabo simultáneamente. El dispositivo 24 puede almacenar múltiples firmas calculadas en la memoria 58 intermedia de firma, permitiendo, por tanto, la obtención de múltiples datos antes de realizar en realidad la verificación de autenticidad. Tras la SOLICITUD DE AUTENTICACIÓN, el núcleo 48 de procesamiento se detiene y la lógica 52 de autenticación lee las firmas originales respectivas de la memoria 28 externa y compara las firmas original con respecto a la calculada. Tras la verificación de todas las firmas calculadas pendientes, el núcleo 48 de procesamiento reanuda la ejecución.

La configuración de la realización anteriormente descrita es una configuración a modo de ejemplo, y, alternativamente, puede usarse cualquier otra configuración de elementos de entrada y memoria adecuada. Por ejemplo, también pueden aplicarse otros tamaños de bloques de datos y tamaños de firma. Como otro ejemplo, también puede usarse cualquier tamaño de memoria intermedia de firma adecuado. En una realización a modo de ejemplo, las firmas de 32-bit se calculan con respecto a bloques de datos de 128-bit. Los bloques de datos se incluyen en la memoria caché en una memoria caché que tiene una línea de memoria caché de 128-bit, y pueden almacenarse hasta cinco firmas no validadas en una memoria intermedia de firma de 160-bit.

La configuración de la máquina de estados descrita con referencia a la figura 3 es una configuración a modo de ejemplo que el inventor ha encontrado que resulta adecuada para su implementación. En realizaciones alternativas, pueden usarse cualquier otro número adecuado de estados y cualquier regla de transición adecuada entre los estados.

La figura 4 es un diagrama de flujo que ilustra esquemáticamente un método para la autenticación que puede implementarse en el dispositivo 24 informático asegurado, según una realización de la presente invención. El método comienza con el dispositivo 24 recibiendo instrucciones de programa informático para su ejecución por el núcleo 48 de procesamiento en una etapa 100 de recepción de código. Tras recibir las instrucciones por medio del puente 44 de entrada, el dispositivo 24 cambia al estado 84 no asegurado. El dispositivo 24 comprueba si existe una solicitud de autenticación pendiente en una etapa 104 de comprobación de solicitud. Si en la etapa 104 no se requiere autenticación, el núcleo 48 de procesamiento ejecuta las instrucciones de programa recibidas en una etapa 108 de ejecución. De otro modo, el dispositivo 24 avanza a una etapa 116 de autenticación (descrita a continuación).

Al tiempo que se lleva a cabo la ejecución de instrucciones, el dispositivo 24 comprueba si el núcleo 48 de procesamiento está ejecutando en ese momento una instrucción neutra o una instrucción que requiere el acceso a las salidas 64 de sistema asegurado, en una etapa 112 de comprobación de instrucción. Siempre y cuando el núcleo 48 de procesamiento esté ejecutando una instrucción neutra, el dispositivo 24 vuelve de nuevo a la etapa 104. De

otro modo, puede concluirse que el núcleo 48 de procesamiento está intentando obtener acceso a las salidas 64 de sistema asegurado ejecutando una instrucción de salida, que todavía no se ha autenticado. Por tanto, el dispositivo 24 avanza a la etapa 116 de autenticación, en la que el dispositivo 24 cambia al estado 88 de autenticación. En este estado, la lógica 52 de control de autenticación detiene la ejecución del núcleo 48 de procesamiento, inhibe el puente 60 de salida activando una señal de DETENCIÓN DE SALIDA, y realiza la validación de autenticación comparando las firmas originales con las calculadas tal como se describió anteriormente.

En una etapa 120 de verificación de autenticación, el dispositivo 24 comprueba si se encontró una coincidencia de firma en la etapa 116. Si las firmas coinciden, el dispositivo 24 cambia al estado 80 asegurado, en una etapa 124 de transición de estado asegurado, y núcleo 48 de procesamiento reanuda la ejecución. Cuando se encuentra en el estado 80 asegurado, se permite que el dispositivo 24 obtenga instrucciones de programa procedentes de la memoria externa, y que acceda de manera segura a las salidas 64 de sistema asegurado. Si la autenticación en la etapa 120 falla, la lógica 52 de autenticación genera una señal de alerta, en una etapa 132 de alerta, y vuelve a la etapa 100 para obtener instrucciones de programa adicionales. El dispositivo 24 puede responder a la señal de alerta de diversas formas, tal como se describió anteriormente.

El dispositivo 24 comprueba si la ejecución de todas las instrucciones obtenidas se ha realizado, en una etapa 128 de comprobación de ejecución. Si se ha realizado la ejecución, el dispositivo 24 vuelve a la etapa 100 para obtener instrucciones de programa posteriores. De otro modo, el dispositivo 24 vuelve a la etapa 104 para comprobar si existe una solicitud de autenticación pendiente.

En el presente documento, el método de la figura 4 se muestra y describe a modo de ejemplo, y métodos alternativos para lograr los fines de este método también se encuentran dentro del alcance de la presente invención. Por ejemplo, en lugar de detener el núcleo de procesamiento en la etapa 116, el núcleo puede continuar ejecutando instrucciones neutras y/o retrasar el acceso real a las salidas 64 de sistema asegurado hasta que la instrucción de salida se haya autenticado.

Aunque las realizaciones descritas en el presente documento se refieren, principalmente, a la autenticación de datos leídos desde la memoria, los métodos y sistemas descritos en el presente documento también pueden usarse en otras aplicaciones en las que va a protegerse un dispositivo informático frente a una salida no autorizada de información sensible.

Se apreciará que las realizaciones descritas anteriormente se enumeran a modo de ejemplo, y que la presente invención no se limita a lo que se ha mostrado y descrito de manera particular anteriormente en el presente documento. En su lugar, el alcance de la presente invención incluye tanto las combinaciones como las subcombinaciones de las diversas características descritas anteriormente en el presente documento, así como las variaciones y modificaciones de las mismas que resultaran evidentes para los expertos en la técnica tras la lectura de la descripción anterior y que no se dan a conocer en la técnica anterior.

REIVINDICACIONES

1. Dispositivo (24) informático, que comprende:

un puente (44) de entrada, que se acopla para recibir una secuencia de elementos de datos para su uso mediante el dispositivo al ejecutar un programa;

un puente de salida;

un núcleo (48) de procesamiento, que se acopla para recibir los elementos de datos procedentes del puente de entrada y ejecutar el programa para provocar que el puente de salida emita una señal en respuesta a un elemento de datos dado en la secuencia;

caracterizado por una lógica (52) de autenticación, que se acopla para recibir y autenticar los elementos de datos al tiempo que el núcleo de procesamiento ejecuta el programa, y para inhibir la emisión de la señal mediante el puente de salida hasta que el elemento de datos dado se haya autenticado.

2. Dispositivo según la reivindicación 1, en el que los elementos de datos comprenden instrucciones de programa y el elemento de datos dado comprende una instrucción de salida, y en el que el núcleo de procesamiento está configurado para ejecutar el programa ejecutando las instrucciones de programa, incluyendo la instrucción de salida.

3. Dispositivo según la reivindicación 1 o 2, en el que la lógica de autenticación está configurada para autenticar los elementos de datos de manera asíncrona con la ejecución del programa mediante el núcleo de procesamiento, y/o en el que la lógica de autenticación está configurada para autenticar el elemento de datos dado después de haber usado el elemento de datos dado en la ejecución del programa mediante el núcleo de procesamiento, y para retrasar la salida de la señal mediante el puente de salida hasta que la autenticación del elemento de datos dado se haya completado, y/o en el que la lógica de autenticación está configurada para autenticar los elementos de datos calculando una o más firmas digitales de los elementos de datos y comparando las firmas calculadas con firmas originales respectivas recibidas por el dispositivo por medio del puente de entrada, y/o en el que la lógica de autenticación está configurada para generar una señal de alerta si al menos una de las firmas calculadas no coincide con la firma original respectiva.

4. Dispositivo según la reivindicación 3, en el que el puente de entrada está configurado para recibir los elementos de datos recibiendo bloques de elementos de datos primero y segundo, en el que la recepción del segundo bloque se permite solo tras la autenticación de todos los elementos de datos del primer bloque usando la lógica de autenticación.

5. Método, que comprende:

recibir en un dispositivo informático por medio de un puente de entrada una secuencia de elementos de datos para su uso en la ejecución de un programa mediante un núcleo de procesamiento del dispositivo;

ejecutar el programa mediante el núcleo de procesamiento para provocar la emisión de una señal del dispositivo en respuesta a un elemento de datos dado en la secuencia;

caracterizado por autenticar los elementos de datos usando la lógica de autenticación al tiempo que el núcleo de procesamiento ejecuta el programa, e inhibir la salida de la señal hasta que el elemento de datos dado se haya autenticado.

6. Método según la reivindicación 5, en el que los elementos de datos comprenden instrucciones de programa, y el elemento de datos dado comprende una instrucción de salida, y en el que ejecutar el programa comprende ejecutar las instrucciones de programa, incluyendo la instrucción de salida.

7. Método según la reivindicación 5 o 6, en el que autenticar los elementos de datos comprende autenticar los elementos de datos de manera asíncrona con la ejecución del programa mediante el núcleo de procesamiento, y/o en el que autenticar los elementos de datos comprende autenticar el elemento de datos dado tras haber usado el elemento de datos dado en la ejecución del programa mediante el núcleo de procesamiento, y retrasar las salida de la señal hasta que la autenticación del elemento de datos dado se haya completado, y/o en el que autenticar los elementos de datos comprende calcular una o más firmas digitales de los elementos de datos y comparar las firmas calculadas con firmas originales respectivas recibidas por el dispositivo por medio del puente de entrada, y/o en el que autenticar los elementos de datos comprende generar una señal de alerta si al menos una de las firmas calculadas no coincide con la firma original respectiva.

8. Método según la reivindicación 7, en el que recibir la secuencia de elementos de datos comprende recibir bloques de elementos de datos primero y segundo, en el que la recepción del segundo bloque se permite solo tras autenticar todos los elementos de datos del primer bloque usando la lógica de autenticación.

9. Sistema informático, que comprende:

un dispositivo (28) externo, que está configurado para proporcionar una secuencia de elementos de datos; y

un dispositivo (24) informático según una o más de las reivindicaciones 1 a 4 que comprende:

un puente (44) de entrada, que está acoplado para recibir desde el dispositivo externo la secuencia de elementos de datos para su uso mediante el dispositivo informático al ejecutar un programa;

un puente de salida;

un núcleo (48) de procesamiento, que se acopla para recibir los elementos de datos del puente de entrada y ejecutar el programa para provocar que el puente de salida emita una señal en respuesta a un elemento de datos dado en la secuencia;

caracterizado por una lógica (52) de autenticación, que se acopla para recibir y autenticar los elementos de datos al tiempo que el núcleo de procesamiento ejecuta el programa, y para inhibir la salida de la señal mediante el puente de salida hasta que el elemento de datos dado se haya autenticado.

10. Sistema según la reivindicación 9, en el que el dispositivo externo comprende a dispositivo de memoria que está configurado para almacenar los elementos de datos y la información de autenticación, y en el que el dispositivo informático comprende, además, un motor de firma que está configurado para generar al menos parte de la información de autenticación.

11. Sistema según la reivindicación 9 o 10, en el que el dispositivo externo comprende un dispositivo de memoria asegurado que está configurado para generar al menos parte de la información de autenticación.

12. Sistema según la reivindicación 11, en el que el dispositivo de memoria asegurado está configurado para generar información de autenticación sobre la marcha con respecto a al menos algunos de los elementos de datos que se comunican mediante el dispositivo de memoria asegurado al dispositivo informático, y en el que la lógica de autenticación está configurada para autenticar los elementos de datos usando la información de autenticación.

13. Sistema según la reivindicación 11 o 12, en el que el dispositivo de memoria asegurado comprende una memoria no volátil.

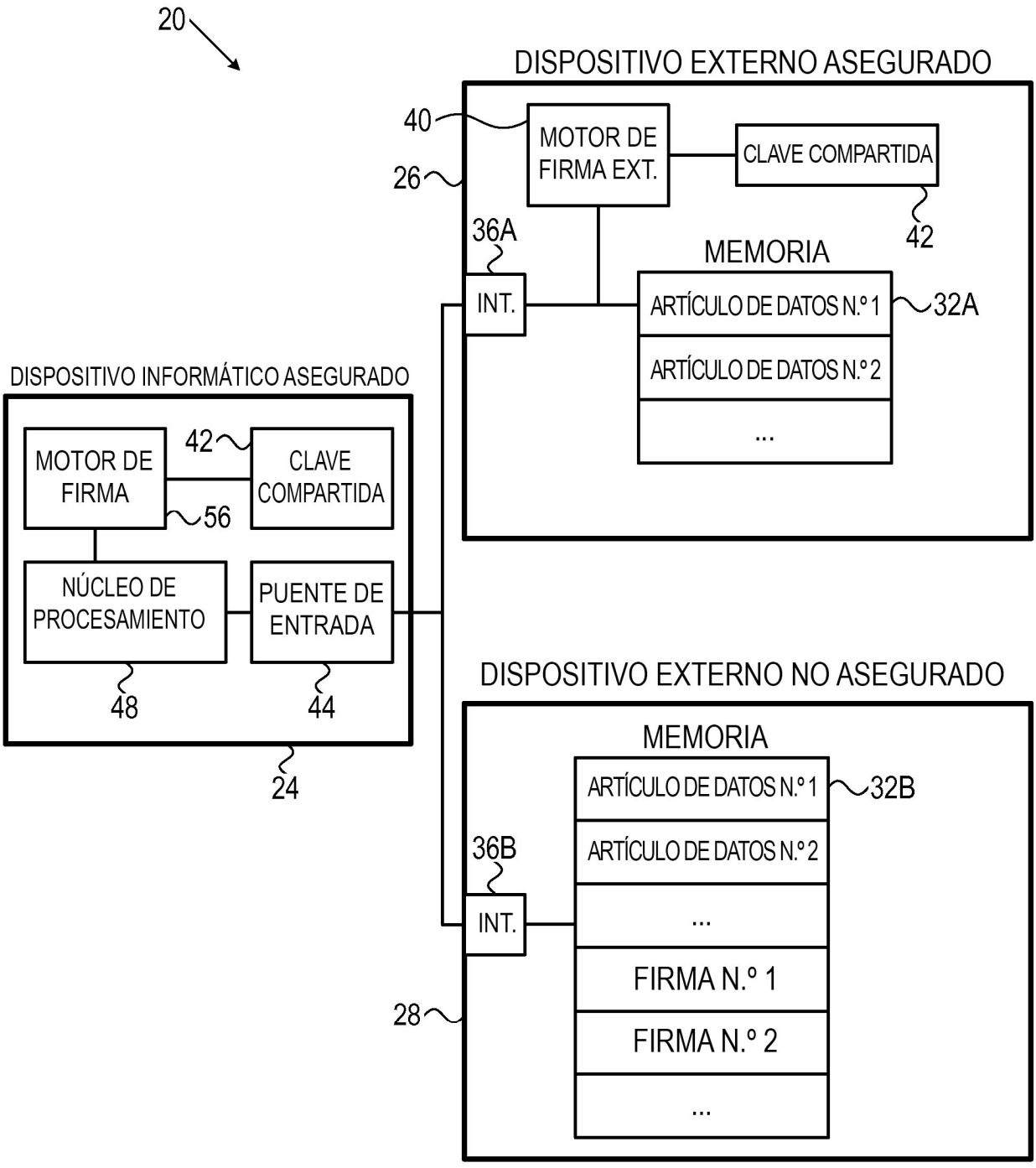
20
DISPOSITIVO EXTERNO ASEGURADO
40
MOTOR DE FIRMA EXT.
CLAVE COMPARTIDA
42
26
36A
MEMORIA
INT.
ARTÍCULO DE DATOS N.º 1
32A
ARTÍCULO DE DATOS N.º 2
...
DISPOSITIVO INFORMÁTICO ASEGURADO
MOTOR DE FIRMA
42
CLAVE COMPARTIDA
56
NÚCLEO DE PROCESAMIENTO
PUENTE DE ENTRADA
48
44
24
DISPOSITIVO EXTERNO NO ASEGURADO
MEMORIA
ARTÍCULO DE DATOS N.º 1
32B
36B
ARTÍCULO DE DATOS N.º 2
INT.
...
FIRMA N.º 1
28
FIRMA N.º 2
...

FIG. 1

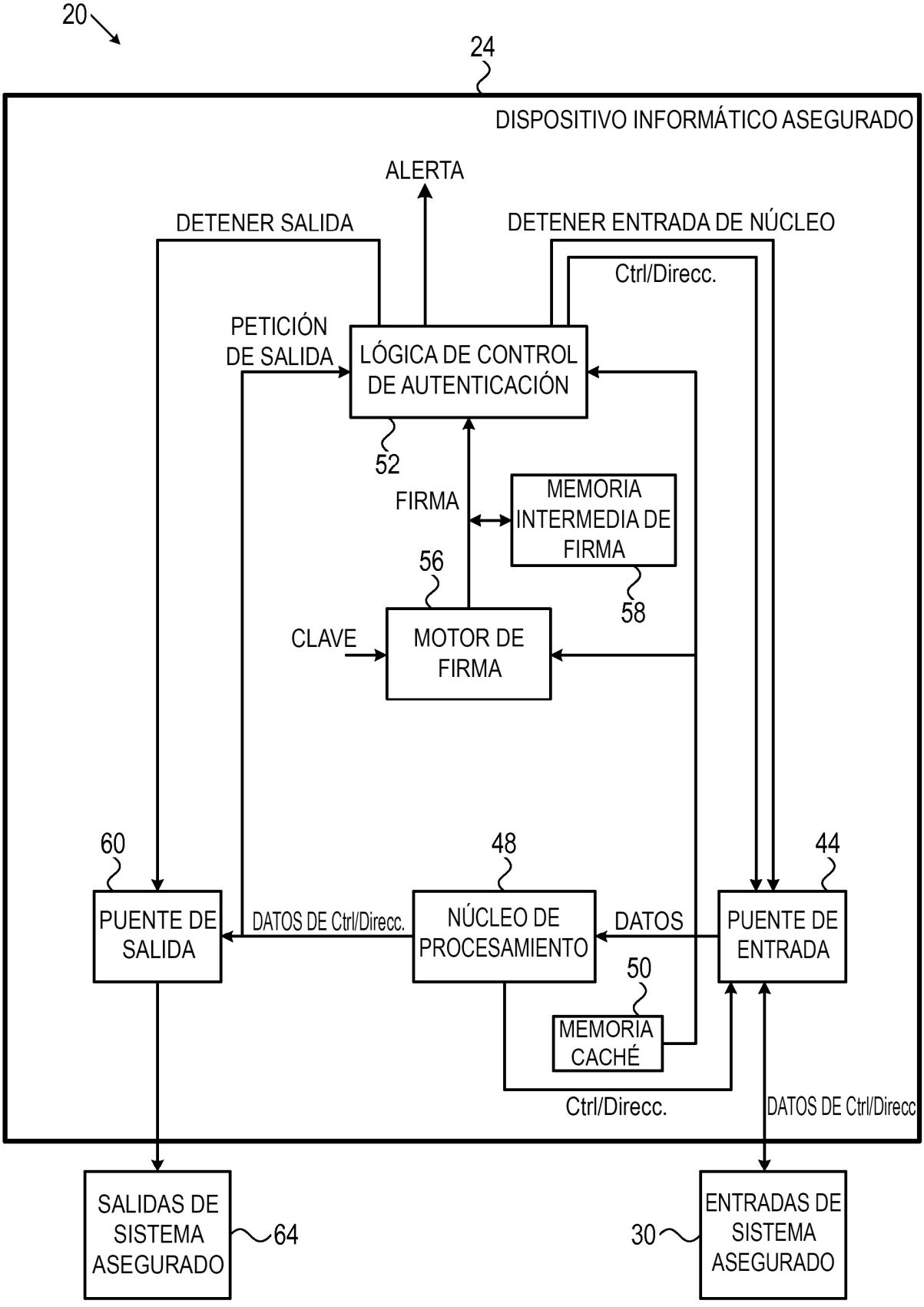
20
24
DISPOSITIVO INFORMÁTICO ASEGURADO
ALERTA
DETENER SALIDA
DETENER ENTRADA DE NÚCLEO
Ctrl/Direcc.
PETICIÓN DE SALIDA
LÓGICA DE CONTROL DE AUTENTICACIÓN
52
FIRMA
MEMORIA INTERMEDIA DE FIRMA
58
56
CLAVE
MOTOR DE FIRMA
60
48
44
PUENTE DE SALIDA
DATOS DE Ctrl/Direcc.
NÚCLEO DE PROCESAMIENTO
DATOS
PUENTE DE ENTRADA
50
MEMORIA CACHÉ
Ctrl/Direcc.
DATOS DE Ctrl/Direcc
SALIDAS DE SISTEMA ASEGURADO
64
30
ENTRADAS DE SISTEMA ASEGURADO

FIG. 2

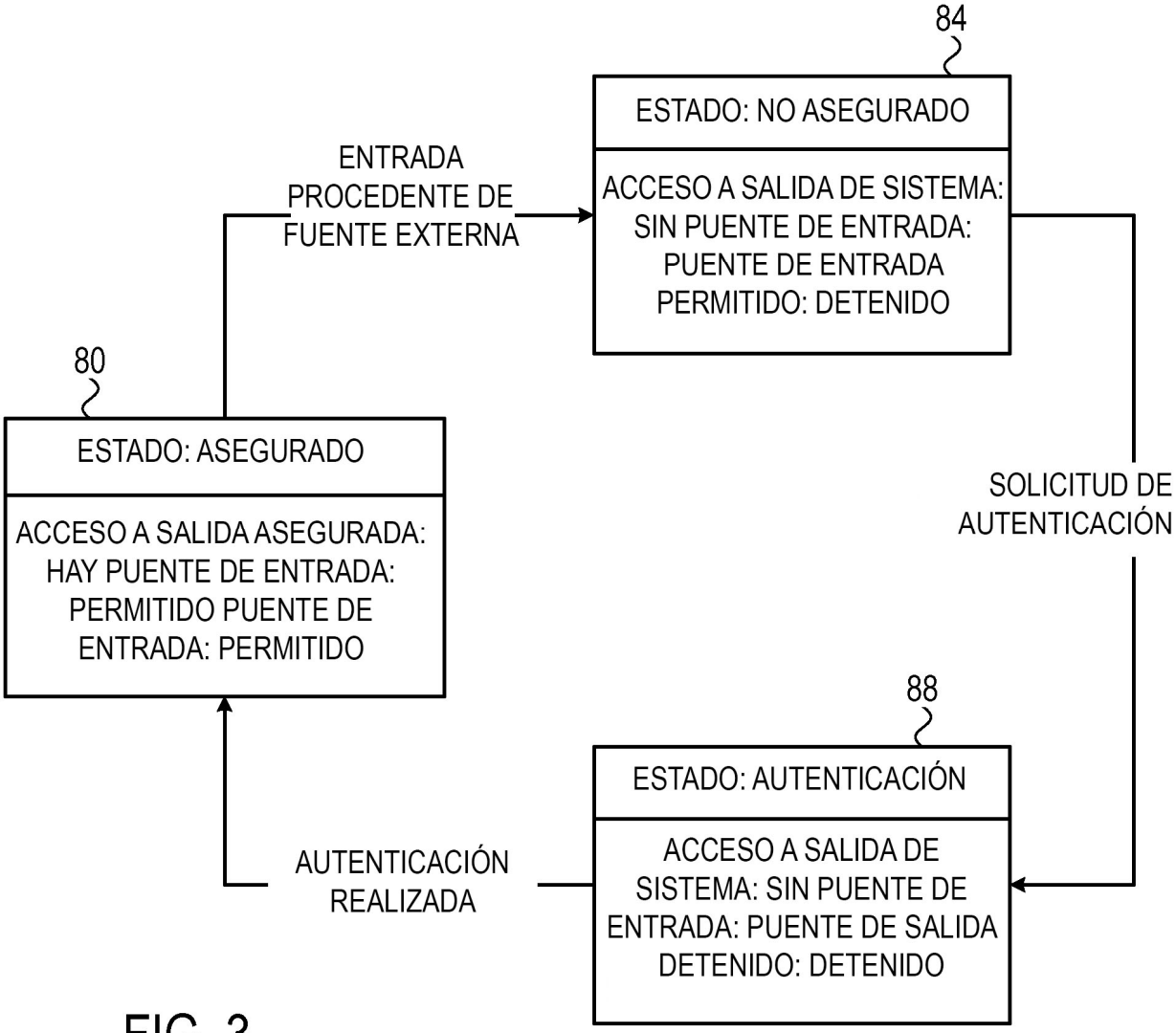
84
ESTADO: NO ASEGURADO
ACCESO A SALIDA DE SISTEMA: SIN PUENTE DE ENTRADA: PUENTE DE ENTRADA PERMITIDO: DETENIDO
ENTRADA PROCEDENTE DE FUENTE EXTERNA
80
ESTADO: ASEGURADO
ACCESO A SALIDA ASEGURADA: HAY PUENTE DE ENTRADA: PERMITIDO PUENTE DE ENTRADA: PERMITIDO
SOLICITUD DE AUTENTICACIÓN
88
ESTADO: AUTENTICACIÓN
ACCESO A SALIDA DE SISTEMA: SIN PUENTE DE ENTRADA: PUENTE DE SALIDA DETENIDO: DETENIDO
AUTENTICACIÓN REALIZADA

FIG. 3

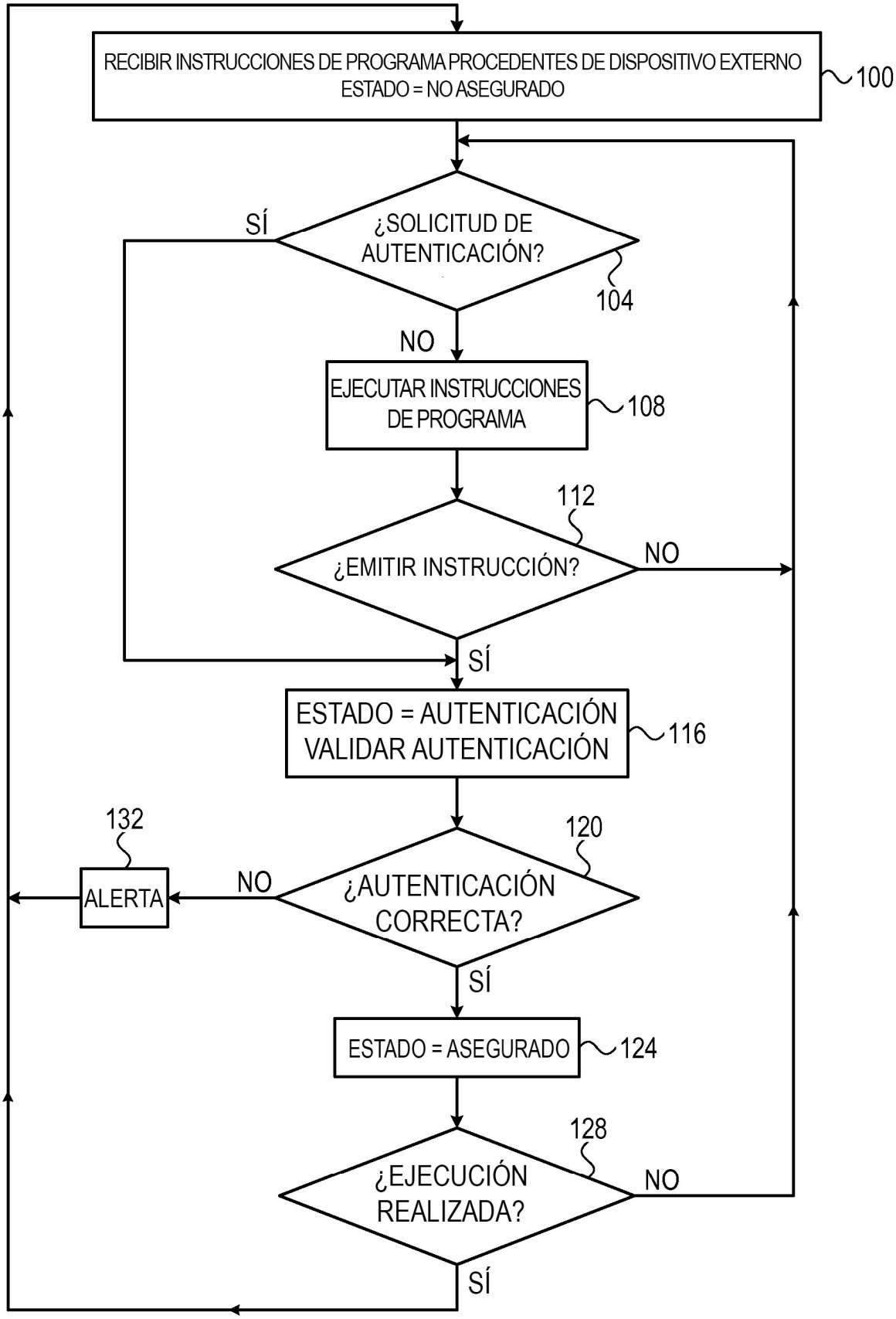
RECIBIR INSTRUCCIONES DE PROGRAMA PROCEDENTES DE DISPOSITIVO EXTERNO
ESTADO = NO ASEGURADO
100
¿SOLICITUD DE AUTENTICACIÓN?
SÍ
104
NO
EJECUTAR INSTRUCCIONES DE PROGRAMA
108
112
¿EMITIR INSTRUCCIÓN?
NO
SÍ
ESTADO = AUTENTICACIÓN
VALIDAR AUTENTICACIÓN
116
132
120
ALERTA
NO
¿AUTENTICACIÓN CORRECTA?
SÍ
ESTADO = ASEGURADO
124
128
¿EJECUCIÓN REALIZADA?
NO
SÍ

FIG. 4