(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 802 265**

(51) Int. CI.:

G06F 21/33 (2013.01)
G06F 21/30 (2013.01)
H04L 29/06 (2006.01)
H04L 9/08 (2006.01)
H04L 9/32 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **01.07.2014 PCT/US2014/045022**

(87) Fecha y número de publicación internacional: **19.03.2015 WO15038220**

(96) Fecha de presentación y número de la solicitud europea: **01.07.2014 E 14748330 (9)**

(97) Fecha y número de publicación de la concesión europea: **29.04.2020 EP 3039604**

(54) Título: **Método de autorización de una operación que va a realizarse en un dispositivo informático objetivo**

(30) Prioridad:

12.09.2013 US 201314025560

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
18.01.2021

(73) Titular/es:

THE BOEING COMPANY (100.0%)
100 North Riverside Plaza
Chicago, IL 60606-2016, US

(72) Inventor/es:

STERN, ALLON J.

(74) Agente/Representante:

CARVAJAL Y URQUIJO, Isabel

DESCRIPCIÓN

Método de autorización de una operación que va a realizarse en un dispositivo informático objetivo

Antecedentes

El campo de la presente divulgación se refiere, generalmente, a dispositivos de comunicación móviles y, más específicamente, a un dispositivo de comunicación móvil que permite el funcionamiento seguro de uno o más sistemas operativos virtualizados, aislados que se ejecutan en el mismo.

Los dispositivos de comunicación móviles, tales como teléfonos inteligentes, teléfonos celulares, y asistentes digitales personales (PDA) han incrementado su uso y popularidad entre una variedad de diferentes tipos de usuarios. Al menos algunos dispositivos conocidos incluyen una unidad de procesamiento central (CPU) que puede virtualizarse para ejecutar, de manera simultánea, múltiples sistemas operativos (OS) en un dispositivo. Por ejemplo, puede usarse un programa de software conocido como un hipervisor para separar los diferentes OS gestionando operaciones de acceso de entrada/salida (I/O) transmitidas entre los OS y dispositivos de hardware incluidos en el sistema informático. Más específicamente, el hipervisor facilita la separación de hardware subyacente, tal como la CPU y los periféricos asociados (por ejemplo, dispositivos de visualización, pantallas táctiles, e interfaces de comunicación), de los OS que se ejecutan en el hardware.

Aunque la virtualización del dispositivo puede facilitar la separación de un conjunto de software de otro conjunto de software en los dispositivos informáticos conocidos, la plataforma subyacente puede ser susceptible de experimentar una variedad de vulnerabilidades de seguridad. Debido a esto, cada vez resulta más importante para aquellos en el sector informático aumentar la seguridad de los dispositivos informáticos conocidos. Como tal, puede resultar deseable incorporar un aumento de seguridad en una arquitectura de virtualización del dispositivo.

En la publicación de solicitud de patente estadounidense US 2010/106963 A1, se describe un sistema que incluye una autorización de terceros en comunicación con un ordenador de cliente y un ordenador objetivo. La autorización de terceros está configurada para recibir una solicitud que incluye información de autenticación y una solicitud de acceso procedentes del ordenador de cliente. La autorización de terceros está configurada para autenticar el ordenador de cliente basándose en la información de autenticación y para procesar la solicitud de acceso para otorgar al ordenador de cliente acceso al ordenador objetivo para realizar una tarea en el ordenador objetivo, incluyendo la solicitud de acceso la tarea. La autorización de terceros está configurada, además, para enviar un token de acceso al ordenador de cliente para acceder al ordenador objetivo para realizar la tarea, para recibir el token de acceso del ordenador objetivo para su validación, para validar el token de acceso recibido basándose en la solicitud para que el ordenador objetivo procese la tarea, y para otorgar al ordenador objetivo el permiso para procesar la tarea tras su validación.

En la patente estadounidense US 7 809 953 B2, se describe un sistema y un método de distribución de información de autenticación para acceder de manera remota a una fuente informática. Una solicitud de información de autenticación, que incluye información de identidad, se recibe procedente de un usuario de un dispositivo remoto. Cuando el usuario se autentica basándose en la información de identidad, la información de autenticación solicitada se obtiene y se devuelve al dispositivo remoto. La información de autenticación, o la información generada a partir de la información de autenticación, se usa, entonces, para acceder de manera remota a la fuente informática.

Breve descripción

Se describe un método de autorización de una operación que va a realizarse en un dispositivo informático objetivo, comprendiendo dicho método: generar, en un dispositivo de solicitud, una solicitud para realizar una operación en el dispositivo informático objetivo; firmar, en el dispositivo de solicitud, la solicitud con una clave privada de un primer par de claves pública, privada; transmitir la solicitud desde el dispositivo de solicitud hasta un servidor de autenticación; recibir la solicitud en el servidor de autenticación desde el dispositivo de solicitud para realizar una operación en el dispositivo informático objetivo; verificar, en el servidor de autenticación, la solicitud con una clave pública del primer par de claves pública, privada; formar, en el servidor de autenticación, una respuesta de autorización que incluye la solicitud y un token de autorización; firmar, mediante el servidor de autenticación, la respuesta de autorización con una clave privada de un segundo par de claves pública, privada; transmitir la respuesta de autorización desde el servidor de autenticación hasta el dispositivo de solicitud; recibir, en el dispositivo de solicitud, la respuesta de autorización procedente del servidor de autenticación que incluye la solicitud y el token de autorización; verificar, en el dispositivo de solicitud, la respuesta de autorización con una clave pública del segundo par de claves pública, privada; firmar, mediante el dispositivo de solicitud, la respuesta de autorización con la clave privada del primer par de claves pública, privada; transmitir, mediante el dispositivo de solicitud, la respuesta de autorización al dispositivo informático objetivo; recibir mediante el dispositivo informático objetivo, la respuesta de autorización procedente del dispositivo de solicitud, incluyendo la respuesta de autorización la solicitud para realizar una operación en el dispositivo informático objetivo y el token de autorización; verificar, mediante el dispositivo informático objetivo, la respuesta de autorización con la clave pública del primer par de claves pública, privada; y otorgar, mediante el dispositivo informático objetivo, autorización para realizar la operación tras la verificación de la respuesta de autorización.

Breve descripción de los dibujos

La figura 1 es una vista en perspectiva frontal de un dispositivo de comunicación móvil a modo de ejemplo.

La figura 2 vista en perspectiva trasera del dispositivo de comunicación móvil mostrado en la figura 1.

La figura 3 es una ilustración esquemática de una arquitectura de hardware a modo de ejemplo que puede usarse con el dispositivo de comunicación móvil mostrado en la figura 1.

La figura 4 es una ilustración esquemática de una arquitectura de software a modo de ejemplo que puede usarse con el dispositivo de comunicación móvil mostrado en la figura 1.

La figura 5 es un diagrama de flujo de un método a modo de ejemplo de reivindicar la titularidad de una persona que puede usarse con el dispositivo de comunicación móvil mostrado en la figura 1.

La figura 6 es una ilustración esquemática de un sistema a modo de ejemplo para su uso en la autorización de una operación que va a realizarse en el dispositivo de comunicación móvil mostrado en la figura 1.

La figura 7 es un diagrama de flujo de un método a modo de ejemplo de actualizar software personal que puede usarse con el dispositivo de comunicación móvil mostrado en la figura 1.

La figura 8 es un diagrama de flujo de un método a modo de ejemplo de cambiar la titularidad de una persona que puede usarse con el dispositivo de comunicación móvil mostrado en la figura 1.

La figura 9 es un diagrama de flujo de un método a modo de ejemplo de cargar una nueva persona que puede usarse con el dispositivo de comunicación móvil mostrado en la figura 1.

Descripción detallada

Los sistemas y métodos descritos en el presente documento pueden usarse para hacer funcionar un dispositivo de comunicación móvil. En la implementación a modo de ejemplo, el dispositivo de comunicación móvil se gestiona mediante una arquitectura de software y de hardware que usa criptografía, tal como criptografía basada en claves privada y pública, para facilitar que los sistemas operativos de seguridad se ejecuten en el mismo. Más específicamente, el dispositivo de comunicación móvil soporta múltiples sistemas operativos virtualizados que se ejecutan simultáneamente en el dispositivo y teniendo cada uno raíces de confianza independientes. Como tales, el acceso de los sistemas operativos virtualizados al hardware en el dispositivo se ve reforzado mediante políticas de seguridad predeterminadas para permitir un funcionamiento fiable del dispositivo.

Las figuras 1 y 2 ilustran un dispositivo 10 de comunicación móvil a modo de ejemplo. En la implementación a modo de ejemplo, se proporciona el dispositivo 10 de comunicación móvil para soportar la comunicación por voz con otro dispositivo, tal como otro dispositivo de comunicación móvil. Además, el dispositivo 10 de comunicación móvil puede incluir una variedad de funcionalidades adicionales, que incluyen acceso de red, mensajería SMS, alojamiento de una o más aplicaciones, procesamiento de datos, encriptación, y/u otras funciones. El dispositivo 10 de comunicación móvil puede ser un teléfono inteligente, configurado para comunicarse a través de una o más redes celulares. En una implementación alternativa, el dispositivo 10 de comunicación móvil puede funcionar exclusivamente en una red no celular tal como una red WiFi y/o por satélite.

Tal como se muestra, el dispositivo 10 de comunicación móvil incluye un alojamiento 12 y múltiples dispositivos 14 de presentación dispuestos al menos parcialmente dentro del alojamiento 12. El dispositivo 14 de presentación emite información tal como, pero no limitada a, datos relacionados con el funcionamiento del dispositivo 10 de comunicación móvil, órdenes, datos solicitados, mensajes, uno o más dispositivos de entrada (tal como, un teclado virtual), y/o cualquier otro tipo de datos a un usuario. En varios ejemplos, el dispositivo 14 de presentación puede incluir, por ejemplo, una pantalla de cristal líquido (LCD), una visualización de diodo emisor de luz (LED), un diodo emisor de luz (LED), un flash de cámara, una visualización de LED orgánico (OLED), y/o una visualización de “tinta electrónica”. En algunas implementaciones, pueden incluirse múltiples dispositivos 14 de presentación para presentar datos a un usuario de manera visual y/o auditiva. En la implementación a modo de ejemplo, el dispositivo 14 de presentación incluye una salida de audio para su uso en la comunicación por voz.

El dispositivo 10 de comunicación móvil incluye, además, múltiples dispositivos 16 de entrada dispuestos al menos parcialmente dentro del alojamiento 12. Cada dispositivo 16 de entrada puede estar configurado para recibir selecciones, solicitudes, órdenes, información, datos, y/o cualquier otro tipo de entradas, según uno o más de los métodos y/o procedimientos descritos en el presente documento. Los dispositivos 16 de entrada pueden incluir, por ejemplo, botones, un teclado, un micrófono, un vibráfono, un dispositivo de señalado, una pluma, un panel sensible táctil (por ejemplo, un panel táctil o una pantalla táctil), un giroscopio, un acelerómetro, una brújula digital, un detector de posición, una cámara, una segunda cámara, un sensor de luz ambiental, y/o una interfaz de entrada de audio. En la implementación a modo de ejemplo, un único componente, tal como una pantalla 18 táctil, funciona en tanto en cuanto dispositivo 14 de presentación como dispositivo 16 de entrada.

En una implementación, el dispositivo 10 de comunicación móvil incluye características de seguridad que facilitan un funcionamiento seguro del dispositivo 10 de comunicación móvil. Las características de seguridad incluyen un dispositivo 16 de entrada tal como un botón 17 de seguridad y un dispositivo 14 de presentación tal como una pluralidad de LED. Más específicamente, el dispositivo 10 de comunicación móvil incluye un primer LED 19 y un segundo LED 21. Tal como se describirá más detalladamente a continuación, las características de seguridad pueden usarse para cambiar y/o verificar un estado fiable, operativo del dispositivo 10 de comunicación móvil. En una implementación alternativa, el dispositivo 10 de comunicación móvil puede incluir cualquier tipo y/o número de dispositivos de presentación que permitan que las características de seguridad funcionen tal como se describe en el presente documento.

El dispositivo 10 de comunicación móvil incluye un panel 20 trasero enganchado con el alojamiento 12. El panel 20 trasero define una sección transversal sustancialmente consistente con el alojamiento 12, formando de ese modo una unidad sustancialmente solidaria con el alojamiento 12 cuando se acopla al mismo. El panel 20 trasero puede retirarse del dispositivo 10 de comunicación móvil para proporcionar acceso a uno o más aspectos del dispositivo 10 de comunicación móvil.

La figura 3 es una ilustración esquemática de una arquitectura de hardware a modo de ejemplo que puede usarse con el dispositivo 10 de comunicación móvil (mostrado en la figura 1). En la implementación a modo de ejemplo, el dispositivo 10 de comunicación móvil incluye una memoria 22 y un procesador 24 acoplado a la memoria 22 para ejecutar instrucciones programadas. El procesador 24 puede incluir una o más unidades de procesamiento (por ejemplo, en una configuración de múltiples núcleos) y/o incluir un acelerador criptográfico (no mostrado). El dispositivo 10 de comunicación móvil puede programarse para realizar una o más operaciones descritas en el presente documento programando la memoria 22 y/o el procesador 24. Por ejemplo, el procesador 24 puede programarse codificando una operación como instrucciones ejecutables y proporcionando las instrucciones ejecutables a la memoria 22.

El procesador 24 puede incluir, pero no se limita a, una unidad de procesamiento central (CPU) con fines generales, un microcontrolador, un procesador informático con conjunto de instrucciones reducido (RISC), una plataforma de aplicaciones multimedia abierta (OMAP), un circuito integrado de aplicación específica (ASIC), un circuito lógico programable (PLC), y/o cualquier otro circuito o procesador que pueda ejecutar las funciones descritas en el presente documento. Los métodos descritos en el presente documento pueden codificarse como instrucciones ejecutables realizadas en un medio legible por ordenador que incluye, sin limitación, un dispositivo de almacenamiento y/o un dispositivo de memoria. Tales instrucciones, cuando se ejecutan por el procesador 24, provocan que el procesador 24 realice al menos una parte de las funciones descritas en el presente documento. Los ejemplos anteriores son solo a modo de ejemplo, y por tanto no están destinados a limitar en absoluto la definición y/o significado del término procesador.

La memoria 22, tal como se describe en el presente documento, es uno o más dispositivos que permiten que información tal como instrucciones ejecutables y/u otros datos se almacenen y obtengan. La memoria 22 puede incluir uno o más medios legibles por ordenador, tal como, sin limitación, memoria de acceso aleatorio dinámica (DRAM), memoria de acceso aleatorio dinámica síncrona (SDRAM), memoria de acceso aleatorio estática (SRAM), un disco de estado sólido, y/o un disco duro. La memoria 22 puede estar configurada para almacenar, sin limitación, instrucciones ejecutables, sistemas operativos, aplicaciones, recursos, *scripts* de instalación y/o cualquier otro tipo de datos adecuados para su uso con los métodos y sistemas descritos en el presente documento.

Las instrucciones para sistemas operativos y aplicaciones se ubican en un formato funcional en una memoria 22 no transitoria para su ejecución por el procesador 24 para realizar uno o más de los procedimientos descritos en el presente documento. Estas instrucciones en las diferentes implementaciones pueden realizarse en diferentes medios legibles por ordenador físicos o tangibles, tales como la memoria 22 u otra memoria, tales como los medios 26 legibles por ordenador, que pueden incluir, sin limitación, una memoria flash y/o un dispositivo USB. Además, las instrucciones se ubican en un formato funcional en los medios 26 legibles por ordenador no transitorios, que pueden incluir, sin limitación, memoria de medios inteligente (SM), memoria flash compacta (CF), memoria digital segura (SD), memoria de memoria extraíble (MS), memoria de tarjeta multimedia (MMC), tarjeta multimedia integrada (e-MMC), y memoria micro. Los medios 26 legibles por ordenador pueden insertarse y/o extraerse de manera selectiva del dispositivo 10 de comunicación móvil para permitir el acceso y/o la ejecución mediante el procesador 24. En algunas implementaciones, los medios 26 legibles por ordenador no son extraíbles.

Haciendo referencia de nuevo a la figura 3, el dispositivo 10 de comunicación móvil puede incluir un componente 30 de GPS, que está configurado para proporcionar datos de ubicación para el procesador 24. Los datos de ubicación permiten que el procesador 24 determine la ubicación del dispositivo 10 de comunicación móvil y/o proporcionan funcionalidad que depende de la ubicación del dispositivo 10 de comunicación móvil, tal como, por ejemplo, funcionalidad de navegación. En una implementación alternativa, pueden obtenerse datos de ubicación para el dispositivo 10 de comunicación móvil usando una red celular, identificando estaciones o dispositivos de base próximos 802.11 y/o Bluetooth, y/o una combinación de los mismos.

En algunas implementaciones, el dispositivo 10 de comunicación móvil incluye, además, al menos un criptoprocesador. Más específicamente, el dispositivo 10 de comunicación móvil incluye un primer módulo 60 de plataforma fiable (TPM)

y un segundo TPM 62. Los TPM encriptan al menos una parte de los datos a los que se accede por el procesador 24 para su comunicación hasta/desde el dispositivo 10 de comunicación móvil y/o para su almacenamiento en el mismo. Por consiguiente, algunos datos pueden segregarse desde otras aplicaciones y/u operaciones del dispositivo 10 de comunicación móvil, y mantenerse a un nivel de seguridad más alto que tales aplicaciones/operaciones. Como tal, los TPM 60 y 62 facilitan permitir un arranque fiable, arranque medido, arranque seguro, confirmación remota, y almacenamiento de claves protegido, por ejemplo.

Además, el dispositivo de comunicación móvil incluye un elemento 64 seguro acoplado al procesador 24. Más específicamente, el elemento 64 seguro puede estar integrado con el dispositivo 10 de comunicación móvil como al menos uno de una tarjeta integrada de circuito universal (UICC), una tarjeta microSD, y/o integrarse dentro del dispositivo 10 de comunicación móvil. El elemento 64 seguro es un entorno de almacenamiento y ejecución inviolable que puede usarse como un dispositivo de almacenamiento de claves y/o como clave pública de hardware para una plataforma que se ejecuta en el dispositivo 10 de comunicación móvil. Más específicamente, el elemento 64 seguro almacena claves, contraseñas, e información de configuración de hardware y software de encriptación de datos. Además, el elemento 64 seguro genera pares de claves públicas y facilita la limitación de la exportación de claves privadas asociadas. En una implementación alternativa, el elemento 64 seguro puede implementarse con un TPM.

El dispositivo 10 de comunicación móvil también incluye una memoria 66 de supervisión de seguridad. La memoria 66 de supervisión de seguridad almacena datos que reaccionan a la violabilidad que pueden incluir una pluralidad de claves, y pueden usarse para envolver los datos dentro del elemento 64 seguro y/o primer TPM 60 o segundo TPM 62. En funcionamiento, los datos que reaccionan a la violabilidad pueden eliminarse de manera que los datos envueltos no pueden recuperarse tras la detección de una situación de violabilidad. La memoria 66 de supervisión de seguridad puede contener cualquier cantidad de datos que reaccionan a la violabilidad, que permite que el dispositivo 10 de comunicación móvil funcione tal como se describe en el presente documento.

El dispositivo 10 de comunicación móvil incluye, además, un controlador 31 celular acoplado al procesador 24. El controlador 31 celular permite que el dispositivo 10 de comunicación móvil se comunique con una o más redes celulares (no mostradas) para proporcionar una comunicación por voz y/o de datos con la red celular. En este ejemplo, el dispositivo 10 de comunicación móvil incluye dos ranuras 33A y 33B de tarjeta de módulo de identificación de abonado (SIM) acopladas al controlador 31 celular. De esta manera, el dispositivo 10 de comunicación móvil puede recibir dos tarjetas SIM asociadas con dos cuentas celulares diferentes, que pueden seleccionarse por un usuario del dispositivo 10 de comunicación móvil. Por ejemplo, el dispositivo 10 de comunicación móvil puede acceder a una cuenta celular personal y a una cuenta celular de negocios, lo que permite que el usuario seleccione entre las mismas para separar uso personal y uso profesional. Debe apreciarse que puede incluirse un número diferente de ranuras de tarjeta SIM en otras implementaciones.

Además, el dispositivo 10 de comunicación móvil incluye un controlador 35 USB acoplado al procesador 24. Tal como se muestra en la figura 3, el controlador 35 USB es accesible a través del conector 37. De esta manera, uno o más dispositivos diferentes pueden comunicarse con el dispositivo 10 de comunicación móvil. De manera similar, el dispositivo 10 de comunicación móvil incluye, además, un controlador 39 de interfaz multimedia de alta definición (HDMI) acoplado al procesador 24 y accesible a través de un conector 41. En al menos una implementación, los conectores 37 y/o 41 pueden proporcionar conexiones micro-USB y/o micro-HDMI al dispositivo 10 de comunicación móvil.

Adicional o alternativamente, el dispositivo 10 de comunicación móvil puede incluir uno o más de un controlador Bluetooth, un controlador ZigBee, y/o un controlador Wi-Fi para proporcionar uno o más canales de comunicación inalámbricos. Aunque el componente 30 de GPS, el primer TPM 60, el segundo TPM 62, y el controlador 31 celular se proporcionan al menos parcialmente en hardware, debe apreciarse adicionalmente que pueden proporcionarse uno o más componentes integrados en el dispositivo 10 de comunicación móvil a través de software y/o firmware asociados con el procesador 24. En un ejemplo, el procesador 24 proporciona un cortafuegos de interfaz aérea, configurado para analizar protocolos de interfaz aérea de bajo nivel del dispositivo 10 de comunicación móvil y permitir o denegar transmisiones de red basándose en identidades y características de red aprobadas. En este ejemplo, los datos de protocolo de interfaz aérea del controlador 31 celular que contienen identidades y características de red celular se proporciona para el procesador 24 y se analizan mediante el procesador 24 para determinar si debe permitirse que el dispositivo 10 de comunicación móvil dirija las transmisiones de red por medio de redes celulares identificadas por el controlador 31 celular. En este ejemplo, el nivel de análisis proporciona seguridad de red adicional al dispositivo 10 de comunicación móvil al tener un procesador 24 que autentica adicionalmente las conexiones de red del controlador 31 celular más allá del uso de mecanismos de autenticación de protocolo de red celular habituales del controlador 31 celular en sí mismos. Debe observarse que otros componentes de interfaz aérea del dispositivo 10 de comunicación móvil, tal como, por ejemplo, un controlador Bluetooth y/o un controlador Wi-Fi, también pueden monitorizarse por el cortafuegos de interfaz aérea. En una implementación alternativa, el primer TPM 60 y el segundo TPM 62 pueden implementarse en software.

Debe apreciarse que otras implementaciones de dispositivo de comunicación móvil pueden incluir más o menos componentes integrados con o externos al procesador 24.

La figura 4 es una ilustración esquemática de una arquitectura 100 de software a modo de ejemplo que puede usarse

con el dispositivo 10 de comunicación móvil (mostrado en la figura 1). En la implementación a modo de ejemplo, la arquitectura 100 de software incluye un sistema 104 operativo instalado en una plataforma 102 de hardware que incluye el procesador 24 y la memoria 22. La plataforma 102 de hardware incluye los componentes del dispositivo 10 de comunicación móvil descrito anteriormente. La arquitectura 100 de software también incluye una capa de software de virtualización, tal como un hipervisor 106, que se ejecuta en la parte superior del sistema 104 operativo (es decir, un hipervisor de tipo 2) y un supervisor 108 de seguridad acoplado en comunicación con el hipervisor 106. En una implementación alternativa, el hipervisor 106 puede instalarse y funcionar en la plataforma 102 de hardware (es decir, un hipervisor de tipo 1). El hipervisor 106 soporta una pluralidad de espacios de ejecución de máquina virtual de manera que una pluralidad de máquinas virtuales puede iniciarse y ejecutarse al mismo tiempo.

El hipervisor 106 virtualiza una primera persona 110 y una segunda persona 120 que pueden ejecutarse y realizarse en la parte superior del hipervisor 106. La primera persona 110 incluye un sistema operativo de primera persona (OS) 112 y un primer entorno 114 de ejecución fiable (TEE), y la segunda persona 120 incluye un sistema 12 operativo de segunda persona y un segundo entorno 124 de ejecución fiable.

Cada una de la primera persona 110 y la segunda persona 120 tiene una clave pública raíz definida que puede usarse para validar la fiabilidad y para autorizar acciones realizadas por cada persona. Más específicamente, la primera persona 110 tiene una primera clave pública raíz y la segunda persona 120 tiene una segunda clave pública raíz que es independiente de la primera clave pública raíz. Tal como se usa en el presente documento, el término “clave pública raíz” se refiere a una o más claves de encriptación secretas (es decir, un certificado criptográfico) que define la titularidad de la persona y que puede usarse para firmar elementos de persona. Por el contrario, tal como se usa en el presente documento, los términos “titular” y/o “titularidad” se refieren a una persona o entidad que tiene control administrativo de una persona al tener en posesión la clave pública raíz. En algunas implementaciones, el certificado de clave pública raíz puede usarse para firmar una autorización de certificado intermedio que firma los elementos del paquete personal.

Cada clave pública raíz tiene su origen en una autoridad de certificado raíz, que puede ser una organización empresarial y/o puede definirse de manera ligera para un único usuario en un ordenador de escritorio. Como tal, los recursos de primera persona 110 pueden mantenerse independientes de la segunda persona 120, y pueden reforzarse las políticas de acceso que se han acordado y firmado por cada clave pública raíz. La autoridad de certificado raíz puede almacenarse fuera de línea y en una ubicación segura. Además, la clave pública raíz puede incluir una pluralidad de autoridades de certificado intermedias que tienen capacidades definidas de manera específica. Las capacidades a modo de ejemplo incluyen, pero no se limitan a, el derecho a definir un sistema operativo, el derecho a definir TEE, el derecho a definir políticas de seguridad, el derecho a definir otras autoridades de certificado intermedias y/o certificados de usuario, capacidades de respaldo, política de respaldo, la capacidad de actualizar un sistema operativo, la capacidad de actualizar TEE, funcionalidad de gestión de dispositivo móvil (MDM), e importación y/o exportación de claves.

Cada uno del software fiable de primera persona 110 y segunda persona 120 se ejecuta en un contexto que se encuentra aislado de los otros en condiciones por defecto. Más específicamente, tal como se describió anteriormente, el hipervisor 106 facilita la separación y aislamiento del primer TEE 114 y el segundo TEE 124 uno con respecto a otro. Como tal, cada persona no se verá afectada por otros sistemas operativos que se ejecutan en el dispositivo 10 de comunicación móvil. Además, la primera persona 110 y la segunda persona 120 pueden estar configuradas para establecer una confianza mutua entre el primer TEE 114 y el segundo TEE 124. Al establecer tal confianza mutua se permite la formación de una trayectoria de comunicación fiable entre la primera persona 110 y la segunda persona 120. La comunicación entre el primer TEE 114 y el segundo TEE 124 puede solo permitirse mediante acuerdo mutuo en las políticas de seguridad de la primera persona 110 y la segunda persona 120. Además, puede implementarse una protección de alta seguridad (no mostrada) para facilitar la limitación de un flujo de datos entre la primera persona 110 y la segunda persona 120. Por ejemplo, la protección de alta seguridad puede facilitar la limitación del flujo de datos sensibles y/o clasificados entre la primera persona 110 y la segunda persona 120, al tiempo que permite el flujo de datos sin clasificar entre las mismas.

Aunque la primera persona 110 y los elementos de la misma se describirán en detalle adicional a continuación, debe comprenderse que puede aplicarse la misma descripción a la segunda persona 120 y los elementos de la misma. En la implementación a modo de ejemplo, el OS 112 de primera persona es un entorno de ejecución que tiene recursos y memorias de dispositivo virtual que permiten la ejecución de un sistema operativo completo. Un sistema operativo completo a modo de ejemplo puede incluir, pero no se limita a, un sistema operativo de proyecto de código abierto (AOSP) de Android®. El OS 112 de primera persona puede incluir una librería que permite que el OS 112 de primera persona se comunique con el primer TEE 114. Además, pueden adquirirse una pluralidad de aplicaciones 130 desde una fuente externa (no mostrada) y ejecutarse en la parte superior del OS 112 de primera persona.

El primer TEE 114 es un entorno de ejecución ligero que es independiente de y está acoplado en comunicación con el OS 112 de primera persona. El primer TEE 114 es un entorno seguro que proporciona una zona que puede usarse para almacenar datos sensibles y para ejecutar aplicaciones sensibles. En implementaciones alternativas, el primer TEE 114 puede ser un entorno de ejecución que tiene recursos y memorias de dispositivo virtual que permiten ejecutar un sistema operativo completo y/o pueden ejecutarse en una pieza independiente de hardware. Además, la primera persona 110 puede incluir más de un entorno de ejecución fiable.

El primer TEE 114 tiene acceso directo a una interfaz de módulo de identificación de abonado (SIM) ISO7816 y/o a un TPM. Más específicamente, el primer TPM 60 (mostrado en la figura 3) se asigna a la primera persona 110, y el segundo TPM 62 (mostrado en la figura 3) se asigna a la segunda persona 120. Como tal, el primer TPM 60 puede usarse como clave pública raíz de hardware para un titular de la primera persona 110, y el segundo TPM 62 puede usarse como clave pública raíz de hardware para un titular de la segunda persona 120. Además, el primer TEE 114 tiene acceso directo al primer TPM 60 y a servicios de entorno de ejecución fiable tales como autenticación, acceso a almacenamiento de claves, configuración de red privada virtual (VPN), y/o software de protocolo de transmisión de voz por internet (VoIP), por ejemplo. El aislamiento de tales trayectorias de datos sensibles dentro del primer TEE 114 y alejándose del OS 112 de primera persona facilita garantizar un funcionamiento fiable del dispositivo 10 de comunicación móvil al tiempo que se mantiene el control de los servicios de TEE con la persona titular. Además, al permitir que el primer TEE 114 controle el primer TPM 60 se facilita el aislamiento de información sensible del OS 112 de primera persona de manera que la información se encuentra en un entorno más seguro y protegido.

Además, el primer TEE 114 puede tener acceso a servicios criptográficos de manera que pueden realizarse operaciones criptográficas en representación del OS 112 de primera persona sin exponerlo a una clave de texto sencillo. Más específicamente, el primer TEE 114 puede usar módulos de encriptación en el primer TPM 60 que permiten criptografía acelerada de hardware sin certificar, paquete B, y/o encriptación certificada FIPS-140-2. El dispositivo 10 de comunicación móvil también puede incluir un módulo de VPN y/o un módulo de VoIP. El módulo de VPN permite que la primera persona 110 autentique una VPN y se comunique con encriptación sin autenticación o siendo visibles las claves de encriptación para el código no fiable. Adicionalmente, el módulo de VoIP permite que la primera persona 110 establezca y autentique una llamada de VoIP y se comunique con encriptación sin autenticación o siendo visibles las claves de encriptación para el código no fiable.

La fiabilidad del OS 112 de primera persona y el OS 122 de segunda persona se define mediante la integridad de una imagen de arranque de cada persona cargada por el hardware 102 de plataforma. Por ejemplo, la fiabilidad el primer TEE 114 se define mediante la integridad de su imagen estática cuando se carga por el hardware 102 de plataforma tal como se describirá más detalladamente a continuación. Más específicamente, el código cargado en el primer TEE 114 se valida frente a una clave pública raíz durante la carga, y la imagen es inmutable una vez está cargada. Como la imagen es inmutable, el primer TEE 114 solo puede cambiarse mediante la carga de una nueva imagen firmada en el primer TEE 114. Además, el OS 112 de primera persona y el OS 122 de segunda persona pueden usar recursos fuera de su propio entorno de ejecución para gestionar su integridad. Por ejemplo, la carga de los sistemas operativos puede encriptarse y validarse, y el acceso de los sistemas operativos a recursos de hardware puede verse limitado y reforzado a través de configuraciones que están fuera de su control.

La arquitectura 100 de software también incluye un cargador 140 de arranque principal que carga el sistema 104 operativo, un primer cargador 142 de arranque secundario que carga el OS 112 de primera persona, y un segundo cargador 144 de arranque secundario que carga el OS 122 de segunda persona. En la implementación a modo de ejemplo, el dispositivo 10 de comunicación móvil usa un procesador que facilita el establecimiento de la fiabilidad de plataforma durante el procedimiento de arranque. Más específicamente, el procesador permite la validación de firma de los cargadores de arranque para facilitar el establecimiento de una fiabilidad durante la carga de cada sistema operativo. Por ejemplo, el dispositivo 10 de comunicación móvil usa una combinación de valores de cálculo de direccionamiento fijos y validación de firma de manera que una cadena de fiabilidad permanece irrompible a medida que se extiende desde la plataforma 102 de hardware hasta la primera persona 110 y la segunda persona 120.

En funcionamiento, el procesador 24 carga el cargador 140 de arranque principal si se firma digitalmente por una raíz de confianza del fabricante del dispositivo. Tal como se usa en el presente documento, el término “raíz de confianza del fabricante del dispositivo” se refiere a una o más claves de encriptación secretas (es decir, un certificado criptográfico) usado por un fabricante de dispositivo para firmar elementos que se encuentran instalados en el dispositivo 10 de comunicación móvil. La cadena de fiabilidad continúa siendo irrompible a través del hipervisor 106 para facilitar el establecimiento de entornos de ejecución aislados, validar componentes dentro del dispositivo 10 de comunicación móvil, y/o almacenar mediciones en los módulos de plataforma fiables para un uso posterior por el código de usuario para que no interfiera en el estado fiable.

El control del primer TPM 60 se transfiere a la primera persona 110, y el control del segundo TPM 62 se transfiere a la segunda persona 120 de manera que los aspectos de arranque medidos de los TPM 60 y 62 pueden usarse por la primera persona 110 y la segunda persona 120. Más específicamente, los TPM 60 y 62 se inician mediante el software de arranque fiable del dispositivo 10 de comunicación móvil, y, entonces, el control se transfiere a cada persona para su uso exclusivo tras haber cargado a las personas. Si una persona usa un TPM para un arranque fiable, entonces los cambios de hardware y/o software pueden dar como resultado la incapacidad de recuperar claves que han ligado contra las configuraciones originales de manera que la persona no puede reiniciarse sin reconfigurar todo el dispositivo.

Durante el procedimiento de arranque, los TPM miden (es decir, calculan el direccionamiento) los componentes de software y firmware críticos usados dentro del dispositivo 10 de comunicación móvil. Por ejemplo, puede establecerse una raíz de confianza para medir cuando las mediciones para el cargador 140 de arranque principal, el sistema 104 operativo, el hipervisor 106, el supervisor 108 de seguridad, el cargador 142 de arranque, y el OS 112 de primera persona se extienden dentro del primer TPM 60. Las mediciones pueden almacenarse dentro de los registros de

configuración de plataforma (PCR) ubicados en el primer TPM 60 y pueden usarse para validar una imagen de sistema operativo frente a una clave pública raíz asociada en el momento de arranque. Como tal, puede verificarse la integridad del sistema antes de permitir el acceso a la información sensible que puede estar ligada con los PCR.

Las personas pueden ser responsables de su propia integridad una vez que el control cambia de la fiabilidad del fabricante de dispositivo durante la carga de arranque. Por ejemplo, es responsabilidad del OS 112 de primera persona validar las aplicaciones 130 que se instalan y ejecutan en el OS 112 de primera persona. Como tal, en el caso de que una aplicación falsa (no mostrada) comprometa la integridad de un sistema operativo huésped que se ejecuta en el dispositivo 10 de comunicación móvil, el compromiso no afectará a la integridad de los otros sistemas operativos huésped si no tienen una relación de fiabilidad con el sistema operativo comprometido.

El supervisor 108 de seguridad se acopla en comunicación con las OS 112 y 122 de personas primera y segunda. El supervisor 108 de seguridad es un sistema operativo que facilita el almacenamiento y ejecución de políticas de seguridad para su uso en el funcionamiento del dispositivo 10 de comunicación móvil. El supervisor 108 de seguridad se ejecuta en un entorno aislado y puede tener acceso a los recursos de plataforma, interfaces adicionales, y/o capacidades adicionales. En algunas implementaciones, la primera persona 110 y la segunda persona 120 se separan a través de un mecanismo fiable (es decir, virtualización de CPU) de manera que un titular individual no puede configurar una política de seguridad de una persona que no pertenece a ese titular individual. Por ejemplo, la política de seguridad de la primera persona 110 solo puede configurarse por un titular de primera persona, y la política de seguridad de la segunda persona 120 solo puede configurarse por un titular de segunda persona. Más específicamente, cada política de seguridad puede firmarse mediante la clave privada del titular individual y la firma puede validarse por el dispositivo 10 de comunicación móvil usando una clave pública correspondiente del titular individual antes de que el supervisor 108 de seguridad aplique la política de seguridad a la persona asociada. Las políticas de titularidad y seguridad para la primera persona 110 y la segunda persona 120 se almacenan en un archivo de configuración que puede mantenerse por el supervisor 108 de seguridad. Además, las políticas de titularidad y seguridad se validan mediante certificados criptográficos. Como tal, cada titular individual puede definir el sistema operativo, el entorno de ejecución fiable, y la política de seguridad para la persona a la que pertenece.

Las políticas de seguridad de la primera persona 110 y la segunda persona 120 pueden definirse por los titulares individuales, y pueden definirse, almacenarse, y reforzarse de manera aislada del código de persona. Las políticas de seguridad definen cómo cada persona asociada puede acceder a los dispositivos físicos en el dispositivo 10 de comunicación móvil. Por ejemplo, las políticas de seguridad limitan el acceso de una persona a uno o más dispositivos físicos, definen pautas para el acceso exclusivo de una persona a uno o más dispositivos físicos, y/o definen pautas para el acceso a dispositivos compartidos para la primera persona 110 y la segunda persona 120. Más específicamente, las pautas para el acceso a un dispositivo compartido pueden permitir compartir el dispositivo de manera que solo la persona que posee el control de una interfaz de usuario tenga acceso al dispositivo compartido. Además, las normas específicas en una o más políticas de seguridad para el acceso a un dispositivo compartido pueden permitir compartir el dispositivo de manera que una persona ejecutándose en segundo plano puede seguir teniendo acceso al dispositivo compartido. Como tal, las normas definidas por las políticas de seguridad permiten que los titulares individuales personalicen el dispositivo 10 de comunicación móvil en una variedad de configuraciones para satisfacer sus necesidades.

La imagen de referencia y/o los sistemas de archivo de la primera persona 110 pueden encriptarse y almacenarse en medios internos y/o extraíbles. Además, el volumen de arranque de la primera persona 110 puede encriptarse de manera que puede requerirse la autenticación previa al arranque del procedimiento de arranque fiable antes de que la primera persona 110 puede arrancarse y acceder a los datos sensibles almacenados en la misma. Más específicamente, durante el procedimiento de arranque fiable, puede obligarse a que un usuario introduzca sus credenciales antes de que se autorice a la primera persona 110 a arrancarse. El usuario puede desear verificar un estado del dispositivo 10 de comunicación móvil antes de introducir sus credenciales. Por ejemplo, el usuario puede solicitar la verificación de que el dispositivo 10 de comunicación móvil se encuentra en un estado fiable antes de introducir una contraseña y/o número de identificación personal (PIN) para garantizar que la pantalla de entrada es auténtica. Tal como se describió anteriormente, el dispositivo 10 de comunicación móvil incluye características de seguridad tales como el botón 17 de seguridad y/o los LED 19 y 21 (mostrados en la figura 1). Las características de seguridad se aíslan en hardware al que no puede accederse desde un código no fiable ejecutado en el dispositivo 10 de comunicación móvil para facilitar la verificación de que la pantalla de entrada es auténtica.

En funcionamiento, un usuario puede accionar el botón 17 de seguridad cuando aparece un diálogo de autenticación en la pantalla 18 táctil (mostrada en la figura 1). El accionamiento del botón 17 de seguridad visualiza información de raíz de confianza para el dispositivo 10 de comunicación móvil y/o visualiza información de raíz de confianza para el software que solicita que aparezca el diálogo de autenticación. Por ejemplo, la información de raíz de confianza puede incluir información de raíz de confianza para el dispositivo 10 de comunicación móvil y/o para una persona que se ejecuta en el dispositivo 10 de comunicación móvil. Como tal, el usuario puede verificar la información de raíz de confianza e introducir de manera segura las credenciales solicitadas. En una implementación alternativa, el diálogo de autenticación puede verificarse cuando los LED 19 y 21 se activan en una configuración predeterminada.

En una implementación, el usuario puede desear cambiar un estado operativo del dispositivo de comunicación móvil. Más específicamente, el usuario puede desear cambiar un enfoque del dispositivo 10 de comunicación móvil entre

personas que se ejecutan en el dispositivo 10 de comunicación móvil. Por ejemplo, el accionamiento del botón 17 de seguridad facilita el cambio de enfoque entre la primera persona 110 y la segunda persona 120. Además, el primer LED 19 se asigna a la primera persona 110, y el segundo LED 21 se asigna a la segunda persona 120. El primer LED 19 puede activarse y el segundo LED 21 puede desactivarse cuando la primera persona 110 está enfocada, y el segundo LED 21 puede activarse y el primer LED 19 puede desactivarse cuando la segunda persona 120 está enfocada. Como tal, el primer LED 19 y el segundo LED 21 proporcionan retroalimentación visual al usuario basándose en el estado operativo del dispositivo 10 de comunicación móvil.

Al menos uno de los TPM 60 y 62 tiene una característica de presencia física que obliga a un usuario a verificar su presencia con respecto al dispositivo 10 de comunicación móvil. Por ejemplo, la característica de presencia física puede implementarse para verificar que una operación que se ejecuta en el dispositivo 10 de comunicación móvil no se está realizando de manera remota. Como tal, el botón 17 de seguridad puede presionarse para verificar la presencia física del usuario.

La figura 5 es un diagrama de flujo de un método a modo de ejemplo de reivindicar la titularidad de una persona que puede usarse con el dispositivo 10 de comunicación móvil. En la implementación a modo de ejemplo, el dispositivo 10 de comunicación móvil usa raíces de confianza criptográficas para definir la titularidad de la primera persona 110 y la segunda persona 120. Por ejemplo, la primera persona 110 puede estar configurada para su uso por una entidad, y la segunda persona 120 puede estar configurada para su uso por otra entidad. Un emisor (es decir, una empresa) del dispositivo 10 de comunicación móvil puede emitir uno o más dispositivos 10 de comunicación móviles a un usuario (por ejemplo, un cliente y/o un empleado). En una implementación de este tipo, la primera persona 110 puede estar configurada para uso empresarial y la segunda persona 120 puede estar configurada para uso personal. En una implementación alternativa, el dispositivo 10 de comunicación móvil puede estar configurado para separar las personas asignando SIM independientes, servicios independientes, y/o aislando los datos, los sistemas operativos, y las comunicaciones celulares de la primera persona 110 y la segunda persona 120.

El uso de raíces de confianza criptográficas permite que el dispositivo 10 de comunicación móvil verifique la integridad de una configuración de persona, y limite los derechos de modificación de la persona a las partes autorizadas. Por ejemplo, el dispositivo 10 de comunicación móvil puede proporcionarse a un usuario final con al menos una persona por defecto (es decir, una persona sin una titularidad definida) instalada en el mismo. La persona por defecto se firma mediante una clave pública raíz por defecto por el fabricante, lo que indica que la persona está sin modificar y tiene una política por defecto asignada a la misma. Entonces, el usuario final puede usar la persona por defecto, pero no puede personalizarla sin, en primer lugar, hacerse titular definiendo una raíz de confianza.

Un operario 200 reivindica la titularidad de una persona, tal como la segunda persona 120, creando 212 una raíz de confianza para la persona en una estación de trabajo de un gestor 202 de persona (PM). En algunas implementaciones, el PM 202 también puede permitir que el operario 200 edite y/o defina la política de seguridad para la persona, y/o actualice las imágenes de la persona y/o un entorno de ejecución fiable, tal como el segundo TEE 124. El operario 200 solicita que un gestor 204 de dispositivo (DM) genere 214 un comprobante de licencia para reivindicar un sistema operativo, tal como el OS 122 de segunda persona, para transferir la titularidad de la clave pública raíz por defecto a la raíz de confianza creada 212. Entonces, se autoriza la transferencia 216 y el dispositivo 10 de comunicación móvil se reinicia 218.

Durante el reinicio 218, el operario 200 acopla un cable de bus en serie universal (USB) entre el DM 204 y el dispositivo 10 de comunicación móvil, y el dispositivo 10 de comunicación móvil detecta la conexión USB e introduce un modo de programación de manera que los sistemas operativos de persona no se cargan. Entonces, el operario 200 solicita 220, desde la estación de trabajo, que el DM 204 ejecute el software para transferir la persona al nuevo titular. La solicitud se dirige 222 hacia el supervisor 206 de seguridad y puede definir una nueva clave pública raíz de persona. Entonces, el supervisor 206 de seguridad usa el comprobante de licencia generado 214 para solicitar 224 la autorización del operario 200 para verificar su identidad, y el operario 200 introduce 226 una contraseña de dispositivo predeterminada en respuesta a la solicitud 224 de autorización. La solicitud 224 también puede firmarse por la raíz de confianza creada 212.

Entonces, el dispositivo 10 de comunicación móvil presenta una solicitud 228 de autenticación procedente del supervisor 206 de seguridad a un usuario para introducir sus credenciales para desbloquear el elemento 208 seguro. Si se confirma que la persona no es titular por la clave pública raíz por defecto, los cálculos de direccionamiento de elemento de la persona anterior y las firmas se transfieren 234 al DM 204. El DM 204 verifica las firmas y vuelve a firmar los cálculos de direccionamiento con la clave de firma de la nueva persona que se autoriza para firmar los elementos relevantes. Además, la clave de persona que permite el acceso a las claves de medios de persona se cambia. Entonces, las firmas de sustitución se transfieren 236 desde el DM 204 hasta el dispositivo 10 de comunicación móvil, y el dispositivo 10 de comunicación móvil valida las firmas y sustituye las firmas anteriores en los elementos de persona por las nuevas firmas.

Entonces, se crea 238 un archivo de transición de persona, y el archivo de configuración para la persona se comprueba en cuanto a validez y conflictos con otros archivos de configuración que ya se encuentran en el dispositivo 10 de comunicación móvil. El procedimiento avanza si se valida el archivo de configuración, y la actualización de software se detiene si existe un conflicto entre los archivos de configuración. La autenticación de persona de usuario se actualiza

240 tras la autorización para avanzar de manera que puede accederse a las claves de medios mediante la nueva raíz de confianza y se devuelve 242 al DM 204.

El DM 204 firma los elementos que se actualizan y devuelve los cálculos de direccionamiento firmados. Por ejemplo, los elementos que se actualizan pueden o bien tener firmas que se actualizan con cálculos de direccionamiento que se firman de nuevo y/o pueden actualizarse 246 con nuevas firmas. El archivo de transición de persona se comprueba 244 tras cada actualización para permitir que se reinicie el procedimiento a partir de una actualización interrumpida. Después de que la actualización esté completa, los datos almacenados temporalmente se envían 248 a la memoria flash 210, se borra 250 el archivo de transición de persona y se reinicia 252 el dispositivo 10 de comunicación móvil.

La figura 6 es una ilustración esquemática de un sistema 300 a modo de ejemplo para su uso en la autorización de una operación que va a realizarse en el dispositivo 10 de comunicación móvil. En la implementación a modo de ejemplo, puede necesitarse la autorización de una entidad antes de permitirse que modifique el software instalado en un dispositivo informático objetivo, tal como el dispositivo 10 de comunicación móvil. Por ejemplo, una vez que se ha cargado una persona en el dispositivo 10 de comunicación móvil, un propietario de dispositivo mantiene la autoridad para eliminar y/o sustituir a esa persona, pero el titular individual tiene la autoridad para modificarla. Como tal, puede requerirse que se autorice a una entidad que actúa en representación del titular individual para tener permisos predeterminados concedidos a la misma por el titular individual para modificar una persona. Tal como se usa en el presente documento, el término “propietario de dispositivo” se refiere a una entidad que usa una persona por defecto para hacer funcionar el dispositivo 10 de comunicación móvil.

Un ordenador de administración, tal como el gestor 302 de dispositivo (DM), puede generar y transmitir una solicitud a un servidor 304 de autorización en busca de autorización para realizar una operación en el dispositivo 10 de comunicación móvil. La solicitud es un archivo que especifica los parámetros para la operación que va a realizarse en el dispositivo 10 de comunicación móvil. Parámetros a modo de ejemplo incluyen, pero no se limitan a, la identificación de un dispositivo informático objetivo (por ejemplo, el dispositivo 10 de comunicación móvil), la operación que va a realizarse en el dispositivo informático objetivo, un periodo de tiempo en el que se realizará la operación, y una ubicación geográfica del dispositivo informático objetivo. Además, la solicitud se firma mediante una primera clave privada de un par de claves pública, privada asignadas a un administrador. En algunas implementaciones, la solicitud puede transmitirse por medio de un medio extraíble (no mostrado).

El servidor 304 de autorización recibe la solicitud desde el DM 302 y verifica la firma del DM 302 con una clave pública del primer par de claves pública, privada. El servidor 304 de autorización también determina si los parámetros para la operación que va a realizarse se alinean con la política de seguridad para el dispositivo 10 de comunicación móvil. Los parámetros autorizados pueden almacenarse en una base 306 de datos de autorización, a la que puede accederse mediante el servidor 304 de autorización. Entonces, el servidor 304 de autorización genera una respuesta de autorización si la solicitud se ha autorizado. La respuesta de autorización puede incluir la solicitud desde el DM 302 y un token de autorización creado por el servidor 304 de autorización. El token de autorización puede usarse para autorizar la operación solicitada. En algunas realizaciones, el token de autorización puede tener un periodo de autorización predeterminado en el que puede realizarse la operación solicitada, puede limitarse para otorgar la autorización para un dispositivo informático objetivo particular, y/o puede autorizar la realización de una única o múltiples operaciones en el dispositivo 10 de comunicación móvil. Solamente como ejemplo, el token de autorización puede incluir una autorización para realizar la operación en un dispositivo informático objetivo predeterminado, y/o una autorización para realizar una operación predeterminada en el dispositivo informático objetivo. Además, el token de autorización puede generarse al menos uno de antes de recibir la solicitud para realizar la operación en el dispositivo 10 de comunicación móvil y en respuesta a una verificación de la solicitud para realizar la operación en el dispositivo 10 de comunicación móvil. Entonces, la respuesta de autorización puede firmarse por una segunda clave privada de un par de claves pública, privada asociadas con el ordenador de servidor de autorización y transmitirse al ordenador de administración. En una implementación alternativa, la respuesta de autorización puede firmarse por un operario de autenticación. Por ejemplo, la solicitud puede ponerse en cola y o bien firmarse, otorgarse, o denegarse por el operario de autenticación. En algunas implementaciones, la respuesta de autorización puede transmitirse por medio de un medio extraíble (no mostrado).

El DM 302 recibe la respuesta de autorización y determina si el token de autorización autoriza la operación solicitada. Por ejemplo, el DM 302 puede verificar la respuesta de autorización con una clave pública del segundo par de claves pública, privada, en el que la respuesta de autorización se firma con una clave privada del segundo par de claves pública, privada. Entonces, el DM 302 transmite el archivo de respuesta de autorización al dispositivo 10 de comunicación móvil para solicitar una operación que va a realizarse si la solicitud se ha autorizado. La transmisión de la respuesta de autorización puede incluir firmar la respuesta de autorización con la clave privada del primer par de claves pública, privada. El dispositivo 10 de comunicación móvil recibe la respuesta de autorización y verifica las firmas con una clave pública del primer par de claves pública, privada asociadas con el ordenador de administración, y determina si los parámetros especificados en la respuesta de autorización se alinean con la política de seguridad para el dispositivo 10 de comunicación móvil. El dispositivo 10 de comunicación móvil permite la realización de la operación solicitada si las firmas se verifican y los parámetros se alinean. Entonces, puede realizarse la operación autorizada en el dispositivo 10 de comunicación móvil. En una implementación alternativa, la respuesta de autorización puede incluir una cadena de certificación a una raíz de confianza de autorización. Además, en una implementación alternativa, el token de autorización puede generarse y transmitirse por medio de medios físicos.

La figura 7 es un diagrama de flujo de un método de actualización de software de persona a modo de ejemplo que puede usarse con el dispositivo 10 de comunicación móvil. En la implementación a modo de ejemplo, el operario 400 puede actualizar un OS de persona existente, tal como la segunda persona 120, acoplando un cable USB desde una estación 402 de trabajo de gestor de dispositivo (DM) hasta el dispositivo 10 de comunicación móvil. El software de gestión de dispositivo se ejecuta y el operario 400 dirige el dispositivo 10 de comunicación móvil al reinicio 410. Durante el reinicio 410, el dispositivo 10 de comunicación móvil detecta la conexión USB y entra en modo de programación de manera que los sistemas operativos de persona no se cargan. Entonces, el operario 400 dirige el software 412 de DM para solicitar 414 una actualización a un OS de persona en el dispositivo 10 de comunicación móvil. La estación 402 de trabajo de DM entra en contacto con un servidor de autorización para obtener un token de autorización. El token de autorización puede almacenarse temporalmente y/o cargarse de una fuente fuera de línea. Entonces, el supervisor 404 de seguridad puede autorizar 416 la solicitud 414, y puede procederse a la actualización 418 de persona. En algunas implementaciones, el software de DM alertará al operario 400 y rechazará realizar el procedimiento de actualización si no está presente un token de autorización válido.

La estación 402 de trabajo de DM incluye una clave secreta compartida que puede usarse para desbloquear el elemento 406 seguro. Solo las claves de encriptación de almacenamiento relacionadas con la persona autorizada pueden recuperarse del elemento 406 seguro usando la autenticación proporcionada por la clave secreta compartida. Entonces, el dispositivo 10 de comunicación móvil valida el token de autorización para verificar que el operario 400 tiene los privilegios para realizar la operación solicitada. El usuario se autentica 420 mediante el elemento 406 seguro, y la operación se aborta si el operario 400 no tiene las credenciales apropiadas.

Entonces, el software de DM solicita 422 los datos de geometría de dispositivo de la persona desde el dispositivo 10 de comunicación móvil. Los datos de geometría de dispositivo pueden incluir, pero no se limitan a, un tamaño de los componentes de OS y TEE de una persona. La actualización de software avanza si la geometría de persona coincide con la geometría de dispositivo, y la actualización de software se detiene y se indica un error si existe una disparidad. En una implementación alternativa, el número de revisión de paquetes que pertenecen a persona también puede proporcionarse de modo que el titular individual puede verificar la compatibilidad de la actualización.

El software de DM inicia el procedimiento de carga transmitiendo 424 el software que va a actualizarse al dispositivo 10 de comunicación móvil. En una implementación, la actualización de software comienza transmitiendo 426 la configuración de la persona si está incluida en la actualización. Entonces, el supervisor 404 de seguridad examina y evalúa la geometría del archivo de configuración, la raíz de confianza, y la firma para determinar si se producirá un conflicto con otros archivos de configuración que ya se han cargado en el dispositivo 10 de comunicación móvil. La actualización de software avanza si el archivo de configuración se valida 428 y/o si el archivo de configuración no se está actualizando, y la actualización de software se detiene si existe un conflicto entre archivos de configuración. Además, un sistema operativo actualizado y/o un entorno de ejecución fiable pueden cargarse 430 y 432 en el dispositivo 10 de comunicación móvil.

Las actualizaciones de software transmitidas se almacenan en la memoria 408 flash y se validan frente a la clave pública raíz. Entonces, se crea 434 un archivo de transición de persona para indicar qué software va a actualizarse, el software se escribe en flash 408, y se crea un punto de comprobación en el archivo de transición después de cada actualización. Por ejemplo, el nuevo archivo de configuración se escribe 436 en flash 408 y el archivo de transición se comprueba 438, se escribe 440 el nuevo sistema de archivos de OS de persona en flash 408 y se comprueba 442 el archivo de transición, y se escribe 444 el nuevo sistema de archivos de TEE de persona en flash 408 y se comprueba 446 el archivo de transición. En la implementación a modo de ejemplo, los sistemas de archivos flash objetivos se programan a partir del contenido de memoria almacenado anteriormente, y se encriptan durante la transferencia usando claves de almacenamiento procedentes del archivo de configuración. Después de que la actualización está completa, los datos almacenados temporalmente se envían 448 a flash 408, se borra 450 el archivo de transición de persona, y se reinicia 452 el dispositivo 10 de comunicación móvil.

La figura 8 es un diagrama de flujo de un método de cambio de titularidad de una persona a modo de ejemplo que puede usarse con el dispositivo 10 de comunicación móvil. La titularidad de una persona cargada en el dispositivo 10 de comunicación móvil puede cambiarse a un nuevo titular sin actualizar los datos de persona. En la implementación a modo de ejemplo, el nuevo titular genera 510 un comprobante de transferencia dentro del gestor de dispositivo (DM) (nueva RoT) 502. El comprobante de transferencia puede ser un bloque de datos que detalla el dispositivo específico que va a cambiar y la raíz de confianza actual prevista. Entonces, el bloque de datos se envía al titular individual actual, y el titular individual actual verifica la información dentro del DM de titular individual actual (nueva RoT) 502.

Entonces, el operario 500 que trabaja en representación del titular individual actual obtiene un token de autorización que indica si el operario y el titular individual actual se autorizan 512 y 514 mediante DM (RoT anterior) 503 para transferir la persona. Entonces, el token de autorización se adjunta y firma el comprobante de transferencia, y el comprobante de transferencia firmado se transfiere a y se almacena 516 en flash 508. El comprobante de transferencia firmado también puede devolverse al posible nuevo titular individual junto con una clave de autenticación para la ranura de persona dentro del elemento 506 seguro. En una implementación de este tipo, la clave de autenticación puede envolverse usando la clave pública de operario de DM del nuevo titular individual que está unida al comprobante de transferencia. Entonces, el operario que trabaja en representación del nuevo titular individual puede usar el comprobante de transferencia envuelto para iniciar el procedimiento de transferencia. Más específicamente, el

dispositivo 10 de comunicación móvil puede verificar las credenciales del nuevo titular individual y autorizar la transferencia.

Entonces, el operario 500 acopla un cable USB desde una estación de trabajo de DM (nueva RoT) 502 hasta el dispositivo 10 de comunicación móvil. El software de gestión de dispositivo se ejecuta y el operario 500 dirige el dispositivo 10 de comunicación móvil a su reinicio 518. Durante el reinicio 518, el dispositivo 10 de comunicación móvil detecta la conexión USB y entra en un modo de programación de manera que los sistemas operativos de persona no se cargan. Entonces, el operario 500 ordena al software de DM que cambie de persona perteneciente al titular individual actual al nuevo titular individual. El comprobante de transferencia incluye información requerida para la autorización, y un certificado de operario 500 de infraestructura de clave pública (PKI) que sirve para autenticar la solicitud firmada por la raíz de confianza para el titular anterior de la persona cambiada.

El software de DM usa la clave secreta del operario 500 para desenvolver la clave de autenticación del comprobante de transferencia. Entonces, la clave de autenticación puede usarse 520 para solicitar 522 la transferencia de persona, y para autenticar 524 al operario para desbloquear el elemento 506 seguro en el dispositivo 10 de comunicación móvil. En una implementación de este tipo, la autenticación 524 solo permite recuperar claves de encriptación de almacenamiento relacionadas con la persona autorizada a partir del elemento 506 seguro.

La transición incluye, además, transferir 530 los cálculos de direccionamiento de persona anterior del elemento al DM 502. El DM 502 verifica las firmas y vuelve a firmar los cálculos de direccionamiento con la clave de firma de nueva persona que está autorizada para firmar los elementos relevantes. Además, la clave de persona que permite el acceso a las claves de medios de persona se cambia, y el nuevo valor se transfiere al DM 502. Entonces, las firmas de sustitución se transfieren 532 desde el DM 502 hasta el dispositivo 10 de comunicación móvil, y el dispositivo 10 de comunicación móvil valida la firmas y sustituye las firmas anteriores en los elementos de persona por las nuevas firmas.

Entonces, se crea 534 un archivo de transición de persona, y el archivo de configuración para la persona se comprueba en cuanto a validez y conflictos con otros archivos de configuración que ya se han cargado en el dispositivo 10 de comunicación móvil. El procedimiento avanza si el archivo de configuración se valida, y la actualización de software se detiene si existe un conflicto entre archivos de configuración. La autenticación de persona de usuario se actualiza 536 tras la autorización para proceder de manera que puede accederse a las claves de medios mediante la nueva raíz de confianza y se devuelven 538 al DM 502.

El DM 502 firma los elementos que se están actualizando y devuelve los cálculos de direccionamiento firmados. Por ejemplo, los elementos que se están actualizando pueden tener o bien firmas que se actualizan con cálculos de direccionamiento firmados de nuevo y/o pueden actualizarse 542 con nuevas firmas. El archivo de transición de persona se comprueba 540 después de cada actualización para permitir que el procedimiento se reinicie a partir de una actualización interrumpida. Después de que la actualización está completa, los datos almacenados temporalmente se envían 544 a flash 508, el archivo de transición de persona se borra 546, y el dispositivo 10 de comunicación móvil se reinicia 548.

Después de haber transferido la titularidad de persona al nuevo titular individual, puede requerirse establecer una nueva relación de confianza entre la persona cambiada y cualquier persona que tuviera una relación de confianza con el titular individual anterior. Más específicamente, la configuración de persona de las otras personas que se ejecutan en el dispositivo 10 de comunicación móvil puede tener que actualizarse para establecer una relación de confianza con el nuevo titular individual para mantener la misma funcionalidad que con el titular individual anterior.

La figura 9 es un diagrama de flujo de un método de carga de una nueva persona a modo de ejemplo que puede usarse con el dispositivo 10 de comunicación móvil. En la implementación a modo de ejemplo, el operario 600 acopla un cable USB desde una estación 602 de trabajo de gestor de dispositivo (DM) hasta el dispositivo 10 de comunicación móvil. El software de gestión de dispositivo se ejecuta y el operario 600 dirige el dispositivo 10 de comunicación móvil a su reinicio 612. Durante el reinicio 612, el dispositivo 10 de comunicación móvil detecta la conexión USB y entra en modo de programación de manera que los sistemas operativos de persona no se cargan. Entonces, se hace que el operario 600 autorice 614 la conexión USB con una contraseña de dispositivo a disposición del propietario del dispositivo, y se introduce 616 la contraseña de dispositivo y se autentica 618 para desbloquear el elemento 606 seguro. En una implementación alternativa, el dispositivo 10 de comunicación móvil puede reiniciarse y reconfigurarse a una configuración de fábrica.

Entonces, el software de DM solicita 620 los datos de geometría de dispositivo de la persona a partir del dispositivo 10 de comunicación móvil, y el operario 600 dirige la estación 602 de trabajo de DM para cargar 622 el paquete de persona en una ranura de persona específica. Los datos de geometría de dispositivo pueden incluir, pero no se limitan a, un tamaño de los componentes de OS y TEE de una persona. La actualización de software avanza si la geometría de persona coincide con la geometría de dispositivo, y la actualización de software se detiene y se indica un error si existe una disparidad. En una implementación alternativa, el número de revisión de paquetes pertenecientes a persona también puede proporcionarse de modo que el titular individual puede verificar la compatibilidad de la actualización.

El software de DM inicia el procedimiento de carga transmitiendo el software que va a cargarse en el dispositivo 10 de comunicación móvil. En una implementación, la carga de software comienza transmitiendo 624 el archivo de configuración de la persona al dispositivo 10 de comunicación móvil. Entonces, el supervisor 604 de seguridad examina y evalúa la geometría del archivo de configuración, raíz de confianza, y firma para determinar si se producirá un conflicto con otros archivos de configuración que ya se han cargado en el dispositivo 10 de comunicación móvil. La carga de software avanza si el archivo de configuración se valida 626, y la carga de software se detiene si existe un conflicto entre archivos de configuración. En algunas implementaciones, un nuevo OS y un nuevo TEE de persona se cargan 628 y 630 en el dispositivo 10 de comunicación móvil.

El software transmitido se almacena en la memoria 608 flash y se valida frente a la clave pública raíz. Entonces, se crea 632 un archivo de transición de persona y se escribe para indicar que se ha sobrescrito. La indicación de sobrescrito es un valor centinela escrito de una manera persistente de manera que pueden tomarse medidas de recuperación apropiadas para recuperarse de un fallo si el procedimiento de actualización se interrumpe. Más específicamente, las claves de medios de almacenamiento en el elemento 606 seguro para la persona se borran 634, el archivo de configuración de persona anterior se elimina 636, los sistemas de archivos flash de persona se eliminan 638, y el módulo 610 de plataforma fiable (TPM) se limpia 640.

Entonces, la nueva persona puede cargarse en el dispositivo 10 de comunicación móvil de una manera persistente. Más específicamente, se escribe 642 el nuevo archivo de configuración en flash 608, se leen 644 los datos de autenticación de usuario por el supervisor 604 de seguridad, y se autentica 646 el usuario para desbloquear el elemento 606 seguro. Entonces, una clave de encriptación pública (PEK) de un par de claves pública, privada puede crearse 648 y exportarse 650 al titular individual desde el elemento 606 seguro. El titular individual firma la PEK con su autorización de certificado y la carga 654 de software avanza si el archivo de configuración se valida 652. Entonces, la PEK se devuelve a y se almacena 656 en el elemento 606 seguro.

La clave secreta del par de claves pública, privada PEK se almacena y protege dentro del elemento 606 seguro de manera que no se exportará del elemento 606 seguro. Esto permite que un titular individual verifique, mediante la respuesta firmada por la clave privada, que una solicitud para realizar un servicio provino de un dispositivo autorizado. La PEK puede crearse en el momento en que se define la titularidad de persona y puede usarse para autenticar una actualización, solicitud, y/o paquete de software, por ejemplo. En una implementación alternativa, puede crearse un segundo par de claves pública, privada y usarse para la encriptación de manera que un titular individual puede encriptar datos cuyo objetivo es un dispositivo específico y de manera que otros dispositivos no fueran capaces de desencriptar los datos.

Entonces, se escribe 658 el nuevo sistema de archivos de OS de persona en flash 608, el nuevo sistema de archivos de TEE de persona se escribe 660 en flash 608, y se crea 662 una división de datos de nueva persona. Los sistemas de archivos flash objetivos se programan a partir de contenidos de memoria almacenados anteriormente, y se encriptan durante la transferencia usando claves de almacenamiento procedentes del archivo de configuración. Después de que la actualización está completa, el archivo de transición de persona se borra 664 y el dispositivo 10 de comunicación móvil se reinicia 666.

Esta descripción escrita usa ejemplos para dar a conocer diversas implementaciones, que incluyen el mejor modo, y también para permitir que cualquier experto en la técnica lleve a la práctica las diversas implementaciones, que incluyen realizar y usar cualquier dispositivo o sistema y realizar cualquier método incorporado. El alcance de patentabilidad de la divulgación se define mediante las reivindicaciones, y puede incluir otros ejemplos que resulten evidentes para los expertos en la técnica. Tales ejemplos adicionales están destinados a encontrarse dentro del alcance de las reivindicaciones si tienen elementos estructurales que no se diferencian del lenguaje literal de las reivindicaciones, o si incluyen elementos estructurales equivalentes con diferencias insustanciales con respecto al lenguaje literal de las reivindicaciones.

REIVINDICACIONES

1. Método de autorización de una operación que va a realizarse en un dispositivo (10) informático objetivo, comprendiendo dicho método: generar, en un dispositivo (302) de solicitud, una solicitud para realizar una operación en el dispositivo (10) informático objetivo; firmar, en el dispositivo de solicitud, la solicitud con una clave privada de un primer par de claves pública, privada; transmitir la solicitud desde el dispositivo de solicitud hasta un servidor (304) de autenticación; recibir la solicitud en el servidor de autenticación desde el dispositivo de solicitud para realizar una operación en el dispositivo informático objetivo; verificar, en el servidor de autenticación, la solicitud con una clave pública del primer par de claves pública, privada; formar, en el servidor de autenticación, una respuesta de autorización que incluye la solicitud y un token de autorización; firmar, mediante el servidor de autenticación, la respuesta de autorización con una clave privada de un segundo par de claves pública, privada; transmitir la respuesta de autorización desde el servidor de autenticación hasta el dispositivo de solicitud; recibir, en el dispositivo de solicitud, la respuesta de autorización desde el servidor de autenticación que incluye la solicitud y el token de autorización; verificar, en el dispositivo de solicitud, la respuesta de autorización con una clave pública del segundo par de claves pública, privada; firmar, mediante el dispositivo de solicitud, la respuesta de autorización con la clave privada del primer par de claves pública, privada; transmitir, mediante el dispositivo de solicitud, la respuesta de autorización al dispositivo informático objetivo; recibir, mediante el dispositivo informático objetivo, la respuesta de autorización desde el dispositivo de solicitud, incluyendo la respuesta de autorización la solicitud para realizar una operación en el dispositivo informático objetivo y el token de autorización; verificar, mediante el dispositivo informático objetivo, la respuesta de autorización con la clave pública del primer par de claves pública, privada; y otorgar, mediante el dispositivo informático objetivo, autorización para realizar la operación tras la verificación de la respuesta de autorización.

2. Método según la reivindicación 1, en el que generar la solicitud comprende generar la solicitud para incluir al menos uno de una identificación del dispositivo (10) informático objetivo, la operación que va a realizarse en el dispositivo (10) informático objetivo, un periodo de tiempo en el que se realizará la operación, y una ubicación geográfica del dispositivo (10) informático objetivo.

3. Método según la reivindicación 1, en el que recibir la respuesta de autorización comprende recibir la respuesta de autorización que incluye un token de autorización que tiene al menos uno de un periodo de autorización predeterminado, autorización para realizar la operación en un dispositivo (10) informático objetivo predeterminado, y autorización para realizar operaciones predeterminadas en el dispositivo (10) informático objetivo.

4. Método según la reivindicación 1, en el que transmitir la respuesta de autorización comprende transmitir la respuesta de autorización tras la verificación de la respuesta de autorización con la clave pública del segundo par de claves pública, privada.

5. Método según la reivindicación 1, que comprende, además, firmar la respuesta de autorización con la clave privada del primer par de claves pública, privada.

6. Método según la reivindicación 1, en el que recibir la respuesta de autorización comprende determinar si el token de autorización autoriza la operación solicitada.

7. Método según la reivindicación 1, en el que transmitir la solicitud comprende transportar la solicitud al servidor (304) de autenticación por medio de medios extraíbles.

8. Método según la reivindicación 1, que comprende, además, determinar si se otorga la solicitud basándose en una política de seguridad para el dispositivo (10) informático objetivo.

9. Método según la reivindicación 8, en el que determinar si se otorga la solicitud comprende determinar si los parámetros para la operación que va a realizarse se alinean con la política de seguridad para el dispositivo (10) informático objetivo.

10. Método según la reivindicación 1, que comprende, además, crear el token de autorización al menos uno de antes de recibir la solicitud para realizar la operación en el dispositivo (10) informático objetivo y en respuesta a la verificación de la solicitud para realizar la operación en el dispositivo (10) informático objetivo.

11. Método según la reivindicación 1, en el que formar la respuesta de autorización comprende crear el token de autorización para tener al menos uno de un periodo de autorización predeterminado, autorización para realizar la operación en un dispositivo (10) informático objetivo predeterminado, y autorización para realizar operaciones predeterminadas en el dispositivo (10) informático objetivo.

12. Sistema configurado para realizar el método según cualquiera de las reivindicaciones 1 a 11, comprendiendo el sistema el dispositivo de solicitud, el servidor de autenticación y el dispositivo informático objetivo.

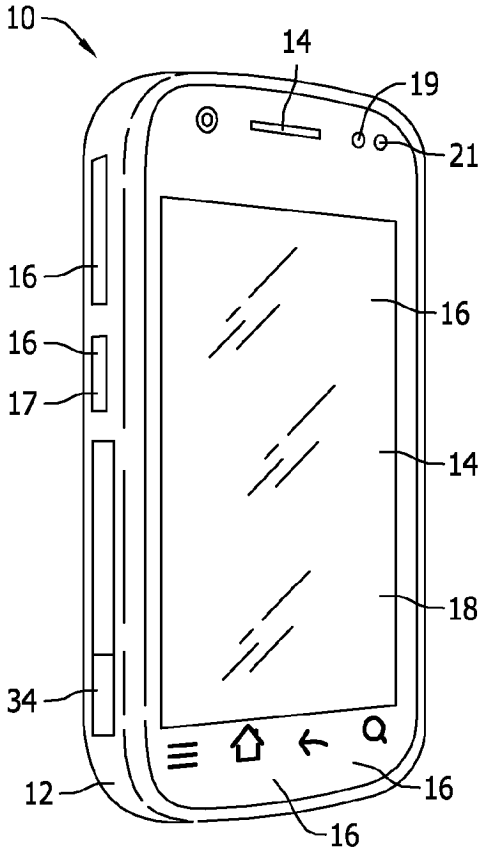

FIG. 1

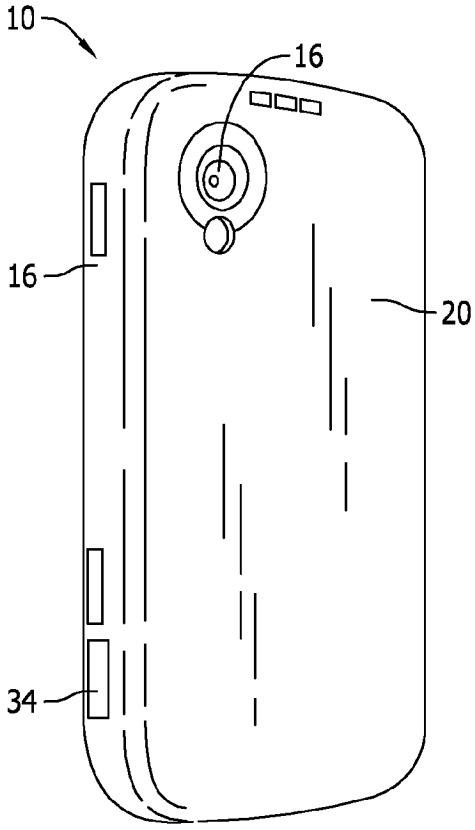

FIG. 2

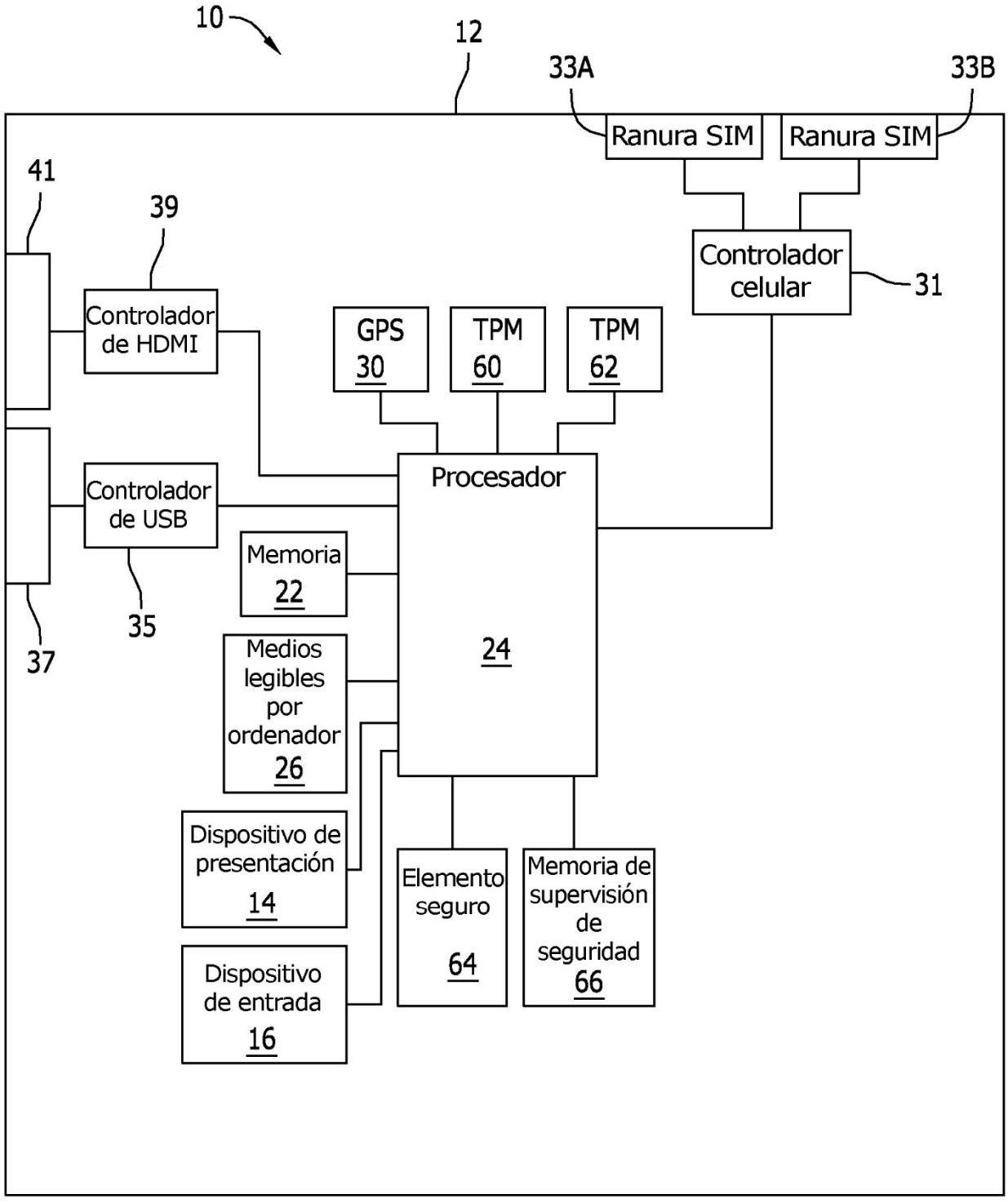
10
12
33A
33B
Ranura SIM
Ranura SIM
41
39
Controlador celular
31
Controlador de HDMI
GPS 30
TPM 60
TPM 62
Procesador
24
Controlador de USB
Memoria 22
35
37
Medios legibles por ordenador 26
Dispositivo de presentación 14
Elemento seguro 64
Memoria de supervisión de seguridad 66
Dispositivo de entrada 16

FIG. 3

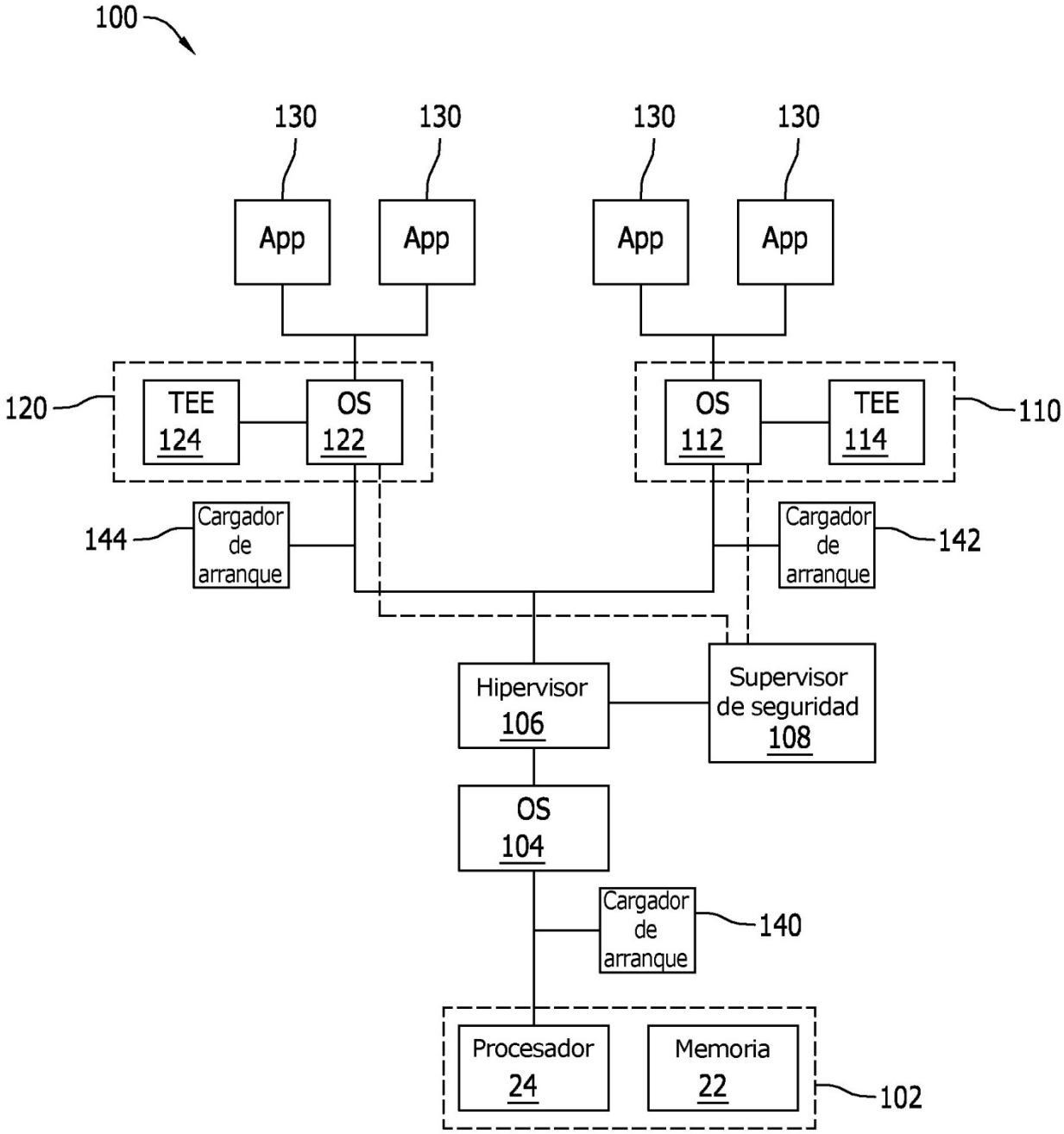
100
130
130
130
130
App
App
App
App
120
TEE
124
OS
122
OS
112
TEE
114
110
144
Cargador de arranque
Cargador de arranque
142
Hipervisor
106
Supervisor de seguridad
108
OS
104
Cargador de arranque
140
Procesador
24
Memoria
22
102

FIG. 4

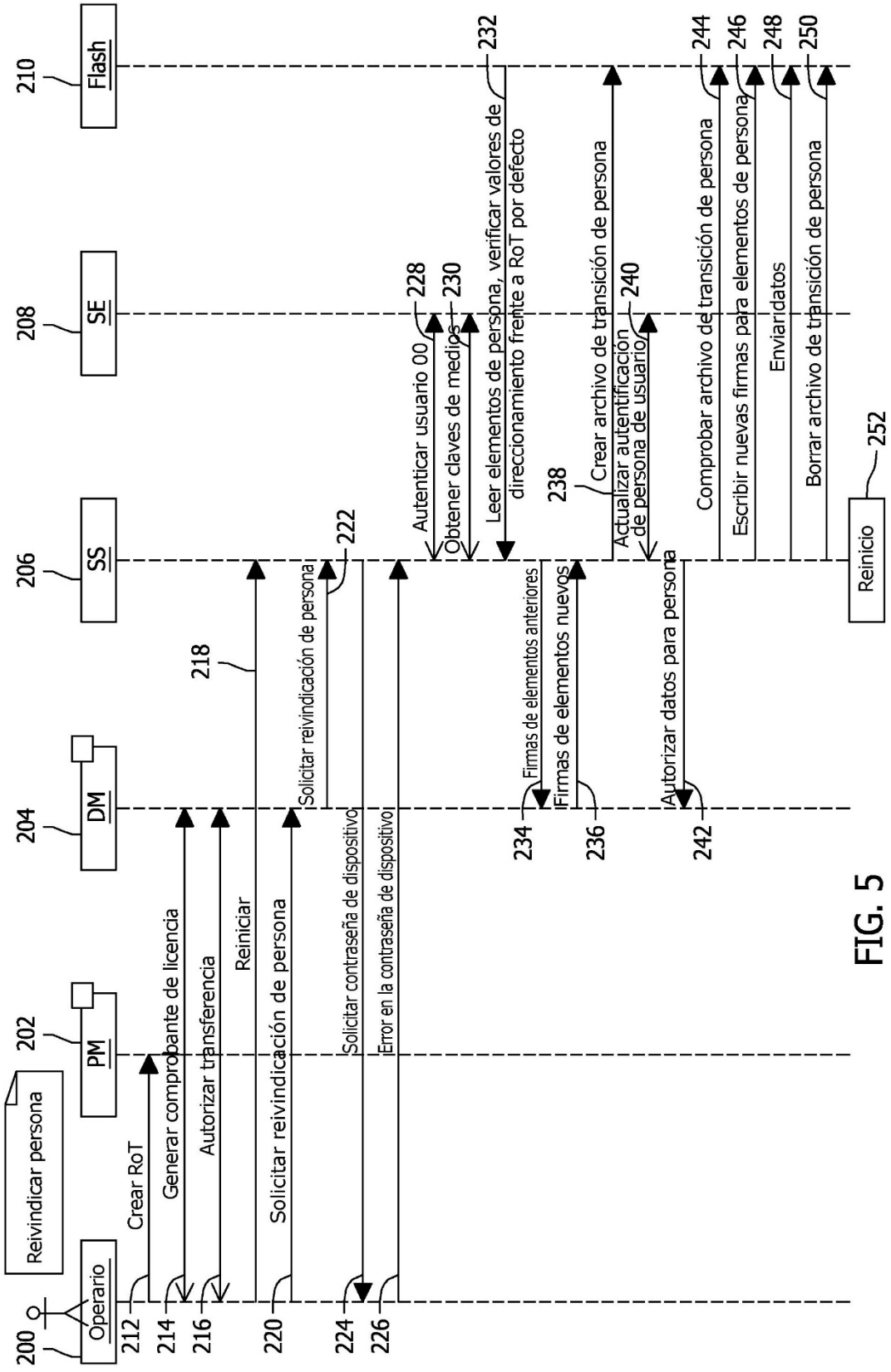
Reivindicar persona
Operario
PM
DM
SS
SE
Flash
200
202
204
206
208
210
212
214
216
218
220
222
224
226
228
230
232
234
236
238
240
242
244
246
248
250
252
Crear RoT
Generar comprobante de licencia
Autorizar transferencia
Reiniciar
Solicitar reivindicación de persona
Solicitar reivindicación de persona
Solicitar contraseña de dispositivo
Error en la contraseña de dispositivo
Autenticar usuario 00
Obtener claves de medios
Leer elementos de persona, verificar valores de direccionamiento frente a RoT por defecto
Firmas de elementos anteriores
Firmas de elementos nuevos
Crear archivo de transición de persona
Actualizar autentificación de persona de usuario
Autorizar datos para persona
Comprobar archivo de transición de persona
Escribir nuevas firmas para elementos de persona
Enviar datos
Borrar archivo de transición de persona
Reinicio

FIG. 5

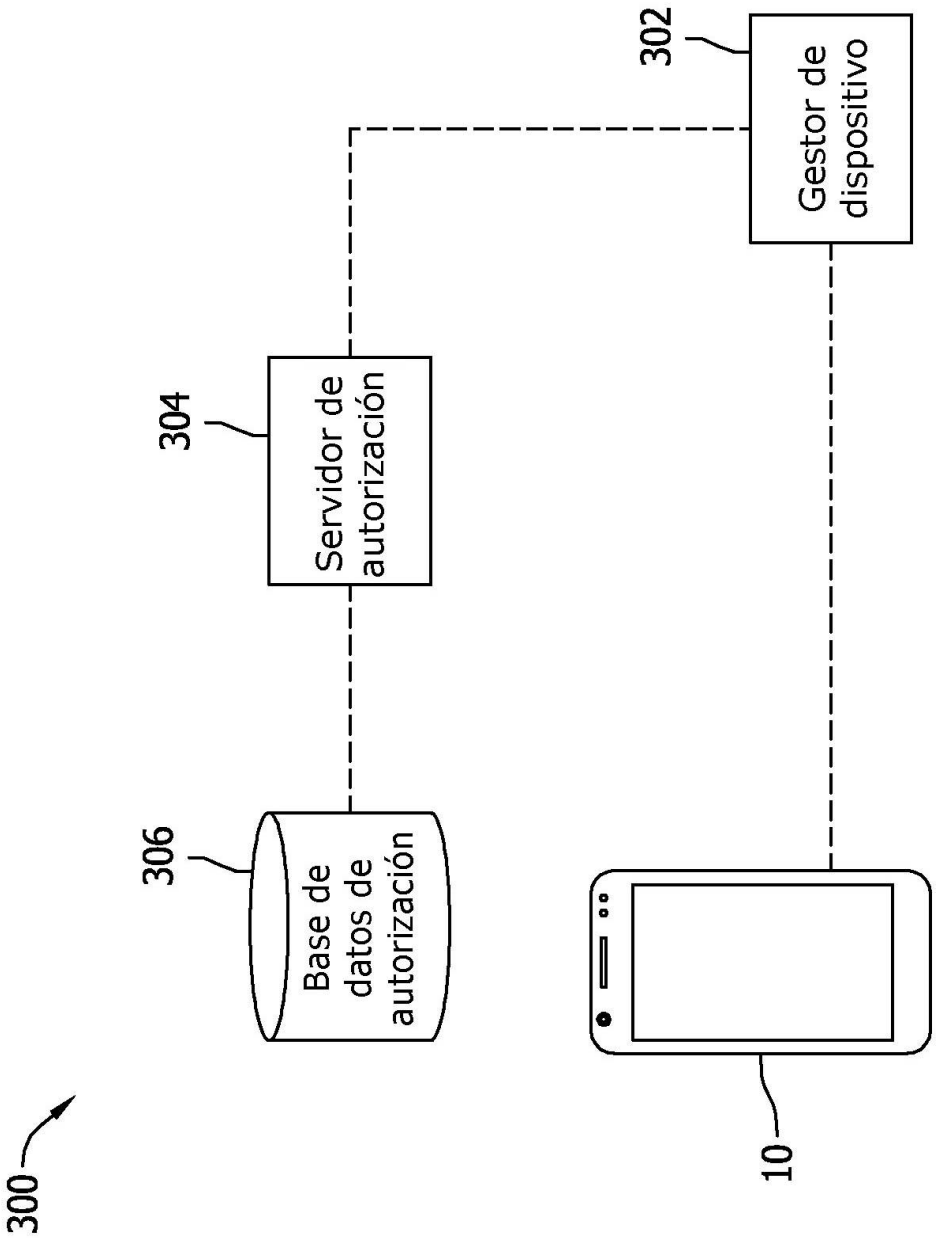
300
302
Gestor de dispositivo
304
Servidor de autorización
306
Base de datos de autorización
10

FIG. 6

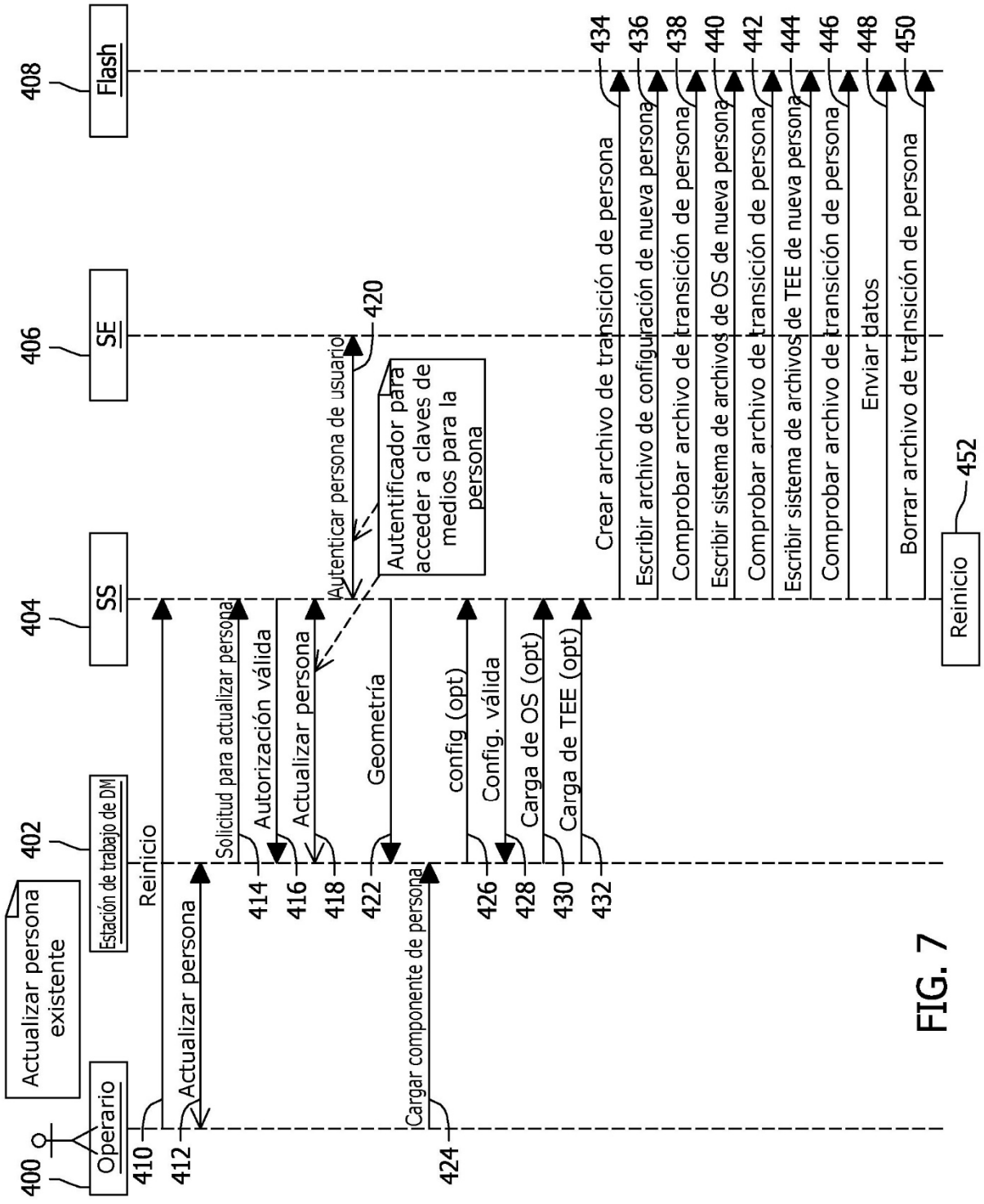
Actualizar persona existente
Operario
Estación de trabajo de DM
SS
SE
Flash
400
402
404
406
408
Reinicio
Actualizar persona
Solicitud para actualizar persona
Autorización válida
Actualizar persona
Geometría
Autenticar persona de usuario
Autentificador para acceder a claves de medios para la persona
config (opt)
Config. válida
Carga de OS (opt)
Carga de TEE (opt)
Cargar componente de persona
Crear archivo de transición de persona
Escribir archivo de configuración de nueva persona
Comprobar archivo de transición de persona
Escribir sistema de archivos de OS de nueva persona
Comprobar archivo de transición de persona
Escribir sistema de archivos de TEE de nueva persona
Comprobar archivo de transición de persona
Enviar datos
Borrar archivo de transición de persona
Reinicio
410
412
414
416
418
420
422
424
426
428
430
432
434
436
438
440
442
444
446
448
450
452

FIG. 7

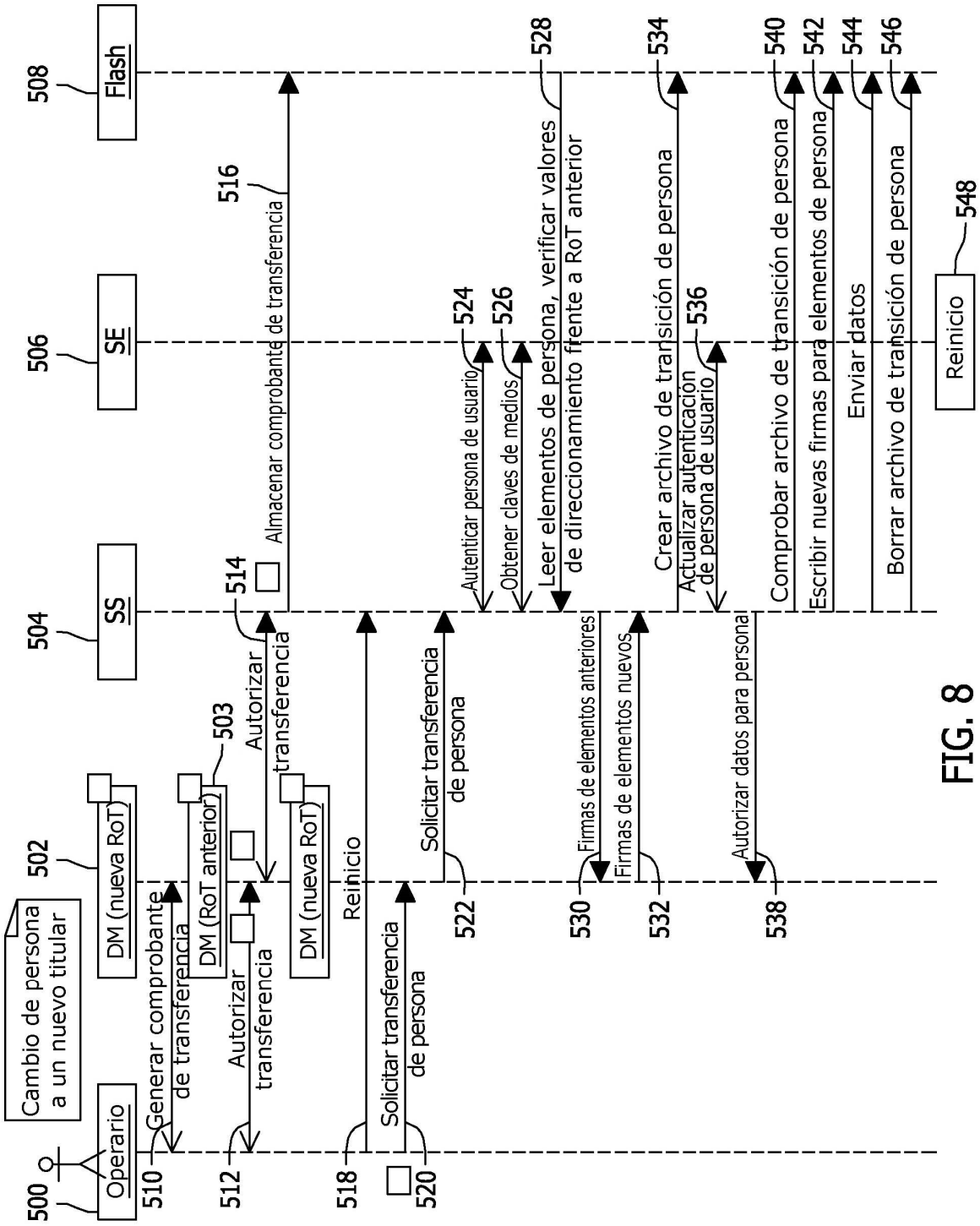
Cambio de persona a un nuevo titular
Operario
DM (nueva RoT)
DM (RoT anterior)
DM (nueva RoT)
SS
SE
Flash
500
502
503
504
506
508
510
512
514
516
518
520
522
524
526
528
530
532
534
536
538
540
542
544
546
548
Generar comprobante de transferencia
Autorizar transferencia
Autorizar transferencia
Almacenar comprobante de transferencia
Reinicio
Solicitar transferencia de persona
Solicitar transferencia de persona
Autenticar persona de usuario
Obtener claves de medios
Leer elementos de persona, verificar valores de direccionamiento frente a RoT anterior
Firmas de elementos anteriores
Firmas de elementos nuevos
Crear archivo de transición de persona
Actualizar autenticación de persona de usuario
Autorizar datos para persona
Comprobar archivo de transición de persona
Escribir nuevas firmas para elementos de persona
Enviar datos
Borrar archivo de transición de persona
Reinicio

FIG. 8

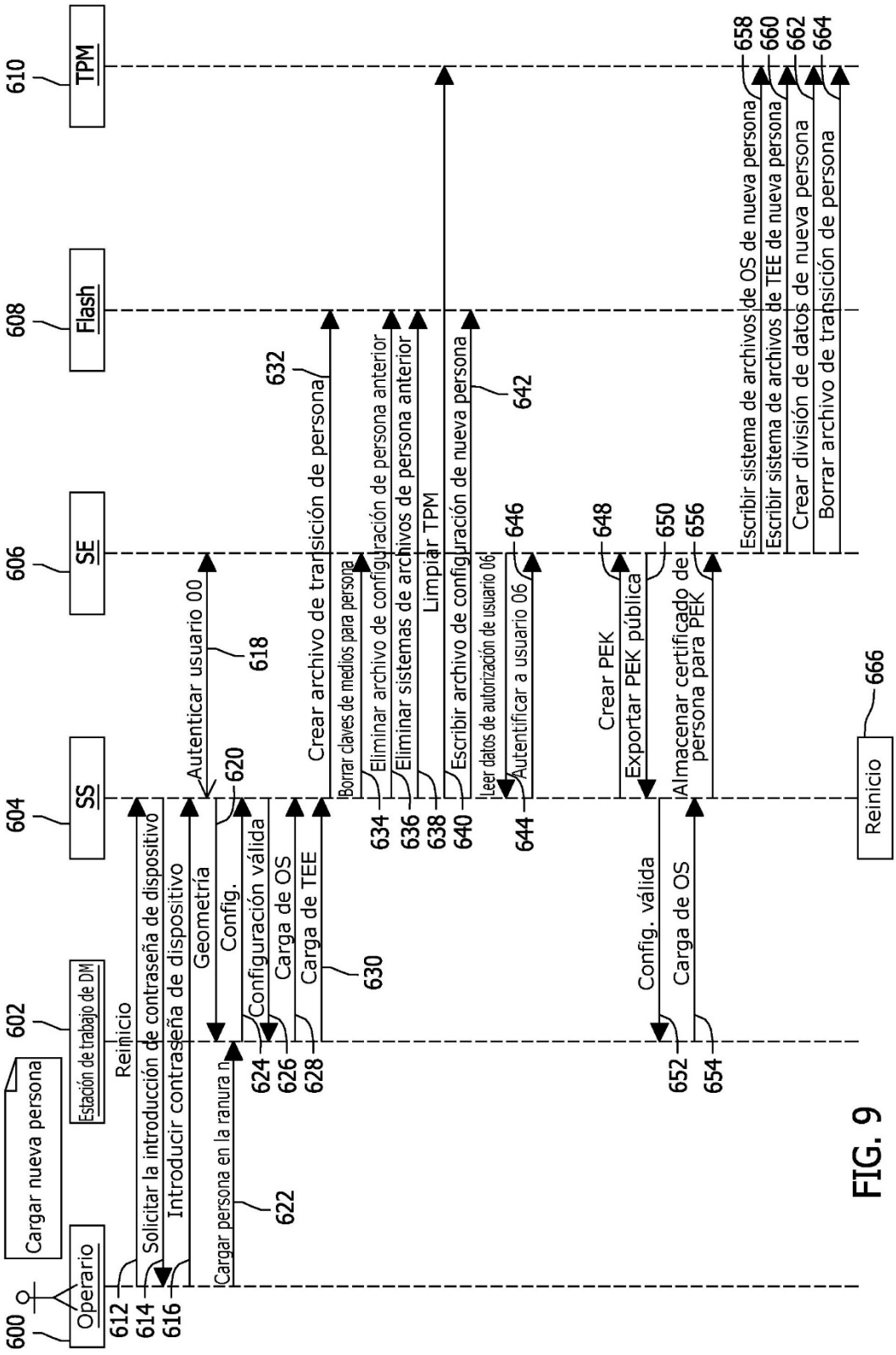
600
Operario
602
Estación de trabajo de DM
604
SS
606
SE
608
Flash
610
TPM
Cargar nueva persona
Reinicio
612
Solicitar la introducción de contraseña de dispositivo
614
Introducir contraseña de dispositivo
616
Cargar persona en la ranura n
622
Autenticar usuario 00
618
Geometría
Config.
620
Configuración válida
624
Carga de OS
626
Carga de TEE
628
630
Crear archivo de transición de persona
632
Borrar claves de medios para persona
634
Eliminar archivo de configuración de persona anterior
Eliminar sistemas de archivos de persona anterior
636
Limpiar TPM
638
Escribir archivo de configuración de nueva persona
640
642
Leer datos de autorización de usuario 06
644
Autentificar a usuario 06
646
Crear PEK
648
Exportar PEK pública
650
Almacenar certificado de persona para PEK
656
Config. válida
652
Carga de OS
654
Escribir sistema de archivos de OS de nueva persona
658
Escribir sistema de archivos de TEE de nueva persona
660
Crear división de datos de nueva persona
662
Borrar archivo de transición de persona
664
Reinicio
666

FIG. 9