

19



OFICINA ESPAÑOLA DE
PATENTES Y MARCAS

ESPAÑA



11 Número de publicación: **2 964 986**

51 Int. Cl.:

G06F 21/32 (2013.01)

G06F 21/57 (2013.01)

G06F 9/4401 (2008.01)

G06V 40/50 (2012.01)

12

TRADUCCIÓN DE PATENTE EUROPEA

T3

86 Fecha de presentación y número de la solicitud internacional: **26.04.2017 PCT/CN2017/082067**

87 Fecha y número de publicación internacional: **01.11.2018 WO18195832**

96 Fecha de presentación y número de la solicitud europea: **26.04.2017 E 17907773 (0)**

97 Fecha y número de publicación de la concesión europea: **04.10.2023 EP 3608809**

54 Título: **Método de encendido de dispositivo utilizando un botón de encendido integrado con sensor de huellas digitales**

45 Fecha de publicación y mención en BOPI de la traducción de la patente:
10.04.2024

73 Titular/es:

**HUAWEI TECHNOLOGIES CO., LTD. (100.0%)
Huawei Administration Building Bantian
Longgang DistrictShenzhen, Guangdong 518129,
CN**

72 Inventor/es:

GUAN, XIANGSHAN

74 Agente/Representante:

SÁNCHEZ SILVA, Jesús Eladio

ES 2 964 986 T3

Aviso: En el plazo de nueve meses a contar desde la fecha de publicación en el Boletín Europeo de Patentes, de la mención de concesión de la patente europea, cualquier persona podrá oponerse ante la Oficina Europea de Patentes a la patente concedida. La oposición deberá formularse por escrito y estar motivada; sólo se considerará como formulada una vez que se haya realizado el pago de la tasa de oposición (art. 99.1 del Convenio sobre Concesión de Patentes Europeas).

DESCRIPCIÓN

Método de encendido de dispositivo utilizando un botón de encendido integrado con sensor de huellas digitales

5 Campo técnico

Esta solicitud se refiere al campo de las tecnologías de electrónica y, en particular, a un método para encender un dispositivo y a un dispositivo.

10 Antecedentes

Con el rápido desarrollo de las tecnologías de la información, los terminales (por ejemplo, un teléfono inteligente, un ordenador de tableta y un ordenador portátil) son cada vez más populares. Como tecnología estándar de un terminal, la tecnología de reconocimiento de huellas digitales se utiliza ampliamente en aspectos tales como el desbloqueo del terminal, la reactivación del dispositivo desde la pantalla apagada hasta la pantalla encendida y el pago con móvil.

15 Sin embargo, la tecnología de reconocimiento de huellas digitales se utiliza únicamente para la autenticación de identidad de usuario realizada cuando el terminal está en estado de inicio o en estado de espera. La patente US 2016/0086010 A1 describe un sistema que incluye un sensor de huellas digitales y un procesador auxiliar. El sensor de huellas digitales puede configurarse como un botón pulsador. Cuando se pulsa el botón pulsador, puede ejecutarse una segunda función además de la detección de huellas digitales. Un ejemplo de la segunda función puede ser hacer que el procesador auxiliar salga de un modo de baja energía o de reposo.

20 La patente US 2017/0091515 A1 describe un conjunto de botón para un dispositivo electrónico. El conjunto de botón integra un sensor biométrico debajo de una superficie superior del botón. El conjunto de botón está posicionado con respecto a una pantalla secundaria de un dispositivo electrónico. La pantalla secundaria puede posicionarse en relación con un teclado, tal como, por ejemplo, encima de una fila superior de teclas del teclado.

25 La patente US 2016/0314291 A1 describe un periférico informático específico de misión, que incorpora un sistema de inicio de sesión biométrico integrado y proporciona una plataforma de trabajo vinculable portátil. El dispositivo incluye un botón de encendido que contiene un escáner de huellas digitales integrado (utilizado para capturar datos biométricos para autenticación junto con un código de identificación de dispositivo único).

Resumen

35 La invención se define por las reivindicaciones independientes. Las realizaciones ventajosas de la invención se dan mediante las reivindicaciones dependientes.

Esta solicitud proporciona un método para poner en marcha un dispositivo y un dispositivo, de modo que la autenticación de identidad de usuario se realice simultáneamente cuando se pone en marcha un dispositivo, para iniciar sesión en un sistema operativo del dispositivo. Es decir, la autenticación de puesta en marcha y de identidad de usuario puede establecerse realizando una operación de puesta en marcha con un solo botón por un usuario. Esto puede reducir las operaciones de usuario y la duración requeridas para la puesta en marcha del dispositivo y el inicio de sesión de sistema, y mejorar la eficiencia de la puesta en marcha del dispositivo y el inicio de sesión de sistema.

45 Para lograr los objetivos anteriores, en esta solicitud se utilizan las siguientes soluciones técnicas:

Según un primer aspecto de la presente invención, esta solicitud proporciona un método para poner en marcha un dispositivo. El dispositivo incluye un botón de encendido y un sensor de huellas digitales, el botón de encendido está integrado con el sensor de huellas digitales, el método para poner en marcha un dispositivo puede aplicarse a un proceso en el que un usuario pulsa el botón de encendido para poner en marcha el dispositivo, y el método para poner en marcha el dispositivo incluye: detectar una operación táctil realizada por el usuario en el botón de encendido; en respuesta a la operación táctil, obtener, mediante una primera unidad de microcontrolador (MCU), información de huellas digitales adquirida por el sensor de huellas digitales, y guardar, mediante la primera MCU, la información de huellas digitales; en respuesta a detectar que el botón de encendido del dispositivo está pulsado: encender una CPU del dispositivo y obtener, por la primera MCU, una solicitud de autenticación de huellas digitales después del encendido de la CPU. El método comprende, además: si la primera MCU detecta dentro de una primera duración preestablecida que el botón de encendido del dispositivo está pulsado y después de obtener la solicitud de autenticación de huellas digitales, la primera MCU proporciona la información de huellas digitales a un controlador de huellas digitales para realizar la autenticación de huellas digitales, para iniciar sesión en un sistema operativo del dispositivo; y, si la primera MCU no detecta dentro de la primera duración preestablecida que se pulsa el botón de encendido del dispositivo, la primera MCU elimina la información de huellas digitales.

65 En esta solicitud, el botón de encendido está integrado con el sensor de huellas digitales. Por lo tanto, en el proceso en el que el usuario pulsa el botón de encendido para poner en marcha el dispositivo, el sensor de huellas digitales puede adquirir la información de huellas digitales del usuario cuando el usuario toca el botón de encendido, y el dispositivo puede obtener la información de huellas digitales adquirida por el sensor de huella digital y guardar la información de huellas digitales. De este modo, después de que se pone en marcha el dispositivo, la información de

huellas digitales guardada en el dispositivo puede utilizarse para realizar la autenticación de identidad de usuario, y el usuario no necesita tocar el botón de encendido nuevamente para inscribir la información de huellas digitales del usuario para la autenticación de identidad de usuario.

5 Después de “obtener la información de huellas digitales adquirida por el sensor de huellas digitales y guardar la información de huellas digitales”, el método en esta solicitud incluye además: detectar si se pulsa el botón de encendido; y eliminar la información de huellas digitales si no se detecta que se pulsa el botón de encendido dentro de la primera duración preestablecida. La primera duración preestablecida puede comenzar desde que se guarda la información de huellas digitales.

10 Puede entenderse que, si un usuario normal desea poner en marcha el dispositivo, el usuario pulsa el botón de encendido del dispositivo dentro de un corto período de tiempo (por ejemplo, de 1 a 3 segundos) que transcurre después de que un dedo del usuario toca el botón de encendido. En este caso, si el usuario normal va a poner en marcha el dispositivo, se pulsa el botón de encendido dentro del corto período de tiempo que comienza desde que se guarda la información de huellas digitales (es decir, la primera duración preestablecida, por ejemplo, de 1 a 3 segundos). De lo contrario, si el botón de encendido no se pulsa dentro del corto período de tiempo que comienza desde que se guarda la información de huellas digitales, esto indica que la información de huellas digitales adquirida por el sensor de huellas digitales puede generarse al tocar por error el botón de encendido por el usuario. Para evitar que un usuario malintencionado utilice la información de huellas digitales adquirida por el sensor de huellas digitales y que se genera al tocar por error el botón de encendido por el usuario normal, para realizar la autenticación de identidad de usuario y sustraer información guardada en el dispositivo, el dispositivo puede eliminar la información de huellas digitales si no se detecta que se pulsa el botón de encendido dentro de la primera duración preestablecida a partir de guardar la información de huellas digitales por el dispositivo.

25 En otra realización, “detectar si el botón de encendido está pulsado” puede incluir: detectar si una interfaz de entrada/salida de propósito general preestablecida (Entrada y Salida de Propósito General, GPIO) en una placa base del dispositivo está establecida en un nivel alto, donde cuando el dispositivo está en modo en reposo o modo inactivo, si se pulsa el botón de encendido, la interfaz de GPIO preestablecida se establece desde un nivel bajo hasta un nivel alto.

30 Por lo tanto, “eliminar la información de huellas digitales si no se detecta que se pulsa el botón de encendido dentro de la primera duración preestablecida a partir de guardar la información de huellas digitales” puede incluir: eliminar la información de huellas digitales si no se detecta que la interfaz de GPIO preestablecida está establecida al nivel alto dentro de la primera duración preestablecida a partir de guardar la información de huellas digitales.

35 En otra realización, puede que no se reciba una solicitud de autenticación de huellas digitales dentro de la segunda duración preestablecida a partir de guardar la información de huellas digitales por el dispositivo. En este caso, el usuario normal puede dejar el dispositivo durante un período de tiempo porque el dispositivo no puede iniciar sesión en un escritorio de sistema operativo a tiempo. Dentro del período de tiempo en que el usuario normal se va, debido a que el dispositivo ha guardado la información de huellas digitales que puede utilizarse para realizar la autenticación de identidad de usuario, puede existir el riesgo de que un usuario malintencionado utilice la información de huellas digitales para realizar la autenticación de identidad de usuario y sustraiga información guardada en el dispositivo. En este caso, para garantizar seguridad de información del dispositivo, una primera MCU puede eliminar la información de huellas digitales guardada por la primera MCU. Específicamente, después de “obtener la información de huellas digitales adquirida por el sensor de huellas digitales y guardar la información de huellas digitales”, el método de esta solicitud puede incluir además: eliminar la información de huellas digitales si la solicitud de autenticación de huellas digitales no se obtiene dentro de la segunda duración preestablecida a partir de guardar la información de huellas digitales.

50 En otra realización, el método en esta solicitud puede incluir además: eliminar la información de huellas digitales después de que se proporciona la información de huellas digitales para realizar la autenticación de huellas digitales.

55 Después de que el dispositivo proporciona la información de huellas digitales para realizar la autenticación de huellas digitales, el dispositivo guarda además la información de huellas digitales del usuario. Para evitar que un usuario malintencionado utilice la información de huellas digitales para realizar la autenticación de identidad de usuario y sustraer información guardada en el dispositivo, el dispositivo puede eliminar la información de huellas digitales después de proporcionar la información de huellas digitales para realizar la autenticación de huellas digitales, para evitar la reutilización de la información de huellas digitales.

60 En una realización, el método en esta solicitud puede incluir, además: si una configuración de inicio de sesión del dispositivo indica que el dispositivo no necesita realizar autenticación de huellas digitales después de la puesta en marcha, eliminar la información de huellas digitales después de que transcurra la tercera duración preestablecida a partir de la finalización de la carga de un controlador de huellas digitales por el dispositivo.

65 Puede entenderse que, para facilitar el uso, algunos usuarios puedan establecer que el dispositivo cargue directamente una interfaz de sistema operativo sin realizar la autenticación de identidad de usuario después de la

puesta en marcha. En este caso, el controlador de huellas digitales no necesita realizar autenticación de identidad de usuario, y el dispositivo puede eliminar la información de huellas digitales después de que transcurra la tercera duración preestablecida a partir de que se complete la carga del controlador de huellas digitales.

5 Breve descripción de los dibujos

La Figura 1 es un diagrama estructural esquemático de un ordenador portátil según un ejemplo de ejecución;

la Figura 2 es un diagrama esquemático de una interfaz de visualización de un ordenador portátil en la técnica anterior;

10 la Figura 3 es el diagrama esquemático 1 de una interfaz de visualización de un ordenador portátil según un ejemplo de ejecución;

la Figura 4 es el diagrama de flujo 1 de un método para poner en marcha un dispositivo según un ejemplo de ejecución;

15 la Figura 5A y la Figura 5B son el diagrama de flujo 2 de un método para poner en marcha un dispositivo según un ejemplo de ejecución;

20 la Figura 6 es un diagrama esquemático 2 de una interfaz de visualización de un dispositivo según un ejemplo de ejecución;

la Figura 7 es un diagrama esquemático 3 de una interfaz de visualización de un dispositivo según un ejemplo de ejecución;

25 la Figura 8 es un diagrama esquemático 4 de una interfaz de visualización de un dispositivo según un ejemplo de ejecución;

la Figura 9 es un diagrama esquemático 5 de una interfaz de visualización de un dispositivo según un ejemplo de ejecución;

30 la Figura 10 es un diagrama esquemático 6 de una interfaz de visualización de un dispositivo según un ejemplo de ejecución;

35 la Figura 11A y la Figura 11B son el diagrama de flujo 3 de un método para poner en marcha un dispositivo según un ejemplo de ejecución;

la Figura 12 es un diagrama esquemático 1 de una secuencia temporal de funcionamiento de componentes de un dispositivo según un ejemplo de ejecución;

40 la Figura 13A y la Figura 13B son el diagrama de flujo 4 de un método para poner en marcha un dispositivo según un ejemplo de ejecución;

la Figura 14A y la Figura 14B son el diagrama de flujo 5 de un método para poner en marcha un dispositivo según un ejemplo de ejecución;

45 la Figura 15A y la Figura 15B son el diagrama de flujo 6 de un método para poner en marcha un dispositivo según una realización de la presente invención;

50 la Figura 16 es un diagrama esquemático de una secuencia de tiempo de configuración de GPIO según un ejemplo de ejecución;

la Figura 17A y la Figura 17B son el diagrama de flujo 7 de un método para poner en marcha un dispositivo según una realización de la presente invención;

55 la Figura 18 es un diagrama esquemático 2 de una secuencia de tiempo de funcionamiento de componentes de un dispositivo según un ejemplo de ejecución;

la Figura 19A y la Figura 19B son el diagrama de flujo 8 de un método para poner en marcha un dispositivo según una realización de la presente invención;

60 la Figura 20A y la Figura 20B son el diagrama de flujo 9 de un método para poner en marcha un dispositivo según un ejemplo de ejecución;

65 la Figura 21 es un diagrama esquemático 7 de una interfaz de visualización de un dispositivo según un ejemplo de ejecución;

la Figura 22 es un diagrama estructural esquemático 1 de un dispositivo según un ejemplo de ejecución;

la Figura 23 es un diagrama estructural esquemático 2 de un dispositivo según un ejemplo de ejecución;

5 la Figura 24 es un diagrama estructural esquemático 3 de un dispositivo según un ejemplo de ejecución;

la Figura 25 es un diagrama estructural esquemático 1 de una MCU según un ejemplo de ejecución;

la Figura 26 es un diagrama estructural esquemático 2 de una MCU según un ejemplo de ejecución;

10 la Figura 27 es un diagrama estructural esquemático 4 de un dispositivo según un ejemplo de ejecución;

la Figura 28 es un diagrama estructural esquemático de un teléfono móvil según un ejemplo de ejecución; y

15 la Figura 29 es un diagrama esquemático de una interfaz de visualización de un teléfono móvil según un ejemplo de ejecución;

Descripción de las realizaciones

20 En la memoria descriptiva y los dibujos adjuntos de esta solicitud, los términos “primero”, “segundo”, etc., pretenden distinguir entre objetos o procesamiento distintos en un mismo objeto, pero no pretenden indicar un orden específico de un objeto. Por ejemplo, una primera MCU y una segunda MCU son MCU distintas, y la primera duración preestablecida y la segunda duración preestablecida pueden ser períodos de tiempo o duraciones diferentes.

25 Puede aplicarse un método para poner en marcha un dispositivo proporcionado en esta solicitud a un proceso de puesta en marcha de un dispositivo e iniciar sesión en un sistema operativo después de que se pone en marcha el dispositivo. Según el método para poner en marcha un dispositivo, la autenticación de identidad de usuario puede hacerse simultáneamente cuando se pone en marcha el dispositivo, para iniciar sesión en el sistema operativo del dispositivo.

30 El dispositivo en esta solicitud incluye un botón de encendido y un sensor de huellas digitales (sensor), el botón de encendido está integrado con el sensor de huellas digitales y el sensor de huellas digitales está configurado para adquirir información de huellas digitales de un usuario.

35 Por ejemplo, los sensores de huellas digitales en esta solicitud pueden clasificarse en un sensor de huellas digitales óptico, un sensor semiconductor de capacitancia, un sensor semiconductor termosensible, un sensor semiconductor sensible a la presión, un sensor ultrasónico, un sensor de radiofrecuencia RF, o similares según un principio de detección (es decir, un principio y tecnología de formación de imágenes de huellas digitales). Esto no se limita en esta solicitud.

40 Por ejemplo, el dispositivo en esta aplicación puede ser un ordenador portátil (por ejemplo, un ordenador portátil 100 mostrado en la Figura 1A o la Figura 3), un teléfono móvil, un ordenador personal (ordenador personal, PC), un dispositivo electrónico llevable (por ejemplo, un reloj inteligente), un ordenador de tableta o similar. No se impone ninguna limitación especial a una forma específica del dispositivo en las siguientes realizaciones.

45 El sensor de huellas digitales puede estar integrado en una o más superficies, que el usuario puede tocar con el dedo, del botón de encendido. Por ejemplo, en esta solicitud, el dispositivo proporcionado en esta solicitud se describe utilizando un ejemplo en el que el dispositivo es el ordenador portátil 100 mostrado en la Figura 1A.

50 Como se muestra en la Figura 1A, el ordenador portátil 100 incluye un botón 101 de encendido y un sensor 102 de huellas digitales. El botón 101 de encendido está integrado con el sensor 102 de huellas digitales. La Figura 1B es un diagrama ampliado localmente del botón 101 de encendido del ordenador portátil 100 mostrado en la Figura 1A. Como se muestra en la Figura 1B, el sensor 102 de huellas digitales puede integrarse en una superficie superior del botón 101 de encendido.

55 Para distinguir entre el dispositivo proporcionado en esta solicitud y un dispositivo de la técnica anterior, en esta solicitud se proporcionan breves descripciones para un proceso de puesta en marcha e inicio de sesión en el sistema del ordenador portátil 100 mostrado en la Figura 1A y un proceso de puesta en marcha e inicio de sesión en el sistema de un ordenador portátil de la técnica anterior (por ejemplo, un ordenador portátil 200 mostrado en la Figura 2).

60 Como se muestra en la Figura 2, el ordenador portátil 200 de la técnica anterior también incluye un botón 201 de encendido y un sensor 202 de huellas digitales, pero el botón 201 de encendido y el sensor 202 de huellas digitales normalmente están dispuestos por separado, o el sensor 202 de huellas digitales puede integrarse además en un módulo 203 táctil del ordenador portátil 200.

65

Como se muestra en la Figura 2A, cuando un usuario pulsa el botón 201 de encendido del ordenador portátil 200, el ordenador portátil 201 puede responder a la operación de pulsado realizada por el usuario en el botón 201 de encendido, ponerse en marcha y mostrar una interfaz de inicio de sesión de sistema que se muestra en la Figura 2B y que incluye un icono 204 de cuenta de usuario y un cuadro 205 de entrada de contraseña de usuario, para que el usuario introduzca una contraseña de usuario o para que el usuario registre información de huellas digitales del usuario utilizando el sensor 202 de huellas digitales, para iniciar sesión en un sistema operativo del ordenador portátil 200.

Como se muestra en la Figura 2C, cuando un usuario toca el sensor 202 de huellas digitales del ordenador portátil 200, el sensor 202 de huellas digitales puede adquirir información de huellas digitales del usuario para realizar una autenticación de identidad de usuario e iniciar sesión en el sistema operativo del ordenador portátil 200; apareciendo un escritorio de sistema mostrado en la Figura 2D después de que la autenticación de identidad de usuario haya tenido éxito.

Puede entenderse que, en un proceso de puesta en marcha e inicio de sesión de sistema del ordenador portátil 200 mostrado en la Figura 2, el usuario necesita poner en marcha el ordenador portátil 200 presionando un botón una vez y, a continuación, inscribir la información de huellas digitales utilizando el sensor 202 de huellas digitales, para realizar autenticación de identidad de usuario e iniciar sesión en el sistema operativo del ordenador portátil 200.

La Figura 3 es un diagrama esquemático de un ejemplo de proceso de puesta en marcha e inicio de sesión del sistema del ordenador portátil 100 mostrado en la Figura 1A.

Un usuario puede pulsar el botón 101 de encendido del ordenador portátil 100 para controlar la puesta en marcha del ordenador portátil 100. Por lo tanto, como se muestra en la Figura 3A, cuando el usuario pulsa el botón 101 de encendido del ordenador portátil 100, un dedo del usuario toca definitivamente el botón 101 de encendido. Cuando el dedo del usuario toca el botón 101 de encendido, el sensor 102 de huellas digitales integrado en el botón 101 de encendido puede adquirir información de huellas digitales del usuario que toca el botón 101 de encendido.

Por lo tanto, el ordenador portátil 100 puede iniciarse en respuesta a la operación de presión realizada por el usuario en el botón 101 de encendido, y realizar directamente autenticación de identidad de usuario utilizando la información de huellas digitales adquirida por el sensor 102 de huellas digitales, para iniciar sesión en el sistema operativo del ordenador portátil 100; y, después de que la autenticación de identidad de usuario haya tenido éxito, muestra el escritorio de sistema mostrado en la Figura 3B.

Puede entenderse que, en un proceso de puesta en marcha e inicio de sesión de sistema del ordenador portátil 100 mostrado en la Figura 3, la puesta en marcha del ordenador portátil 100 y la autenticación de identidad de usuario pueden ejecutarse a través de una operación de puesta en marcha del usuario con un solo botón, es decir, la autenticación de identidad de usuario puede realizarse simultáneamente cuando se pone en marcha el ordenador portátil 100, para iniciar sesión en el sistema operativo del ordenador portátil 100. Esto puede reducir la duración requerida para la puesta en marcha y el inicio de sesión de sistema del ordenador portátil 100 y mejorar la eficiencia de puesta en marcha del ordenador portátil 100 y la eficiencia del inicio de sesión de sistema.

Todos los métodos en las siguientes realizaciones pueden realizarse mediante el ordenador portátil 100.

Esta solicitud proporciona un método para poner en marcha un dispositivo. El dispositivo puede incluir un botón de encendido y un sensor de huellas digitales, estando integrado el botón de encendido en el sensor de huellas digitales, y el método para poner en marcha un dispositivo puede aplicarse a un proceso en el que un usuario presione el botón de encendido para poner en marcha el dispositivo. Como se muestra en la Figura 4, el método para poner en marcha un dispositivo puede incluir S401 y S402.

S401. El dispositivo obtiene la información de las huellas digitales adquirida por el sensor de huellas digitales y guarda la información de huellas digitales obtenida.

En el proceso en el que el usuario pulsa el botón de encendido para poner en marcha el dispositivo, un dedo del usuario puede tocar el botón de encendido. Cuando el dedo del usuario toca el botón de encendido, el sensor de huellas digitales integrado en el botón de encendido puede adquirir información de huellas digitales del usuario.

El dispositivo puede obtener la información de huellas digitales adquirida por el sensor de huellas digitales y, a continuación, guardar la información de huellas digitales, de modo que cuando un usuario pulsa el botón de encendido para controlar la puesta en marcha del dispositivo, puede realizarse la autenticación de huellas digitales, es decir, la autenticación de identidad de usuario, utilizando la información de huellas digitales, para iniciar sesión en un sistema operativo. El dispositivo puede cifrar la información de huellas digitales y guardar temporalmente la información de huellas digitales cifrada, de modo que la información de huellas digitales pueda proporcionarse para realizar autenticación de huella digital, para iniciar sesión en el sistema operativo del dispositivo.

S402. El dispositivo proporciona la información de huellas digitales para realizar autenticación de huella digital, para iniciar sesión en un sistema operativo del dispositivo.

Quando se detecta que se pulsa el botón de encendido, el dispositivo puede activar el encendido de una unidad central de procesamiento (Unidad Central de Procesamiento, CPU) del dispositivo, reactivar el sistema operativo del dispositivo, a continuación, cargar un controlador de huellas digitales y, a continuación, proporcionar la información de huellas digitales al controlador de huellas digitales, y el controlador de huellas digitales utiliza la información de huellas digitales para realizar la autenticación de huellas digitales, e iniciar sesión en el sistema operativo.

De forma alternativa, cuando se detecta que se pulsa el botón de encendido, el dispositivo puede obtener una solicitud de autenticación de huellas digitales enviada por el controlador de huellas digitales. Después de obtener la solicitud de autenticación de huellas digitales, el dispositivo puede proporcionar la información de huellas digitales para realizar autenticación de huellas digitales para iniciar sesión en el sistema operativo. El controlador de huellas digitales en esta solicitud puede utilizarse como componente del sistema operativo.

Según el método para poner en marcha un dispositivo proporcionado en esta solicitud, el botón de encendido está integrado con el sensor de huellas digitales. Por lo tanto, en el proceso en el que el usuario pulsa el botón de encendido para poner en marcha el dispositivo, el sensor de huellas digitales puede adquirir la información de huellas digitales del usuario cuando el usuario toca el botón de encendido, y el dispositivo puede obtener la información de huellas digitales adquirida por el sensor de huella digital y guardar la información de huellas digitales. De este modo, después de que se pone en marcha el dispositivo, la información de huellas digitales guardada en el dispositivo puede utilizarse para realizar la autenticación de identidad de usuario, y el usuario no necesita tocar el botón de encendido nuevamente para inscribir la información de huellas digitales del usuario para la autenticación de identidad de usuario.

En una primera situación de aplicación, se proporcionan descripciones para un proceso de puesta en marcha e inicio de sesión de sistema realizado cuando un dispositivo (por ejemplo, un ordenador portátil 100) se enciende por primera vez.

Antes de la entrega del ordenador portátil 100, todos los componentes (incluyendo un sensor 102 de huellas digitales) del ordenador portátil 100 están en un estado apagado. Después de la entrega del ordenador portátil 100, cuando un usuario utiliza el ordenador portátil 100 por primera vez, el usuario puede pulsar un botón 101 de encendido del ordenador portátil 100 para controlar que el ordenador portátil 100 se encienda por primera vez, para poner en marcha el ordenador portátil 100. Además, después de que el usuario pulsa el botón de encendido, el sensor 102 de huellas digitales integrado con el botón 101 de encendido puede encenderse y puede adquirir información de huellas digitales del usuario que toca el botón 101 de encendido, de modo que después de que se ponga en marcha el ordenador 100, la información de huellas digitales adquirida por el sensor 102 de huellas digitales puede utilizarse para realizar autenticación de identidad de usuario, para iniciar sesión en un sistema operativo del ordenador portátil 100. Específicamente, como se muestra en la Figura 5A y la Figura 5B, un método para poner en marcha un dispositivo proporcionado en esta solicitud puede incluir las siguientes etapas.

S500. Se pulsa un botón de encendido de un dispositivo.

Quando se pulsa el botón de encendido del dispositivo, puede activarse el encendido y la inicialización de un sensor de huellas digitales integrado en el botón de encendido, y, después de que se completa la inicialización, se comienza a adquirir la información de huellas digitales de un usuario, es decir, S501, y se realiza el procedimiento del método posterior del mismo. Además, cuando se pulsa el botón de encendido del dispositivo, puede activarse además el encendido de una segunda MCU. La segunda MCU activa el encendido de una CPU del dispositivo y reactiva el sistema operativo del dispositivo, es decir, se llevan a cabo S601 y un procedimiento de método posterior.

S501. Se enciende e inicializa un sensor de huellas digitales integrado en el botón de encendido del dispositivo.

Después de completar la inicialización, el sensor de huellas digitales puede adquirir la información de las huellas digitales del usuario que toca el botón de encendido.

S502. El sensor de huellas digitales adquiere información de huellas digitales de un usuario.

Quando el usuario pulsa el botón de encendido del dispositivo, un dedo del usuario toca el botón de encendido. En este caso, el sensor de huellas digitales integrado con el botón de encendido puede detectar que el usuario está tocando el sensor de huellas digitales y adquirir la información de huellas digitales del usuario.

Por ejemplo, como se muestra en la Figura 3A, cuando el usuario pulsa el botón 101 de encendido del ordenador portátil 100, el dedo del usuario toca definitivamente el botón 101 de encendido. En este caso, el sensor 102 de huellas digitales puede adquirir la información de las huellas digitales del usuario que toca el botón 101 de encendido.

Puede entenderse que, en el primer escenario de aplicación, si el usuario toca por error el botón de encendido del dispositivo, pero no pulsa el botón de encendido, no puede adquirirse la información de huellas digitales del usuario porque el sensor de huellas digitales no está encendido. La información de huellas digitales en esta aplicación puede ser una imagen de la huella digital.

S503. El sensor de huellas digitales envía una indicación de reactivación a una primera MCU.

Si el sensor de huellas digitales adquiere la información de las huellas digitales del usuario, indica que el usuario puede necesitar poner en marcha el dispositivo. En este caso, el sensor de huellas digitales puede activar la primera MCU, para que la primera MCU pueda comenzar a funcionar.

S504. La primera MCU recibe la indicación de reactivación enviada por el sensor de huellas digitales.

S505. La primera MCU obtiene la información de las huellas digitales adquirida por el sensor de huellas digitales y guarda la información de huellas digitales obtenida.

Después de recibir la indicación de reactivación enviada por el sensor de huellas digitales, la primera MCU puede entrar en un estado de funcionamiento y puede obtener la información de huellas digitales adquirida por el sensor de huellas digitales, de modo que cuando se reciba una solicitud de inscripción de huellas digitales o una solicitud de autenticación de huellas digitales enviada por el controlador de huellas digitales, la primera MCU puede enviar la información de huellas digitales al controlador de huellas digitales para realizar la autenticación de identidad de usuario.

S601. Se enciende la segunda MCU.

La segunda MCU en esta aplicación puede ser la MCU de firmware de sistema del dispositivo. La segunda MCU puede configurarse para: activar el encendido de una CPU del dispositivo después de pulsar el botón de encendido y reactivar el sistema operativo del dispositivo. El firmware de sistema del dispositivo puede incluir un sistema básico de entrada/salida (Sistema Básico de Entrada y Salida, BIOS)/un controlador integrado (Controlador Integrado, EC) del dispositivo.

S602. La segunda MCU activa el encendido de una CPU del dispositivo y reactiva un sistema operativo del dispositivo.

S603. Después de que se reactiva el sistema operativo del dispositivo, se inicializa y carga un controlador de huellas digitales del dispositivo.

Normalmente, cuando el dispositivo se inicia por primera vez después de la entrega, es posible que no se introduzca ninguna contraseña de inicio de sesión (por ejemplo, información de huellas digitales del usuario) del sistema operativo en el dispositivo. Por lo tanto, después de que se reactiva el sistema operativo, puede iniciarse sesión directamente en un escritorio de sistema. Es decir, después de S603, el método en esta solicitud puede incluir además S604:

S604. El sistema operativo inicia sesión en un escritorio de sistema operativo.

Por ejemplo, como se muestra en la Figura 6A, cuando un usuario pulsa el botón 101 de encendido del ordenador portátil 100 (es decir, realiza S500), el ordenador portátil 100 puede responder a la operación de pulsar realizada por el usuario en el botón 101 de encendido, y poner en marcha. Esta es la primera vez que el ordenador portátil 100 se pone en marcha después de la entrega del ordenador portátil 100, y no se introduce ninguna contraseña de inicio de sesión (por ejemplo, información de huellas digitales de usuario) para entrar al sistema operativo en el ordenador portátil 100. Por lo tanto, después de que se enciende la CPU y se reactive el sistema operativo del dispositivo, puede mostrarse directamente un escritorio de sistema operativo como se muestra en la Figura 6B.

Además, para mejorar la seguridad de la información durante el uso de un dispositivo y reducir la posibilidad de revelar información guardada en el dispositivo, después de cargar un escritorio de sistema, el dispositivo puede mostrar, además, en el escritorio de sistema, una ventana de aviso utilizada para dar instrucción al usuario que inscriba información de huellas digitales. Por ejemplo, después de iniciar sesión en el escritorio de sistema, el dispositivo puede mostrar, en el escritorio de sistema, una ventana 601 de inscripción de huellas digitales de "iniciar sesión con un solo botón" mostrada en la Figura 7A. Específicamente, después de S604, el método en esta solicitud puede incluir además S605:

S605. El sistema operativo muestra una ventana de inscripción de huellas digitales en el escritorio del sistema operativo.

Por ejemplo, después de que se muestra el escritorio de sistema operativo mostrado en la Figura 6B durante un periodo de tiempo, el ordenador portátil 100 puede mostrar, en el escritorio de sistema operativo, la ventana 610 de inscripción de huellas digitales mostrada en la Figura 7A. Como se muestra en la Figura 7A, la ventana 610 de inscripción de huellas digitales puede incluir una "lista de funciones de huellas digitales" 611 y una "lista de huellas digitales" 614. La "lista de funciones de huellas digitales" 611 puede incluir al menos una opción de uso de huellas digitales y un conmutador de opción de la misma. Por ejemplo, la "lista de funciones de huellas digitales" 611 puede incluir una opción de "inicio de sesión en el sistema operativo" y un conmutador 612 de opción de la misma y una opción de "puesta en marcha e inicio de sesión con un solo botón" y un conmutador de opción 613 de la misma. La "lista de huellas digitales" 614 puede incluir una opción 615 de "añadir huella digital".

El usuario puede activar el conmutador de la opción de uso de huellas digitales correspondiente en la “lista de funciones de huellas digitales” 611 para especificar el uso de información de huellas digitales añadida posteriormente. Por ejemplo, como se muestra en la Figura 7A, el conmutador de opción 613 de la opción “puesta en marcha e inicio de sesión con un solo botón” en la “lista de funciones de huellas digitales” 611 está en un estado activado, y otros conmutadores de opciones en otra “lista de funciones de huellas digitales” 611 están en un estado desactivado. Por lo tanto, como se muestra en la Figura 7A, cuando el usuario controla un cursor 620 para moverse a la opción 615 “añadir huella digital”, hace clic en la opción 615 “añadir huella digital” y realiza una operación de inscripción de huellas digitales posterior, la información de huellas digitales registrada puede utilizarse para realizar “puesta en marcha e inicio de sesión con un solo botón” del ordenador portátil 100.

S606. El sistema operativo envía una solicitud de inscripción de huellas digitales al controlador de huellas digitales en respuesta a un comando de entrada del usuario en la ventana de inscripción de huellas digitales.

La solicitud de inscripción de huellas digitales se utiliza para dar instrucción al controlador de huellas digitales que obtenga la información de huellas digitales adquirida por el sensor de huellas digitales.

S607. Después de recibir la solicitud de inscripción de huellas digitales, el controlador de huellas digitales envía la solicitud de inscripción de huellas digitales a la primera MCU.

Puede entenderse que, como se describe en S501 a S505, después de inicializarse y encenderse, el sensor de huellas digitales puede adquirir la información de huellas digitales del usuario que toca el botón de encendido y reactivar la primera MCU, y la primera MCU obtiene y guarda la información de huellas digitales adquirida por el sensor de huellas digitales. Por lo tanto, el controlador de huellas digitales puede enviar el controlador de huellas digitales a la primera MCU, para obtener, desde la primera MCU, la información de huellas digitales adquirida por el sensor de huellas digitales.

S608. La primera MCU recibe la solicitud de inscripción de huellas digitales enviada por el controlador de huellas digitales.

S609. La primera MCU envía, al controlador de huellas digitales, la información de huellas digitales guardada por la primera MCU.

S610. El controlador de huellas digitales recibe la información de huellas digitales y guarda la información de huellas digitales recibida en un área de almacenamiento preestablecida.

Por ejemplo, como se muestra en la Figura 7A, después de que el usuario controla el cursor 620 para moverse a la opción “añadir huella digital” 615 y hace clic en la opción “añadir huella digital” 615, el sistema operativo puede enviar una solicitud de inscripción de huellas digitales al controlador de huellas digitales (es decir, realizar S606), y se muestra la primera información de aviso 630 en la ventana 610 de inscripción de huellas digitales mostrada en la Figura 7B. Por ejemplo, la primera información 630 de aviso puede consistir en caracteres de aviso que incluyen “Utilizar una huella digital en lugar de una contraseña para establecer la ‘puesta en marcha e inicio de sesión con un solo botón’ y ‘Primero, poner el pulgar u otro dedo en el en el botón de encendido’”. A continuación, como se muestra en la Figura 8A, después de que un dedo de un usuario toca el “botón de encendido” 101, el sensor 102 de huellas digitales puede adquirir información de huellas digitales del usuario, y la primera MCU también puede obtener y guardar la información de huellas digitales adquirida por el sensor 102 de huellas digitales, es decir, realizar S502 a S505. Además, después de recibir la solicitud de inscripción de huellas digitales, el controlador de huellas digitales puede obtener, desde la primera MCU, la información de huellas digitales adquirida por el sensor 102 de huellas digitales (es decir, realizar S606 a S609).

Puede entenderse que, en el proceso de inscripción de huellas digitales anterior, la primera MCU puede no guardar la información de huellas digitales, pero después de recibir la solicitud de inscripción de huellas digitales enviada por el controlador de huellas digitales, obtiene la información de huellas digitales adquirida por el sensor de huellas digitales y envía directamente la información de huellas digitales obtenida al controlador de huellas digitales. Es decir, en el proceso de registro de huellas digitales, S505 puede ser sustituida por S505'.

S505'. La primera MCU obtiene la información de huellas digitales adquirida por el sensor de huellas digitales.

Por ejemplo, como se muestra en la Figura 8A, después de que el dedo del usuario toca el “botón de encendido” 101, el sistema operativo puede mostrar una segunda información 640 de aviso y una ventana 650 de llenado de huellas digitales en la ventana 610 de inscripción de huellas digitales mostrada en la Figura 8B. Por ejemplo, como se muestra en la Figura 8B, la segunda información 640 de aviso puede consistir en caracteres de aviso que incluyen “Ponga un dedo en el 'botón de encendido', a continuación, aleje el dedo y repita las operaciones”.

Cabe señalar que, en un proceso de repetición, por el usuario, de la acción “Ponga un dedo en el 'botón de encendido', a continuación, aleje el dedo” basada en un aviso de la segunda información 640 de aviso, puede mostrarse una

imagen dinámica de llenado gradual de líneas de huellas digitales en la ventana 650 de llenado de huellas digitales en la ventana 650 de llenado de huellas digitales.

Después de que el controlador de huellas digitales recibe la información de huellas digitales enviada por la primera MCU y guarda la información de huellas digitales recibida en un área de almacenamiento preestablecida, el sistema operativo puede mostrar la ventana 610 de inscripción de huellas digitales mostrada en la Figura 9. En este caso, pueden mostrarse la tercera información 660 de aviso y la ventana 650 de llenado de huellas digitales llena de líneas de huellas digitales en la ventana 610 de inscripción de huellas digitales. Por ejemplo, como se muestra en la Figura 9, la tercera información 660 de aviso puede consistir en caracteres de aviso que incluyen "La huella digital ha sido inscrita, y puede ejecutar la ' puesta en marcha e inicio de sesión con un solo botón' del dispositivo utilizando únicamente la huella digital inscrita".

Además, dentro de un período de tiempo especificado después de que se inscriba la huella digital, es decir, dentro del período de tiempo especificado después de que se muestre la ventana 610 de inscripción de huellas digitales mostrada en la Figura 9, el sistema operativo puede mostrar una ventana 610 de inscripción de huellas digitales mostrada en la Figura 10. En comparación con la "lista de huellas digitales" 614 de la ventana 610 de inscripción de huellas digitales mostrada en la Figura 7A, se añade una "huella digital 1" 616 a la "lista de huellas digitales" 614 de la ventana 610 de inscripción de huellas digitales mostrada en la Figura 10. La "huella digital 1" 616 puede utilizarse para ejecutar "puesta en marcha e inicio de sesión con un solo botón" del dispositivo.

Puede entenderse que, el usuario puede inscribir información de huellas digitales de distintos dedos en el ordenador portátil 100 de la forma anterior de inscripción de huellas digitales, de modo que los diferentes dedos puedan utilizarse para pulsar el botón de encendido del ordenador portátil 100, para ejecutar "una puesta en marcha e inicio de sesión con un solo botón" del ordenador portátil 100.

En algunos casos, después de que la primera MCU guarda la información de huellas digitales, es posible que el sistema operativo no pueda enviar una solicitud de autenticación de huella digital al controlador de huellas digitales debido a un fallo del sistema u otra causa del dispositivo. Por lo tanto, el controlador de huellas digitales no puede enviar la solicitud de autenticación de huellas digitales a la primera MCU a tiempo. De forma alternativa, el sistema operativo envía una solicitud de autenticación de huellas digitales al controlador de huellas digitales a tiempo, pero el controlador de huellas digitales no envía la solicitud de autenticación de huellas digitales a la primera MCU a tiempo. En este caso, el dispositivo no puede iniciar sesión en el escritorio de sistema operativo a tiempo. Debido a que el dispositivo no puede iniciar sesión en el escritorio de sistema operativo a tiempo, un usuario normal puede dejar el dispositivo durante un período de tiempo. En el período de tiempo posterior a la salida del usuario normal, se corre el riesgo de que la información de huellas digitales guardada en la primera MCU sea sustraída por un usuario malintencionado para realizar la autenticación de identidad de usuario e iniciar sesión en el sistema operativo, existiendo además un riesgo de sustracción malintencionada de información guardada en el dispositivo. Para garantizar seguridad de información del dispositivo, la primera MCU puede eliminar la información de huellas digitales guardada por la primera MCU. Específicamente, como se muestra en la Figura 11B, después de S505, el método en esta solicitud puede incluir además S1101.

S1101. La primera MCU elimina la información de huellas digitales si la primera MCU no recibe la solicitud de autenticación de huellas digitales o la solicitud de inscripción de huellas digitales dentro de la segunda duración preestablecida que comienza a partir de guardar la información de huellas digitales por la primera MCU.

Por ejemplo, en una primera situación de aplicación, como se muestra en la Figura 12, en un punto temporal t1, se pulsa el botón de encendido del dispositivo y, en este caso, una pantalla del dispositivo cambia de un estado de pantalla apagada a un estado de pantalla encendida, y el sensor de huellas digitales se enciende e inicializa; se alcanza un punto temporal t2 cuando transcurre la duración T1 después del punto temporal t1, y en el punto temporal t2, se completa la inicialización del sensor de huellas digitales, comienza a adquirirse la información de huellas digitales del usuario y se reactiva la primera MCU; y la primera MCU obtiene la información de las huellas digitales del sensor de huellas digitales y guarda la información de huellas digitales. Se alcanza un punto temporal t3 cuando la duración T2 (es decir, la segunda duración preestablecida) transcurre después del punto temporal t2 (un punto temporal en el que la primera MCU guarda la información de huellas digitales). Dentro del periodo de tiempo desde el punto temporal t2 hasta el punto temporal t3, la primera MCU puede eliminar la información de huellas digitales si la primera MCU no recibe la solicitud de autenticación de huellas digitales o la solicitud de inscripción de huellas digitales.

Por ejemplo, la segunda duración preestablecida en esta aplicación puede ser la duración (por ejemplo, duración t) requerida desde que se pulsa el botón de encendido del dispositivo hasta completar la carga del controlador de huellas digitales del dispositivo, o la segunda duración preestablecida puede ser ligeramente mayor que la duración t, por ejemplo, la segunda duración preestablecida puede ser 40 segundos más larga que la duración t. Por ejemplo, la segunda duración preestablecida puede ser dos minutos o tres minutos. Ciertamente, la segunda duración preestablecida puede ser, de forma alternativa, otra duración, y esto no está limitado en esta solicitud.

En esta solicitud, si la primera MCU no recibe la solicitud de autenticación de huellas digitales dentro de la segunda duración preestablecida que empieza con guardar la primera MCU la información de huellas digitales, la primera MCU

puede eliminar la información de huellas digitales guardada por la primera MCU. Esto puede evitar que un usuario malintencionado utilice la información de huellas digitales para realizar la autenticación de identidad de usuario y sustraiga información guardada en el dispositivo cuando el usuario normal deje el dispositivo porque el dispositivo no puede iniciar sesión en el escritorio de sistema operativo a tiempo.

Opcionalmente, después de inicializar y cargar el controlador de huellas digitales, el sistema operativo puede enviar además la solicitud de autenticación de huellas digitales al controlador de huellas digitales, y el controlador de huellas digitales obtiene la información de huellas digitales de la primera MCU, para realizar la autenticación de huellas digitales e iniciar sesión en el sistema operativo. Sin embargo, esta es la primera vez para iniciar sesión en el sistema operativo después de que se enciende el dispositivo por primera vez y no se inscribe ninguna información de huellas digitales utilizada para realizar la autenticación de huellas digitales en el controlador de huellas digitales. Por lo tanto, el controlador de huellas digitales no puede realizar la autenticación de huellas digitales o un resultado de la autenticación de huellas digitales indica que la autenticación de huellas digitales falla. En este caso, el sistema operativo puede iniciar sesión directamente en el escritorio de sistema operativo y mostrar una ventana de inscripción de huellas digitales en el escritorio de sistema operativo, para instruir al usuario para que inscriba la información de huellas digitales. Específicamente, después de S603 y antes de S605, el método en esta solicitud puede incluir además S1301.

Por ejemplo, como se muestra en la Figura 13A y en la Figura 13B, después de S603 y antes de S605 mostrados en la Figura 11, el método de esta solicitud puede incluir además S1301 a S1308. Para descripciones detalladas de las etapas del método mostradas en la Figura 13A y Figura 13B, consúltense las descripciones detalladas de las etapas del método correspondientes en la Figura 11 en esta solicitud, los detalles no se describirán otra vez en esta solicitud.

S1301. El sistema operativo envía una solicitud de autenticación de huellas digitales al controlador de huellas digitales.

S1302. El controlador de huellas digitales recibe la solicitud de autenticación de huellas digitales enviada por el sistema operativo.

S1303. El controlador de huellas digitales envía la solicitud de autenticación de huellas digitales a la primera MCU.

S1304. La primera MCU recibe la solicitud de autenticación de huellas digitales enviada por el controlador de huellas digitales.

S 1305. La primera MCU envía la información de huellas digitales al controlador de huellas digitales.

S1306. El controlador de huellas digitales recibe la información de huellas digitales y realiza la autenticación de huellas digitales para obtener un resultado de autenticación.

Es la primera vez que inicia sesión en el sistema operativo después de que se enciende el dispositivo por primera vez y no se inscribe ninguna información de huellas digitales utilizada para realizar la autenticación de huellas digitales en el controlador de huellas digitales. Por lo tanto, el controlador de huellas digitales no puede realizar la autenticación de huellas digitales o un resultado de la autenticación de huellas digitales indica que la autenticación de huellas digitales falla.

S 1307. El controlador de huellas digitales envía el resultado de autenticación al sistema operativo.

S1308. El sistema operativo determina, basándose en el resultado de la autenticación, si la autenticación de huellas digitales tiene éxito.

En una primera situación de aplicación, si falla la autenticación de huellas digitales, se puede continuar realizando S605 a S610.

En esta solicitud, el botón de encendido está integrado con el sensor de huellas digitales. Por lo tanto, en el proceso en el que el usuario pulsa el botón de encendido para encender y poner en marcha el dispositivo por primera vez, el sensor de huellas digitales puede encenderse e inicializarse cuando el usuario pulsa el botón de encendido, adquirir la información de huellas digitales del usuario después de que se ha completado la inicialización y reactivar la primera MCU para guardar la información de huellas digitales. Así, después de que se pone en marcha el dispositivo, la información de huellas digitales guardada por la primera MCU puede utilizarse para realizar la autenticación de identidad de usuario, y el usuario no necesita tocar el botón de encendido nuevamente para inscribir la información de huellas digitales del usuario para la autenticación de identidad de usuario.

Además, en el proceso de inicio de sesión del sistema operativo después de encender el dispositivo por primera vez, el sistema operativo puede mostrar una ventana de inscripción de huellas digitales cuando falla la autenticación de huellas digitales, para instruir al usuario para que inscriba la información de huellas digitales utilizada para ejecutar la “puesta en marcha e inicio de sesión con un solo botón” del dispositivo. En este caso, la información de huellas digitales registrada por el usuario puede utilizarse posteriormente para ejecutar la “puesta en marcha e inicio de sesión

con un solo botón” del dispositivo, es decir, el usuario realiza la puesta en marcha y la autenticación de identidad del usuario realizando una operación de puesta en marcha con un solo botón. Esto puede reducir las operaciones de usuario y la duración requeridas para la puesta en marcha del dispositivo y el inicio de sesión de sistema, y mejorar la eficiencia de la puesta en marcha del dispositivo y el inicio de sesión de sistema.

Además, para mejorar la seguridad de la información de huellas digitales y evitar que se sustraiga la información de huellas digitales, la primera MCU puede cifrar la información de huellas digitales adquirida por el sensor de huellas digitales y guardar la información de huellas digitales cifrada. La primera MCU puede cifrar la información de huellas digitales utilizando una contraseña de cifrado preestablecida por el usuario, o la primera MCU puede cifrar la información de huellas digitales utilizando una contraseña de cifrado negociada con el controlador de huellas digitales.

Después de cargarse, el controlador de huellas digitales puede negociar con la primera MCU la contraseña de cifrado de la información de huellas digitales. Específicamente, antes de S606 y S1301, el método en esta solicitud puede incluir, además: enviar, mediante el controlador de huellas digitales, un mensaje de solicitud de contraseña a la primera MCU; enviar, por la primera MCU, un mensaje de respuesta de contraseña que lleva una contraseña de cifrado al controlador de huellas digitales después de recibir el mensaje de solicitud de contraseña enviado por el controlador de huellas digitales; y recibir y guardar, mediante el controlador de huellas digitales, la contraseña de cifrado.

Puede entenderse que, la primera MCU puede cifrar, utilizando la contraseña de cifrado, la información de huellas digitales obtenida del sensor de huellas digitales. Además, la información de huellas digitales enviada por la primera MCU al controlador de huellas digitales es la información de huellas digitales cifrada utilizando la contraseña de cifrado. El controlador de huellas digitales puede descifrar, utilizando la contraseña de cifrado guardada por el controlador de huellas digitales, la información de huellas digitales cifrada recibida por el controlador de huellas digitales.

De forma alternativa, el controlador de huellas digitales y la primera MCU pueden utilizar un algoritmo de cifrado asimétrico para cifrar y descifrar la información de huellas digitales. Por ejemplo, el controlador de huellas digitales puede enviar una clave pública (clave pública) a la primera MCU, para dar instrucción a la primera MCU que cifre la información de huellas digitales utilizando la clave pública, y el controlador de huellas digitales puede utilizar una clave privada (clave privada) correspondiente a la clave pública para descifrar la información de huellas digitales cifrada utilizando la clave pública.

En un segundo escenario de aplicación de esta solicitud, después de que el dispositivo (por ejemplo, un ordenador portátil 100) se enciende por primera vez para iniciar sesión en el sistema operativo, se proporcionan descripciones para el proceso de puesta en marcha y de inicio de sesión en el sistema del dispositivo.

En el segundo escenario de aplicación, se utiliza como ejemplo el dispositivo que es el ordenador portátil 100. Debido a que el sensor 102 de huellas digitales del ordenador portátil 100 se ha encendido e inicializado, incluso si el ordenador portátil 100 está inactivo, el sensor 102 de huellas digitales aún puede adquirir la información de huellas digitales del usuario que toca el botón 101 de encendido.

Además, como se muestra en la Figura 14A, en un ejemplo de ejecución, cuando un dedo del usuario toca el sensor 102 de huellas digitales, el sensor 102 de huellas digitales puede adquirir la información de huellas digitales del usuario (es decir, realizar S502 a S505). Es decir, en el segundo escenario de aplicación de esta solicitud, es posible que no se realice S501.

En el segundo escenario de aplicación, una segunda MCU del dispositivo también completa la inicialización y se enciende. Por lo tanto, la segunda MCU puede detectar, en tiempo real, si se pulsa el botón de encendido del dispositivo. Es decir, como se muestra en la Figura 14A y Figura 14B, el método en esta solicitud puede incluir además S1401 y un procedimiento de método posterior.

S1401. La segunda MCU detecta si se pulsa el botón de encendido del dispositivo.

Si el usuario desea poner en marcha el dispositivo, el usuario puede pulsar el botón de encendido del dispositivo dentro de un corto período de tiempo (por ejemplo, de 1 a 3 segundos) que transcurre después de que un dedo del usuario toca el botón de encendido.

S1402. La segunda MCU determina si el dispositivo está en modo en reposo o en modo inactivo.

En muchos casos, el usuario pulsa el botón de encendido. Por ejemplo, el usuario puede pulsar el botón de encendido cuando controla la puesta en marcha del dispositivo, o el usuario puede pulsar el botón de encendido cuando controla el apagado del dispositivo. Para evitar realizar el método en esta solicitud en otro escenario distinto del escenario en que el usuario controla la puesta en marcha del dispositivo, la segunda MCU puede activar el encendido de la CPU del dispositivo únicamente cuando detecta que se pulsa el botón de encendido y determinar que el dispositivo está en el modo en reposo o en el modo inactivo y reactivar el sistema operativo del dispositivo.

Específicamente, cuando el dispositivo está en modo en reposo o modo inactivo, puede seguirse llevar a cabo la S602. Es decir, en el segundo escenario de aplicación de esta solicitud, puede omitirse S601. Además, la inicialización del controlador de huellas digitales del dispositivo se completó cuando el dispositivo se encendió por primera vez. Por lo tanto, en el segundo escenario de aplicación de esta aplicación, después de realizar S602, el controlador de huellas digitales puede cargarse directamente y no es necesario inicializar el controlador de huellas digitales. Es decir, como se muestra en la Figura 14A, S603 podrá reemplazarse por S603':

S603'. Cargar el controlador de huellas digitales después de que se reactive el sistema operativo.

En el segundo escenario de aplicación, la información de huellas digitales utilizada para realizar la autenticación de huellas digitales para ejecutar la "puesta en marcha e inicio de sesión con un solo botón" puede haberse inscrito en el dispositivo. Por lo tanto, el sistema operativo no puede iniciar sesión directamente en el escritorio de sistema operativo (es decir, realizar S604) sin la autenticación de huellas digitales. En este caso, después de realizar S603', el sistema operativo puede enviar directamente una solicitud de autenticación de huellas digitales al controlador de huellas digitales, es decir, después de realizar S603', pueden realizarse S1301 a S1308. Para descripciones detalladas de S1301 a S1308 en la Figura 14A y Figura 14B, consúltense las descripciones detalladas de S1301 a S1308 en el escenario de aplicación anterior, los detalles no se describirán de nuevo en esta solicitud.

Una diferencia radica en que, en el segundo escenario de aplicación, después de S1308, si el resultado de la autenticación indica que la autenticación de huellas digitales tiene éxito, indica que la autenticación de identidad de usuario tiene éxito y, en este caso, puede seguirse realizando S1403; o, si el resultado de la autenticación indica que la autenticación de huellas digitales tiene éxito, indica que la autenticación de identidad de usuario falla. En este caso, en vez de iniciar sesión directamente en el sistema operativo para mostrar el escritorio de sistema operativo, el usuario necesita volver a introducir un nombre de usuario y una contraseña o necesita volver a inscribir información de huellas digitales para realizar de nuevo la autenticación de identidad de usuario y, en este caso, puede seguirse realizando S1404.

S1403. Iniciar sesión en el sistema operativo y mostrar un escritorio de sistema operativo.

S1404. El sistema operativo muestra una interfaz de inicio de sesión de sistema operativo.

Además, si el resultado de la autenticación indica que la autenticación de huellas digitales falla, el sistema operativo puede mostrar, además, en la interfaz de inicio de sesión del sistema operativo, información de indicación que indica un fallo de inicio de sesión.

Por ejemplo, cuando el resultado de la autenticación indica que la autenticación de huellas digitales falla, el sistema operativo puede mostrar la interfaz de inicio de sesión de sistema operativo mostrada en la Figura 2B.

Según el método para poner en marcha un dispositivo proporcionado en esta solicitud, cuando el usuario toca el sensor de huellas digitales integrado en el botón de encendido del dispositivo, el sensor de huellas digitales puede adquirir la información de huellas digitales del usuario y reactivar la primera MCU para obtener y guardar la información de huellas digitales adquirida, y después de que el usuario pulsa el botón de encendido del dispositivo para controlar la puesta en marcha del dispositivo, la información de huellas digitales guardada por la primera MCU puede utilizarse para realizar la autenticación de identidad de usuario. Después de que el usuario pulsa el botón de encendido para controlar la puesta en marcha del dispositivo y se muestra la interfaz de inicio de sesión del sistema operativo del dispositivo, el usuario no necesita volver a inscribir la información de huellas digitales del usuario para realizar la autenticación de identidad de usuario. Es decir, en esta solución, la autenticación de identidad de usuario puede realizarse simultáneamente cuando se pone en marcha el dispositivo, para iniciar sesión en el sistema operativo del dispositivo. Es decir, la autenticación de puesta en marcha y de identidad de usuario puede ejecutarse realizando una operación de puesta en marcha con un solo botón por el usuario. Esto puede reducir las operaciones de usuario y la duración requeridas para la puesta en marcha del dispositivo y el inicio de sesión de sistema, y mejorar la eficiencia de la puesta en marcha del dispositivo y el inicio de sesión de sistema.

Puede entenderse que, en el segundo escenario de aplicación, cuando el usuario toca por error el botón de encendido del dispositivo, el sensor de huellas digitales también puede adquirir la información de huellas digitales del usuario. La información de huellas digitales puede utilizarse para realizar la autenticación de la identidad del usuario. En este caso, si un usuario malintencionado aprovecha la oportunidad para pulsar el botón de encendido, puede ejecutarse la puesta en marcha del dispositivo y la autenticación de la identidad del usuario, y puede sustraerse la información guardada en el dispositivo.

Además, para evitar que un usuario malintencionado aproveche la oportunidad de sustraer información guardada en el dispositivo, después de que la primera MCU guarda la información de huellas digitales, si no se pulsa el botón de encendido del dispositivo dentro de un período de tiempo especificado, la primera MCU puede eliminar la información de huellas digitales guardada por la primera MCU, para evitar que un usuario malintencionado utilice, después de que el usuario toque por error el botón de encendido del dispositivo, la información de huellas digitales guardada por la primera MCU, para realizar autenticación de identidad de usuario.

Por ejemplo, como se muestra en la Figura 15A, después de realizar S1402, si el dispositivo está en el modo en reposo o en el modo inactivo, es posible continuar llevando a cabo S1501. Además, como se muestra en la Figura 15A, después de realizar S505, el método en esta solicitud puede incluir además S1502 o S1503.

- 5 S1501. La segunda MCU configura una interfaz de GPIO preestablecida en una placa base del dispositivo a un nivel alto desde un nivel bajo.

Como se muestra en la Figura 16, la segunda MCU puede configurar la interfaz de GPIO preestablecida en la placa base del dispositivo al nivel bajo cuando el dispositivo cambia de un estado de pantalla encendida a un estado de pantalla apagada.

En esta solicitud, que el dispositivo esté en estado de pantalla apagada puede incluir: El dispositivo está en un estado de pantalla apagada en un modo de funcionamiento (marcado como S0), o el dispositivo está en un estado de pantalla apagada en un modo en reposo o en modo inactivo (marcado como Sx).

Por ejemplo, suponiendo que el dispositivo es un ordenador portátil 100, que el ordenador portátil 100 esté en un estado de pantalla apagada en un modo de funcionamiento significa que cuando el ordenador portátil 100 está en el modo de funcionamiento, debido a que un usuario no hace funcionar el ordenador portátil 100 dentro de un período de tiempo (por ejemplo, 5 minutos), el ordenador portátil 100 controla una pantalla del ordenador portátil 100 para entrar en un estado de pantalla negra, para reducir el consumo de energía. En el estado de pantalla apagada en el modo de funcionamiento, el ordenador portátil 100 puede volver a entrar en el modo de funcionamiento, siempre que el usuario toque un área táctil del ordenador portátil 100 o cualquier tecla de un teclado o que el usuario mueva un ratón conectado externamente del ordenador portátil 100.

Que el ordenador portátil esté en un estado de pantalla apagada en modo en reposo significa que cuando el ordenador portátil está en el modo de funcionamiento, debido a que el usuario no hace funcionar el ordenador portátil durante un período de tiempo prolongado (por ejemplo, 30 minutos), el ordenador portátil entra automáticamente en modo en reposo y la pantalla del ordenador portátil entra en un estado de pantalla negra, para reducir el consumo de energía y garantizar la seguridad de la información. En estado de pantalla apagada en modo en reposo. El usuario no necesita pulsar el botón de encendido para controlar el reinicio del ordenador portátil, pero para controlar el ordenador portátil para volver a entrar en el modo de funcionamiento, el usuario necesita además volver a introducir un nombre de usuario y una contraseña o volver a inscribir información de huellas digitales en una interfaz de inicio de sesión del sistema operativo, para realizar la autenticación de identidad de usuario.

Que el dispositivo esté en estado de pantalla apagada puede incluir: El dispositivo está en un estado de pantalla apagada en un modo de funcionamiento, el dispositivo está en un estado de pantalla apagada en un modo en reposo o modo inactivo, o similar; y, cuando el dispositivo está en el estado de pantalla apagada en el modo de funcionamiento, no es necesaria la autenticación de identidad de usuario. Por lo tanto, cuando el dispositivo está en modo en reposo o en modo inactivo Sx, si detecta que se pulsa el botón de encendido, la segunda MCU puede establecer la interfaz de GPIO preestablecida en la placa base del dispositivo al nivel alto desde el nivel bajo, de modo que la primera MCU pueda retener la información de huellas digitales después de detectar que la interfaz de GPIO preestablecida está establecida en el nivel alto.

S 1502. La primera MCU detecta si la interfaz de GPIO preestablecida está establecida en un nivel alto.

S1503. La primera MCU retiene la información de huellas digitales si la primera MCU detecta, dentro de la primera duración preestablecida que empieza a partir de la recepción de la indicación de reactivación por la primera MCU, que la interfaz de GPIO preestablecida está configurada en el nivel alto.

S1504. La primera MCU elimina la información de huellas digitales si la primera MCU no detecta, dentro de la primera duración preestablecida que empieza a partir de la recepción de la indicación de reactivación por la primera MCU, que la interfaz de GPIO preestablecida está configurada en el nivel alto.

Si un usuario desea poner en marcha el dispositivo, el usuario usualmente pulsa el botón de encendido del dispositivo dentro de un corto período de tiempo (por ejemplo, de 1 a 3 segundos) que transcurre después de que un dedo del usuario toca el botón de encendido. En este caso, si el usuario normal necesita poner en marcha el dispositivo, la segunda MCU puede detectar, dentro de un corto período de tiempo (es decir, la primera duración preestablecida, por ejemplo, de 1 a 3 segundos) comenzando a partir de guardar la información de huellas digitales por la primera MCU, que se pulsa el botón de encendido, y puede establecer la interfaz de GPIO preestablecida desde el nivel bajo al nivel alto. Es decir, la primera MCU puede detectar, dentro del corto período de tiempo (es decir, la primera duración preestablecida, por ejemplo, de 1 a 3 segundos) comenzando a partir de guardar la información de huellas digitales por la primera MCU, que la interfaz de GPIO preestablecida está establecida al nivel alto. Por el contrario, si la segunda MCU detecta que el botón de encendido no se pulsa dentro de un corto período de tiempo (es decir, la primera duración preestablecida, por ejemplo, de 1 a 3 segundos) que comienza desde que se guarda la información de huellas digitales, indica que la información de huellas digitales adquirida por el sensor de huellas digitales puede generarse al tocar por error el botón de encendido por el usuario.

Para evitar que un usuario malintencionado utilice la información de huellas digitales adquirida por el sensor de huellas digitales cuando el usuario normal toca por error el botón de encendido, para realizar la autenticación de identidad de usuario y sustraer información guardada en el dispositivo, la primera MCU elimina la información de huellas digitales si la primera MCU lo hace. no detecta, dentro de la primera duración preestablecida, que la interfaz de GPIO preestablecida está establecida en el nivel alto (es decir, la segunda MCU no establece la interfaz de GPIO preestablecida al nivel alto desde el nivel bajo porque la segunda MCU no detecta que se pulsa el botón de encendido). La primera duración preestablecida puede comenzar desde que la primera MCU guarda la información de huellas digitales.

La primera duración preestablecida puede ser de 1 a 3 segundos. Durante la primera duración preestablecida que transcurre después de que el usuario normal toca por error el botón de encendido, el usuario normal suele seguir mirando el dispositivo. Por lo tanto, existe una posibilidad relativamente pequeña de que un usuario malintencionado utilice, dentro de la primera duración preestablecida que transcurre después de que el usuario normal toca por error el botón de encendido, la información de huellas digitales generada al tocar por error el botón de encendido por el usuario normal, para realizar la autenticación de identidad y sustraer información guardada en el dispositivo. Después de que transcurre la primera duración preestablecida después de que el usuario normal toca por error el botón de encendido, incluso si el usuario malintencionado pulsa el botón de encendido, el usuario malintencionado no puede pasar la autenticación de identidad de usuario y no puede sustraer información guardada en el dispositivo, sin la información de huellas digitales del usuario normal, porque la información de huellas digitales guardada por la primera MCU se ha eliminado.

Por ejemplo, como se muestra en la Figura 18, en un punto temporal t4, el dispositivo cambia del modo de funcionamiento (S0) al modo en reposo o al modo inactivo (Sx). En este caso, el dispositivo cambia de un estado de pantalla encendida a un estado de pantalla apagada y la interfaz de GPIO preestablecida en la placa base del dispositivo se establece en un nivel bajo. En un momento t5 mostrado en la Figura 18, un usuario toca el botón de encendido del dispositivo. En este caso, el sensor de huellas digitales integrado en el botón de encendido puede adquirir la información de huellas digitales del usuario. Si se detecta, en un punto temporal t6 mostrado en la Figura 18, cuando se pulsa el botón de encendido, la segunda MCU puede establecer la interfaz de GPIO preestablecida en el nivel alto; y, si se detecta, dentro de un período de tiempo desde el punto temporal t5 hasta un punto temporal t7 (es decir, la primera duración preestablecida T3 a partir de la recepción de la indicación de reactivación por la primera MCU), que la interfaz de GPIO preestablecida está establecida al nivel alto, la primera MCU puede retener la información de huellas digitales; o, la primera MCU puede eliminar la información de huellas digitales si la primera MCU no detecta, dentro de un período de tiempo desde el punto temporal t5 hasta el punto temporal t7, que la interfaz de GPIO preestablecida está configurada en el nivel alto.

La primera MCU puede eliminar la información de huellas digitales si la primera MCU no detecta, dentro de la primera duración preestablecida que empieza a partir de la recepción de la indicación de reactivación por la primera MCU, que la interfaz de GPIO preestablecida está configurada en el nivel alto. En este caso, después de que la primera MCU recibe la solicitud de autenticación de huellas digitales enviada por el controlador de huellas digitales (es decir, S1303), la primera MCU envía una indicación de expiración de huellas digitales al controlador de huellas digitales en vez de enviar la información de huellas digitales al controlador de huellas digitales (es decir, realizar S1305). Es decir, después de S1303 y S1504, el método en esta solicitud puede incluir: enviar, por la primera MCU, la indicación de expiración de la huella digital al controlador de huellas digitales; recibir, por el controlador de huellas digitales, la indicación de expiración de las huellas digitales y devolver una indicación de fallo de autenticación de huellas digitales a un sistema operativo; y recibir, por el sistema operativo, la indicación de fallo de autenticación de huellas digitales, y mostrar una interfaz de inicio de sesión de sistema operativo.

Opcionalmente, si el sistema operativo recibe la indicación de fallo de autenticación de huellas digitales, el sistema operativo puede mostrar además información de indicación de fallo de inicio de sesión en la interfaz de inicio de sesión del sistema operativo.

En algunos casos, después de que la primera MCU guarda la información de huellas digitales (es decir, realizar S505), es posible que el sistema operativo no pueda enviar la solicitud de autenticación de huella digital al controlador de huellas digitales (es decir, realizar S1303), debido a un fallo del sistema u otra causa del dispositivo. Por lo tanto, el controlador de huellas digitales no puede enviar la solicitud de autenticación de huellas digitales a la primera MCU a tiempo, o el sistema operativo ha enviado una solicitud de autenticación de huellas digitales al controlador de huellas digitales a tiempo, pero el controlador de huellas digitales no envía la solicitud de autenticación de huellas digitales a la primera MCU (es decir, realizar S1303) a tiempo. En este caso, el dispositivo no puede iniciar sesión en el escritorio de sistema operativo a tiempo. Debido a que el dispositivo no puede iniciar sesión en el escritorio de sistema operativo a tiempo, un usuario normal puede dejar el dispositivo durante un período de tiempo. En el período de tiempo posterior a la salida del usuario normal, se corre el riesgo de que la información de huellas digitales guardada en la primera MCU sea sustraída por un usuario malintencionado para realizar la autenticación de identidad de usuario e iniciar sesión en el sistema operativo, existiendo además un riesgo de sustracción malintencionada de información guardada en el dispositivo. Para garantizar seguridad de información del dispositivo, la primera MCU puede eliminar la información de huellas digitales guardada por la primera MCU. Específicamente, como se muestra en la Figura 17B, el método en esta solicitud puede incluir además S 1101.

Por ejemplo, como se muestra en la Figura 18, la primera MCU puede eliminar la información de huellas digitales si la primera MCU no recibe la solicitud de autenticación de huellas digitales o la solicitud de inscripción de huellas digitales dentro de un período de tiempo, para ser específico, la segunda duración preestablecida (T4) de un punto temporal t7 a un punto temporal t8.

En esta solicitud, si la primera MCU no recibe la solicitud de autenticación de huellas digitales dentro de la segunda duración preestablecida que empieza con guardar la primera MCU la información de huellas digitales, la primera MCU puede eliminar la información de huellas digitales guardada por la primera MCU. Esto puede evitar que un usuario malintencionado utilice la información de huellas digitales para realizar la autenticación de identidad de usuario y sustraiga información guardada en el dispositivo cuando el usuario normal deje el dispositivo porque el dispositivo no puede iniciar sesión en el escritorio de sistema operativo a tiempo.

Además, después de que la primera MCU envía la información de huellas digitales al controlador de huellas digitales y el controlador de huellas digitales realiza la autenticación de identidad de usuario, la primera MCU todavía guarda la información de huellas digitales del usuario. Para evitar que un usuario malintencionado utilice la información de huellas digitales para realizar la autenticación de identidad de usuario y sustraer información guardada en el dispositivo, la primera MCU puede eliminar la información de huellas digitales después de proporcionar la información de huellas digitales al controlador de huellas digitales, para evitar la reutilización de la información de huellas digitales. Específicamente, después de S1305, el método en esta solicitud puede incluir además S1901. Por ejemplo, como se muestra en la Figura 19B, después de la S1305 mostrada en la Figura 17B, el método en esta solicitud puede incluir además S1901.

S1901. La primera MCU elimina la información de huellas digitales después de enviar la información de huellas digitales al controlador de huellas digitales.

Puede entenderse que, para facilitar el uso, algunos usuarios puedan establecer que el dispositivo cargue directamente una interfaz de sistema operativo sin realizar la autenticación de identidad de usuario después de la puesta en marcha. En este caso, el controlador de huellas digitales no necesita realizar la autenticación de identidad de usuario. Específicamente, después de S505, el método en esta solicitud puede incluir, además: leer, mediante la primera MCU, información de configuración de inicio de sesión del dispositivo; y eliminar, mediante la primera MCU, la información de huellas digitales si la información de configuración de inicio de sesión del dispositivo indica que el dispositivo no necesita realizar la autenticación de identidad de usuario después de la puesta en marcha.

Por ejemplo, si la información de configuración de inicio de sesión del dispositivo indica que el dispositivo no necesita realizar la autenticación de huellas digitales después del inicio, la primera MCU puede eliminar la información de huellas digitales después de que transcurra la tercera duración preestablecida comenzando a partir de la finalización de la carga del controlador de huellas digitales por el dispositivo.

Según el método para poner en marcha un dispositivo proporcionado en esta solicitud, la autenticación de identidad de usuario puede realizarse simultáneamente cuando se pone en marcha el dispositivo, para iniciar sesión en el sistema operativo del dispositivo. Es decir, la autenticación de puesta en marcha y de identidad de usuario puede ejecutarse realizando una operación de puesta en marcha con un solo botón por el usuario. Esto puede reducir las operaciones de usuario y la duración requeridas para la puesta en marcha del dispositivo y el inicio de sesión de sistema, y mejorar la eficiencia de la puesta en marcha del dispositivo y el inicio de sesión de sistema. Además, la información de huellas digitales puede eliminarse además a tiempo, para evitar que el usuario malintencionado utilice la información de huellas digitales para realizar la autenticación de la identidad de usuario.

En una tercera situación de aplicación de esta solicitud, cuando el dispositivo (por ejemplo, el ordenador portátil 100) está en un estado de pantalla apagada en un modo en reposo o en un modo de funcionamiento, si el usuario pulsa el botón de encendido del dispositivo (por ejemplo, pulsa y mantiene pulsado el botón de encendido del dispositivo), el usuario puede controlar el dispositivo para apagarlo. Lo que sigue de esta solicitud describe el método en esta solicitud utilizando un ejemplo en el que el usuario pulsa y mantiene pulsado el botón de encendido del dispositivo para controlar el apagado del dispositivo. La operación de pulsar y mantener pulsado en la presente memoria puede significar que el momento en que el usuario pulsa el botón de encendido es más largo que la duración de pulsado preestablecida.

Para impedir que un usuario malintencionado apague el dispositivo pulse el botón de encendido del dispositivo y, por lo tanto, impedir la pérdida de información que aún no está guardada en el dispositivo (por ejemplo, un documento que se está editando y que no está guardado en el dispositivo) debido al apagado forzado del dispositivo, como se muestra en la Figura 20A, el método en esta solicitud puede incluir S2001:

S2001. La segunda MCU detecta que se pulsa y mantiene pulsado el botón de encendido.

S2002. La segunda MCU determina si un dispositivo está en modo en reposo o en modo activo.

Específicamente, si la segunda MCU determina que el dispositivo está en el modo en reposo o en el modo activo, la segunda MCU puede continuar realizando S2003 y S2004.

S2003. La segunda MCU controla el dispositivo para que deje de responder temporalmente a una operación de pulsar y mantener pulsado el botón de encendido para evitar el apagado.

Si el usuario pulsa y mantiene pulsado el botón de encendido, el dispositivo puede responder normalmente a la operación de pulsar y mantener pulsado, y se apaga. Sin embargo, en esta solicitud, para evitar que el dispositivo se apague cuando un usuario malintencionado pulse y mantenga pulsado el botón de encendido y, por lo tanto, la información que aún no está guardada en el dispositivo se pierda debido al apagado forzado del dispositivo, la segunda MCU puede controlar el dispositivo para que deje de responder temporalmente a la operación de pulsar y mantener pulsado el botón de encendido, y a continuación activar el sistema operativo para realizar la autenticación de huellas digitales y, una vez que lograda la autenticación de huellas digitales, controlar el dispositivo para que responda a la operación de pulsar y mantener pulsado el botón de encendido, y apagarlo.

En un proceso en el que el usuario pulsa y mantiene pulsado el botón de encendido, el sensor de huellas digitales puede adquirir la información de huellas digitales del usuario. Es decir, como se muestra en la Figura 20A, el método en esta solicitud puede incluir además S502 a S505.

S2004. La segunda MCU activa el sistema operativo para realizar la autenticación de huellas digitales.

Después de S2004, el método en esta solicitud puede incluir además S1301 a S1308. Después de S1308, si el resultado de la autenticación indica que la autenticación de huellas digitales se realizó con éxito, puede continuarse realizando S2005; o, si el resultado de la autenticación indica que la autenticación de huellas digitales falla, puede continuarse realizando S2006.

S2005. El dispositivo responde a la operación de pulsar y mantener pulsado el botón de encendido, y se apaga.

Si el resultado de la autenticación indica que la autenticación de huellas digitales se realizó con éxito, indica que el usuario que pulsa y mantiene pulsado el botón de encendido es el propietario del dispositivo y puede controlar que el dispositivo se apague normalmente.

S2006. El dispositivo entra en modo en reposo y muestra una interfaz de advertencia de apagado.

Si el resultado de la autenticación indica que la autenticación de huellas digitales falla, indica que el usuario que pulsa y mantiene pulsado el botón de encendido no es el propietario del dispositivo, puede controlarse el dispositivo para entrar al modo en reposo y mostrar la interfaz de advertencia de apagado.

Por ejemplo, si el resultado de la autenticación indica que la autenticación de huellas digitales falla, el dispositivo puede entrar al modo en reposo y mostrar la “interfaz de advertencia de apagado” mostrada en la Figura 21. Por ejemplo, la información de aviso que indica “Dispositivo bloqueado” y “Únicamente el propietario puede continuar la operación” 2001 puede aparecer en la “interfaz de advertencia de apagado” mostrada en la Figura 21.

Opcionalmente, si el resultado de la autenticación indica que falla la autenticación de huellas digitales, el dispositivo puede enviar además una alarma de voz para advertir al usuario malintencionado que no haga funcionar el dispositivo y recordar al propietario que detenga una operación de apagado malintencionado de un usuario malintencionado en el dispositivo a tiempo.

Además, en la tercera situación de aplicación, el método para poner en marcha un dispositivo proporcionado en esta solicitud puede incluir además S1101, S1501 a S1504, S1801 u otra etapa, y los detalles no se describen de nuevo en esta solicitud.

Según el método para poner en marcha un dispositivo protegido por esta solicitud, la autenticación de identidad de usuario puede realizarse simultáneamente cuando se pone en marcha el dispositivo, para iniciar sesión en el sistema operativo del dispositivo. Es decir, la autenticación de puesta en marcha y de identidad de usuario puede ejecutarse realizando una operación de puesta en marcha con un solo botón por el usuario. Esto puede reducir las operaciones de usuario y la duración requeridas para la puesta en marcha del dispositivo y el inicio de sesión de sistema, y mejorar la eficiencia de la puesta en marcha del dispositivo y el inicio de sesión de sistema. Además, la información de huellas digitales puede eliminarse además a tiempo, para evitar que el usuario malintencionado utilice la información de huellas digitales para realizar la autenticación de la identidad de usuario.

Además, este método puede impedir además el apagado malintencionado realizado por un usuario malintencionado en el dispositivo y la pérdida de información aún no guardada en el dispositivo.

Puede entenderse que, en esta solicitud, puede utilizarse de forma alternativa otro procesador para reemplazar la primera MCU o la segunda MCU para realizar un proceso de método relacionado. Por ejemplo, el otro procesador puede ser una CPU del dispositivo, o el otro procesador puede ser cualquier procesador tal como un procesador de propósito general o una matriz de puertas programables en campo (matriz de puertas programables en campo, FPGA)

que puede realizar las etapas del método realizadas por la primera MCU o la segunda MCU y ejecutar “puesta en marcha e inicio de sesión con un solo botón” del dispositivo.

Lo anterior describe principalmente la solución proporcionada en las realizaciones de esta solicitud desde una perspectiva de un proceso en el que el usuario pulsa el botón de encendido del dispositivo para ponerlo en marcha. Puede entenderse que, para ejecutar las funciones anteriores, el dispositivo incluye módulos de función correspondientes que realizan las funciones. Un experto en la técnica sabrá que, con referencia a las etapas de terminales y algoritmos en los ejemplos descritos en las realizaciones descritas en esta memoria descriptiva, esta solicitud puede ser ejecutada mediante hardware o una combinación de hardware y software informático. El hecho de que una función se realice mediante hardware o hardware accionado por software informático depende de las aplicaciones particulares y limitaciones de diseño de las soluciones técnicas. Un experto en la técnica puede utilizar distintos métodos para ejecutar las funciones descritas para cada aplicación particular, pero no debe considerarse que la ejecución va más allá del ámbito de esta solicitud.

En esta realización de esta solicitud, puede hacerse una división en el dispositivo basándose en los ejemplos del método. Por ejemplo, los módulos o unidades pueden dividirse basándose en funciones correspondientes, o dos o más funciones pueden integrarse en un módulo de procesamiento. El módulo integrado puede ejecutarse en forma de hardware, o puede ejecutarse en forma de un módulo o unidad de software. En esta realización de esta solicitud, la división de módulo es un ejemplo, y es simplemente división de función lógica o puede ser otra división durante la ejecución real.

La Figura 22 es un posible diagrama estructural esquemático del dispositivo en las realizaciones anteriores. El dispositivo puede incluir un botón de encendido y un sensor de huellas digitales, y el botón de encendido está integrado con el sensor de huellas digitales. Como se muestra en la Figura 22, el dispositivo 2200 puede incluir un módulo 2201 de obtención, un módulo 2202 de almacenamiento y un módulo 2203 de suministro de huellas digitales.

El módulo 2201 de obtención está configurado para soportar una operación de “obtención de información de huellas digitales adquirida por el sensor de huellas digitales” en S401 y S505, S504, S608, y S505' en las realizaciones del método, y/o se utiliza en otro proceso de la tecnología descrita en esta memoria descriptiva.

El módulo 2202 de almacenamiento está configurado para soportar S401, S505, y una operación de “guardar la información de huellas digitales” en S610 en las realizaciones del método, y/o se utiliza en otro proceso de la tecnología descrita en esta memoria descriptiva.

El módulo 2203 de suministro de huellas digitales está configurado para soportar S402 en la realización del método, y/o se utiliza en otro proceso de la tecnología descrita en esta memoria descriptiva.

Además, como se muestra en la Figura 23, el dispositivo 2200 puede incluir además un módulo 2204 de detección y un módulo 2205 de eliminación. El módulo 2204 de detección está configurado para soportar S1401, S1402, S1502, S2001, y S2002 en las realizaciones del método, y/o se utiliza en otro proceso de la tecnología descrita en esta memoria descriptiva. El módulo 2205 de eliminación está configurado para soportar S1101, S1504, y S1901 en los ejemplos del método, y/o se utiliza en otro proceso de la tecnología descrita en esta memoria descriptiva.

Además, el dispositivo 2200 puede incluir además un módulo de encendido e inicialización y un módulo de visualización de inicio de sesión. El módulo de puesta en marcha e inicialización está configurado para soportar S501, S601 a S603, y S603' en los ejemplos del método, y/o se utiliza en otro proceso de la tecnología descrita en esta memoria descriptiva. El módulo de visualización de inicio de sesión está configurado para soportar S604, S605, S1403, y S1404 en los ejemplos del método, y/o se utiliza en otro proceso de la tecnología descrita en esta memoria descriptiva.

Además, el dispositivo puede incluir además módulos de funciones configurados para soportar etapas del método tales como S502, S503, S607, S609, S1301 a S1308, S1501 y S1503. Los módulos de función no se describen uno a uno en la presente solicitud.

Ciertamente, el dispositivo 2200 incluye, aunque no de forma limitativa, los módulos de unidades enumerados. Por ejemplo, el dispositivo 2200 puede incluir además un módulo de envío configurado para enviar datos o una señal a otro dispositivo, un módulo de recepción configurado para recibir datos o una señal enviada por otro dispositivo u otro módulo. Además, las funciones específicas que pueden ser ejecutadas por los módulos anteriores también incluyen, aunque no de forma limitativa, las funciones correspondientes a las etapas del método en los ejemplos anteriores. Para descripciones detalladas de otras unidades del dispositivo 2200 y las unidades del dispositivo 2200, consúltense las descripciones detalladas de las etapas del método correspondientes, cuyos detalles no se describirán de nuevo aquí.

Cuando se utiliza una unidad integrada, el módulo 2201 de obtención, el módulo 2203 de suministro de huellas digitales, el módulo 2204 de detección, el módulo 2205 de eliminación y similares pueden integrarse en una unidad de procesamiento. La unidad de procesamiento puede ser un procesador o un controlador, por ejemplo, una CPU, un

procesador de propósito general, un procesador de señales digitales (Procesador de Señales Digitales, DSP), un circuito integrado específico de la aplicación (Circuito Integrado Específico de la Aplicación, ASIC), un FPGA, una MCU u otro dispositivo lógico programable, un dispositivo de lógica de transistores, un componente de hardware o cualquier combinación de los mismos. La unidad de procesamiento puede aplicar o ejecutar diversos bloques lógicos, módulos y circuitos ilustrativos descritos con referencia a ejemplos descritos en el contenido descrito en esta solicitud. De forma alternativa, la unidad de procesamiento puede ser una combinación de procesadores que ejecutan una función informática, por ejemplo, una combinación de uno o más microprocesadores, o una combinación de un DSP y un microprocesador. El módulo de almacenamiento puede ser una memoria.

Cuando la unidad de procesamiento es un procesador y el módulo de almacenamiento es una memoria, el dispositivo 2200 en esta realización de esta solicitud puede ser un dispositivo 2400 mostrado en la Figura 24. Como se muestra en la Figura 24, el dispositivo 2400 incluye un procesador 2401, una memoria 2402, una pantalla 2403, un botón 2404 de encendido, un sensor 2406 de huellas digitales y un bus 2405. El botón 2404 de encendido está integrado con el sensor 2406 de huellas digitales, y el procesador 2401, la memoria 2402, la pantalla 2403, el botón 2404 de encendido, el sensor 2406 de huellas digitales y el bus 2405 están interconectados utilizando el bus 2405. El procesador 2401 puede incluir una CPU, una primera MCU y una segunda MCU del dispositivo 2400.

El sensor 2406 de huellas digitales está configurado para adquirir información de huellas digitales de un usuario, la memoria 2402 está configurada para almacenar código de programa informático, el código de programa informático incluye una instrucción y, cuando el procesador 2401 del dispositivo 2400 ejecuta la instrucción, el dispositivo 2400 realiza etapas del método relacionadas en cualquiera de la Figura 15A, Figura 15B, Figura 17A, Figura 17B, Figura 19A, y la Figura 19B para ejecutar el método para poner en marcha un dispositivo en las realizaciones anteriores.

El bus 2405 puede ser un bus de interconexión de componentes periféricos (interconexión de componentes periféricos, PCI), un bus de arquitectura estándar industrial extendida (arquitectura estándar industrial extendida, EISA) o similar. El bus 2405 puede clasificarse en un bus de direcciones, un bus de datos, un bus de control y similares. Para facilitar la representación, únicamente se utiliza una línea gruesa para representar el bus en la Figura 24, pero esto no significa que haya un solo bus o únicamente un tipo de bus.

Una realización de la presente invención proporciona además un medio de almacenamiento informático. El medio de almacenamiento informático almacena el código del programa informático y, cuando un procesador 2401 del dispositivo 2400 ejecuta el código de programa informático, el dispositivo 2400 realiza etapas del método relacionadas en una cualquiera de la Figura 15A, Figura 15B, Figura 17A, Figura 17B, Figura 19A, y Figura 19B para implementar el método para poner en marcha un dispositivo en las realizaciones anteriores.

La Figura 25 es un posible diagrama estructural esquemático de la MCU en las realizaciones anteriores. La MCU puede estar incluida en el dispositivo anterior. El dispositivo incluye un botón de encendido y un sensor de huellas digitales, y el botón de encendido está integrado con el sensor de huellas digitales. Como se muestra en la Figura 25, la MCU 2500 puede incluir un módulo 2501 de recepción, un módulo 2502 de obtención, un módulo 2503 de almacenamiento, y un módulo 2504 de suministro de huellas digitales.

El módulo 2501 de recepción está configurado para soportar S504, S608, y S1304 en las realizaciones del método, y/o se utiliza en otro proceso de la tecnología descrita en esta memoria descriptiva. El módulo 2502 de obtención está configurado para soportar una operación de "obtener información de huellas digitales adquirida por el sensor de huellas digitales" en S505 y S505', y/o se utiliza en otro proceso de la tecnología descrita en esta memoria descriptiva. El módulo 2503 de almacenamiento está configurado para soportar una operación de "guardar la información de huellas digitales" en S505 en las realizaciones del método, y/o se utiliza en otro proceso de la tecnología descrita en esta memoria descriptiva. El módulo 2504 de suministro de huellas digitales está configurado para soportar S609 y S1305 en las realizaciones del método, y/o se utiliza en otro proceso de la tecnología descrita en esta memoria descriptiva.

Además, como se muestra en la Figura 26, la MCU 2500 puede incluir además un módulo 2505 de detección y un módulo 2506 de eliminación. El módulo 2505 de detección está configurado para soportar S1502 en las realizaciones del método, y/o se utiliza en otro proceso de la tecnología descrita en esta memoria descriptiva. El módulo 2506 de eliminación está configurado para soportar S1504, S1101, y S1901 en las realizaciones del método, y/o se utiliza en otro proceso de la tecnología descrita en esta memoria descriptiva.

Ciertamente, la MCU 2500 incluye, aunque no de forma limitativa, los módulos de unidades enumerados. Además, las funciones específicas que pueden ser ejecutadas por los módulos anteriores también incluyen, aunque no de forma limitativa, las funciones correspondientes a las etapas del método en los ejemplos anteriores. Para descripciones detalladas de otras unidades de la MCU 2500 y de las unidades de la MCU 2500, consúltense las descripciones detalladas de la etapa del método correspondiente, los detalles no se describen de nuevo en esta realización de esta solicitud.

La MCU 2500 en esta realización de esta solicitud puede incluirse en un dispositivo 2700 mostrado en la Figura 27. Como se muestra en la Figura 27, el dispositivo 2700 incluye un procesador 2701, una memoria 2702, una pantalla

2703, un botón 2704 de encendido, un sensor 2706 de huellas digitales y un bus 2705. El botón 2704 de encendido está integrado con el sensor 2706 de huellas digitales, y el procesador 2701, la memoria 2702, la pantalla 2703, el botón 2704 de encendido, el sensor 2706 de huellas digitales y el bus 2705 están interconectados utilizando el uso del bus 2705. El procesador 2701 puede incluir la primera MCU del dispositivo 2700.

El sensor 2406 de huellas digitales está configurado para adquirir información de huellas digitales de un usuario, la memoria 2702 está configurada para almacenar código de programa informático, el código de programa informático incluye una instrucción y, cuando el procesador 2701 del dispositivo 2700 ejecuta la instrucción, el dispositivo 2700 realiza etapas del método relacionadas en cualquiera de la Figura 15A, Figura 15B, Figura 17A, Figura 17B, Figura 19A, y la Figura 19B para ejecutar el método para poner en marcha un dispositivo en las realizaciones anteriores.

El bus 2704 puede ser un bus PCI, un bus EISA o similares. El bus 2704 puede clasificarse en un bus de direcciones, un bus de datos, un bus de control y similares. Para facilitar la representación, únicamente se utiliza una línea gruesa para representar el bus en la Figura 27, pero esto no significa que haya un solo bus o únicamente un tipo de bus.

Una realización de la presente invención proporciona además un medio de almacenamiento informático. El medio de almacenamiento informático almacena el código del programa informático y, cuando un procesador 2701 de un dispositivo 2700 ejecuta el código de programa informático, el dispositivo 2700 realiza etapas del método relacionadas en una cualquiera de la Figura 15A, Figura 15B, Figura 17A, Figura 17B, Figura 19A, y Figura 19B para ejecutar el método para poner en marcha un dispositivo en las realizaciones anteriores.

Una realización de la presente invención proporciona además un producto de programa informático. Ejecutar el producto de programa informático en un ordenador hace que el ordenador realice las etapas del método relacionadas en una cualquiera de la Figura 15A, Figura 15B, Figura 17A, Figura 17B, Figura 19A y Figura 19B para ejecutar el método para poner en marcha un dispositivo en las realizaciones anteriores.

El dispositivo 2200, el dispositivo 2400, la MCU 2500, el dispositivo 2700, el medio de almacenamiento informático y el producto de programa informático proporcionados en las realizaciones de la presente invención están todos configurados para realizar los métodos correspondientes proporcionados anteriormente. Por lo tanto, para los efectos beneficiosos que se pueden lograr mediante los dispositivos, el medio de almacenamiento informático y el producto de programa informático, consúltense los efectos beneficiosos en los métodos correspondientes proporcionados anteriormente, los detalles no se describen de nuevo en la presente memoria.

Por ejemplo, el dispositivo proporcionado en esta solicitud puede ser de forma alternativa un teléfono 2800 móvil mostrado en la Figura 28. Como se muestra en la Figura 28, el teléfono 2800 móvil incluye un botón 2801 de encendido y un sensor 2802 de huellas digitales, y el botón 2801 de encendido está integrado con el sensor 2802 de huellas digitales. El botón 2801 de encendido del teléfono móvil en esta solicitud es un botón físico en el teléfono 2800 móvil configurado para controlar el teléfono 2800 móvil para poner en marcha, apagar y reiniciar.

Aunque un teléfono móvil de la técnica anterior también incluye un botón de encendido y un sensor de huellas digitales, el botón de encendido y el sensor de huellas digitales están normalmente dispuestos por separado. Por lo tanto, en un proceso de puesta en marcha y desbloqueo del teléfono móvil, un usuario necesita iniciar el teléfono móvil realizando una operación con un solo botón y, a continuación, inscribir información de huellas digitales utilizando el sensor 202 de huellas digitales, para realizar la autenticación de identidad de usuario, desbloquear el teléfono móvil y mostrar un escritorio de operaciones.

Por ejemplo, suponiendo que el teléfono 2800 móvil mostrado en la Figura 29A está en un estado inactivo, como se muestra en la Figura 29A, cuando un usuario pulsa el botón 2801 de encendido del teléfono 2800 móvil, un dedo del usuario toca definitivamente el botón 2801 de encendido. Cuando el dedo del usuario toca el botón 2801 de encendido, el sensor 2802 de huellas digitales integrado en el botón 2801 de encendido puede adquirir información de huellas digitales del usuario que toca el botón 2801 de encendido. Por lo tanto, el teléfono 2800 móvil puede responder a una operación de presión realizada por el usuario en el botón 2801 de encendido, y poner en marcha y, después de la puesta en marcha, utilizar directamente la información de huellas digitales adquirida por el sensor 2802 de huellas digitales para realizar la autenticación de identidad de usuario y desbloquear el teléfono móvil, para mostrar un escritorio de funcionamiento de teléfono móvil mostrado en la Figura 29B.

Puede entenderse que, en un proceso de puesta en marcha y desbloqueo del teléfono 2800 móvil mostrado en la Figura 29, la puesta en marcha y autenticación de identidad de usuario del teléfono 2800 móvil puede ser ejecutada por el usuario realizando una operación de puesta en marcha con un solo botón, es decir, la autenticación de identidad de usuario puede realizarse simultáneamente cuando se pone en marcha el teléfono 2800 móvil, para desbloquear el teléfono 2800 móvil. Esto puede reducir la duración requerida para iniciar y desbloquear el teléfono 2800 móvil, y puede mejorar la eficiencia de poner en marcha y desbloquear el teléfono 2800 móvil.

Cabe señalar que, un ejemplo del teléfono móvil proporcionado en esta solicitud se proporciona como se muestra en la Figura 28 y en la Figura 29. El teléfono móvil proporcionado en esta solicitud incluye, aunque no de forma limitativa, el teléfono móvil mostrado en la Figura 28 o Figura 29, por ejemplo, el botón 2801 de encendido del teléfono móvil

proporcionado en esta solicitud puede estar de forma alternativa en un lado o en la parte posterior del teléfono 2800 móvil.

Las descripciones anteriores acerca de las implementaciones permiten a un experto en la técnica comprender que, con el propósito de una descripción breve y conveniente, la división de los módulos funcionales anteriores se toma como un ejemplo de ilustración. En la aplicación real, las funciones anteriores pueden asignarse a módulos distintos y ejecutarse dependiendo de un requisito, es decir, una estructura interna de un aparato se divide en distintos módulos de funciones para ejecutar todas o parte de las funciones descritas anteriormente. Para un proceso de trabajo específico del sistema, aparato y unidad anteriores, puede hacerse referencia a un proceso correspondiente en las realizaciones del método anterior, y los detalles no se describen en la presente descripción nuevamente.

En las varias realizaciones proporcionadas en esta solicitud, debe entenderse que el sistema, aparato, y método descritos pueden ejecutarse de otras formas. Por ejemplo, la realización del aparato descrito es simplemente un ejemplo. Por ejemplo, la división de módulos o unidades es simplemente una división de funciones lógica o puede ser otra división durante la ejecución real. Por ejemplo, puede combinarse o integrarse una pluralidad de unidades o componentes en otro sistema, o algunas características pueden ignorarse o pueden no realizarse. Además, los acoplamientos mutuos mostrados o analizados o los acoplamientos directos o las conexiones de comunicación pueden implementarse usando algunas interfaces. Los acoplamientos indirectos o las conexiones de comunicación entre los aparatos o unidades pueden establecerse en forma eléctrica, mecánica, u otras formas.

Las unidades descritas como partes separadas pueden o no estar físicamente separadas, y las partes mostradas como unidades pueden o no ser unidades físicas, pueden ubicarse en una posición o pueden distribuirse en una pluralidad de unidades de red. Pueden seleccionarse algunas o todas las unidades basándose en los requisitos reales para alcanzar los objetivos de las soluciones de las realizaciones.

Además, las unidades funcionales en las realizaciones de la presente solicitud pueden integrarse dentro de una unidad de procesamiento, o cada una de las unidades pueden existir físicamente solas, o dos o más unidades se integran dentro de una unidad. La unidad integrada puede implementarse en forma de hardware, o puede implementarse en forma de una unidad funcional de software.

Cuando la unidad integrada se implementa en forma de una unidad funcional de software y se vende o usa como un producto independiente, la unidad integrada puede almacenarse en un medio de almacenamiento legible por ordenador. Sobre la base de tal entendimiento, las soluciones técnicas de esta solicitud, esencialmente, o la parte que contribuye a la técnica anterior, o todas o algunas de las soluciones técnicas, pueden realizarse en forma de un producto de software. El producto de software se almacena en un medio de almacenamiento e incluye varias instrucciones para instruir que un dispositivo informático (que puede ser un ordenador personal, un servidor, un dispositivo de red, o similares) lleve a cabo todas o algunas de las etapas de los métodos descritos en las realizaciones de esta solicitud. El medio de almacenamiento anterior incluye cualquier medio que pueda almacenar código de programa, tal como una memoria flash, un disco duro extraíble, una memoria de solo lectura, una memoria de acceso aleatorio, un disco magnético o un disco óptico.

REIVINDICACIONES

1. Un método para poner en marcha un dispositivo (100, 2400, 2700, 2800), en donde el dispositivo comprende un botón (101, 2404, 2704, 2801) de encendido y un sensor (102, 2406, 2706, 2802) de huellas digitales, el botón de encendido está integrado con el sensor de huellas digitales, y el método comprende:
5 detectar una operación táctil realizada por un usuario en el botón (101, 2402, 2702, 2801) de encendido;
10 en respuesta a la operación táctil, obtener (S505), por una primera unidad de microcontrolador, MCU, información de huellas digitales adquirida por el sensor (102, 2406, 2706, 2802) de huellas digitales, y guardar, mediante la primera MCU, la información de huellas digitales;
15 si se detecta (S1401) que el botón de encendido del dispositivo está presionado: encender una unidad central de procesamiento, CPU, del dispositivo; y obtener (S1304), por la primera MCU, una solicitud de autenticación de huellas digitales después del encendido de la CPU, y
el método comprende, además:
20 si detecta, por la primera MCU, dentro de una primera duración preestablecida que se pulsa el botón de encendido del dispositivo: después de obtener la solicitud de autenticación de huellas digitales, proporcionar (S1305), por la primera MCU, la información de huellas digitales a un controlador de huellas digitales para realizar (S1306) autenticación de huellas digitales, para iniciar sesión (S1403) en un sistema operativo del dispositivo (100, 2400, 2700, 2800); y
25 si no detecta, por la primera MCU, dentro de la primera duración preestablecida que se pulsa el botón de encendido del dispositivo, eliminar (S1504), mediante la primera MCU, la información de huellas digitales.
2. El método según la reivindicación 1, en donde,
30 cuando el dispositivo (100, 2400, 2700, 2800) está en modo en reposo o en modo inactivo, si se pulsa el botón (101, 2404, 2704, 2801) de encendido, se establece una interfaz de entrada-salida de propósito general, GPIO, preestablecida de un nivel bajo a un nivel alto.
3. El método según una cualquiera de las reivindicaciones 1 a 2, en donde después de obtener (S505), mediante la primera MCU, la información de huellas digitales adquirida por el sensor (102, 2406, 2706, 2802) de huellas digitales, y guardar la información de huellas digitales, el método comprende además:
35 eliminar (S1101) la información de huellas digitales si la solicitud de autenticación de huellas digitales no se obtiene dentro de una segunda duración preestablecida comenzando a partir de guardar la información de huellas digitales.
40
4. El método según una cualquiera de las reivindicaciones 1 a 3, en donde el método comprende además:
45 eliminar (S1901) la información de huellas digitales después de que se proporciona la información de huellas digitales para realizar la autenticación de huellas digitales.
5. El método según una cualquiera de las reivindicaciones 1 a 4, en donde el método comprende además:
50 si una configuración de inicio de sesión del dispositivo (100, 2400, 2700, 2800) indica que el dispositivo no necesita realizar la autenticación de identidad de usuario después de la puesta en marcha, eliminar la información de huellas digitales después de que transcurra una tercera duración preestablecida comenzando a partir de la finalización de la carga del controlador de huellas digitales por el dispositivo.
6. El método según la reivindicación 1, que comprende además:
55 recibir (S503), por la primera MCU, una indicación de reactivación enviada por el sensor (102, 2406, 2706, 2802) de huellas digitales;
60 en donde la primera MCU obtiene (S505) la información de huellas digitales adquirida por el sensor (102, 2406, 2706, 2802) de huellas digitales cuando se recibe la indicación de reactivación, y guarda la información de huellas digitales; y
65 en donde la primera MCU recibe (S1304) la solicitud de autenticación de huellas digitales enviada por el controlador de huellas digitales y proporciona (S1305) la información de huellas digitales al controlador de huellas digitales, de modo que el controlador de huellas digitales realiza (S1306) la autenticación de huellas digitales para iniciar sesión (S1403) en un sistema operativo del dispositivo.

7. Un dispositivo (100, 2400, 2700, 2800), en donde el dispositivo comprende un botón (101, 2404, 2704, 2801) de encendido, un sensor (102, 2406, 2706, 2802) de huellas digitales, una memoria (2402, 2702), un procesador (2401, 2701) y una pantalla (2403, 2703), y el botón de encendido está integrado con el sensor de huellas digitales; y
- 5 el botón (101, 2404, 2704, 2801) de encendido, el sensor (102, 2406, 2706, 2802) de huellas digitales, la memoria (2402, 2702), la pantalla (2403, 2703) y el procesador (2401, 2701) están conectados utilizando un bus (2405, 2705), el sensor de huellas digitales está configurado para adquirir información de huellas digitales de un usuario, la memoria está configurada para almacenar código de programa informático, el código de programa informático comprende una instrucción y, cuando el procesador ejecuta la instrucción, el dispositivo (100, 2400, 2700, 2800) realiza el método para poner en marcha un dispositivo según una cualquiera de las reivindicaciones 1 a 6.
- 10
8. Un producto de programa informático, en donde, cuando se ejecuta en un ordenador, el producto de programa informático permite que el ordenador realice el método para poner en marcha un dispositivo (100, 2400, 2700, 2800) según una cualquiera de las reivindicaciones 1 a 6.
- 15

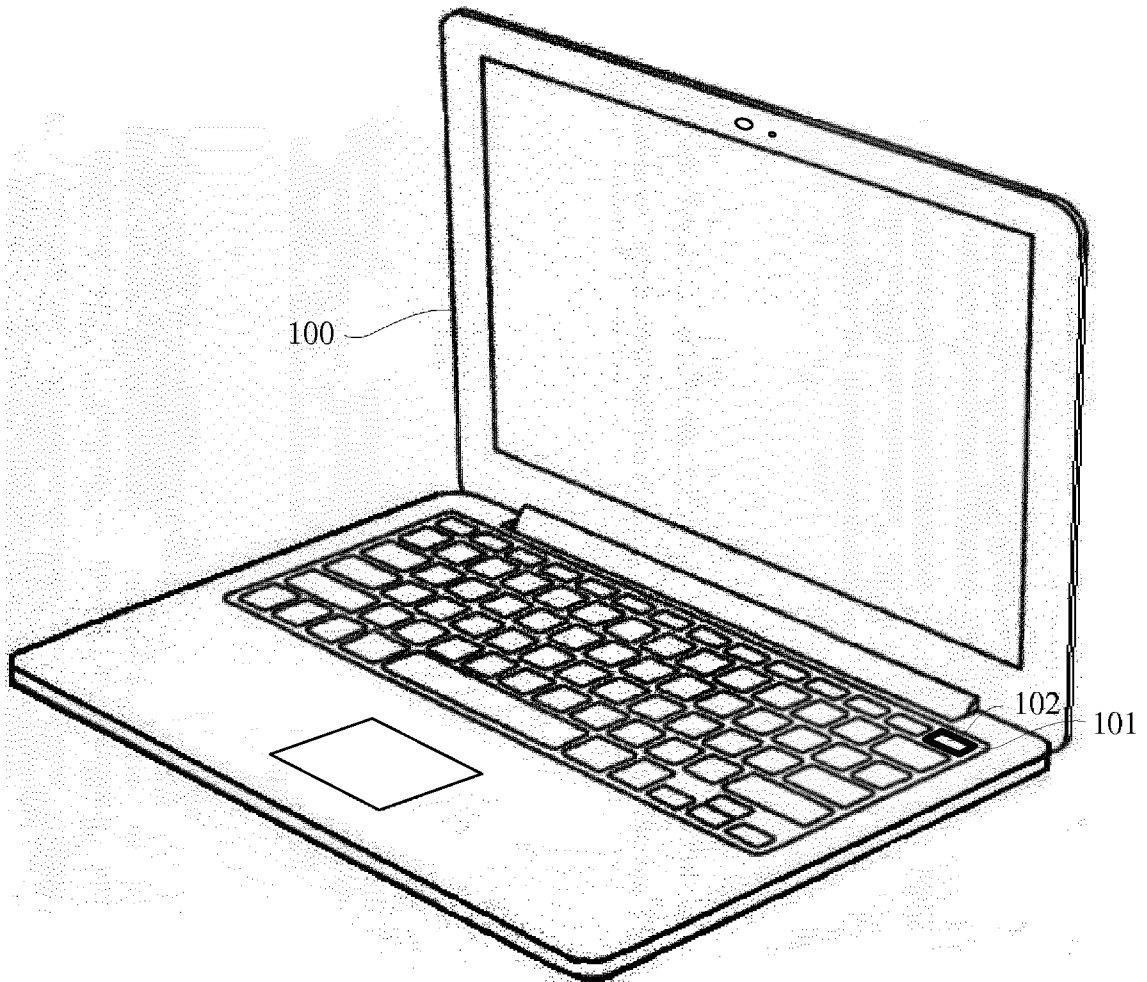


Figura 1A

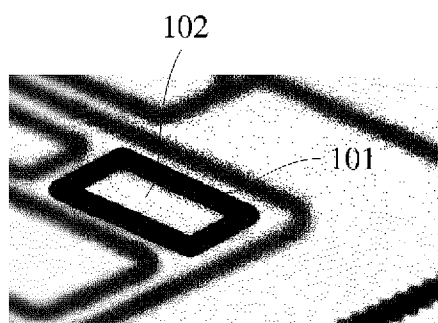


Figura 1B

Figura 1

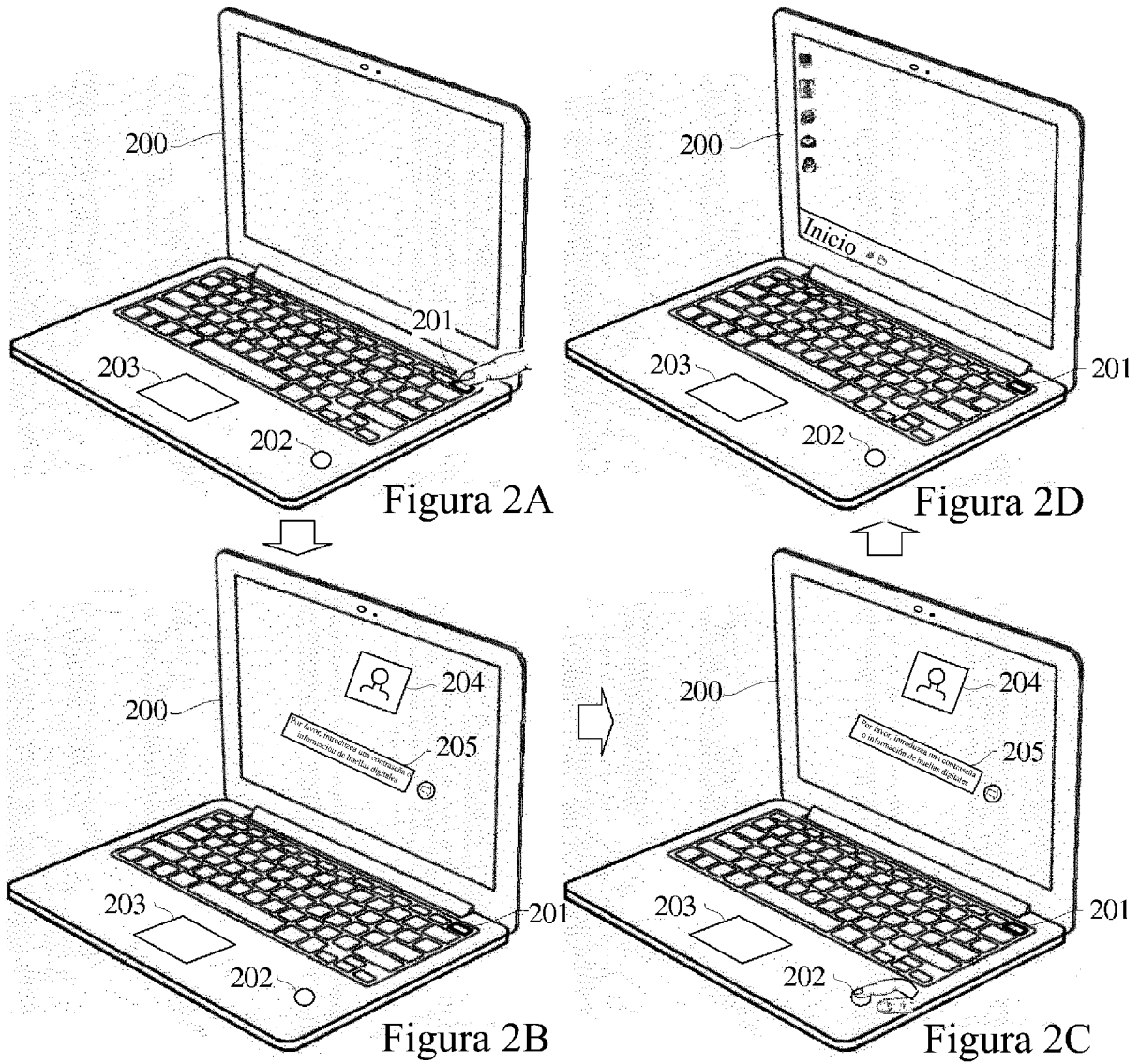


Figura 2

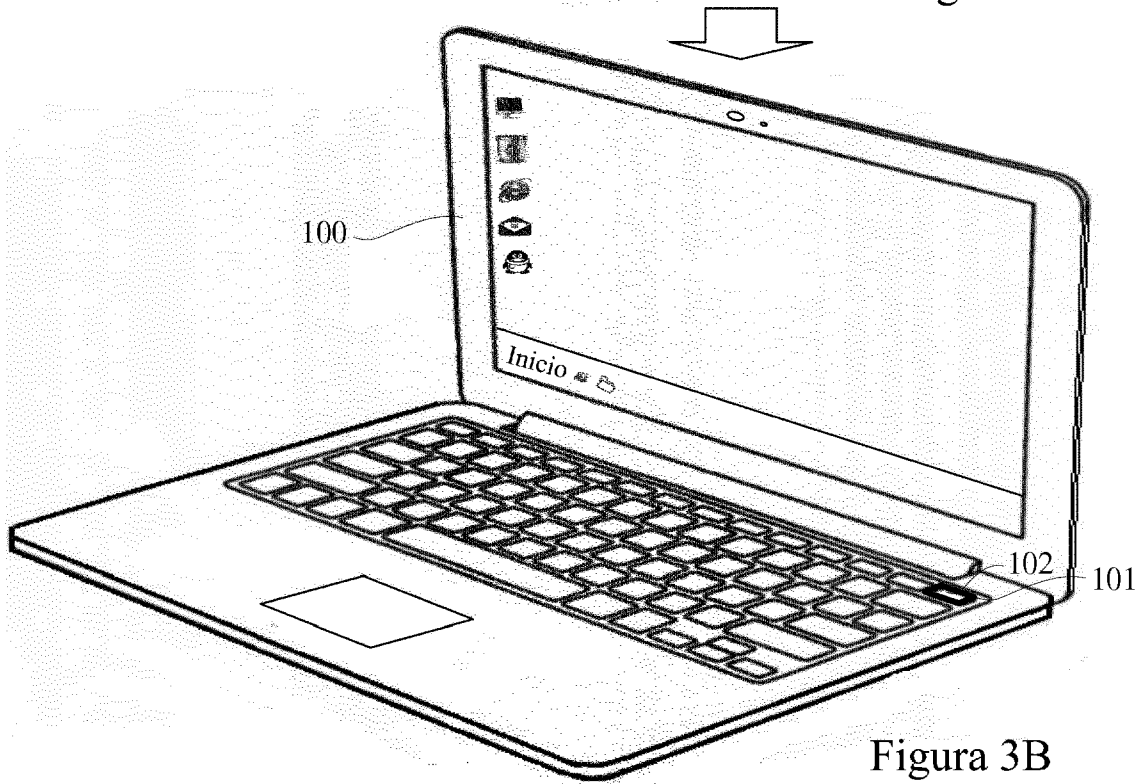
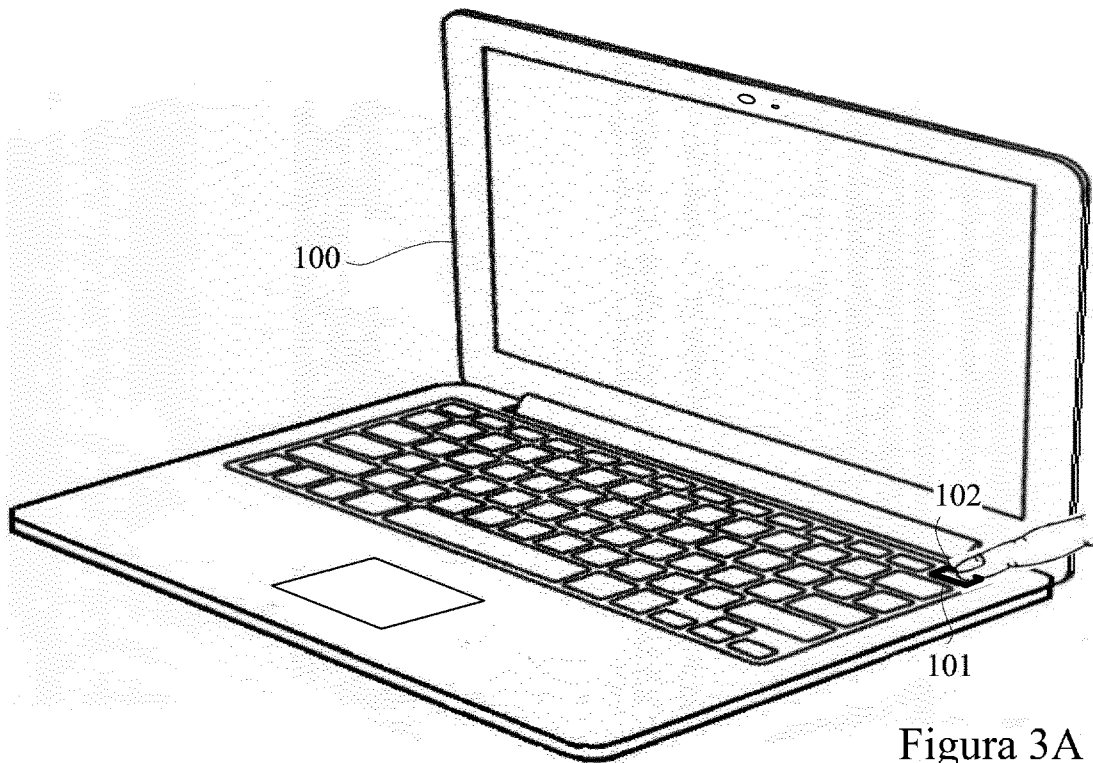


Figura 3

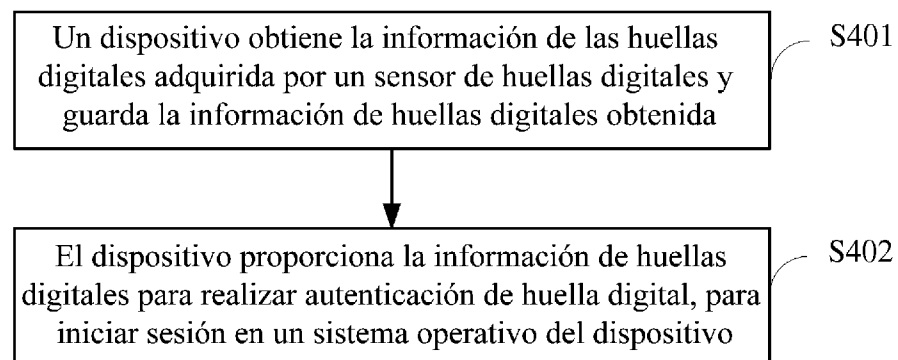


Figura 4

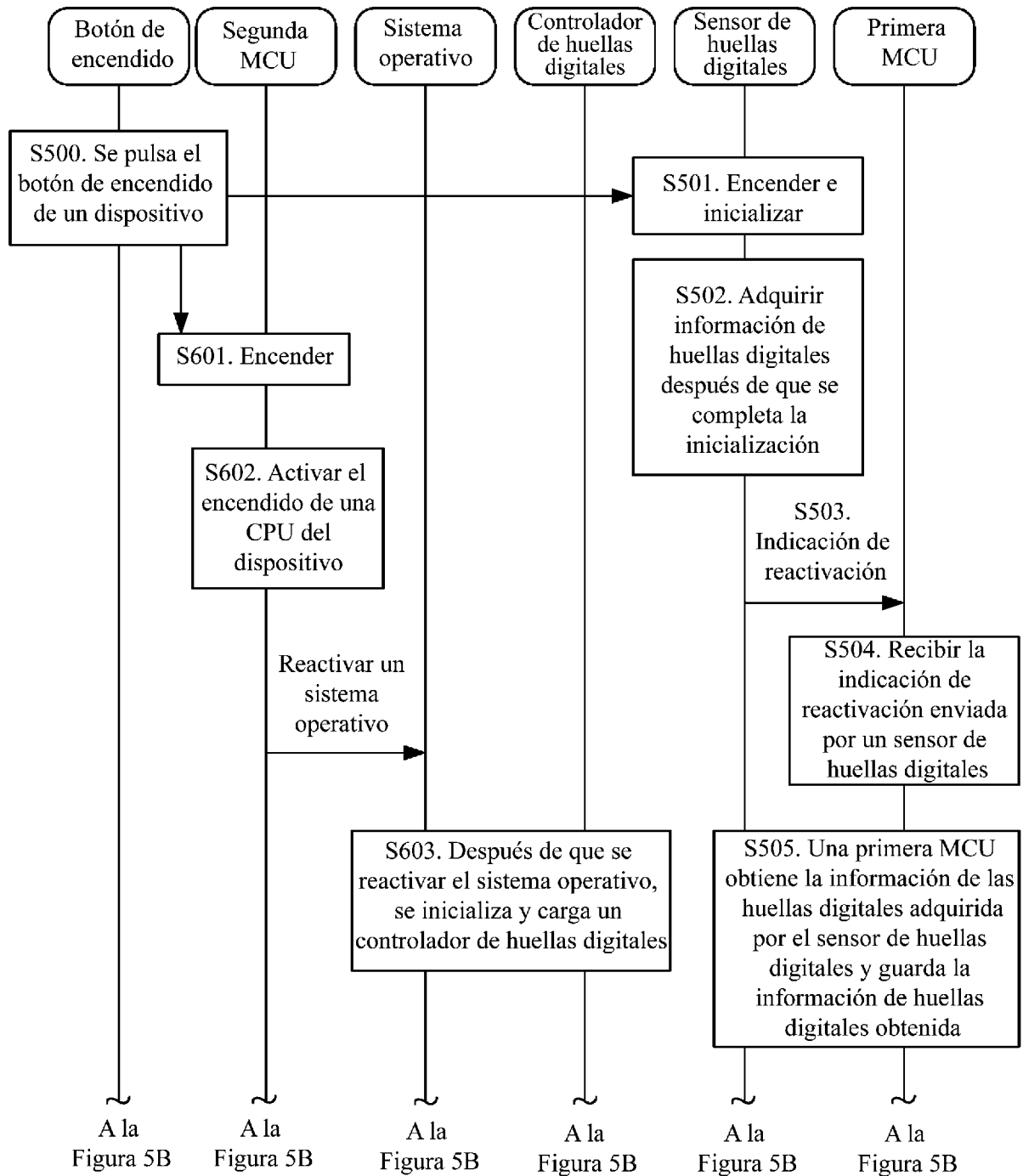


Figura 5A

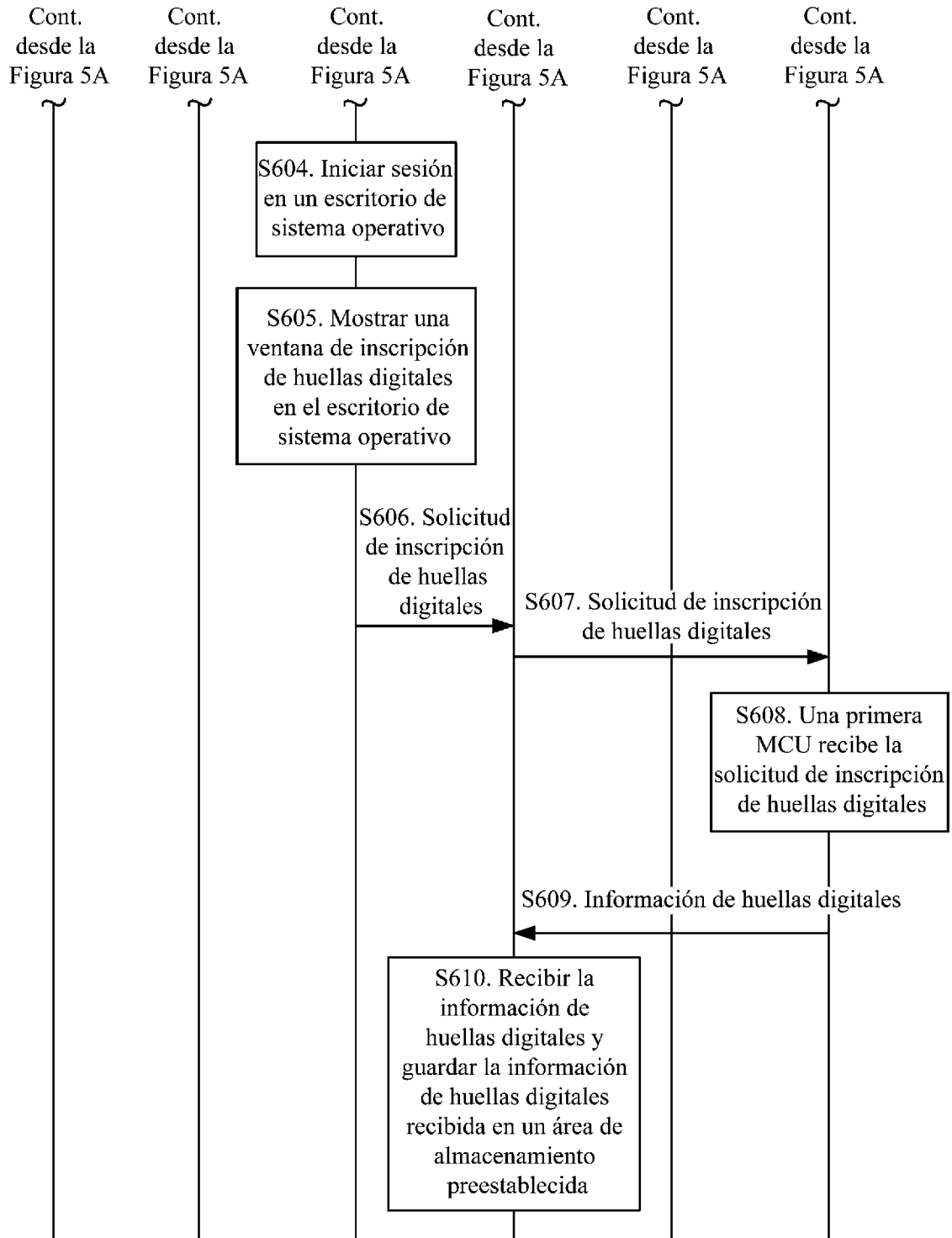


Figura 5B

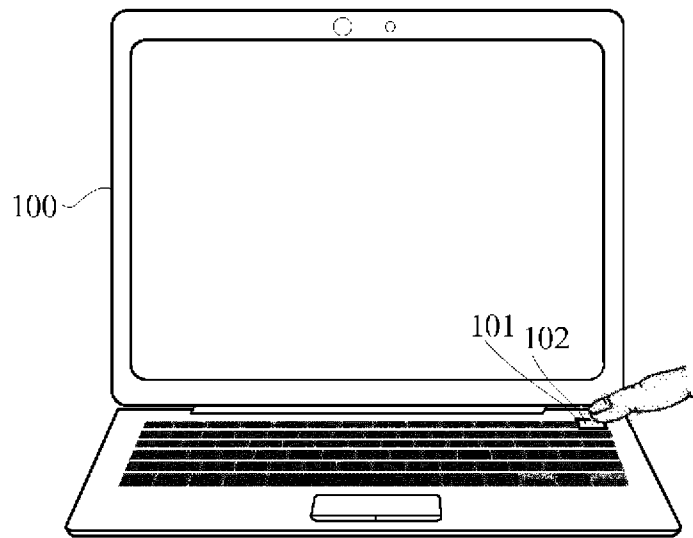


Figura 6A

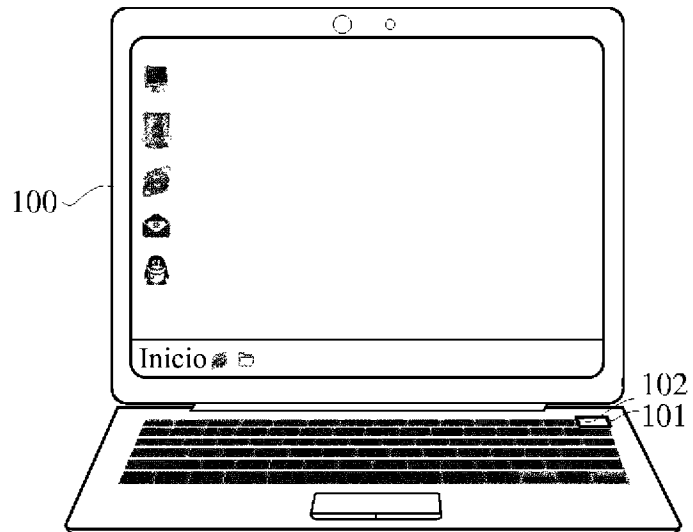


Figura 6B

Figura 6

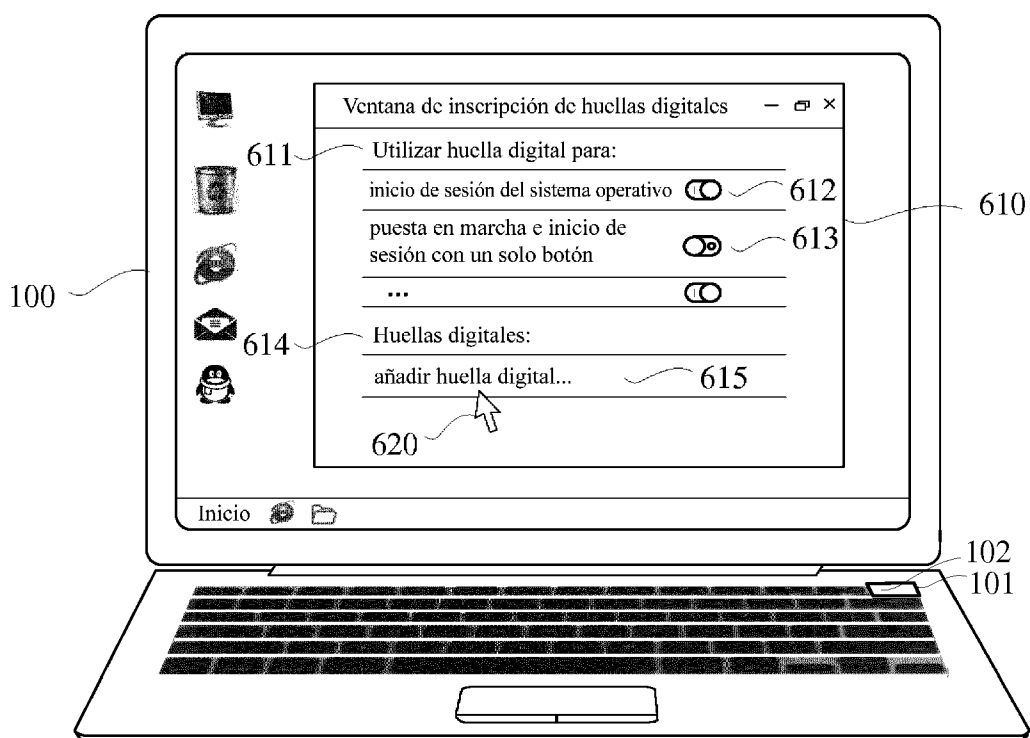


Figura 7A

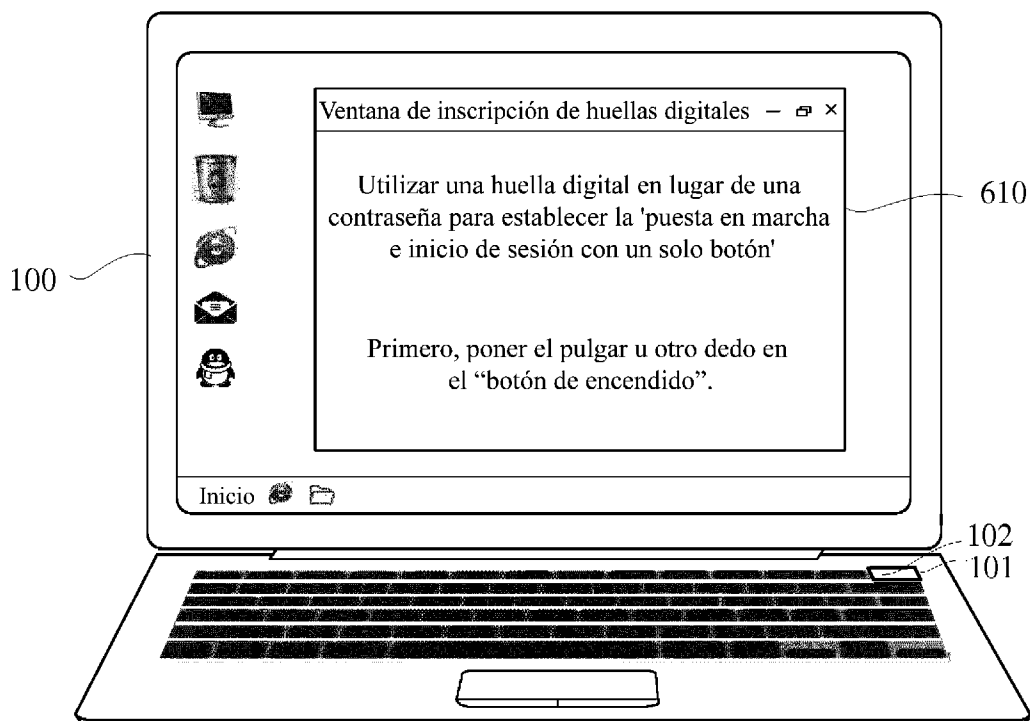


Figura 7B

Figura 7

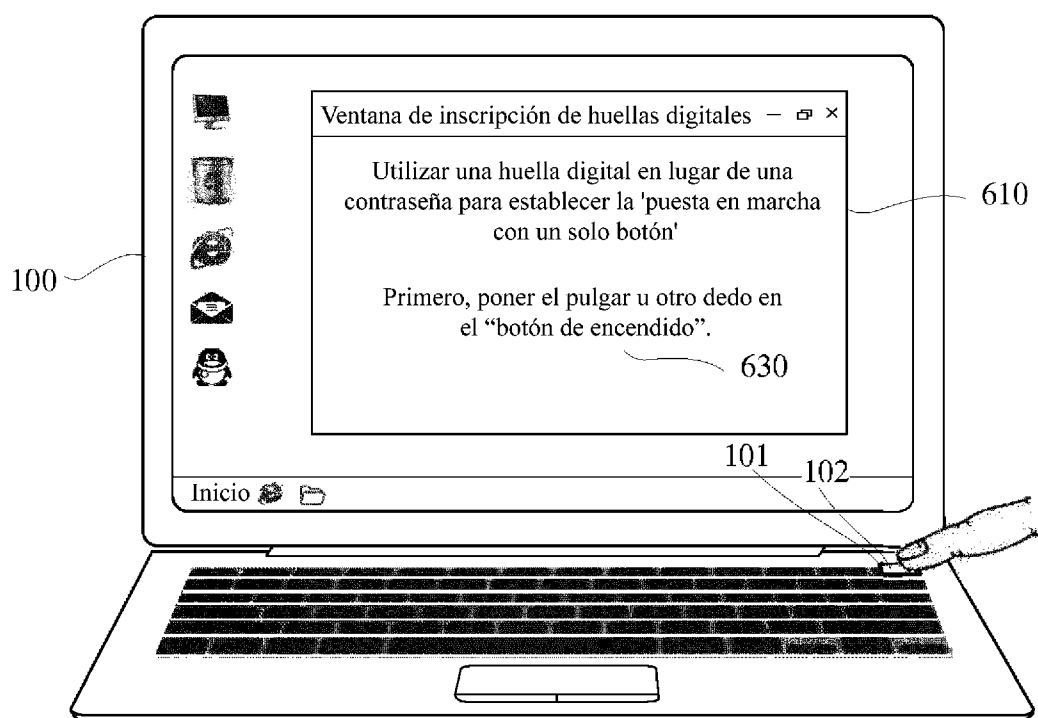


Figura 8A

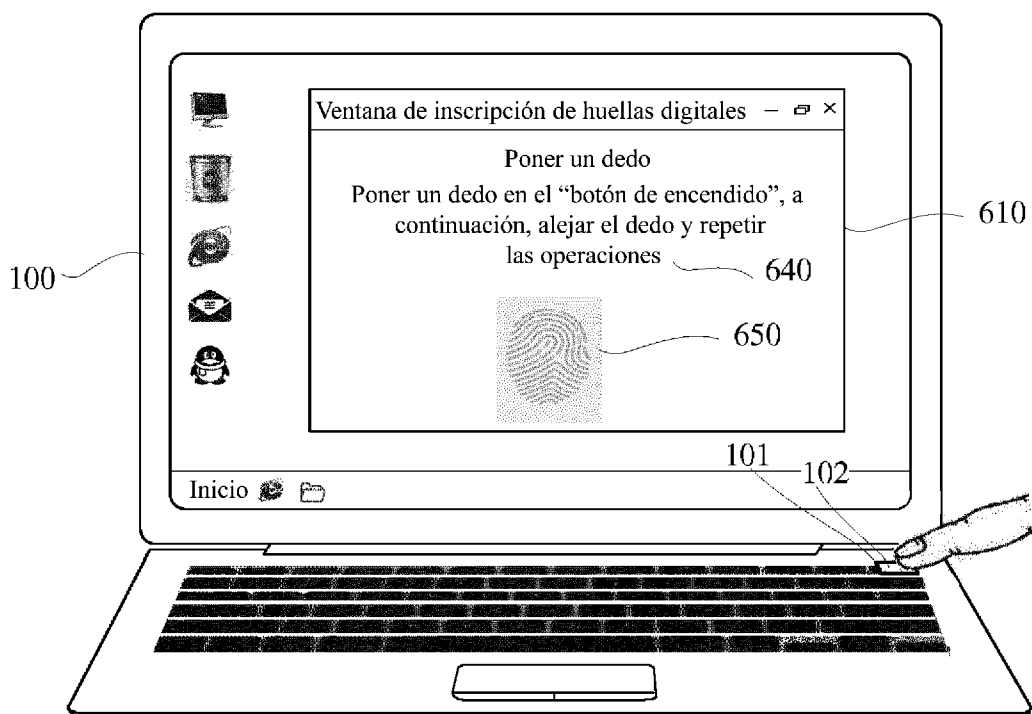


Figura 8B

Figura 8

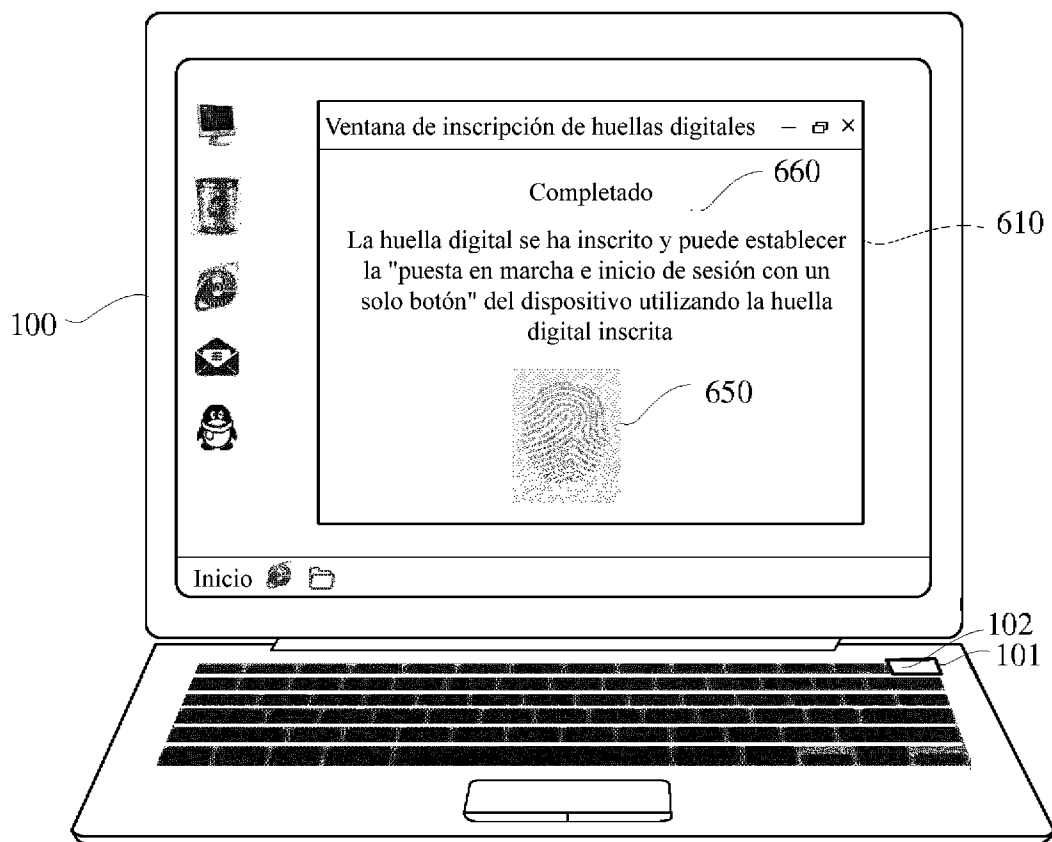


Figura 9

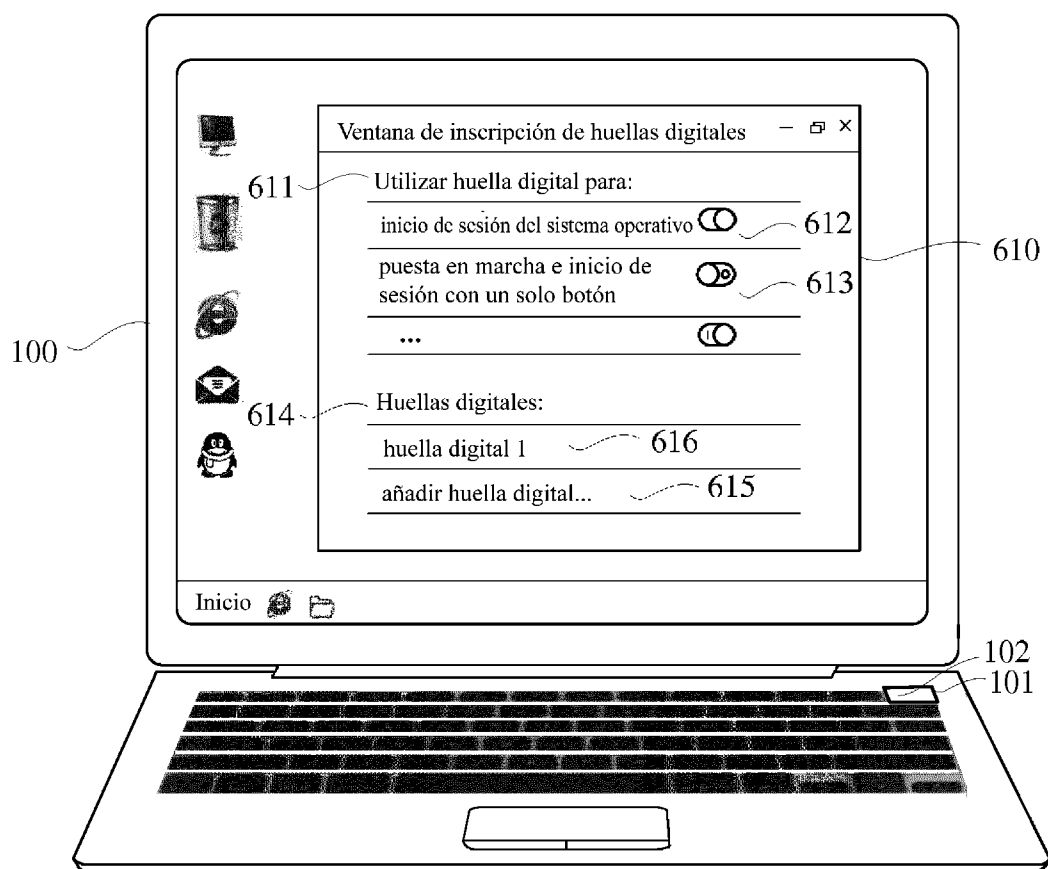


Figura 10

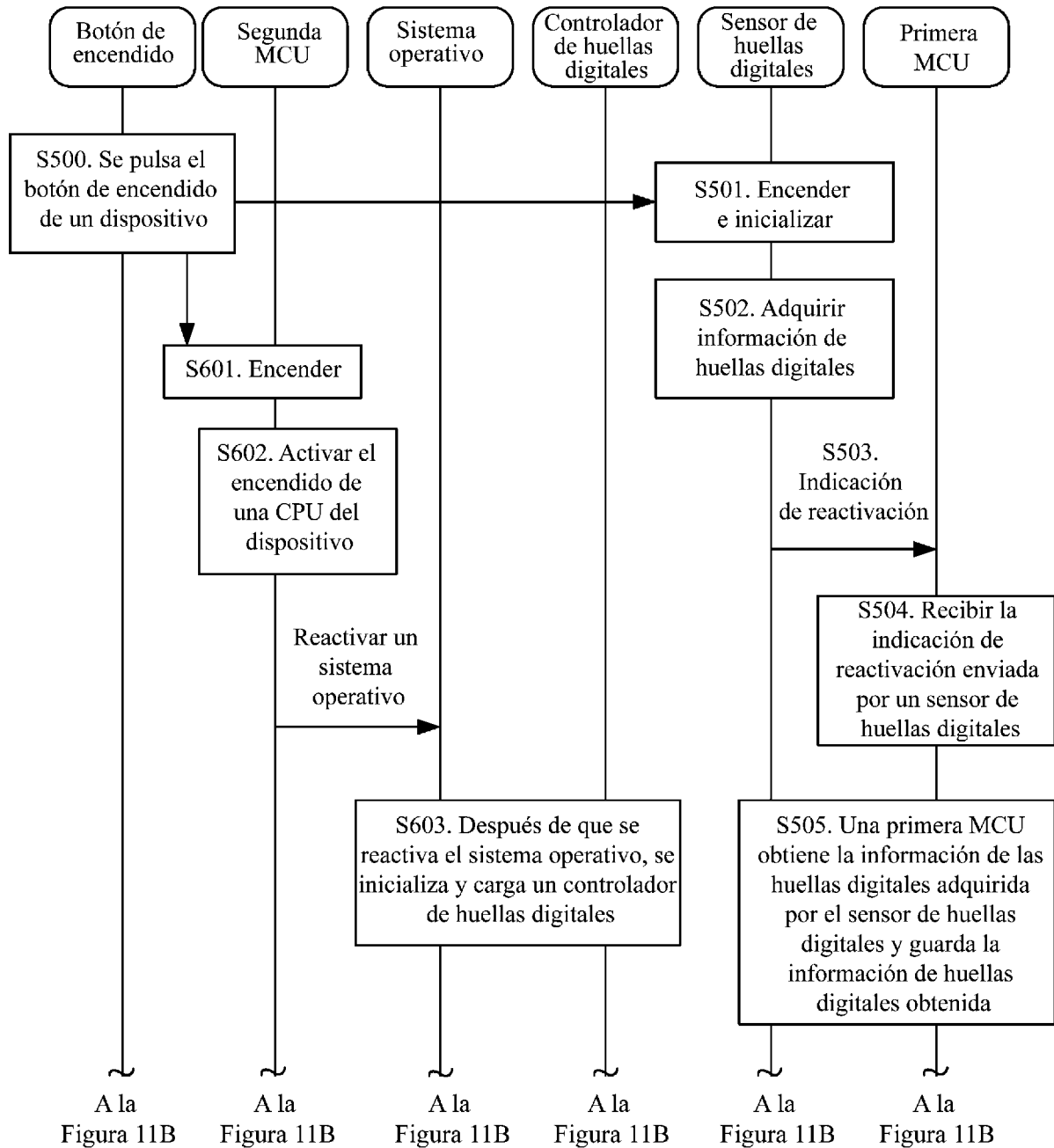


Figura 11A

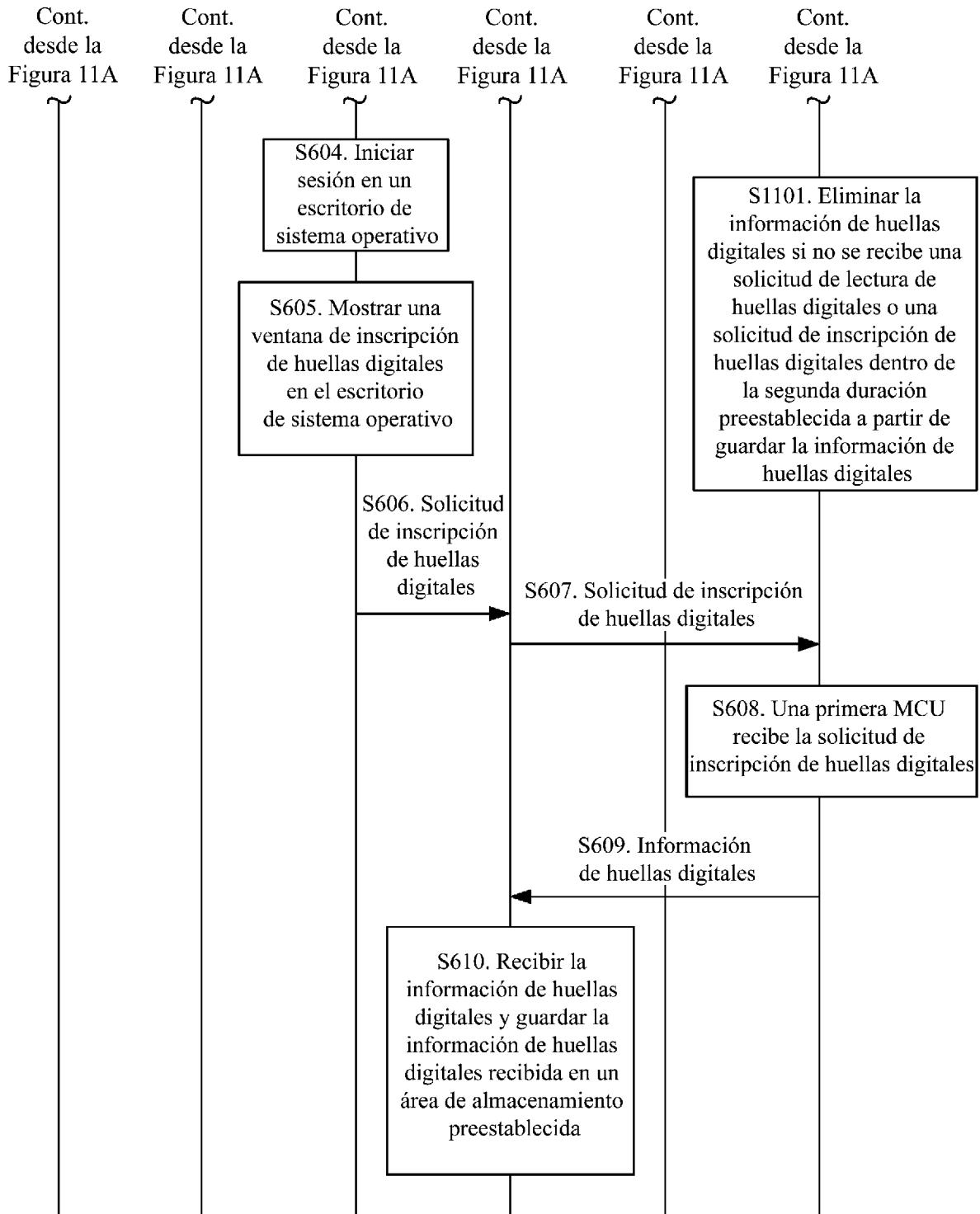


Figura 11B

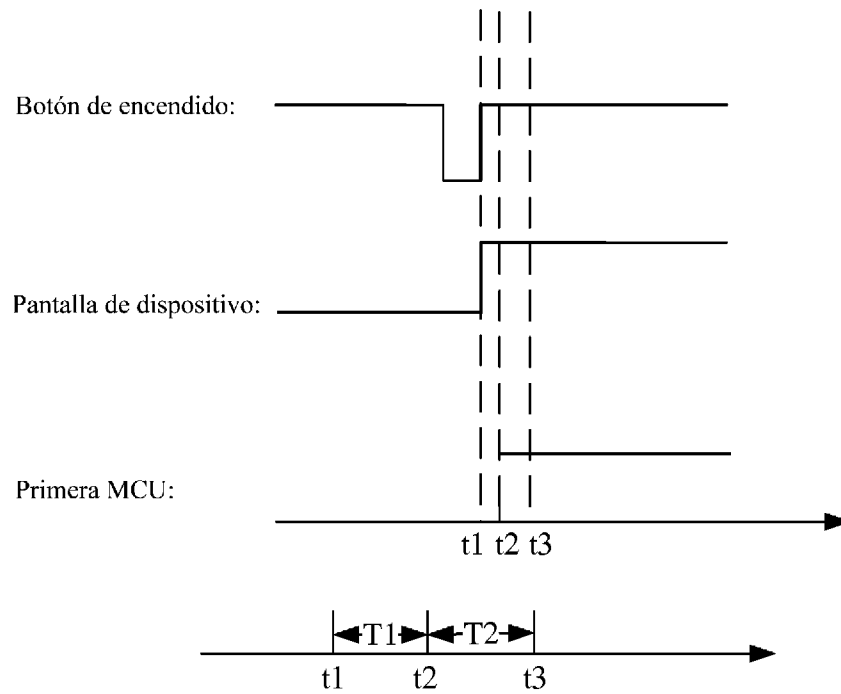


Figura 12

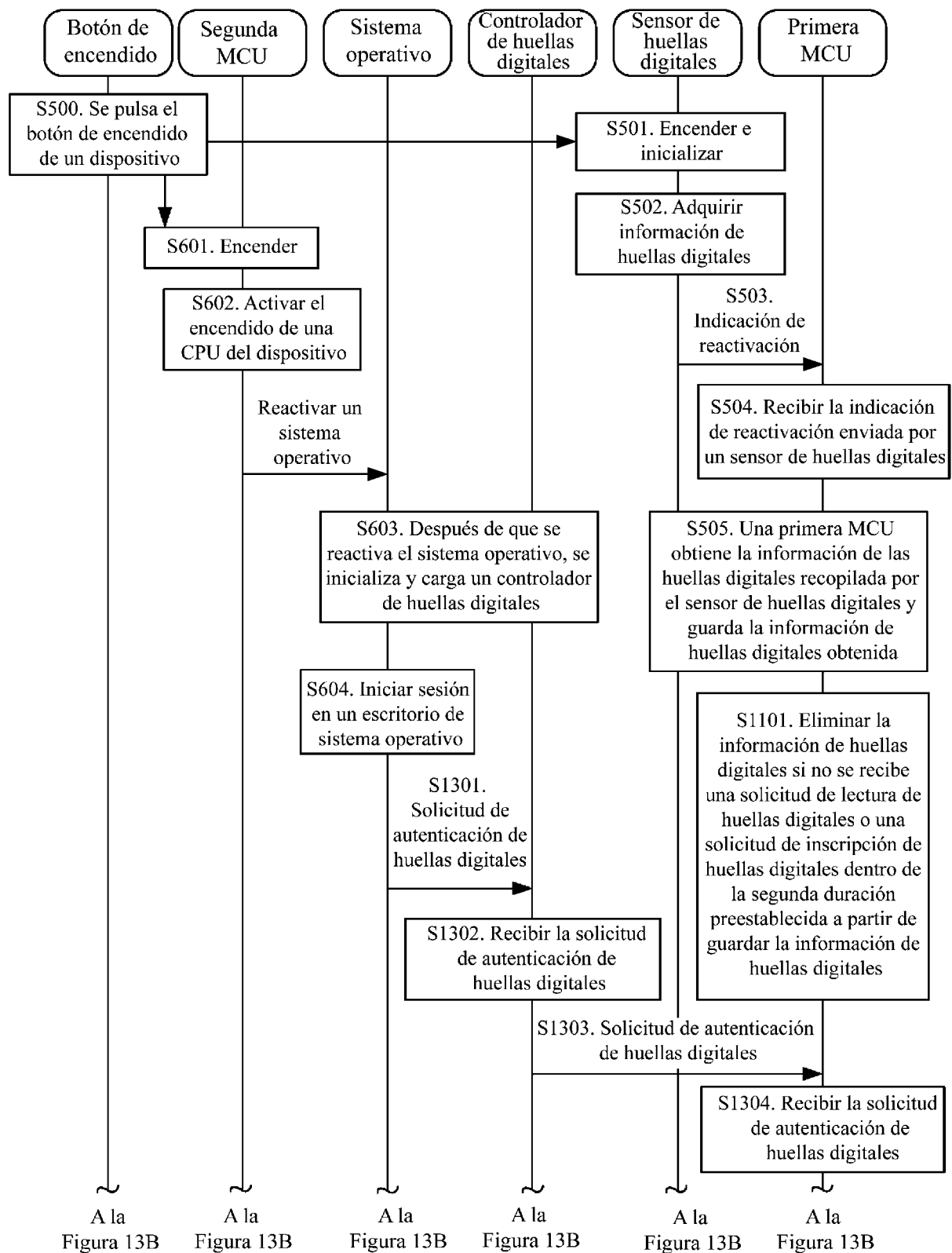


Figura 13A

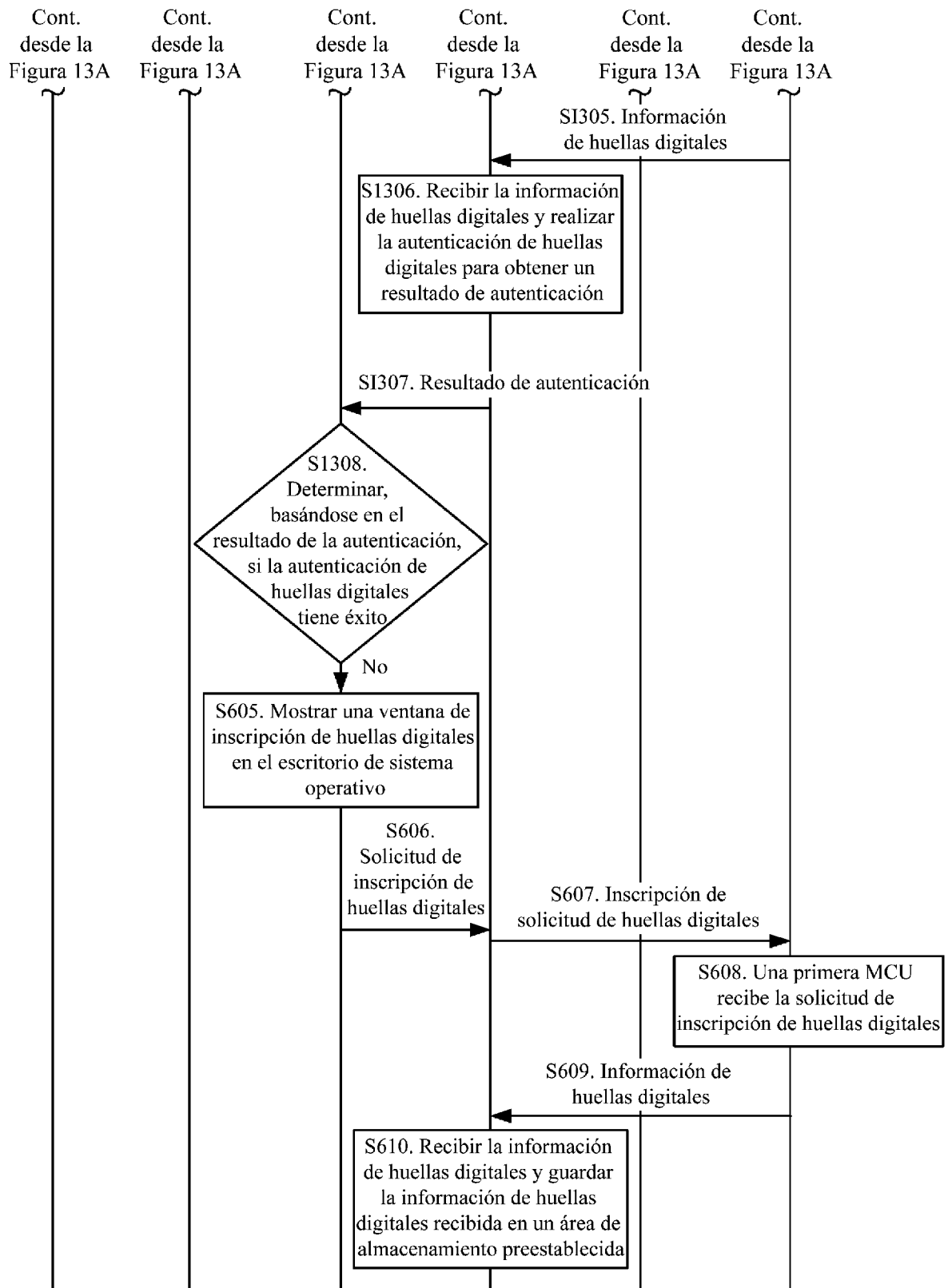


Figura 13B

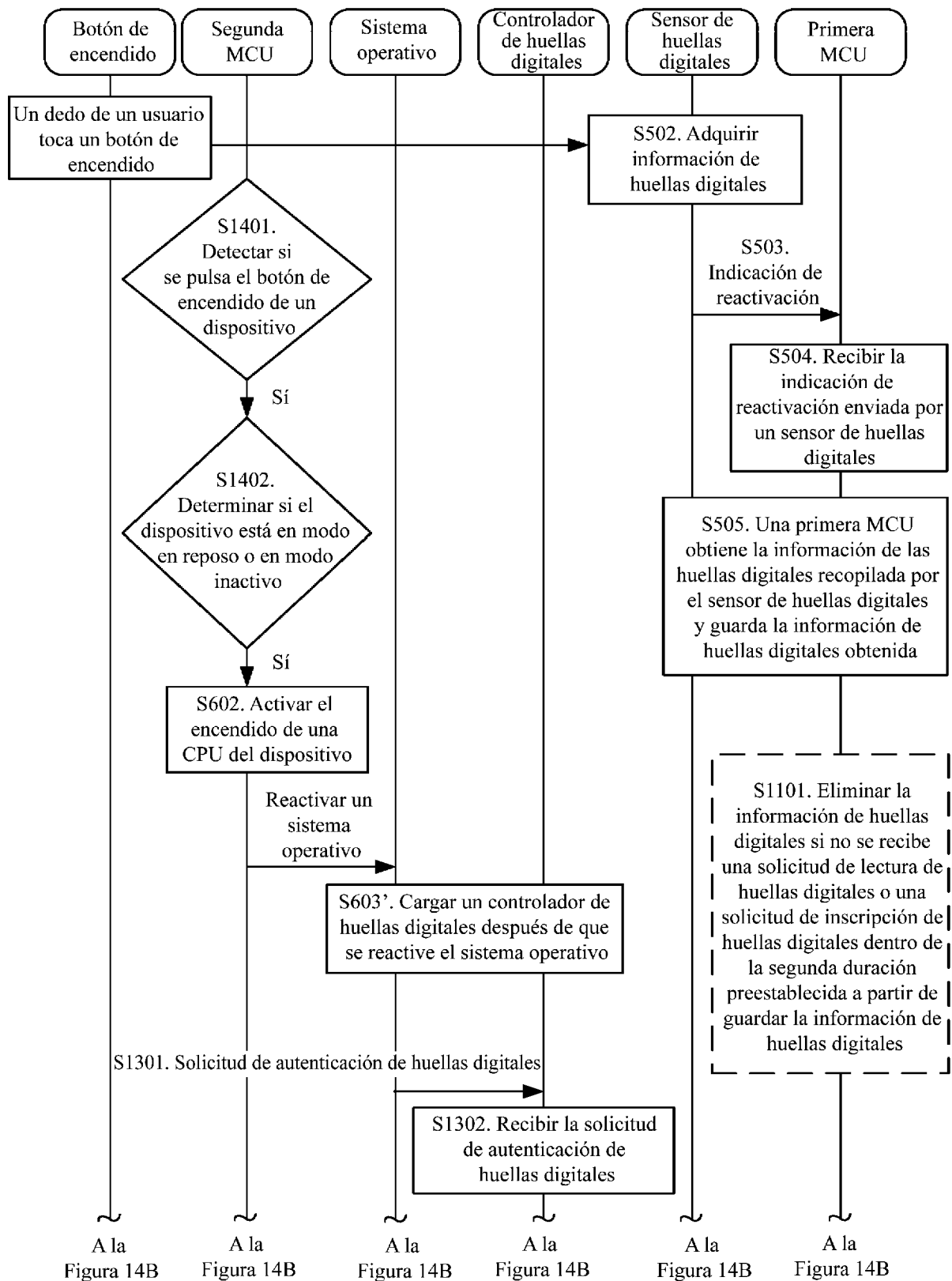


Figura 14A

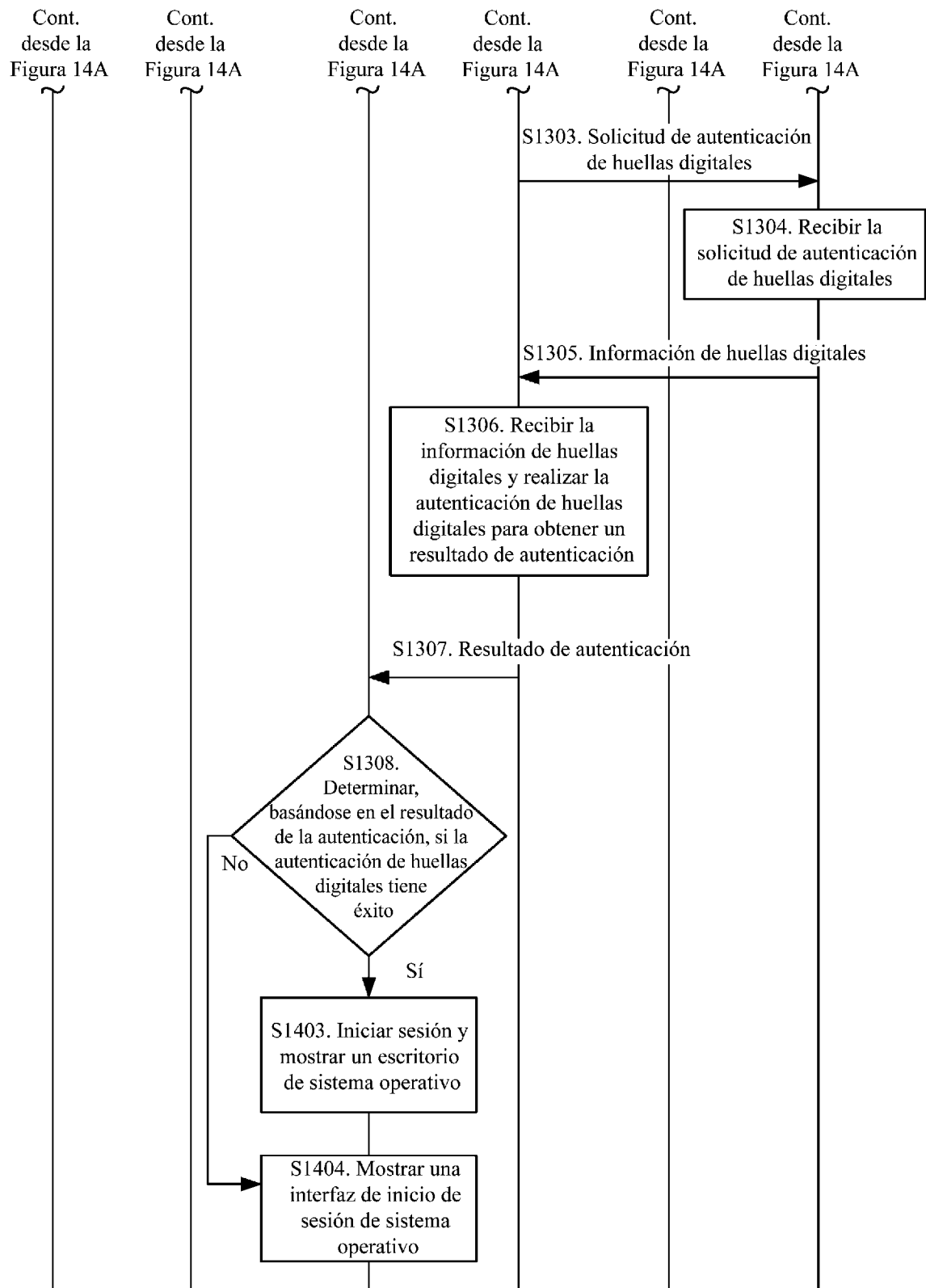


Figura 14B

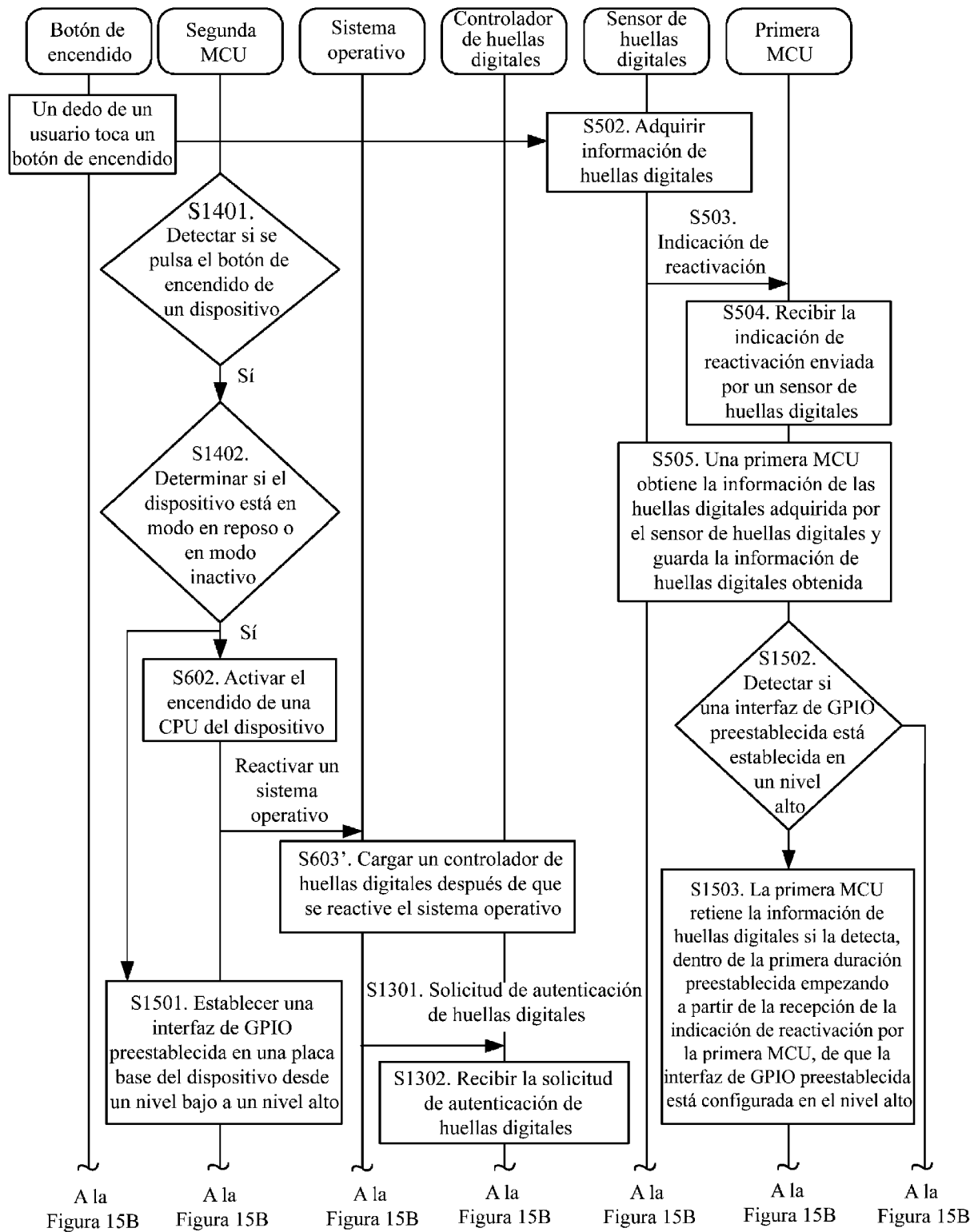


Figura 15A

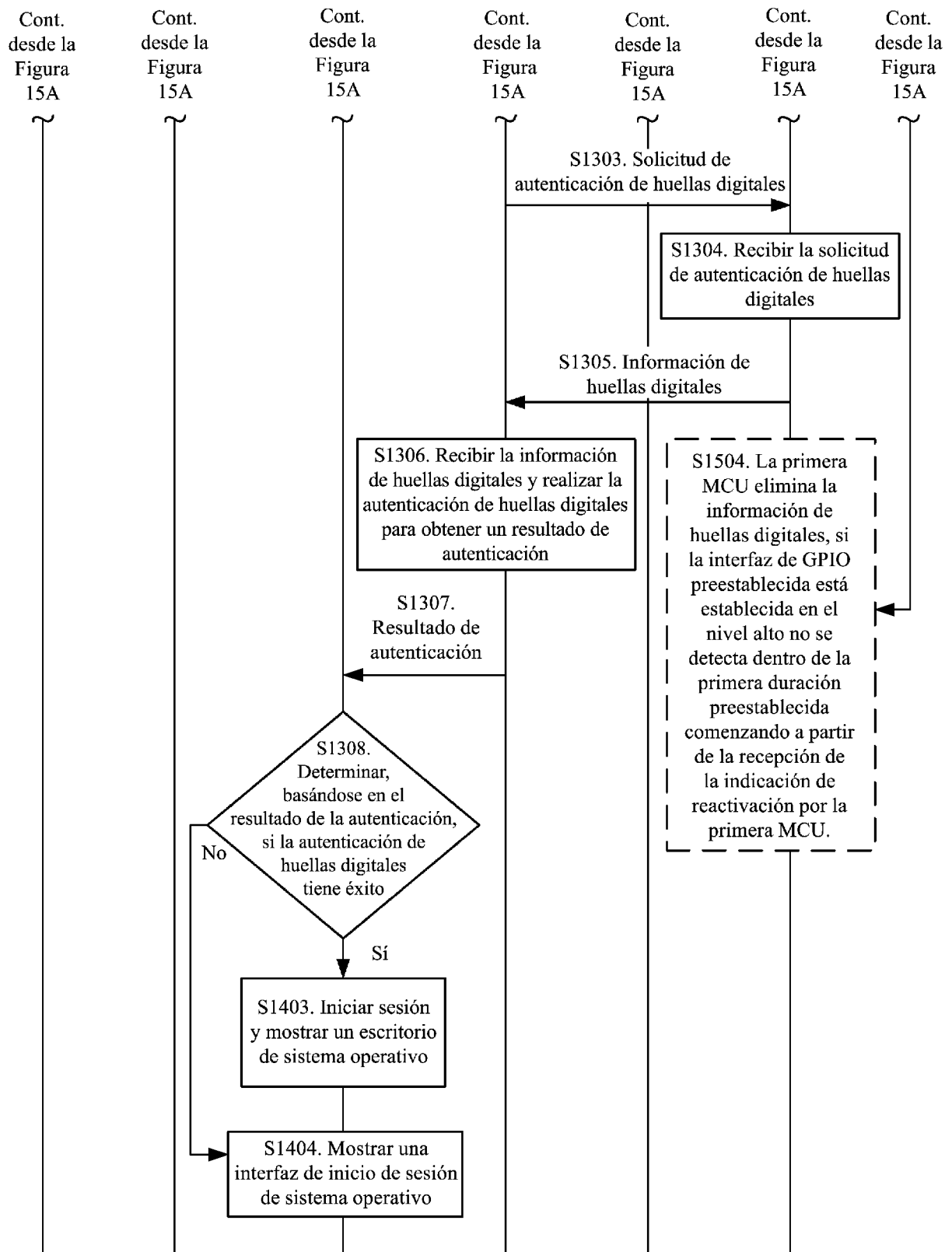


Figura 15B

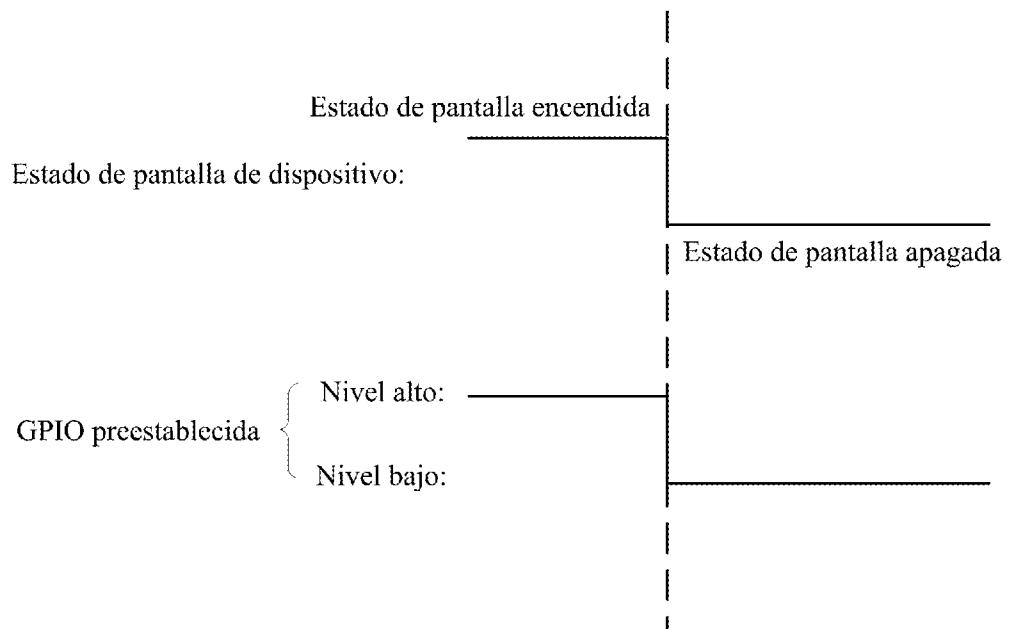


Figura 16

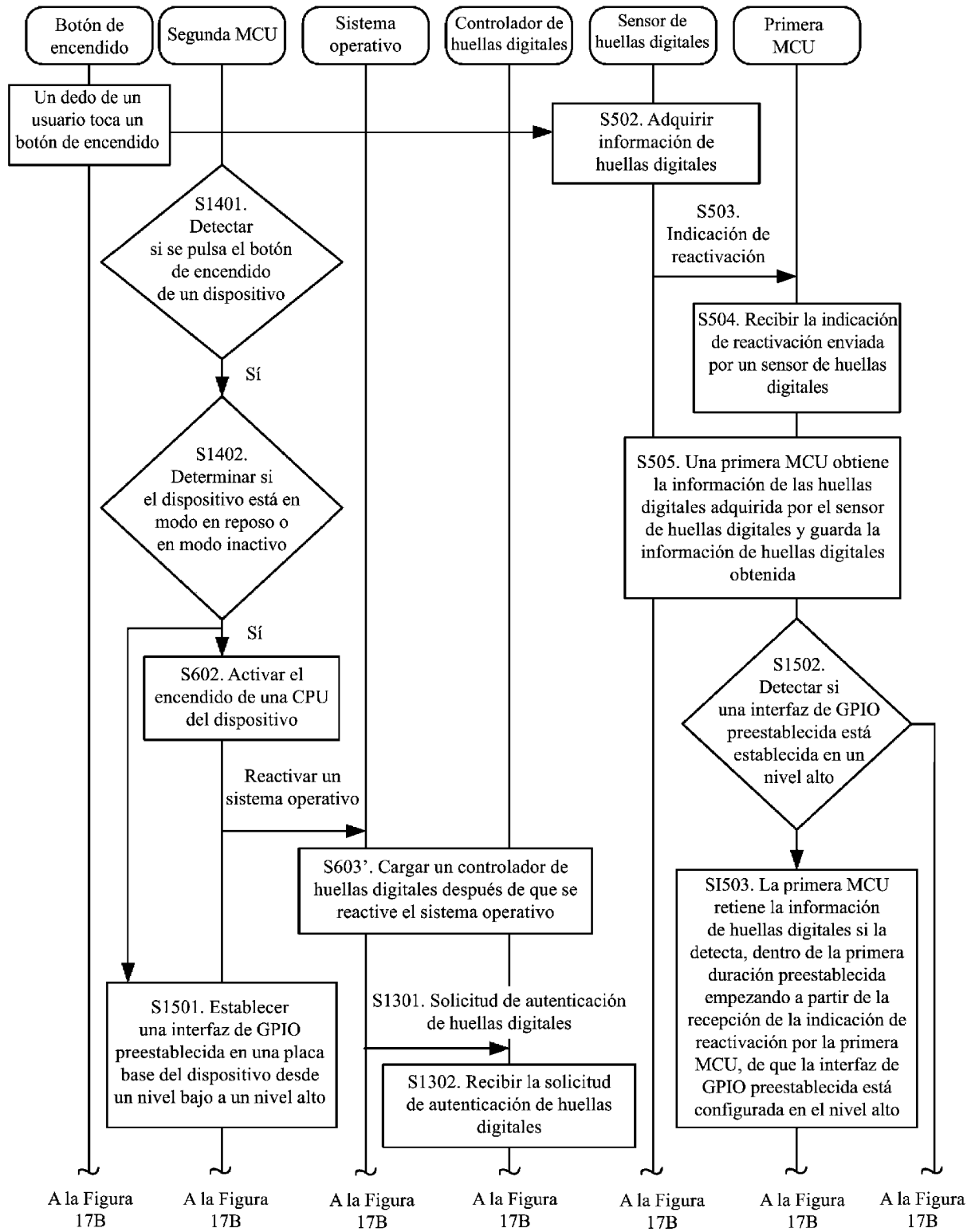


Figura 17A

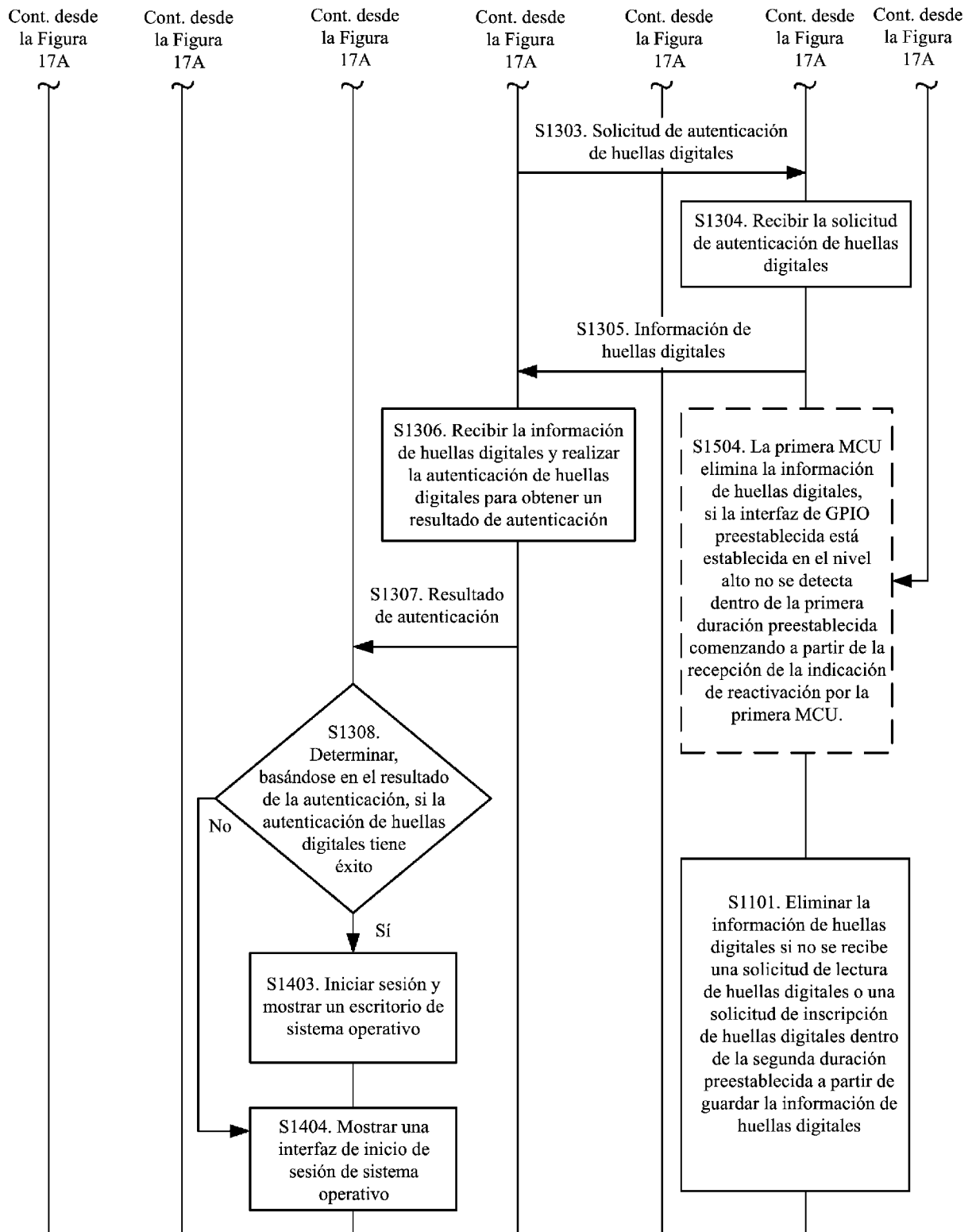


Figura 17B

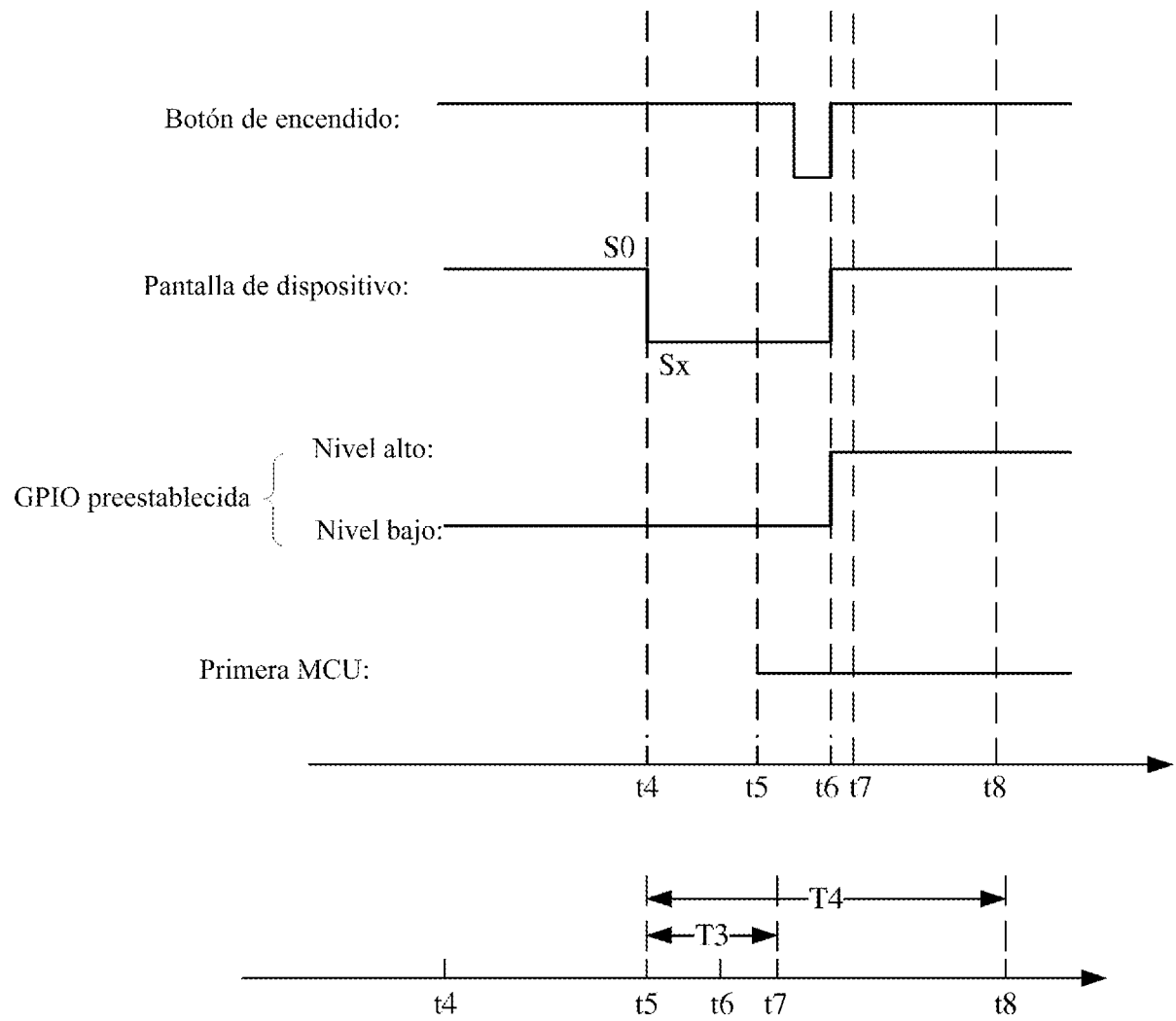


Figura 18

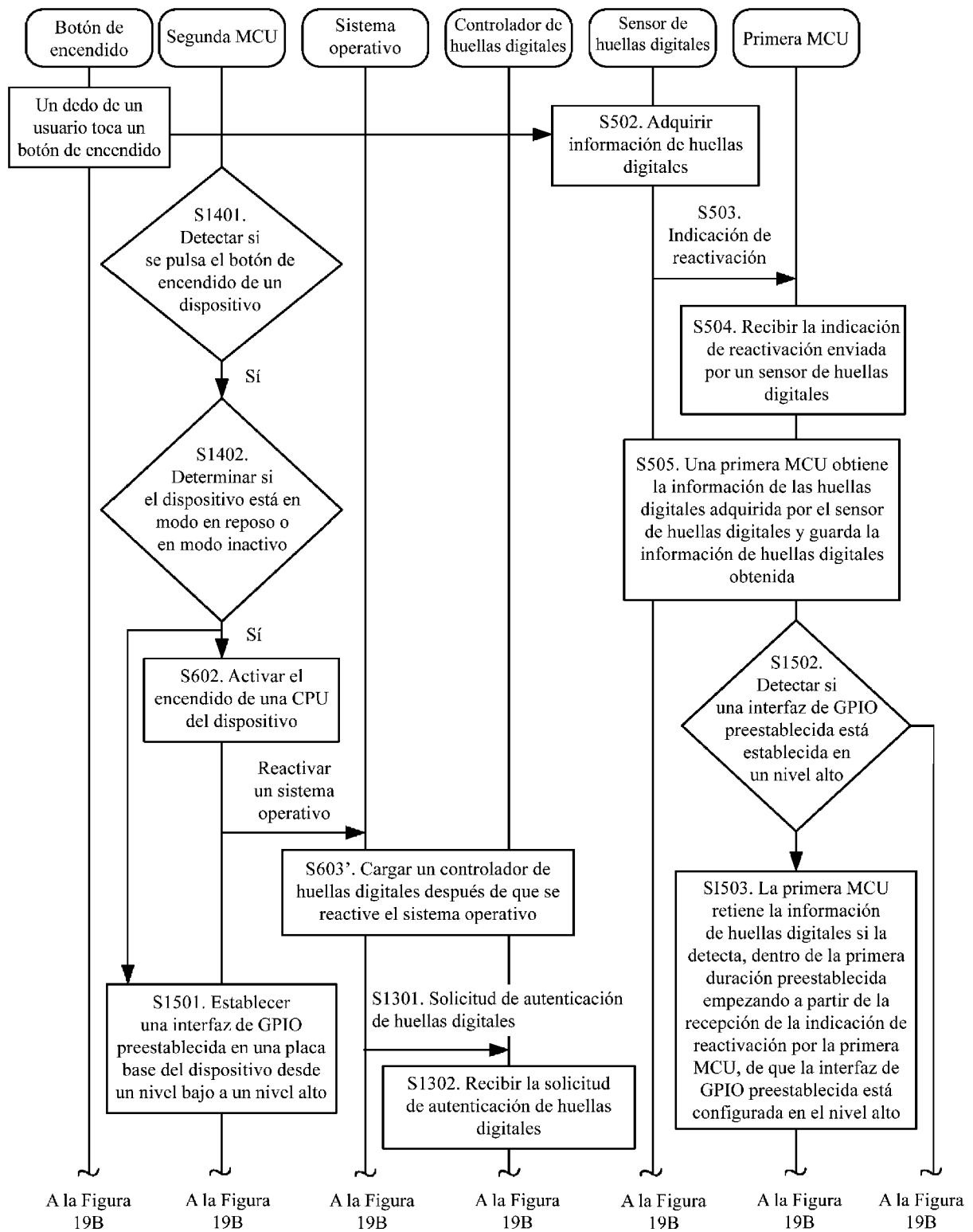


Figura 19A

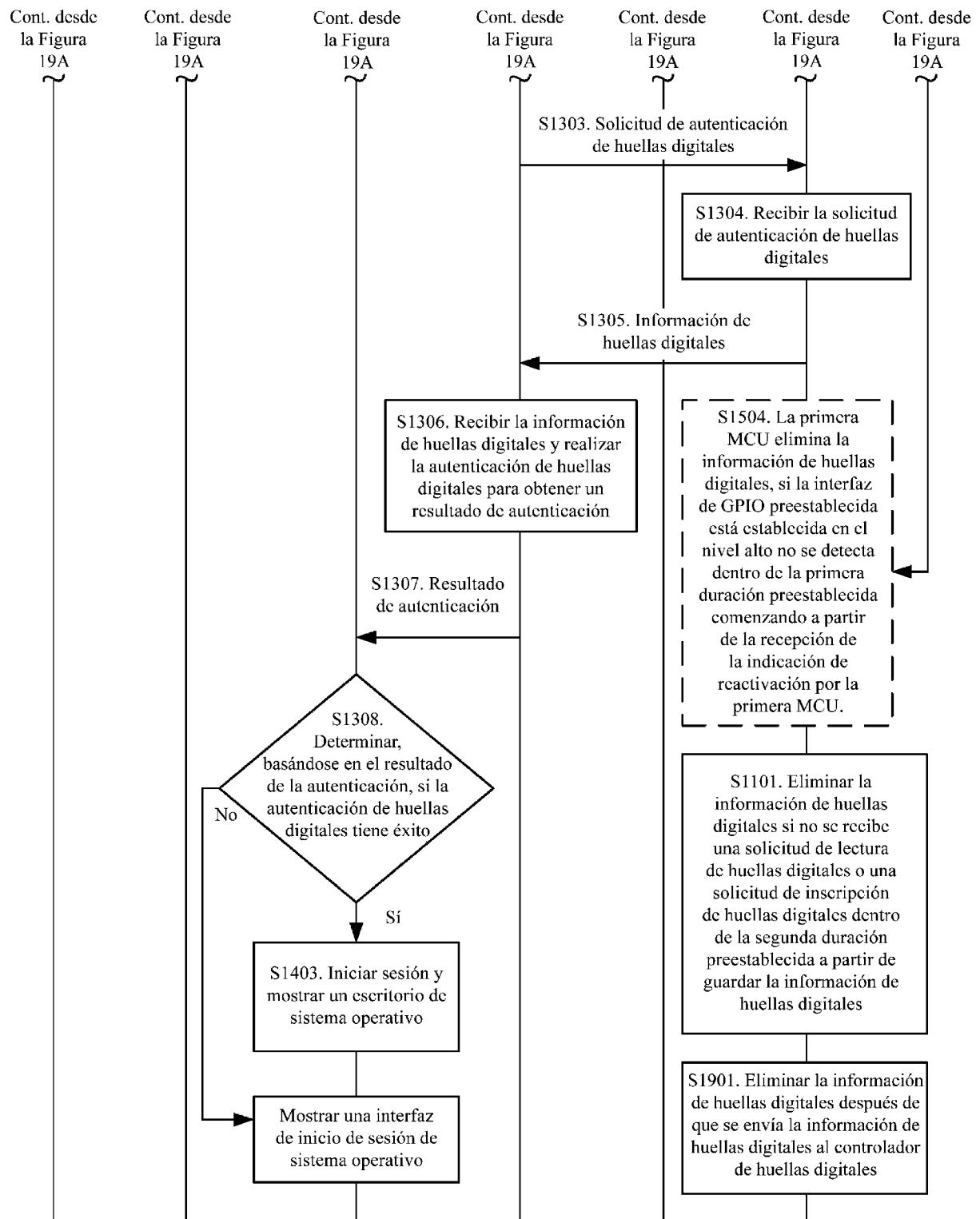


Figura 19B

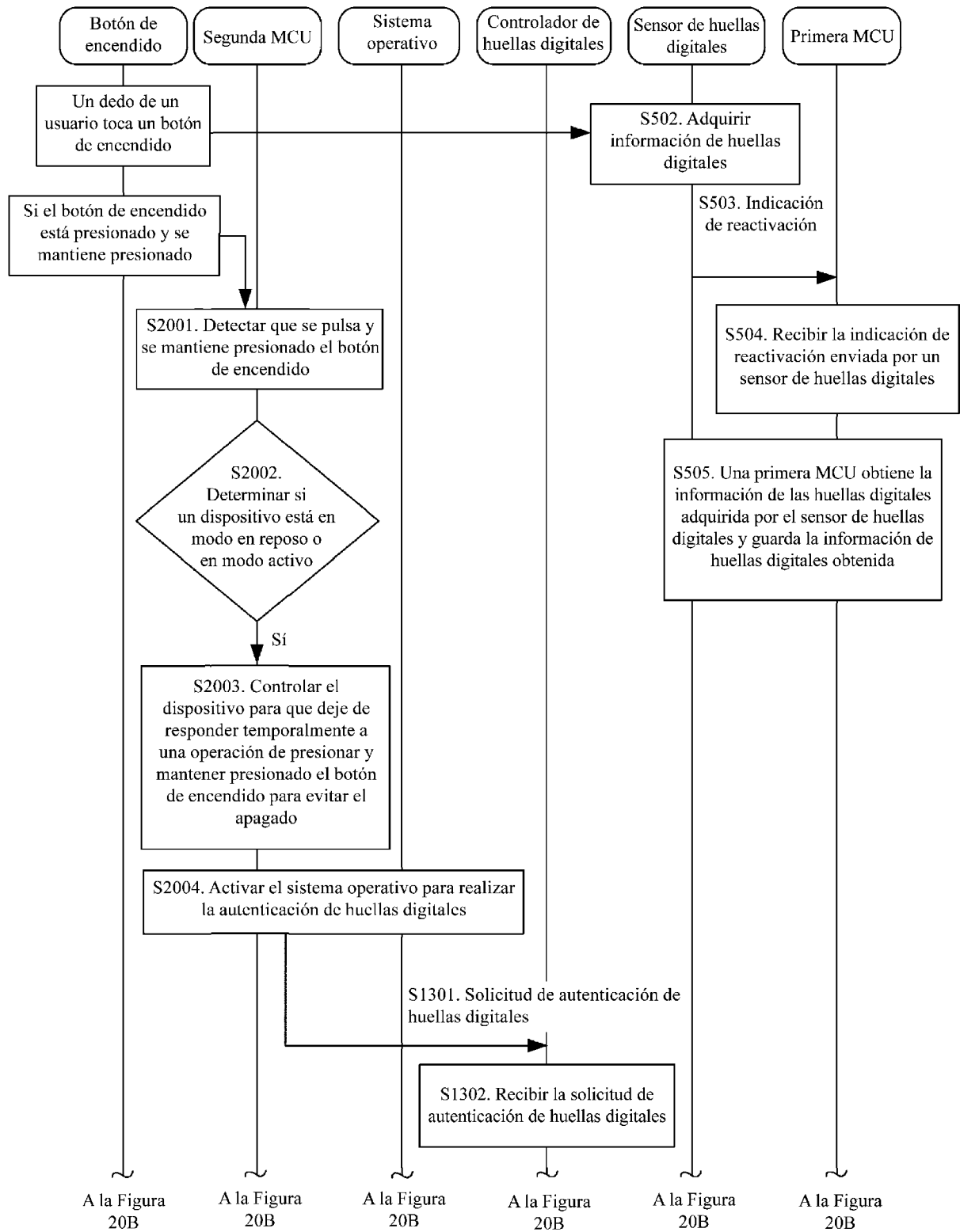


Figura 20A

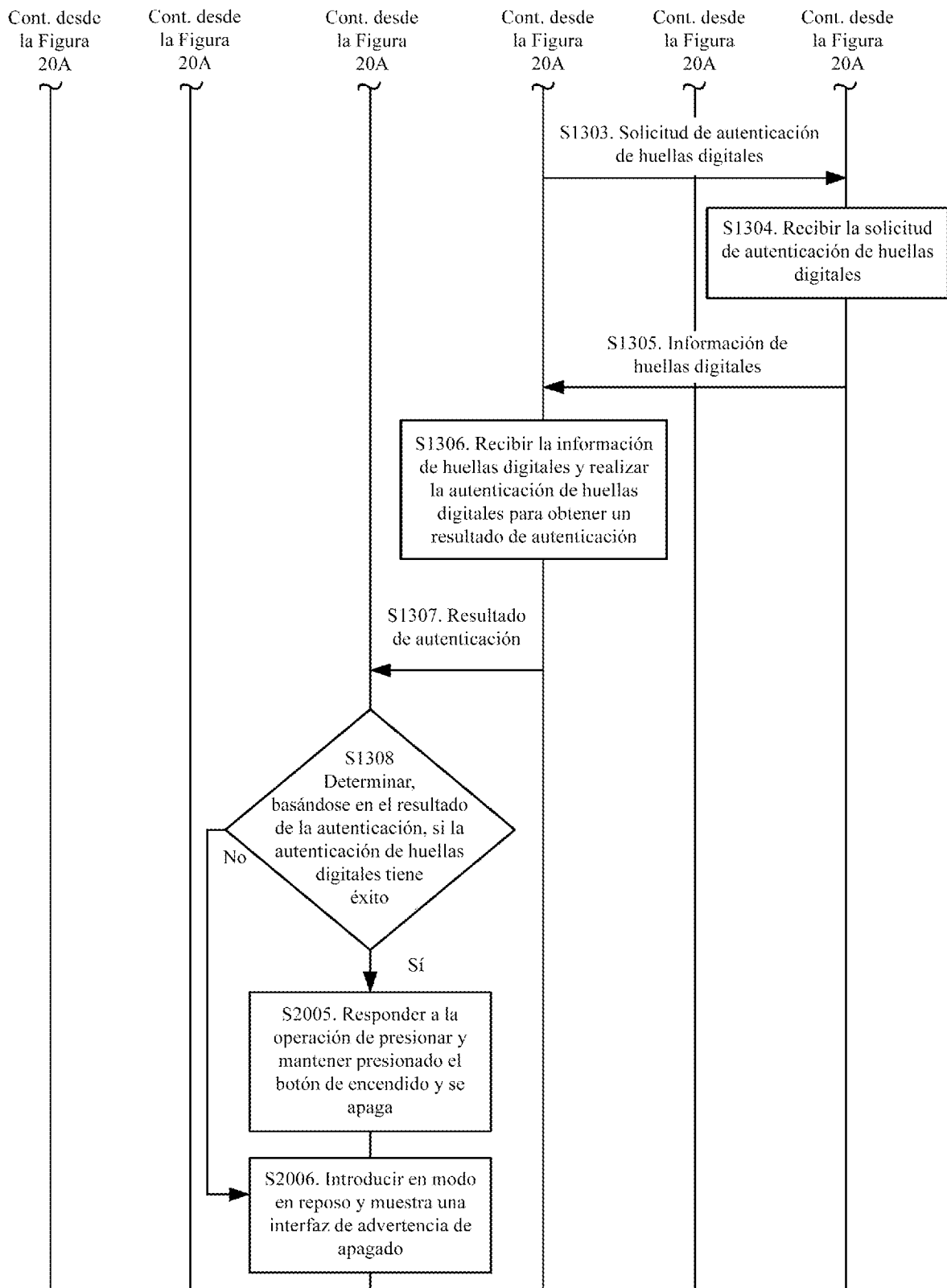


Figura 20B

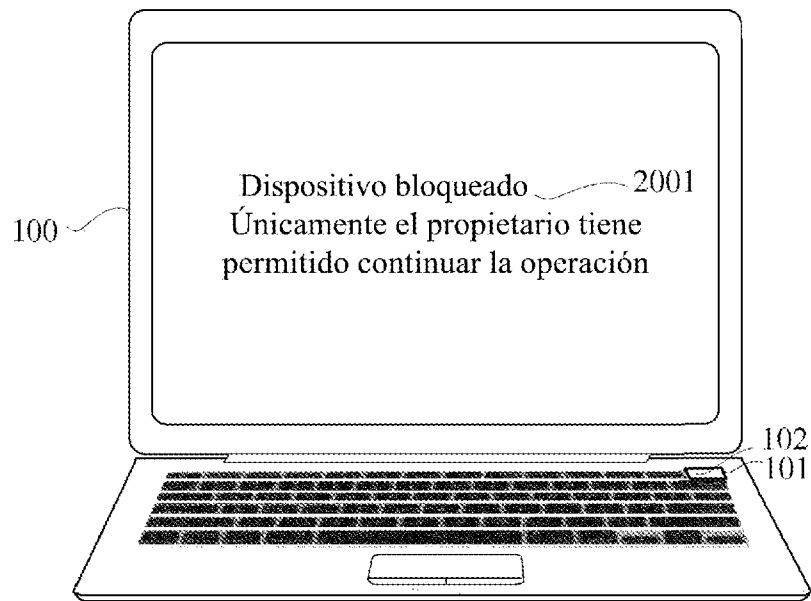


Figura 21

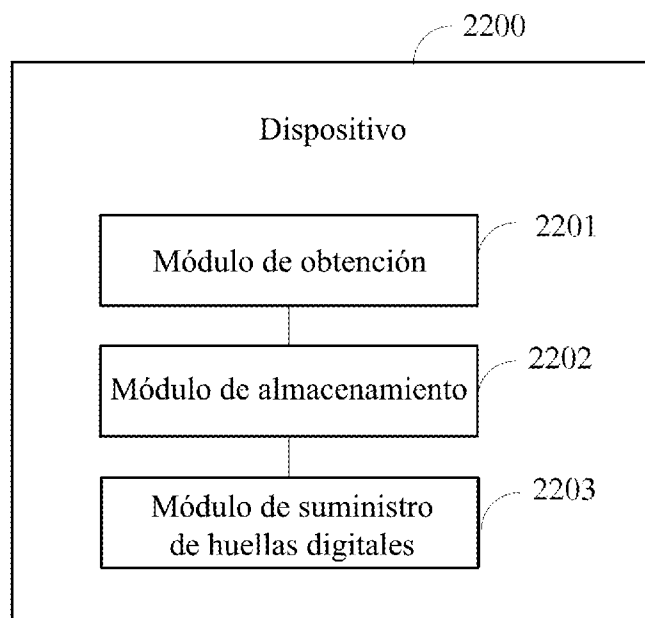


Figura 22

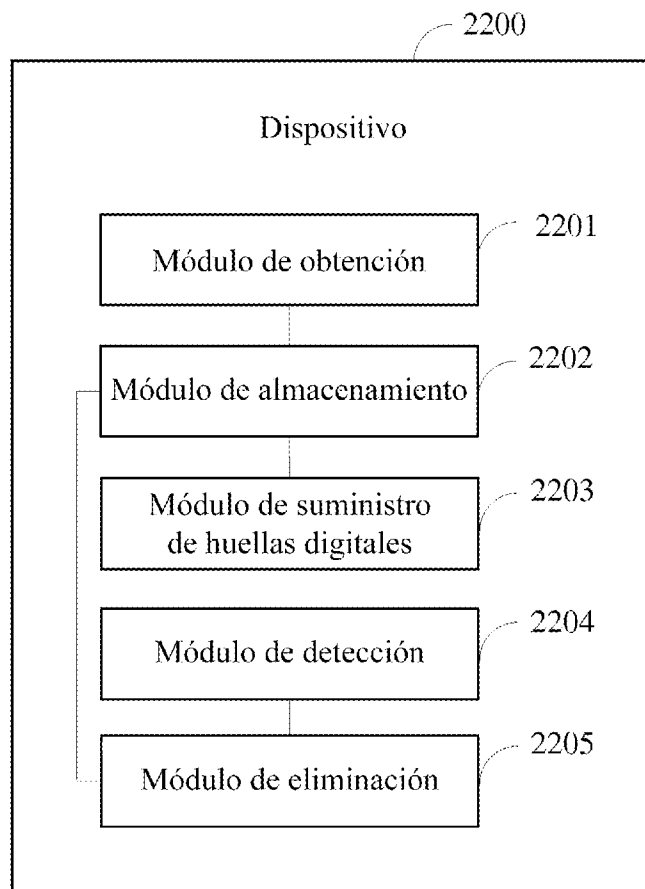


Figura 23

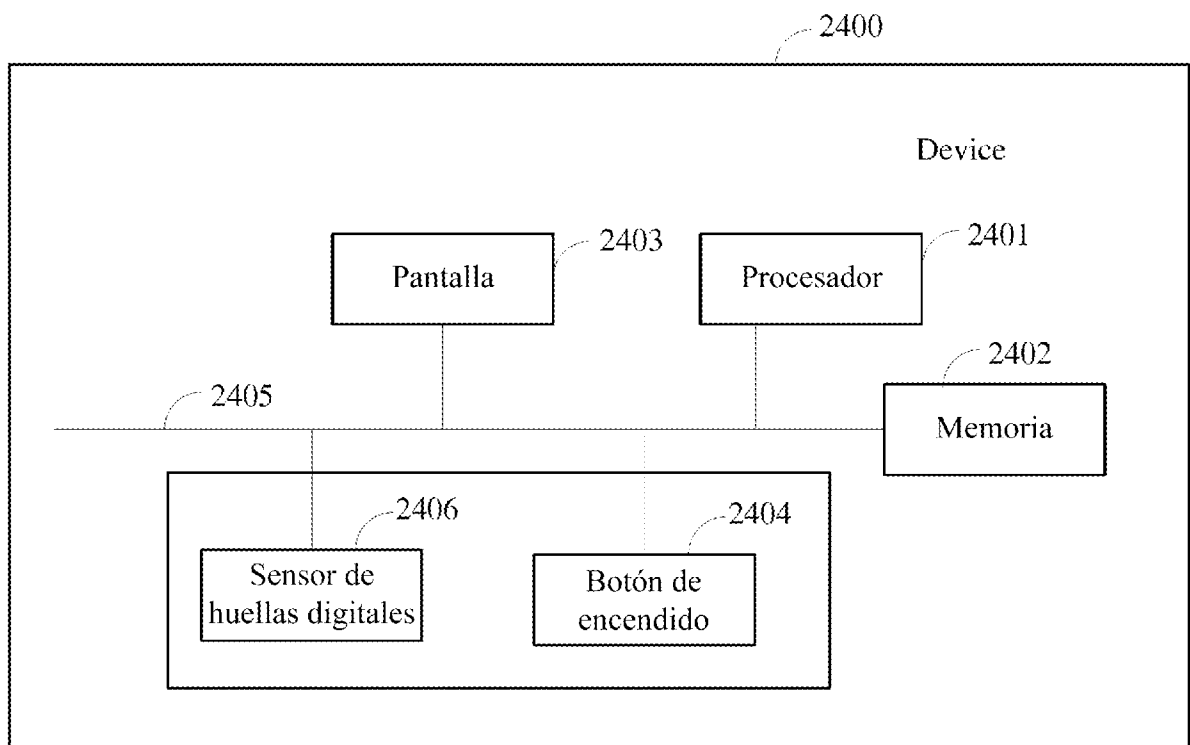


Figura 24

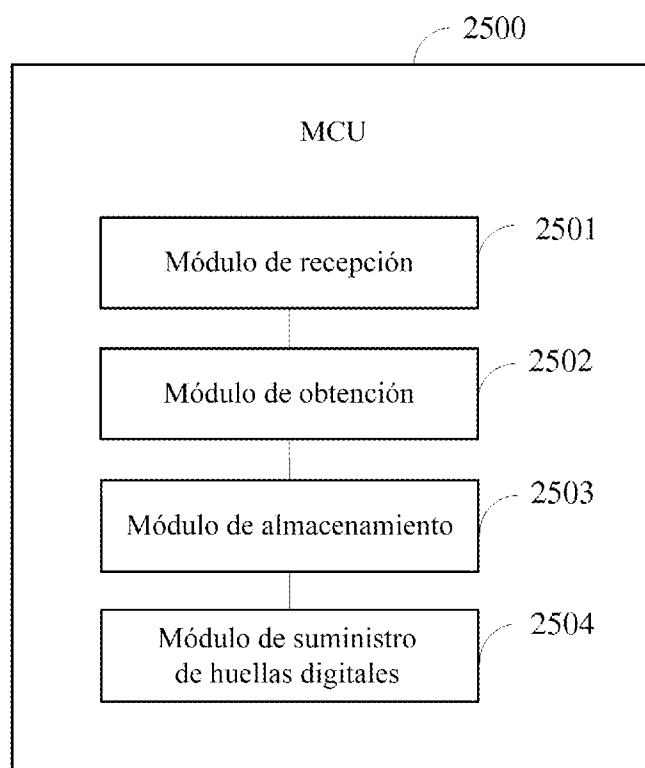


Figura 25

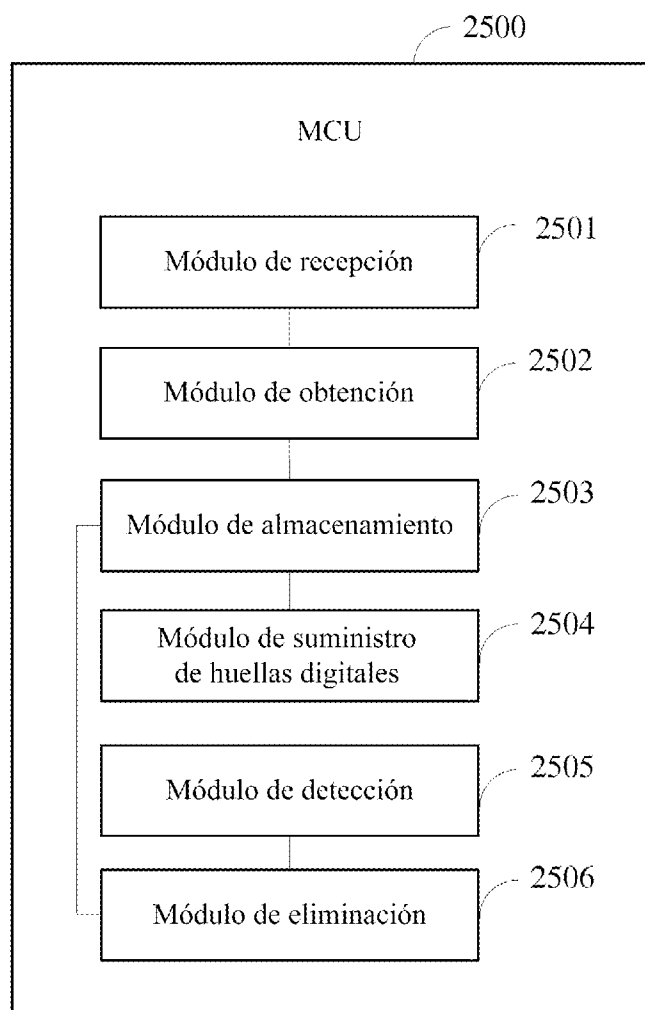


Figura 26

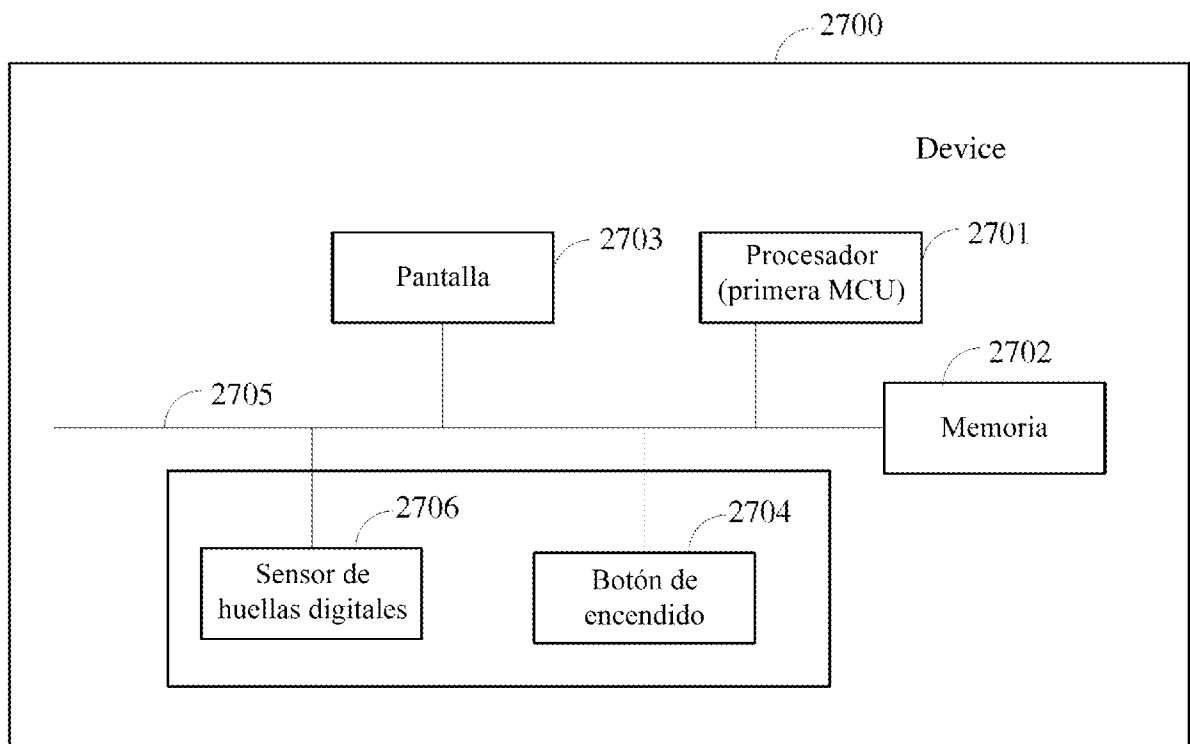


Figura 27

2800

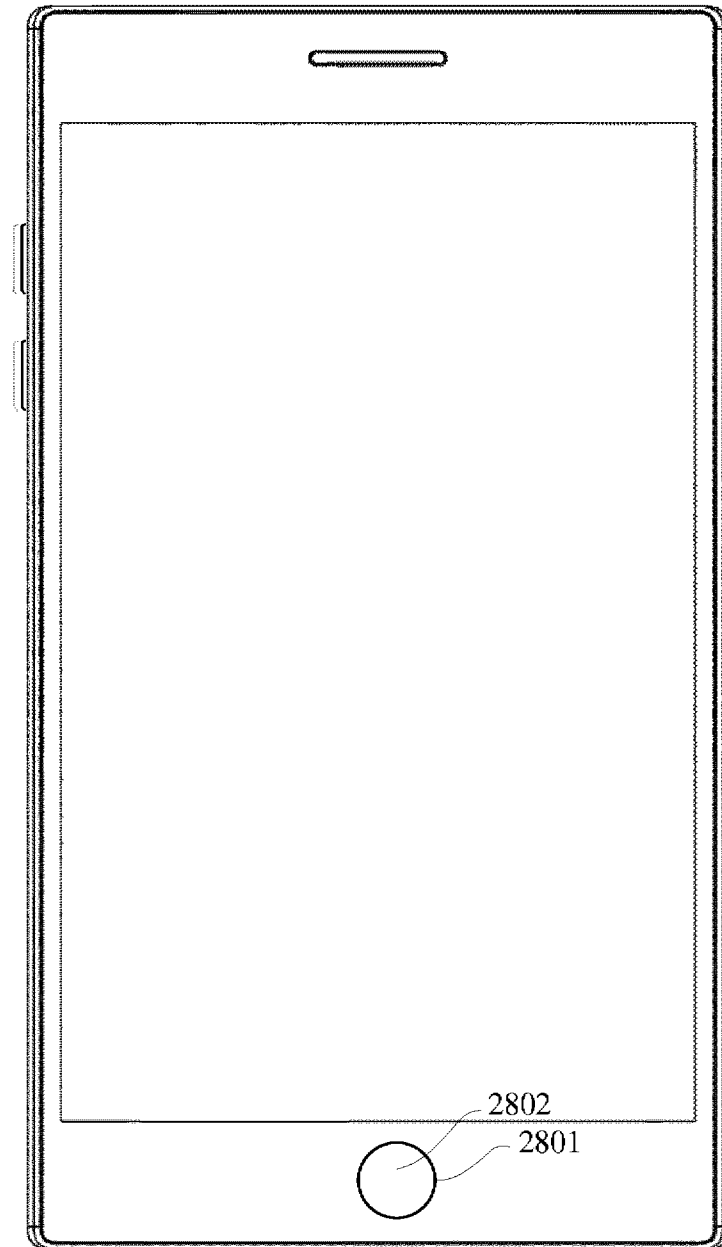


Figura 28

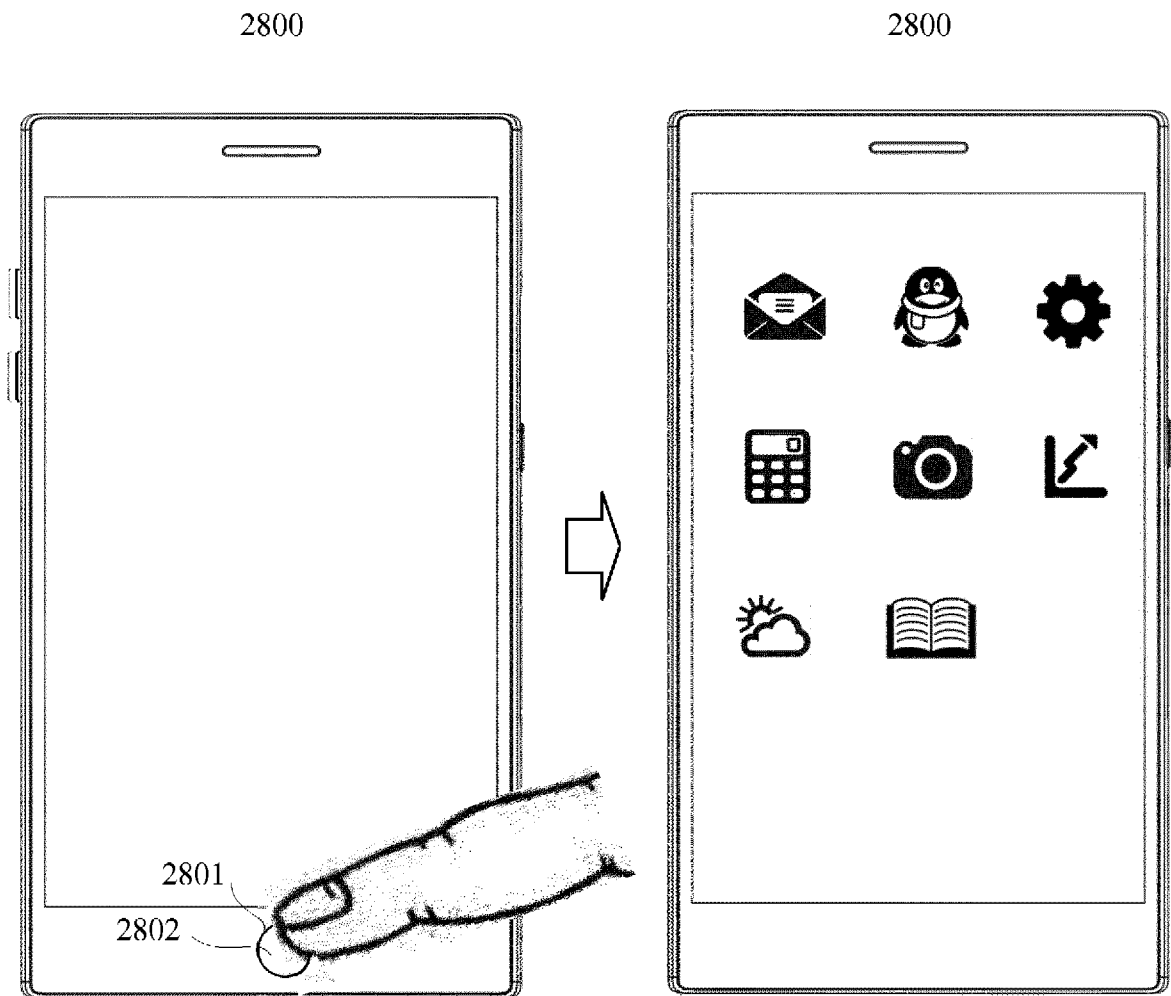


Figura 29A

Figura 29B

Figura 29