(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 741 632**

(51) Int. CI.:

H04L 29/06 (2006.01)
G06F 21/34 (2013.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **25.01.2011 E 11152033 (4)**

(97) Fecha y número de publicación de la concesión europea: **19.06.2019 EP 2355443**

(54) Título: **Procedimiento de autenticación de red y dispositivo para su implementación**

(30) Prioridad:

27.01.2010 TW 099102251

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
11.02.2020

(73) Titular/es:

KEYPASCO AB (100.0%)
Kyrkogatan 44
411 15 Gothenburg, SE

(72) Inventor/es:

LIN, MAW-TSONG

(74) Agente/Representante:

ARIZTI ACHA, Monica

DESCRIPCIÓN

Procedimiento de autenticación de red y dispositivo para su implementación

La presente invención se refiere a un método y dispositivo de autenticación de red, más particularmente a un método y dispositivo de autenticación de red adaptado para autenticar un terminal de usuario que usa un software.

Actualmente, cuando un usuario desea transferir dinero en un banco en la web proporcionado por una institución bancaria, el usuario necesita introducir un código de identificación de usuario (ID del usuario) único y una contraseña para acceder a la banca en web. El ID de usuario puede obtenerse usando un lector de tarjeta que lee una tarjeta de circuito integrado entregada por la institución bancaria o puede ser un código preestablecido fijado por el usuario y certificado por la institución bancaria. Después de acceder a la banca en web, el usuario necesita llenar una hoja de transferencia electrónica e introducir una contraseña de transferencia para completar la transferencia.

Dado que el ID de usuario, la contraseña y la contraseña de transferencia pueden robarse, se usa un identificador (token) o una tarjeta de circuito integrado para proporcionar una contraseña de un solo uso (OTP) para su envío a un servidor de la red de la banca en web para verificar la identidad del usuario. Adicionalmente, puede usarse un identificador o lector de tarjeta que incluye su propia pantalla y teclas o una unidad flash que tiene un certificado de infraestructura de clave pública para impedir que el ID de usuario y la contraseña sean robadas.

Sin embargo, debido a la variedad de transacciones en la web, al número creciente de usuarios de la web y de delitos en la web, y el continuo progreso de las técnicas criminales, los métodos de verificación actuales tienen los siguientes inconvenientes.

Un proveedor de contenidos de la red necesita comprar un dispositivo de verificación de identidad para cada usuario y el coste del servicio al cliente para personalización, distribución y resolución de problemas es considerable. Adicionalmente, es bastante incómodo para el usuario que el usuario necesite tener diferentes dispositivos de verificación de identidad para diferentes sitios web. Más aún, junto con interceptar y robar el ID del usuario, la contraseña y la contraseña de transferencia, los hackers también tratan de manipular los datos de la transacción. Por lo tanto, el proveedor de contenidos de la red está forzado frecuentemente a cambiar sus equipos de hardware y el coste del cambio de los equipos de hardware es considerable.

Los documentos US 2008/298588 A1 y WO 2008/127431 A1 se refieren a un sistema de seguridad informático para su uso en la identificación y autenticación de un usuario. En un aspecto, se proporciona un método para identificar y autenticar a un usuario. El método incluye establecer una confianza entre una máquina del servidor y un agente en una máquina de usuario. El método incluye adicionalmente establecer una clave de sesión para cifrar las comunicaciones entre la máquina del servidor y el agente. El método incluye también recibir un nombre de usuario y contraseña para su uso en la validación del usuario. Adicionalmente, el método incluye crear un ejecutable binario para la extracción de datos del dispositivo desde la máquina del usuario para identificar de modo único la máquina. En otro aspecto, se proporciona un medio legible por ordenador que incluye un conjunto de instrucciones que cuando se ejecutan por un procesador hacen que el procesador identifique y autentique al usuario. En un aspecto adicional, se proporciona un sistema para identificar y autenticar a un usuario.

El documento US 6, 418, 472 B1 describe un sistema y método para controlar el acceso a un objeto. El sistema almacena un objeto y un identificador del procesador. El sistema incluye un agente de verificación que puede acceder a la información embebida en un procesador y calcular a continuación a partir de esa información embebida un valor que puede compararse con el identificador del procesador almacenado. Se usa un agente de comparación para comparar ese valor con el identificador del procesador para determinar si el procesador corresponde al identificador del procesador. Si el valor que el agente de verificación devuelve coincide con el identificador del procesador, entonces el ordenador concede al usuario acceso al objeto.

Por lo tanto, un objeto de la presente invención es proporcionar un método y dispositivo de autenticación de red para autenticar a un terminal de usuario que usa un software.

Este objeto se consigue mediante los dos métodos tal como se definen en las reivindicaciones 1 y 6 independientes.

En consecuencia, un método de autenticación de red de la presente invención se implementará usando un dispositivo de autenticación de red y un terminal de usuario para autenticar el terminal de usuario. El terminal de usuario almacena un programa de terminal e incluye una pluralidad de componentes de hardware cada uno de los cuales tiene un código de identificación único.

El método de autenticación de red comprende las etapas de:

a) configurar el dispositivo de autenticación de red para almacenar información de hardware asociada con los

códigos de identificación de los componentes de hardware del terminal de usuario;
b) cuando se pretende verificar la identidad del terminal de usuario, configurar el terminal de usuario para ejecutar el programa de terminal para escanear los componentes de hardware del mismo para obtener los códigos de identificación de los componentes de hardware del terminal de usuario, para establecer una lista de hardware de acuerdo con los códigos de identificación de los componentes de hardware así obtenidos y para enviar al dispositivo de autenticación de red datos de verificación que se asocian con la lista de hardware; y
c) configurar el dispositivo de autenticación de red para verificar la identidad del terminal de usuario basándose en la relación entre los datos de verificación recibidos desde el terminal de usuario en la etapa b) y la información de hardware almacenada en la etapa a).

Preferentemente, el método de autenticación de red se ha de implementar adicionalmente usando un servidor de red y la etapa b) incluye las subetapas de:

b1) en respuesta a una solicitud de acceso desde el terminal de usuario para acceder al servidor de red a través de un primer canal de comunicación, configurar el servidor de red para redirigir al terminal de usuario para su conexión con el dispositivo de autenticación de red a través de un segundo canal de comunicación; y
b2) configurar el dispositivo de autenticación de red para permitir que el terminal de usuario ejecute el programa de terminal.

Preferentemente, el método de autenticación de red comprende adicionalmente las etapas de:

d) configurar el dispositivo de autenticación de red para generar una clave de acuerdo con la información de hardware almacenada en él y para enviar la clave al terminal de usuario y al servidor de red;
e) cuando el terminal de usuario intenta llevar a cabo una transacción electrónica con el servidor de red, configurar el terminal de usuario para generar una primera firma digital correspondiente a los datos de transacción de la transacción electrónica usando la clave enviada por el dispositivo de autenticación de red y para enviar los datos de transacción y la primera firma digital al servidor de red y configurar el servidor de red para generar una segunda firma digital correspondiente a los datos de transacción recibidos desde el terminal de usuario usando la clave enviada por el dispositivo de autenticación de red; y
f) configurar el servidor de red para comparar la primera firma digital desde el terminal de usuario con la segunda firma digital generada por él y para determinar que los datos de transacción no fueron alterados durante la transmisión desde el terminal de usuario al servidor de red cuando la primera firma digital está de acuerdo con la segunda de firma digital.

De acuerdo con otro aspecto de la presente invención, se usa un dispositivo de autenticación de red para autenticar a un terminal de usuario. El terminal de usuario incluye una pluralidad de componentes de hardware cada uno de los cuales tiene un código de identificación único y se configura para escanear los componentes de hardware del mismo para obtener los códigos de identificación de los componentes de hardware y para establecer datos de verificación asociados con los códigos de identificación de los componentes de hardware así obtenidos.

El dispositivo de autenticación de red comprende un módulo de base de datos para almacenar información del hardware asociada con los códigos de identificación de los componentes de hardware del terminal de usuario y un módulo de verificación para verificar la identidad del terminal de usuario basándose en la relación entre los datos de verificación recibidos desde el terminal de usuario y la información de hardware almacenada en el módulo de base de datos.

Otras características y ventajas de la presente invención se harán evidentes en la siguiente descripción detallada de realizaciones preferidas con referencia a los dibujos adjuntos, de los que:

la Figura 1 es un diagrama de bloques que ilustra una primera realización preferida de un dispositivo de autenticación de red de acuerdo con la presente invención;
la Figura 2 es un diagrama de flujo que ilustra un procedimiento de registro de un método de autenticación de red implementado usando el dispositivo de autenticación de red de la primera realización preferida de acuerdo con la presente invención;
la Figura 3 es un diagrama de flujo que ilustra un procedimiento de acceso del método autenticación de red implementado usando el dispositivo de autenticación de red de la primera realización preferida;
la Figura 4 es un diagrama esquemático que ilustra el dispositivo de autenticación de red que implementa el método de autenticación de seguridad de red para procesamiento de la firma digital;
la Figura 5 es un diagrama de bloques que ilustra una segunda realización preferida de un dispositivo de autenticación de red de acuerdo con la presente invención;
la Figura 6 es un diagrama de flujo que ilustra un procedimiento de registro de un método de autenticación de red implementado usando el dispositivo de autenticación de red de la segunda realización preferida de acuerdo con la presente invención;
la Figura 7 es un diagrama de bloques que ilustra el dispositivo de autenticación de red de la segunda realización

preferida que se configura para implementar procedimientos de acceso y transacción del método de autenticación de red de la presente invención;
la Figura 8 es un diagrama de flujo que ilustra el procedimiento de acceso del método de autenticación de red implementado usando el dispositivo de autenticación de red de la segunda realización preferida; y
la Figura 9 es un diagrama de flujo que ilustra el procedimiento de transacción del método de autenticación de red implementado usando el dispositivo de autenticación de red de la segunda realización preferida.

Antes de que se describa con mayor detalle la presente invención, debería señalarse que elementos iguales se indican por los mismos números de referencia a todo lo largo de la divulgación.

Con referencia a la Figura 1, la primera realización preferida de un dispositivo de autenticación de red de acuerdo con la presente invención es un servidor de verificación 1 operativo para cooperar con una pluralidad de terminales de usuario 2 y un servidor de red 3 (por ejemplo un proveedor de contenidos de Internet o ICP) para implementar un método de autenticación de red. El servidor de verificación 1 incluye un módulo de base de datos 10, un módulo de control 11, un módulo de verificación 12 y un módulo de transmisión 13. Para finalidades de ejemplo, el servidor de red 3 puede ser, pero sin limitación, un servidor de juegos en línea 3a, un servidor de banca en web 3b o cualquier otro servidor que proporcione un servicio de red que requiera verificación de identidad, tal como un portal de sitios web. Los terminales de usuario 2 incluyen un primer, segundo y tercer terminales de usuario 2a, 2b y 2c asociados con el primer, segundo y tercer usuarios 51, 52 y 53, respectivamente. Los terminales de usuario 2a, 2b y 2c pueden ser un equipo electrónico o dispositivos electrónicos portátiles capaces de navegación por Internet o comunicaciones de datos, tales como ordenadores portátiles, teléfonos inteligentes, asistentes digitales personales, etc. Particularmente, los terminales de usuario 2 se conectan al servidor de red 3 a través de un primer canal de comunicación 300a en una red de comunicación 300 y se conectan al servidor de verificación 1 a través de un segundo canal de comunicación 300b en la red de comunicación 300 que está separado del primer canal de comunicación 300a. En consecuencia, es relativamente difícil atacar al primer y segundo canales de comunicación 300a y 300b simultáneamente para robar información asociada con los usuarios 51-53. Más aún, el servidor de red 3 se conecta al servidor de verificación 1 a través de un canal especial. Por ejemplo, el servidor de juegos en línea 3a y el servidor de banca en web 3b se conectan al servidor de verificación 1 a través de canales especiales 301 y 302, respectivamente.

Tomando al primer terminal de usuario 2a como un ejemplo, el primer terminal de usuario 2a incluye una placa madre 20, una unidad de procesamiento central 21, un dispositivo de almacenamiento 22, una interfaz de red 23, una unidad del sistema de entrada/salida básica (BIOS) 24, un módulo de lectura 25, un dispositivo periférico externo 251, un dispositivo de entrada 261 y un dispositivo de visualización 262. En esta realización, la placa madre 20, la unidad de procesamiento central 21 y la unidad de BIOS 24 tienen códigos de identificación únicos (A), (B) y (C), respectivamente. Adicionalmente, el módulo de lectura 25 es una interfaz del bus serie universal (USB) y el dispositivo periférico externo 251 correspondiente es un dispositivo de almacenamiento USB (por ejemplo, una tarjeta de memoria o una unidad flash USB) y tiene un código de identificación único (D). En otras realizaciones, el dispositivo periférico externo 251 puede ser un dispositivo de identificación por radiofrecuencia (RFID) o un dispositivo de comunicación de campo cercano (NFC). Debería señalarse que el código de identificación único de la interfaz de red 23 puede usarse por el método de autenticación de red en otras realizaciones, y los componentes de hardware del primer terminal de usuario 2a tampoco están limitados a la divulgación del presente documento.

Dado que cada uno de los códigos de identificación (A), (B), (C) y (D) de los componentes de hardware (la placa madre 20, la unidad de procesamiento central 21, la unidad de BIOS 24 y el dispositivo periférico externo 251) del primer terminal de usuario 2a son únicos, una combinación de los códigos de identificación (A), (B), (C) y (D) es ciertamente diferente de una combinación de los códigos de identificación de componentes de hardware de cualquier otro de los terminales de usuario 2. Por ello, la combinación de los códigos de identificación del primer terminal de usuario 2a es como una huella dactilar única del primer terminal de usuario 2a y puede usarse para verificar la identidad del primer usuario 51. Por lo tanto, no es posible usar otros terminales de usuario que tengan diferentes componentes de hardware para verificar la identidad del primer usuario 51.

Con referencia a las Figuras 1 y 2, el servidor de verificación 1 coopera con el primer terminal de usuario 2a y con el servidor de red 3 para implementar un procedimiento de registro del método de autenticación de red de acuerdo con la presente invención. El procedimiento de registro del método de autenticación de red incluye las siguientes etapas.

En la etapa S201, el primer usuario 51 introduce información personal, una identificación de usuario (ID) y una contraseña usando el dispositivo de entrada 261 del primer terminal de usuario 2a en un sitio web proporcionado por el servidor de red 3. La información personal, el ID de usuario y la contraseña se transmiten al servidor de red 3 a través del primer canal de comunicación 300a. En respuesta a la recepción de la información personal, el ID de usuario y la contraseña, el servidor de red 3 es operativo para comprobar si la información personal, el ID de usuario y la contraseña son correctas en la etapa S300. Si es afirmativo, el servidor de red 3 es operativo para redirigir al primer terminal de usuario 2a para su conexión con el servidor de verificación 1 en la etapa S301, de modo que el servidor de verificación 1 es operativo para permitir que el primer terminal de usuario 2a descargue un programa de

terminal 411 desde un medio de programas 4 en la etapa S101. En caso contrario, el servidor de red 3 es operativo para enviar un mensaje de error al primer terminal de usuario 2a para su visualización sobre el dispositivo de visualización 262 del primer terminal de usuario 2a en la etapa S205.

Debería señalarse que, aunque el medio de programas 4 es un sitio web separado del servidor de verificación 1 como se muestra en la Figura 1 en la presente realización, puede integrarse como parte del servidor de red 3 o del servidor de verificación 1 en otras realizaciones. Más aún, la invención no está limitada a la descarga del programa de terminal 411 desde la red; por ejemplo, el medio de programas 4 puede ser un disco compacto u otros portadores de datos que almacenan el programa de terminal 411 en la práctica.

Posteriormente, después de que el primer terminal de usuario 2a almacene e instale el programa de terminal 411 en el dispositivo de almacenamiento 22 como un programa de terminal 221, el primer terminal de usuario 2a es operativo para ejecutar el programa de terminal 221, en la etapa S202, para escanear los componentes de hardware del primer terminal de usuario 2a para obtener los códigos de identificación (A)-(D) de los componentes de hardware y para establecer una lista de hardware de referencia 10a de acuerdo con los códigos de identificación de los componentes de hardware así obtenidos después de que el primer usuario 51 introduzca el ID del usuario. En la etapa S203 el primer terminal de usuario 2a es operativo para cifrar la lista de hardware de referencia 10a con una clave de sesión y para enviar directamente la lista de hardware de referencia cifrada al servidor de verificación 1 a través del segundo canal de comunicación 300b.

En la práctica, el programa de terminal 221 permite que el primer usuario 51 decida si el dispositivo periférico externo 251 se escanea en la etapa S202. Adicionalmente, cuando el dispositivo periférico externo 251 del primer terminal de usuario 2a no tiene un código de identificación único, el módulo de control 11 del servidor de verificación 1 es operativo para generar un código de identificación asignado al dispositivo y el módulo de transmisión 13 es operativo para transmitir el código de identificación asignado al dispositivo al primer terminal de usuario 2a para almacenamiento en el dispositivo periférico externo 251 de modo que sirva como el código de identificación del dispositivo periférico externo 251.

Después de que el módulo de transmisión 13 del servidor de verificación 1 reciba la lista de hardware de referencia cifrada desde el primer terminal de usuario 2a, el módulo de control 11 del servidor de verificación 1 es operativo, en la etapa S102, para descifrar la lista de hardware de referencia cifrada de modo que obtenga la lista de hardware de referencia 10a y para almacenar la lista de hardware referencia 10a en el módulo de base de datos 10 como una información de hardware asociada con el primer terminal de usuario 2a. En particular, la lista de hardware de referencia 10a consiste en el ID de usuario asociado con el primer usuario 51, y códigos de identificación (A), (B), (C) y (D) de los componentes de hardware (la placa madre 20, la unidad de procesamiento central 21, la unidad de BIOS 24 y el dispositivo periférico externo 251) del primer terminal de usuario 2a. De modo similar, el módulo de base de datos 10 almacena adicionalmente las listas de hardware de referencia 10b y 10c correspondientes al segundo y tercer terminales de usuario 2b y 2c, respectivamente.

El servidor de verificación 1 es operativo adicionalmente para enviar una notificación al servidor de red 3 después de almacenar la lista de hardware de referencia 10a. A continuación, en respuesta a la notificación desde el servidor de verificación 1, el servidor de red 3 es operativo, en la etapa S302, para afirmar que el procedimiento de registro asociado con el primer usuario 51 se ha completado. Finalmente, el servidor de red 3 es operativo, en la etapa S303, para enviar al primer terminal de usuario 2a una notificación de que el procedimiento de registro se ha completado y el primer terminal de usuario 2a es operativo para recibir la notificación en la etapa S204.

Con referencia a las Figuras 1 y 3, el servidor de verificación 1 coopera con el primer terminal de usuario 2a y el servidor de red 3 para implementar un procedimiento de acceso del método autenticación de red de acuerdo con la presente invención. El procedimiento de acceso del método de autenticación de red incluye las siguientes etapas.

En la etapa S211, el primer usuario 51 introduce el ID de usuario y la contraseña usando el dispositivo de entrada 261 del primer terminal de usuario 2a en el sitio web de servicio proporcionado por el servidor de red 3, y el primer terminal de usuario 2a es operativo para transmitir el ID de usuario y la contraseña al servidor de red 3 a través del primer canal de comunicación 300a. En la etapa S310, el servidor de red 3 es operativo para verificar si el ID de usuario y la contraseña así recibidos son correctos. En particular, el servidor de red 3 es operativo para determinar si el ID de usuario y la contraseña introducidos en la etapa S211 están de acuerdo con el ID de usuario y la contraseña proporcionados en el procedimiento de registro anteriormente mencionado. En realizaciones alternativas, el servidor de verificación 1 puede configurarse para verificar el ID de usuario y la contraseña asociados con el primer usuario 51 en lugar de con el servidor de red 3.

Si se determina que o bien el ID de usuario o bien la contraseña son incorrectos en la etapa S310, el servidor de red 3 es operativo para enviar un mensaje de error al primer terminal de usuario 2a para su visualización sobre el dispositivo de visualización 262 del primer terminal de usuario 2a en la etapa S215. Si se determina que tanto el ID del usuario como la contraseña son correctos en la etapa S310, el servidor de red 3 es operativo para notificar al

servidor de verificación 1 que la identidad del primer terminal de usuario 2a asociado con el primer usuario 51 ha de verificarse en la etapa S311. El servidor de red 3 es operativo adicionalmente para redirigir al primer terminal de usuario 2a para conectar con el servidor de verificación 1 a través del segundo canal de comunicación 300b.

En la etapa S103, el servidor de verificación 1 es operativo para permitir que el primer terminal de usuario 2a ejecute el programa de terminal 221 almacenado en el dispositivo de almacenamiento 22 del primer terminal de usuario 2a. En la etapa S212, el primer terminal de usuario 2a es operativo para ejecutar el programa de terminal 221 para escanear los componentes de hardware del mismo para obtener los códigos de identificación de los componentes de hardware del primer terminal de usuario 2a, y para establecer una lista de hardware de acuerdo con los códigos de identificación de los componentes de hardware así obtenidos. A continuación, en la etapa S213, el primer terminal de usuario 2a es operativo para cifrar la lista de hardware con la clave de sesión y para enviar la lista de hardware cifrada como datos de verificación para verificar la identidad del primer terminal de usuario 2a al servidor de verificación 1 a través del segundo canal de comunicación 300b.

En la etapa S104, el módulo de control 11 del servidor de verificación 1 es operativo para descifrar los datos de verificación desde el primer terminal de usuario 2a para obtener la lista de hardware. A continuación, el módulo de verificación 12 del servidor de verificación 1 es operativo para comparar la lista de hardware así obtenida con la lista de hardware de referencia 10a almacenada en el módulo de base de datos 10 para verificar la identidad del primer usuario 51 asociado con el primer terminal de usuario 2a.

Cuando la lista de hardware así obtenida en la etapa S104 no está de acuerdo con la lista de hardware de referencia 10a almacenada en el módulo de base de datos 10, el módulo de verificación 12 es operativo para determinar que la verificación del primer usuario 51 no tiene éxito y para enviar el mensaje de error al primer terminal de usuario 2a. En consecuencia, se deniega el acceso del primer terminal de usuario 2a al servicio del sitio web proporcionado por el servidor de red 3, y es operativo para visualizar el mensaje de error sobre el dispositivo de visualización 262 en la etapa S215. Por otro lado, cuando la lista de hardware está de acuerdo con la lista de hardware de referencia 10a, el módulo de verificación 12 es operativo para determinar que la verificación del primer usuario 51 tiene éxito y para notificar al servidor de red 3 el resultado de la verificación realizada por él. De ese modo, el servidor de red 3 es operativo para autenticar la identidad del primer usuario 51 en la etapa S312 y, a continuación, para redirigir al primer terminal de usuario 2a asociado con el primer usuario 51 para conectar con el sitio web de servicio proporcionado por el servidor de red 3 en la etapa S313. En la etapa S214, el primer terminal de usuario 2a es autorizado a acceder al sitio web de servicio.

Después de que el primer terminal de usuario 2a sea autorizado a acceder al sitio web de servicio en el procedimiento de acceso, el servidor de verificación 1 coopera con el primer terminal de usuario 2a y con el servidor de red 3 para implementar adicionalmente el método de autenticación de seguridad de red para procesar una firma digital cuando el primer usuario 51 intenta llevar a cabo una transacción electrónica con el servidor de red 3. El método de autenticación de seguridad de red para procesar una firma digital se describirá en detalle a continuación con referencia a las Figuras 1 y 4.

El servidor de verificación 1 incluye adicionalmente una unidad de generación de clave 50 y un módulo de descifrado 45', el programa de terminal 221 incluye una función de codificación 42 y un módulo de descifrado 45 y el servidor de red 3 incluyen un módulo de comparación 46. La unidad de generación de clave 50 del servidor de verificación 1 es operativa para generar una clave 511 de acuerdo con la lista de hardware de referencia 10a almacenada en el módulo de base de datos 10. La clave 511 se envía al primer terminal de usuario 2a a través del segundo canal de comunicación 300b en la red de comunicación 300, y se envía al servidor de red 3 a través del canal especial 301 (302).

Cuando el primer usuario 51 intenta llevar a cabo una transacción electrónica con el servidor de red 3 usando el primer terminal de usuario 2a, el primer terminal de usuario 2a es operativo para generar datos de transacción 41 relacionados con la transacción electrónica y para enviar los datos de transacción 41 al servidor de red 3 a través del primer canal de comunicación 300a en la red de comunicación 300. El programa de terminal 221 del primer terminal de usuario 2a usa la función de codificación 42 para extraer unos extractos de los datos 43 de los datos de transacción 41 y procesa los extractos de los datos 43 en una primera firma digital 44 usando la clave 511 enviada por el servidor de verificación 1. A continuación, el módulo de cifrado 45 es operativo para cifrar la primera firma digital 44 con una clave de sesión 521 y la primera firma digital cifrada se envía al servidor de verificación 1 a través del segundo canal de comunicación 300b. El módulo de descifrado 45' del servidor de verificación 1 es operativo para descifrar la primera firma digital cifrada para obtener la primera firma digital 44 y, a continuación, la primera firma digital 44 se envía al servidor de red 3.

Después de que el servidor de red 3 reciba la clave 511 desde el servidor de verificación 1 y los datos de transacción 41' desde el primer terminal de usuario 2a, el servidor de red 3 es operativo para extraer un extracto de los datos 43' a partir de los datos de transacción 41' usando la función de codificación 42. A continuación, el servidor de red 3 es operativo para procesar el extracto de los datos 43' en una segunda firma digital 44' usando la clave 511

enviada por el servidor de verificación 1. El módulo de comparación 46 del servidor de red 3 es operativo para comparar la segunda firma digital 44' con la primera firma digital 44 generada por el primer terminal de usuario 2a. Cuando la segunda firma digital 44' está de acuerdo con la primera firma digital 44, el servidor de red 3 es operativo para determinar que los datos de transacción 41 no se alteraron durante la transmisión desde el primer terminal de usuario 2a al servidor de red 3 como los datos de transacción 41' a través del primer canal de comunicación 300a. Posteriormente, el servidor de red 3 es operativo para implementar un procedimiento de transacción 47 para completar la transacción electrónica de acuerdo con los datos de transacción 41'. Por otro lado, cuando la segunda firma digital 44' no está de acuerdo con la primera firma digital 44, el servidor de red 3 es operativo para determinar que los datos de transacción 41' se alteraron durante la transmisión desde el primer terminal de usuario 2a al servidor de red de modo que el extracto de los datos 43' a partir de los datos de transacción alterados 41' no es idéntica al extracto de los datos 43 a partir de los datos de transacción originales 41. Por ello, el servidor de red 3 es operativo para implementar un procedimiento de rechazo 48 para rechazar la transacción electrónica.

En realizaciones alternativas, el módulo de comparación 46 del servidor de red 3 puede omitirse y el servidor de red 3 es operativo para enviar la segunda firma digital 44' al servidor de verificación 1. A continuación, el servidor de verificación 1 se configura para comparar la segunda firma digital 44' con la primera firma digital 44 en lugar de un módulo de comparación 46 y para enviar el resultado de la comparación al servidor de red 3. En respuesta al resultado de comparación desde el servidor de verificación 1, el servidor de red 3 es operativo para implementar alternativamente el procedimiento de transacción 47 y el procedimiento de rechazo 48.

Con referencia a la Figura 5, la segunda realización preferida del dispositivo de autenticación de red de acuerdo con la presente invención es un servidor de gestión 8 que integra las funciones del servidor de verificación 1 y del servidor de red 3 de la primera realización preferida. En esta realización, el terminal de usuario es un dispositivo electrónico portátil 6, tal como un teléfono inteligente.

El dispositivo electrónico portátil 6 incluye un microprocesador 60, una pantalla 61, un módulo de comunicación 62, una interfaz de transmisión 66, un dispositivo de memoria 63, un módulo de entrada 64 y un módulo de lectura 65. El módulo de comunicación 62 es operativo para comunicar con el servidor de gestión 8 través de una red de comunicación 300. El dispositivo de memoria 63 almacena un programa de terminal 631, una lista de hardware de referencia 632 y una clave de referencia 633 realizada a partir de la lista de hardware de referencia 632. Por ejemplo, el módulo de lectura 65 es un lector de tarjetas de memoria y un dispositivo periférico externo 651 conectado al mismo es una tarjeta de memoria. La lista de hardware de referencia 632 se asocia con una combinación de los códigos de identificación del microprocesador 60, la pantalla 61, el módulo de comunicación 62, la interfaz de transmisión 66, el dispositivo de memoria 63, el módulo de entrada 64 y/o el dispositivo periférico externo 651. Aunque el programa de terminal 631 es similar al programa de terminal 221 de la primera realización preferida, se requiere introducir un número de identificación personal (PIN) para ejecutar el programa de terminal 631 en esta realización. En otras realizaciones, el usuario asociado con el dispositivo electrónico portátil 6 solo necesita introducir el PIN tras encender el dispositivo electrónico portátil 6 y no necesita introducir el PIN o un nuevo PIN otra vez para ejecutar el programa de terminal 631.

Con referencia a las Figuras 5 y 6, el servidor de gestión 8 es operativo para cooperar con el dispositivo electrónico portátil 6 para implementar un procedimiento de registro del método de autenticación de red de acuerdo con la presente invención. El procedimiento de registro del método de autenticación de red incluye las siguientes etapas.

En la etapa S601, después de que el dispositivo electrónico portátil 6 se conecte al servidor de gestión 8 usando el módulo de comunicación 62 a través de la red de comunicación 300, un usuario asociado con el dispositivo electrónico portátil 6 usa el módulo de entrada 64 del dispositivo electrónico portátil 6 para introducir una identificación de usuario (ID) y una contraseña en un sitio web proporcionado por el servidor de gestión 8. En respuesta a la recepción del ID de usuario y de la contraseña, el servidor de gestión 8 es operativo para comprobar si el ID del usuario y la contraseña son correctos en la etapa S321. Si o bien el ID de usuario o bien la contraseña son incorrectos, el servidor de gestión 8 es operativo para responder con un mensaje de error al dispositivo electrónico portátil 6 en la etapa S322. Por otro lado, si tanto el ID de usuario como la contraseña son correctos, el servidor de gestión 8 es operativo para proporcionar el programa de terminal 631 al dispositivo electrónico portátil 6 en la etapa S323.

Cuando el usuario del dispositivo electrónico portátil 6 introduce el PIN correcto en la etapa S602, el dispositivo electrónico portátil 6 es operativo, en la etapa S603, para ejecutar el programa de terminal 631 para escanear componentes de hardware del dispositivo electrónico portátil 6 para obtener códigos de identificación de los componentes de hardware y para establecer y almacenar la lista de hardware de referencia 632. A continuación, el dispositivo electrónico portátil 6 ejecuta el programa de terminal 631 para generar la clave de referencia 633 basándose en la lista de hardware de referencia 632 en la etapa S604 y es operativo para almacenar la clave de referencia 633 en el dispositivo de memoria 63 en la etapa S605. En la etapa S606, el dispositivo electrónico portátil 6 es operativo para cifrar la clave de referencia 633 con una clave de sesión de modo que obtenga una clave cifrada y para enviar la clave cifrada al servidor de gestión 8. En otras realizaciones, la etapa S602 puede omitirse dado que

el usuario ya introdujo el PIN tras encender el dispositivo electrónico portátil 6.

Después de recibir la clave cifrada desde el dispositivo electrónico portátil 6, el servidor de gestión 8 es operativo para descifrar la clave cifrada de modo que obtenga la clave de referencia 633 en la etapa S324 y para almacenar la clave de referencia en la etapa S325. Finalmente, en la etapa S326, el servidor de gestión 8 es operativo para notificar al dispositivo electrónico portátil 6 que el procedimiento de registro se ha completado.

Con referencia a la Figura 7, el dispositivo electrónico portátil 6 se conecta a un ordenador 7 a través de la interfaz de transmisión 66 que puede ser o bien una interfaz de transmisión por cable o bien una interfaz de transmisión inalámbrica. El módulo de entrada 64 del dispositivo electrónico portátil 6 es un panel de teclado o un panel táctil para generar datos electrónicos en respuesta a una entrada desde el usuario del dispositivo electrónico portátil 6. Los datos electrónicos se transmiten al ordenador 7 a través de la interfaz de transmisión 66 y se envían posteriormente al servidor de gestión 8 a través de la red de comunicación 300. En el caso del dispositivo electrónico portátil 6 sin la interfaz de transmisión 66, el usuario puede usar un teclado del ordenador 7 para introducir los datos electrónicos visualizados sobre la pantalla 61 del dispositivo electrónico portátil 6 de modo que transmita los datos electrónicos al servidor de gestión 8.

Con referencia a las Figuras 7 y 8, el servidor de gestión 8 es operativo para cooperar con el dispositivo electrónico portátil 6 y el ordenador 7 para implementar un procedimiento de acceso al método de autenticación de red de acuerdo con la presente invención. El procedimiento de acceso al método de autenticación de red incluye las siguientes etapas.

Primero, el usuario del dispositivo electrónico portátil 6 necesita introducir el PIN en la etapa S610. A continuación, en la etapa S611, el dispositivo electrónico portátil 6 es operativo para determinar si el PIN introducido en la etapa S610 es correcto. Si se determina que el PIN es incorrecto, el dispositivo electrónico portátil 6 es operativo para generar un mensaje de error en la etapa S614. Si el PIN introducido en la etapa S610 es correcto, el dispositivo electrónico portátil 6 es operativo, en la etapa S612, para ejecutar el programa de terminal 631 para escanear los componentes de hardware del dispositivo electrónico portátil 6 para obtener códigos de identificación de los componentes de hardware, para establecer una nueva lista de hardware de acuerdo con los códigos de identificación así obtenidos y para generar una nueva clave basándose en la nueva lista de hardware 632 así establecida. En otras realizaciones, las etapas S610 y S611 pueden omitirse y el dispositivo electrónico portátil 6 es operativo para implementar directamente la etapa S612 cuando el usuario desea usar el dispositivo electrónico portátil 6 para acceder al sitio web de servicio proporcionado por el servidor de gestión 8.

A continuación, en la etapa S613, el dispositivo electrónico portátil 6 es operativo para ejecutar el programa de terminal 631 para comparar la nueva clave generada en la etapa S612 con la clave de referencia 633 almacenada en el dispositivo de memoria 63. Cuando la nueva clave no está de acuerdo con la clave de referencia 633, puede determinarse que la nueva clave fue alterada o que el programa de terminal 631 y la clave de referencia 633 se desplazaron a otro dispositivo y el flujo prosigue a la etapa S614. Cuando la nueva clave está de acuerdo con la clave de referencia 633, puede determinarse que la nueva clave y la clave de referencia 633 se generaron usando el mismo dispositivo y que el programa de terminal 631 y la clave de referencia 633 no se desplazaron a otro dispositivo y el dispositivo electrónico portátil 6 es operativo para ejecutar el programa de terminal 631 para generar adicionalmente una contraseña de un solo uso (OTP) 40a usando la clave de referencia 633 en la etapa S615. A continuación, la OTP 40a se transmite al ordenador 7 a través de la interfaz de transmisión 66 del dispositivo electrónico portátil 6. En el caso del dispositivo electrónico portátil 6 sin la interfaz de transmisión 66, el usuario puede usar el teclado del ordenador 7 para introducir la OTP 40a visualizada en la pantalla 61 del dispositivo electrónico portátil 6 en la etapa S232.

Para acceder al sitio web de servicio proporcionado por el servidor de gestión 8, el usuario necesita introducir la ID de usuario usando el teclado del ordenador 7 en la etapa S231 y, a continuación, el ID de usuario y la OTP 40a se envían al servidor de gestión 8 a través de la red de comunicación 300.

En la etapa S330, el servidor de gestión 8 es operativo para generar una contraseña de un solo uso de referencia 40b usando la clave de referencia 633 almacenada en él en la etapa S325 del procedimiento de registro. Tras recibir el ID del usuario y la OTP 40a desde el ordenador 7, el servidor de gestión 8 es operativo para comparar la OTP 40a con la OTP de referencia 40b y para determinar si el ID de usuario es correcto en la etapa S331. Si la OTP 40a no está de acuerdo con la OTP de referencia 40b o el ID de usuario es incorrecto, el servidor de gestión 8 es operativo para generar un mensaje de error en la etapa S332. Si la OTP 40a está de acuerdo con la OTP de referencia 40b y el ID de usuario es correcto, el servidor de gestión 8 es operativo para redirigir al ordenador 7 para conectarse con el sitio web de servicio proporcionado por el servidor de gestión 8 en la etapa S333. En la etapa S233, se autoriza al ordenador 7 a acceder al sitio web de servicio.

Después de que el ordenador 7 haya recibido autorización para acceder al sitio web de servicio en el procedimiento de acceso, el servidor de gestión 8 coopera con el dispositivo electrónico portátil 6 y el ordenador 7 para

implementar adicionalmente el método de autenticación de seguridad de red para procesar una firma digital cuando el usuario intenta llevar a cabo una transacción electrónica con el servidor de gestión 8. El método de autenticación de seguridad de red para procesar una firma digital se describirá en detalle a continuación con referencia a las Figuras 7 y 9.

Para llevar a cabo la transacción electrónica con el servidor de gestión 8, el usuario necesita introducir un número de cuenta de recepción en la etapa S621 e introducir una cantidad a transferir en la etapa S622 usando el módulo de entrada 64 del dispositivo electrónico portátil 6. En la etapa S623, el dispositivo electrónico portátil 6 es operativo para generar datos de transacción 41a relacionados con el número de cuenta y la cantidad a transferir y para enviar los datos de transacción 41a al ordenador 7 a través de la interfaz de transmisión 66. Adicionalmente, en la etapa S624, el dispositivo electrónico portátil 6 es operativo para ejecutar el programa de terminal 631 para establecer una primera firma digital 441 usando los datos de transacción 41a y la clave de referencia 633 y para enviar la primera firma digital 441 al ordenador 7 a través de la interfaz de transmisión 66.

En respuesta a la recepción de los datos de transacción 41a y la primera firma digital 441, el ordenador 7 es operativo para enviar los datos de transacción 41a y la primera firma digital 441 al servidor de gestión 8 través de la red de comunicación 300 en las etapas S241 y S242, respectivamente. Debería señalarse que, en el caso del dispositivo electrónico portátil 6 sin la interfaz de transmisión 66, el usuario puede usar el teclado del ordenador 7 para introducir el número de cuenta y la cantidad a transferir de modo que el ordenador 7 sea operativo para obtener los datos de transacción 41a que consisten en el número de cuenta y la cantidad a transferir.

El servidor de gestión 8 es operativo para recibir los datos de transacción 41b correspondientes a los datos de transacción 41a desde el ordenador 7 a través de la red de comunicación 300 en la etapa S341 y, a continuación, para establecer una segunda firma digital 442 usando los datos de transacción recibidos 41b y la clave de referencia 633 en la etapa S342. En la etapa S343, el servidor de gestión 8 es operativo para recibir la primera firma digital 441 y para comparar la primera firma digital 441 con la segunda firma digital 442. Si la primera firma digital 441 no está de acuerdo con la segunda firma digital 442, el servidor de gestión 8 es operativo para determinar que los datos de transacción 41a fueron alterados durante la transmisión y que los datos de transacción recibidos 41b son diferentes de los datos de transacción 41a. Por lo tanto, el servidor de gestión 8 es operativo para rechazar la transacción electrónica y para generar un mensaje de error en la etapa S344. Si la primera firma digital 441 está de acuerdo con la segunda firma digital 442, el servidor de gestión 8 es operativo para determinar que los datos de transacción recibidos 41b son correctos y son idénticos a los datos de transacción 41a. En consecuencia, el servidor de gestión 8 es operativo para implementar la transacción electrónica de acuerdo con el número de cuenta y la cantidad a transferir de los datos de transacción recibidos 41b en la etapa S345. Finalmente, en la etapa S346, el servidor de gestión 8 es operativo para notificar al ordenador 7 que la transacción electrónica se ha completado.

En resumen, el método de autenticación de red implementado usando el dispositivo de autenticación de red de acuerdo con la presente invención tiene las siguientes ventajas. En primer lugar, el terminal de usuario puede ejecutar el programa de terminal para escanear los componentes de hardware del terminal de usuario y para establecer la lista de hardware de acuerdo con los códigos de identificación de los componentes de hardware así obtenidos para su uso posteriormente en la autenticación del usuario. Así, un proveedor de contenidos de red no necesita comprar equipo adicional para autenticación y no necesita proporcionar al usuario un identificador personalizado, tarjeta de circuito integrado, unidad flash USB, etc. También, el usuario no necesita tener dispositivos de autenticación adicionales para diferentes sitios web. Adicionalmente, en la primera realización preferida, dado que el terminal de usuario se conecta al servidor de red a través del primer canal de comunicación y se conecta al servidor de verificación a través del segundo canal de comunicación que está separado del primer canal de comunicación, es relativamente difícil atacar al primer y segundo canales de comunicación simultáneamente para robar y alterar los datos enviados por el terminal de usuario.

REIVINDICACIONES

1. Un método de autenticación de red a ser implementado usando un servidor de red (3), un dispositivo de autenticación de red (1) y un dispositivo de usuario (2) para autenticar el dispositivo de usuario (2), almacenando el dispositivo de usuario (2) un programa de terminal (221) e incluyendo una pluralidad de componentes de hardware cada uno de los cuales tiene un código de identificación único, estando dicho método de autenticación de red **caracterizado por** las siguientes etapas de:

a) configurar el dispositivo de autenticación de red (1) para almacenar información de hardware (10a-10c) asociada con los códigos de identificación de los componentes de hardware del dispositivo de usuario (2);
b) cuando se pretende verificar la identidad del dispositivo de usuario (2) en respuesta a una solicitud de acceso desde el dispositivo de usuario (2) para acceder al servidor de red (3) a través de un primer canal de comunicación (300a), configurar el servidor de red (3) para redirigir al dispositivo de usuario (2) para conectar con el dispositivo de autenticación de red (1) a través de un segundo canal de comunicación (300b) que está separado de dicho primer canal de comunicación (300a) y configurar el dispositivo de usuario (2) para ejecutar el programa de terminal (221) para escanear los componentes de hardware del mismo para obtener los códigos de identificación de los componentes de hardware del dispositivo de usuario (2), para establecer una lista de hardware de acuerdo con los códigos de identificación de los componentes de hardware así obtenidos y para enviar al dispositivo de autenticación de red (1) datos de verificación que se asocian con la lista de hardware;
c) configurar el dispositivo de autenticación de red (1) para verificar la identidad del dispositivo de usuario (2) basándose en la relación entre los datos de verificación recibidos desde el dispositivo de usuario (2) en la etapa b) y la información de hardware (10a-10c) almacenada en la etapa a);
d) configurar el dispositivo de autenticación de red (1) para generar una clave (511) de acuerdo con la información de hardware (10a-10c) almacenada en él y para enviar la clave (511) al dispositivo de usuario (2) y al servidor de red (3);
e) cuando el dispositivo de usuario (2) intenta llevar a cabo una transacción electrónica con el servidor de red (3), configurar el dispositivo de usuario (2) para generar una primera firma digital (44) correspondiente a los datos de transacción (41) de la transacción electrónica usando la clave (511) enviada por el dispositivo de autenticación de red (1) y para enviar los datos de transacción (41) y la primera firma digital (44) al servidor de red (3) y configurar el servidor de red (3) para generar una segunda firma digital (44') correspondiente a los datos de transacción (41') recibidos desde el dispositivo de usuario (2) usando la clave (511) enviada por el dispositivo de autenticación de red (1); y
f) configurar el servidor de red (3) para comparar la primera firma digital (44) desde el dispositivo de usuario (2) con la segunda firma digital (44') generada por él, y para determinar que los datos de transacción (41') no fueron alterados durante la transmisión desde el dispositivo de usuario (2) al servidor de red (3) cuando la primera firma digital (44) está de acuerdo con la segunda de firma digital (44').

2. El método de autenticación de red de acuerdo con la reivindicación 1, adicionalmente **caracterizado por** las etapas, previas a la etapa a), de:

i) configurar el dispositivo de usuario (2) para descargar el programa de terminal (221) desde un sitio web especificado (4); y
ii) configurar el dispositivo de usuario (2) para ejecutar el programa de terminal (221) para escanear los componentes de hardware del mismo para obtener los códigos de identificación de los componentes de hardware, para establecer una lista de hardware de referencia (10a-10c) que sirve como la información de hardware de acuerdo con los códigos de identificación así obtenidos y para enviar la información de hardware al dispositivo de autenticación de red para su almacenamiento en la etapa a).

3. El método de autenticación de red de acuerdo con la reivindicación 2, adicionalmente **caracterizado porque**:

en la etapa i), el dispositivo de usuario (2) se configura para descargar el programa de terminal (221) desde el sitio web especificado (4) durante el registro del dispositivo de usuario (2) en un servidor de red (3);
dicho método de autenticación de red comprende adicionalmente, entre las etapas a) y b), la etapa de configurar el dispositivo de autenticación de red (1) para notificar al servidor de red (3) que la información de hardware del dispositivo de usuario (2) se ha almacenado en el dispositivo de autenticación de red (1).

4. El método de autenticación de red de acuerdo con la reivindicación 1, adicionalmente **caracterizado porque**:

en la etapa b), el servidor de red (3) se configura adicionalmente para notificar al dispositivo de autenticación de red (1) que la identidad del dispositivo de usuario (2) ha de verificarse; y
en la etapa c), el dispositivo de autenticación de red (1) se configura para notificar al servidor de red (3) el resultado de la verificación realizada por él.

5. El método de autenticación de red de acuerdo con una cualquiera de las reivindicaciones 1 a 4, adicionalmente

caracterizado porque:

en la etapa b), los datos de verificación enviados al dispositivo de autenticación de red (1) se obtienen mediante el cifrado de la lista de hardware con una clave de sesión; y
en la etapa c), el dispositivo de autenticación de red (1) se configura para descifrar los datos de verificación para obtener la lista de hardware y para comparar la lista de hardware con la información de hardware (10a-10c) almacenada en él para verificar la identidad del dispositivo de usuario (2).

6. Un método de autenticación de red a ser implementado usando un dispositivo de autenticación de red (8) y un dispositivo electrónico portátil (6) para autenticar el dispositivo electrónico portátil (6), almacenando el dispositivo electrónico portátil (6) un programa de terminal (631) e incluyendo una pluralidad de componentes de hardware cada uno de los cuales tiene un código de identificación único, estando dicho método de autenticación de red **caracterizado por** las siguientes etapas de:

a) configurar el dispositivo de autenticación de red (8) para almacenar información de hardware (633) asociada con los códigos de identificación de los componentes de hardware del dispositivo electrónico portátil (6), en el que la etapa a) incluye las subetapas de

a1) configurar el dispositivo electrónico portátil (6) para ejecutar el programa de terminal (631) para escanear los componentes de hardware del mismo para obtener los códigos de identificación de los componentes de hardware y para generar y almacenar una clave de referencia (633) usando los códigos de identificación así obtenidos,
a2) configurar el dispositivo electrónico portátil (6) para cifrar la clave de referencia (633) con una clave de sesión de modo que obtenga una clave cifrada y para enviar la clave cifrada al dispositivo de autenticación de red (8), y
a3) configurar el dispositivo de autenticación de red (8) para descifrar la clave cifrada recibida desde el dispositivo electrónico portátil (6) de modo que obtenga la clave de referencia (633), siendo dicha clave de referencia la información de hardware (633) a ser almacenada en el dispositivo de autenticación de red (8);

b) cuando se pretende verificar la identidad del dispositivo electrónico portátil (6), configurar el dispositivo electrónico portátil (6) para ejecutar el programa de terminal (631) para escanear los componentes de hardware del mismo para obtener los códigos de identificación de los componentes de hardware del terminal de usuario, para establecer una nueva lista de hardware de acuerdo con los códigos de identificación de los componentes de hardware así obtenidos y para enviar al dispositivo de autenticación de red (8) datos de verificación que se generan usando la clave de referencia;
c) configurar el dispositivo de autenticación de red (8) para verificar la identidad del dispositivo electrónico portátil (6) basándose en la relación entre los datos de verificación recibidos desde el dispositivo electrónico portátil (6) en la etapa b) y la información de hardware (633) almacenada en la etapa a);
d') cuando el dispositivo electrónico portátil (6) intenta llevar a cabo una transacción electrónica con el dispositivo de autenticación de red (8), configurar el dispositivo electrónico portátil (6) para generar una primera firma digital (441) correspondiente a los datos de transacción (41a) de la transacción electrónica usando la clave de referencia (633) y para enviar los datos de transacción (41a) y la primera firma digital (441) al dispositivo de autenticación de red (8) y configurar el dispositivo de autenticación de red (8) para generar una segunda firma digital (442) correspondiente a los datos de transacción (41b) recibidos desde el dispositivo electrónico portátil (6) usando la información de hardware (633) almacenada en él; y
e') configurar el dispositivo de autenticación de red (8) para comparar la primera firma digital (441) desde el dispositivo electrónico portátil (6) con la segunda firma digital (442) generada por él, y para determinar que los datos de transacción (41b) no fueron alterados durante la transmisión desde el dispositivo electrónico portátil (6) al dispositivo de autenticación de red (8) cuando la primera firma digital (441) está de acuerdo con la segunda de firma digital (442).

7. El método de autenticación de red de acuerdo con la reivindicación 6, adicionalmente **caracterizado porque**:

en la etapa b), los datos de verificación enviados al dispositivo de autenticación de red (8) son una contraseña de un solo uso (40a) obtenida usando la clave de referencia (633) generada en la subetapa a1); y
en la etapa c), el dispositivo de autenticación de red (8) se configura para generar una contraseña de un solo uso (40b) usando la información de hardware almacenada en él y para comparar los datos de verificación (40a) con la contraseña de un solo uso de referencia (40b) para verificar la identidad del dispositivo electrónico portátil (6).

8. El método de autenticación de red de acuerdo con una cualquiera de las reivindicaciones 6 y 7, adicionalmente **caracterizado porque**, en la etapa b), el dispositivo electrónico portátil (6) se configura para ejecutar el programa de terminal (631) para generar una nueva clave de referencia usando los códigos de identificación de los componentes de hardware, para comparar la nueva clave de referencia con la clave de referencia (633) generada en la subetapa a1) y para generar los datos de verificación (40a) cuando la nueva clave de referencia está de acuerdo con la clave

de referencia (633).

9. El método de autenticación de red de acuerdo con la reivindicación 1, adicionalmente **caracterizado porque** la información de hardware (10a-10c) almacenada en el dispositivo de autenticación de red (1) en la etapa a) y los datos de verificación enviados al dispositivo de autenticación de red (1) en la etapa b) se asocian con los códigos de identificación de al menos uno de los siguientes componentes de hardware del dispositivo de usuario (2): una unidad de procesamiento central (21); una unidad del sistema de entrada/salida básica (BIOS) (24); un dispositivo de almacenamiento (22); una interfaz de red (23); una placa madre (20) y un dispositivo periférico externo (251).

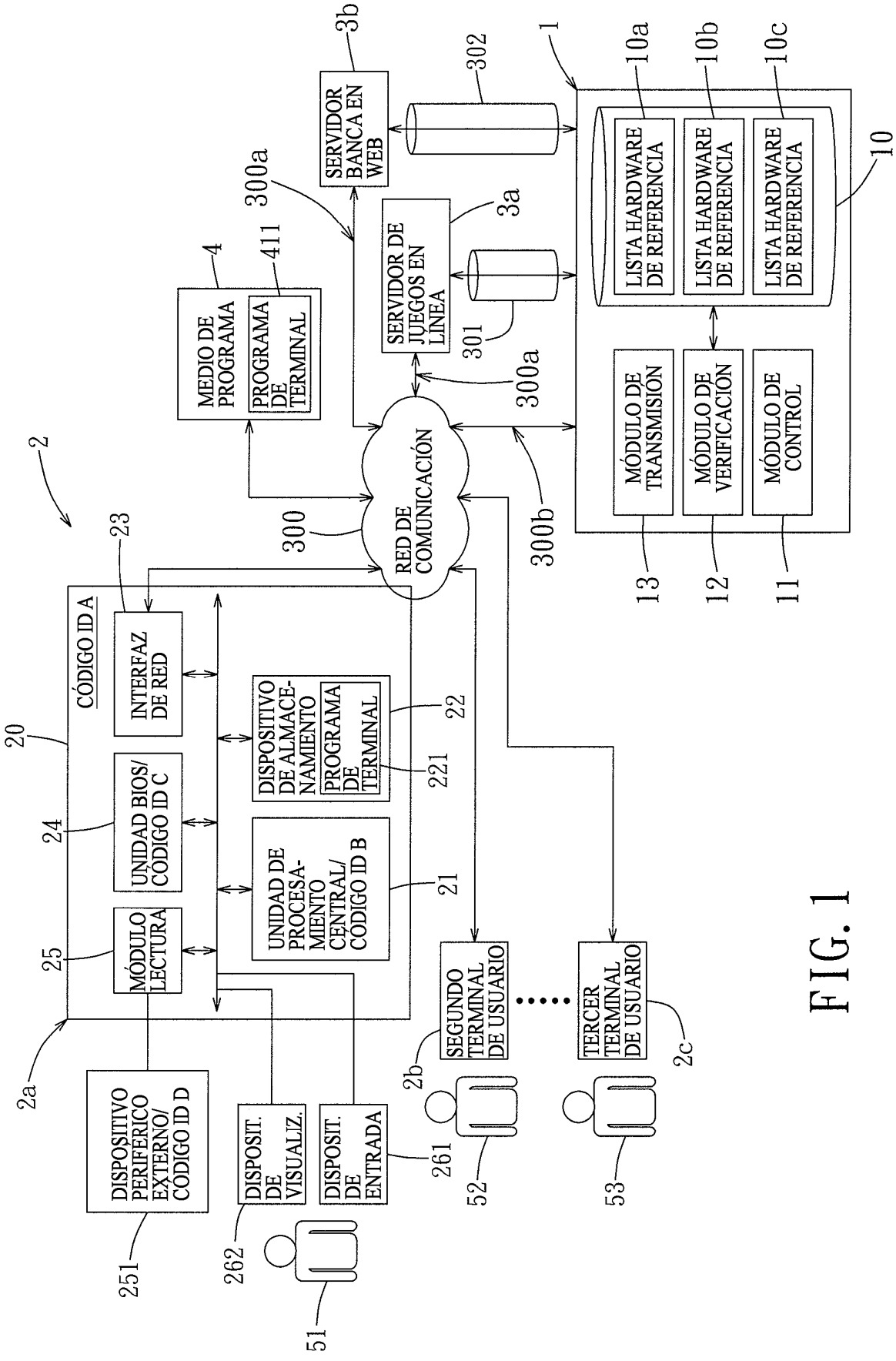
SERVIDOR BANCA EN WEB
3b
302
1
10a
10b
10c
LISTA HARDWARE DE REFERENCIA
LISTA HARDWARE DE REFERENCIA
LISTA HARDWARE DE REFERENCIA
10
300a
SERVIDOR DE JUEGOS EN LINEA
3a
301
MEDIO DE PROGRAMA
4
411
PROGRAMA DE TERMINAL
300a
2
RED DE COMUNICACIÓN
300
300b
MÓDULO DE TRANSMISIÓN
MÓDULO DE VERIFICACIÓN
MÓDULO DE CONTROL
13
12
11
23
CÓDIGO ID A
20
INTERFAZ DE RED
DISPOSITIVO DE ALMACE-NAMIENTO
PROGRAMA DE TERMINAL
22
221
UNIDAD BIOS/ CÓDIGO ID C
24
UNIDAD DE PROCESA-MIENTO CENTRAL/ CÓDIGO ID B
21
MÓDULO LECTURA
25
SEGUNDO TERMINAL DE USUARIO
TERCER TERMINAL DE USUARIO
2a
2b
2c
DISPOSITIVO PERIFÉRICO EXTERNO/ CÓDIGO ID D
DISPOSIT. DE VISUALIZ.
DISPOSIT. DE ENTRADA
261
52
53
251
262
51

FIG. 1

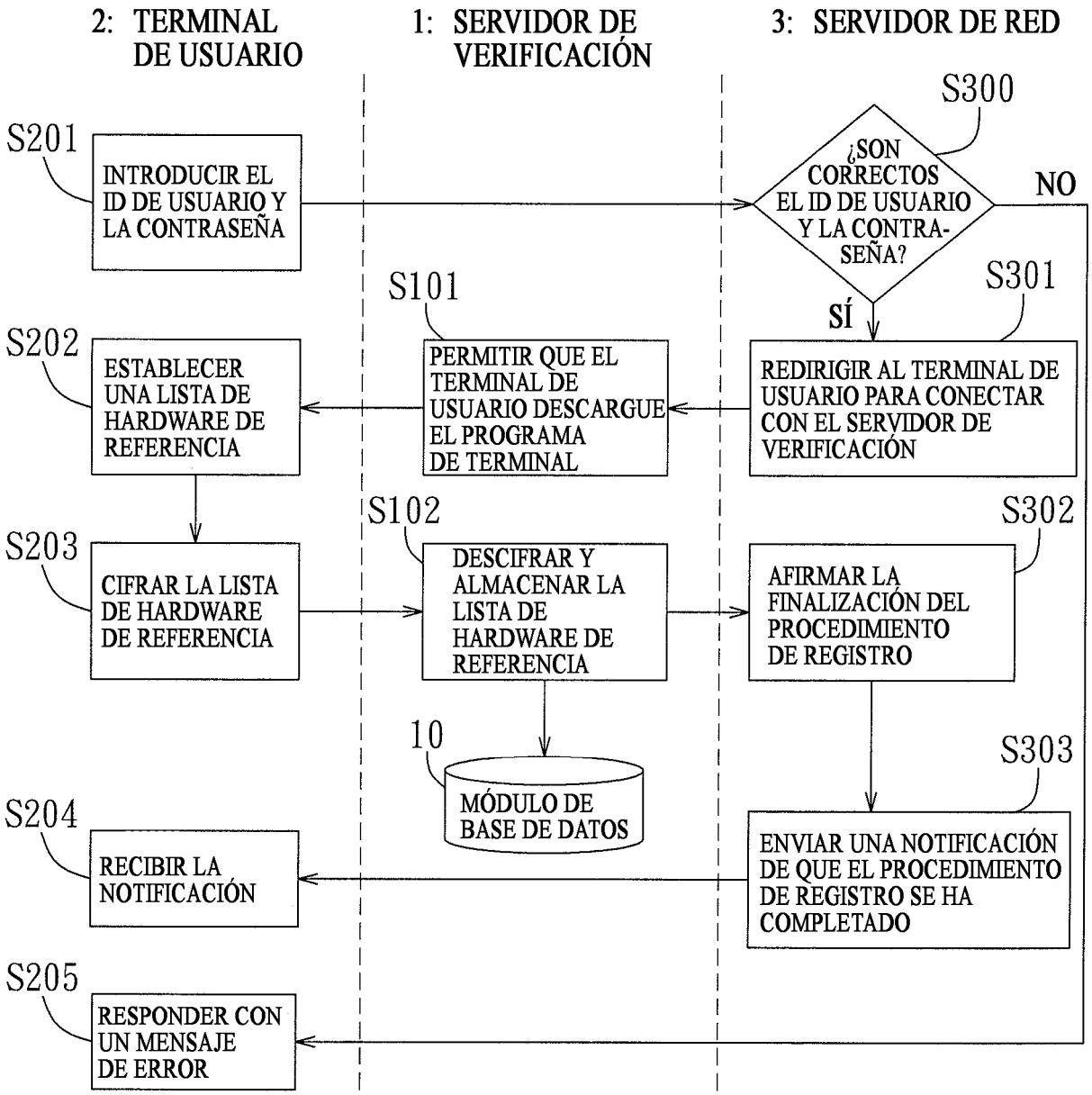
2: TERMINAL DE USUARIO
1: SERVIDOR DE VERIFICACIÓN
3: SERVIDOR DE RED
S201
INTRODUCIR EL ID DE USUARIO Y LA CONTRASEÑA
S300
¿SON CORRECTOS EL ID DE USUARIO Y LA CONTRA-SEÑA?
NO
SÍ
S101
S301
S202
ESTABLECER UNA LISTA DE HARDWARE DE REFERENCIA
PERMITIR QUE EL TERMINAL DE USUARIO DESCARGUE EL PROGRAMA DE TERMINAL
REDIRIGIR AL TERMINAL DE USUARIO PARA CONECTAR CON EL SERVIDOR DE VERIFICACIÓN
S102
S302
S203
CIFRAR LA LISTA DE HARDWARE DE REFERENCIA
DESCIFRAR Y ALMACENAR LA LISTA DE HARDWARE DE REFERENCIA
AFIRMAR LA FINALIZACIÓN DEL PROCEDIMIENTO DE REGISTRO
10
MÓDULO DE BASE DE DATOS
S303
S204
RECIBIR LA NOTIFICACIÓN
ENVIAR UNA NOTIFICACIÓN DE QUE EL PROCEDIMIENTO DE REGISTRO SE HA COMPLETADO
S205
RESPONDER CON UN MENSAJE DE ERROR

FIG. 2

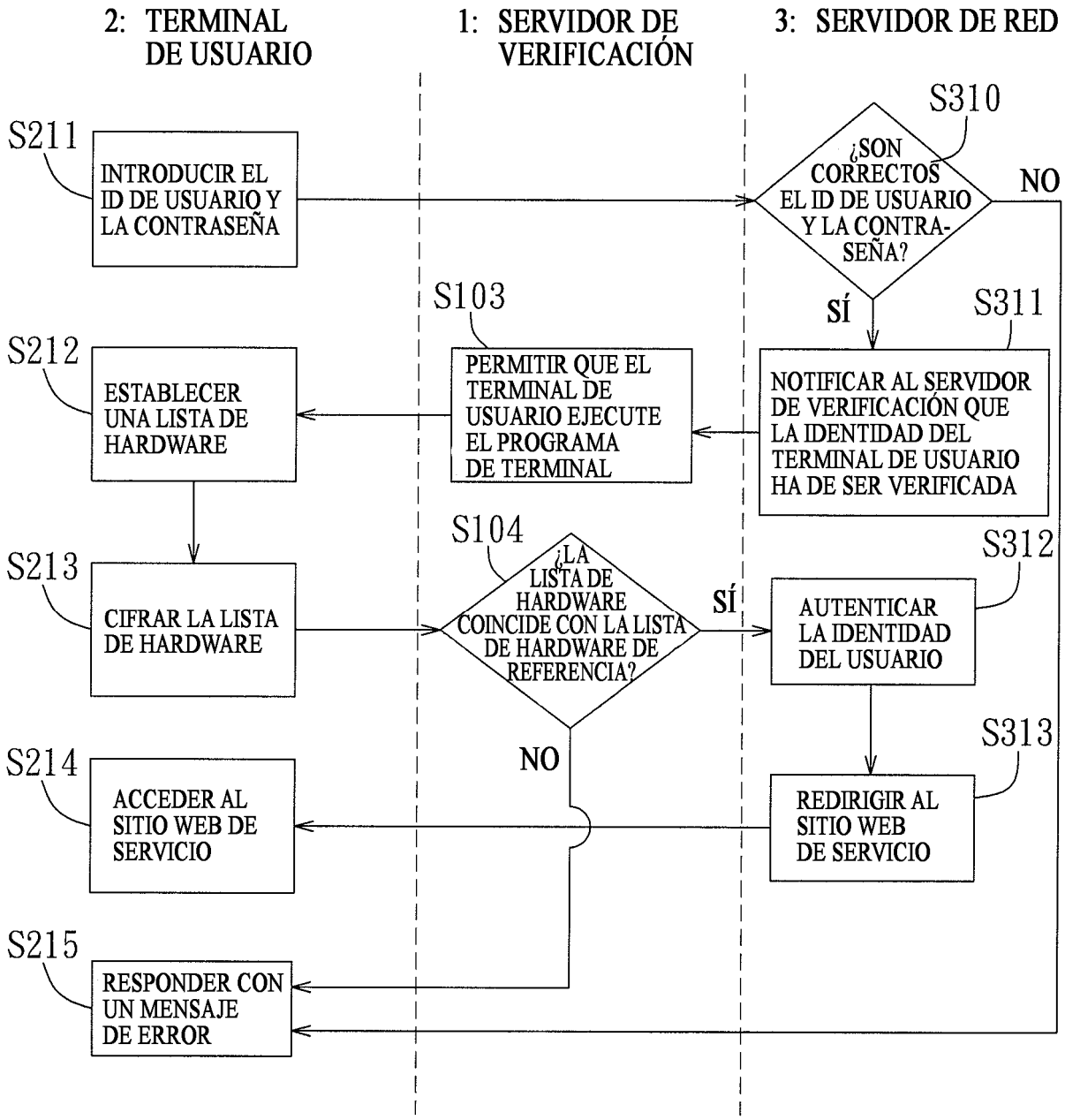
2: TERMINAL DE USUARIO
1: SERVIDOR DE VERIFICACIÓN
3: SERVIDOR DE RED
S211
INTRODUCIR EL ID DE USUARIO Y LA CONTRASEÑA
S310
¿SON CORRECTOS EL ID DE USUARIO Y LA CONTRA-SEÑA?
NO
SÍ
S311
NOTIFICAR AL SERVIDOR DE VERIFICACIÓN QUE LA IDENTIDAD DEL TERMINAL DE USUARIO HA DE SER VERIFICADA
S103
PERMITIR QUE EL TERMINAL DE USUARIO EJECUTE EL PROGRAMA DE TERMINAL
S212
ESTABLECER UNA LISTA DE HARDWARE
S213
CIFRAR LA LISTA DE HARDWARE
S104
¿LA LISTA DE HARDWARE COINCIDE CON LA LISTA DE HARDWARE DE REFERENCIA?
SÍ
S312
AUTENTICAR LA IDENTIDAD DEL USUARIO
S313
REDIRIGIR AL SITIO WEB DE SERVICIO
NO
S214
ACCEDER AL SITIO WEB DE SERVICIO
S215
RESPONDER CON UN MENSAJE DE ERROR

FIG. 3

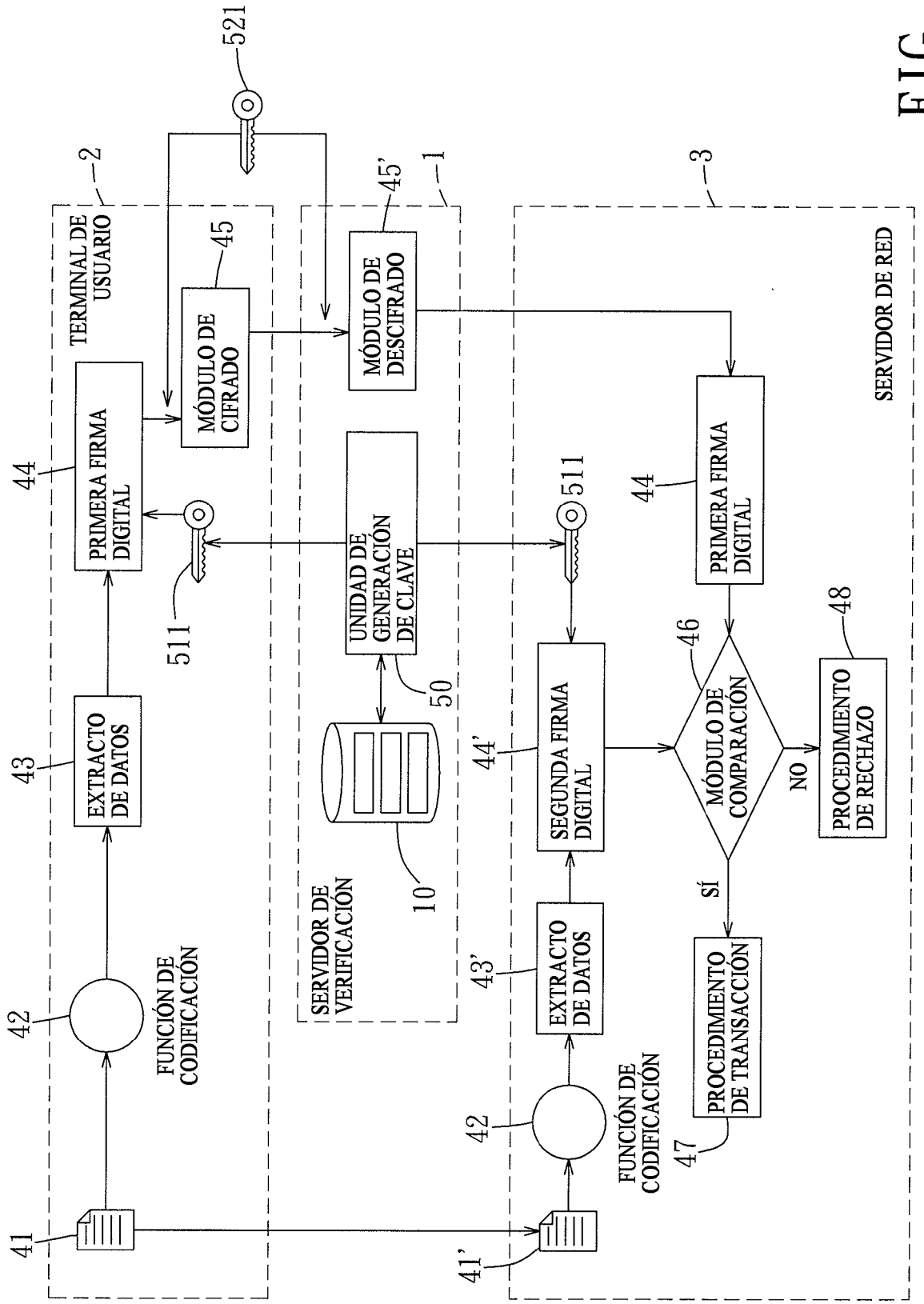
TERMINAL DE USUARIO
2
SERVIDOR DE RED
3
1
521
45
MÓDULO DE CIFRADO
45'
MÓDULO DE DESCIFRADO
44
PRIMERA FIRMA DIGITAL
511
UNIDAD DE GENERACIÓN DE CLAVE
50
SERVIDOR DE VERIFICACIÓN
10
43
EXTRACTO DE DATOS
42
FUNCIÓN DE CODIFICACIÓN
41
41'
42
FUNCIÓN DE CODIFICACIÓN
43'
EXTRACTO DE DATOS
44'
SEGUNDA FIRMA DIGITAL
511
44
PRIMERA FIRMA DIGITAL
46
MÓDULO DE COMPARACIÓN
SÍ
NO
47
PROCEDIMIENTO DE TRANSACCIÓN
48
PROCEDIMIENTO DE RECHAZO

FIG. 4

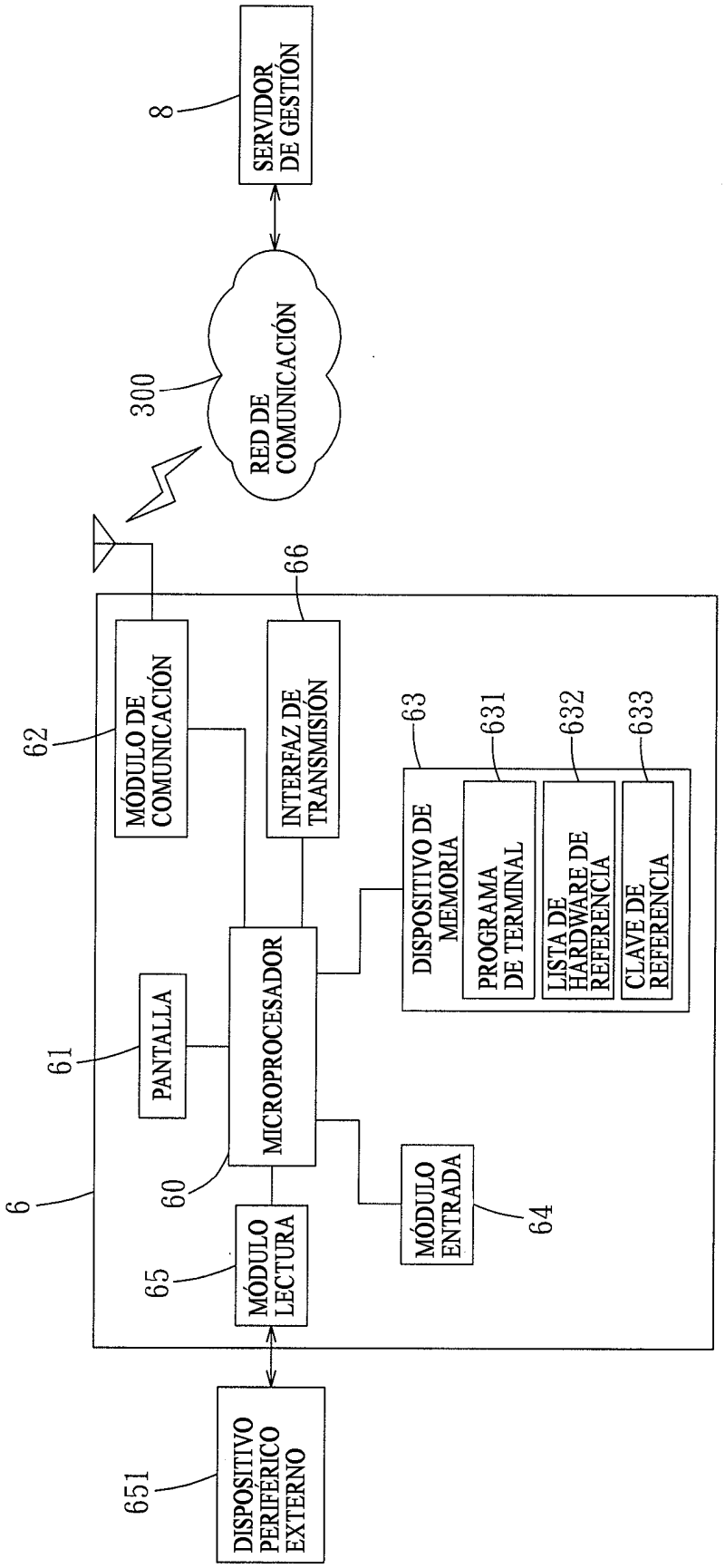
8
SERVIDOR DE GESTIÓN
300
RED DE COMUNICACIÓN
66
62
MÓDULO DE COMUNICACIÓN
INTERFAZ DE TRANSMISIÓN
63
631
632
633
DISPOSITIVO DE MEMORIA
PROGRAMA DE TERMINAL
LISTA DE HARDWARE DE REFERENCIA
CLAVE DE REFERENCIA
61
PANTALLA
MICROPROCESADOR
6
60
MÓDULO ENTRADA
64
65
MÓDULO LECTURA
651
DISPOSITIVO PERIFÉRICO EXTERNO

FIG. 5

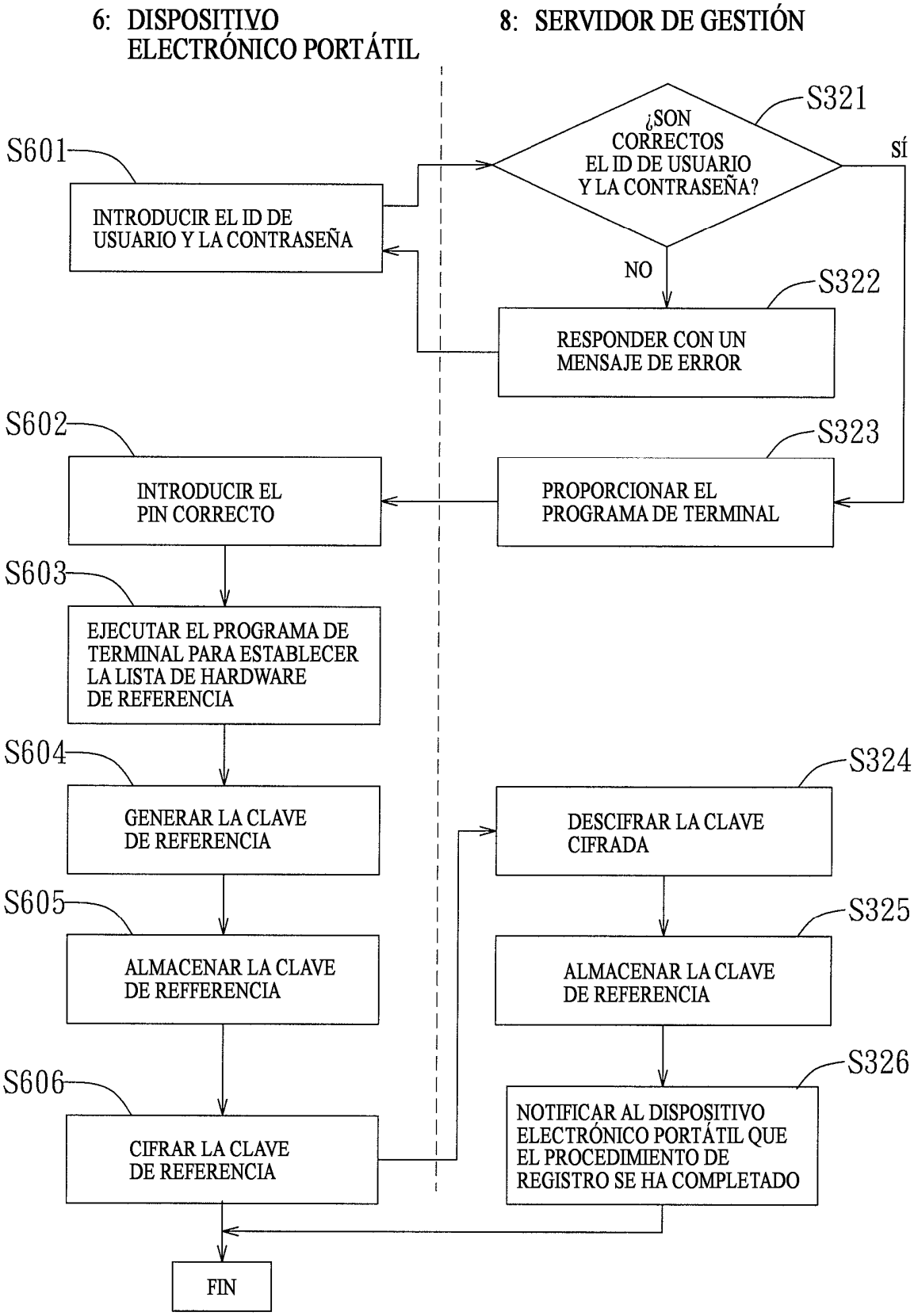
6: DISPOSITIVO ELECTRÓNICO PORTÁTIL
8: SERVIDOR DE GESTIÓN
S601
INTRODUCIR EL ID DE USUARIO Y LA CONTRASEÑA
S321
¿SON CORRECTOS EL ID DE USUARIO Y LA CONTRASEÑA?
SÍ
NO
S322
RESPONDER CON UN MENSAJE DE ERROR
S602
INTRODUCIR EL PIN CORRECTO
S323
PROPORCIONAR EL PROGRAMA DE TERMINAL
S603
EJECUTAR EL PROGRAMA DE TERMINAL PARA ESTABLECER LA LISTA DE HARDWARE DE REFERENCIA
S604
GENERAR LA CLAVE DE REFERENCIA
S324
DESCIFRAR LA CLAVE CIFRADA
S605
ALMACENAR LA CLAVE DE REFFERENCIA
S325
ALMACENAR LA CLAVE DE REFERENCIA
S606
CIFRAR LA CLAVE DE REFERENCIA
S326
NOTIFICAR AL DISPOSITIVO ELECTRÓNICO PORTÁTIL QUE EL PROCEDIMIENTO DE REGISTRO SE HA COMPLETADO
FIN

FIG. 6

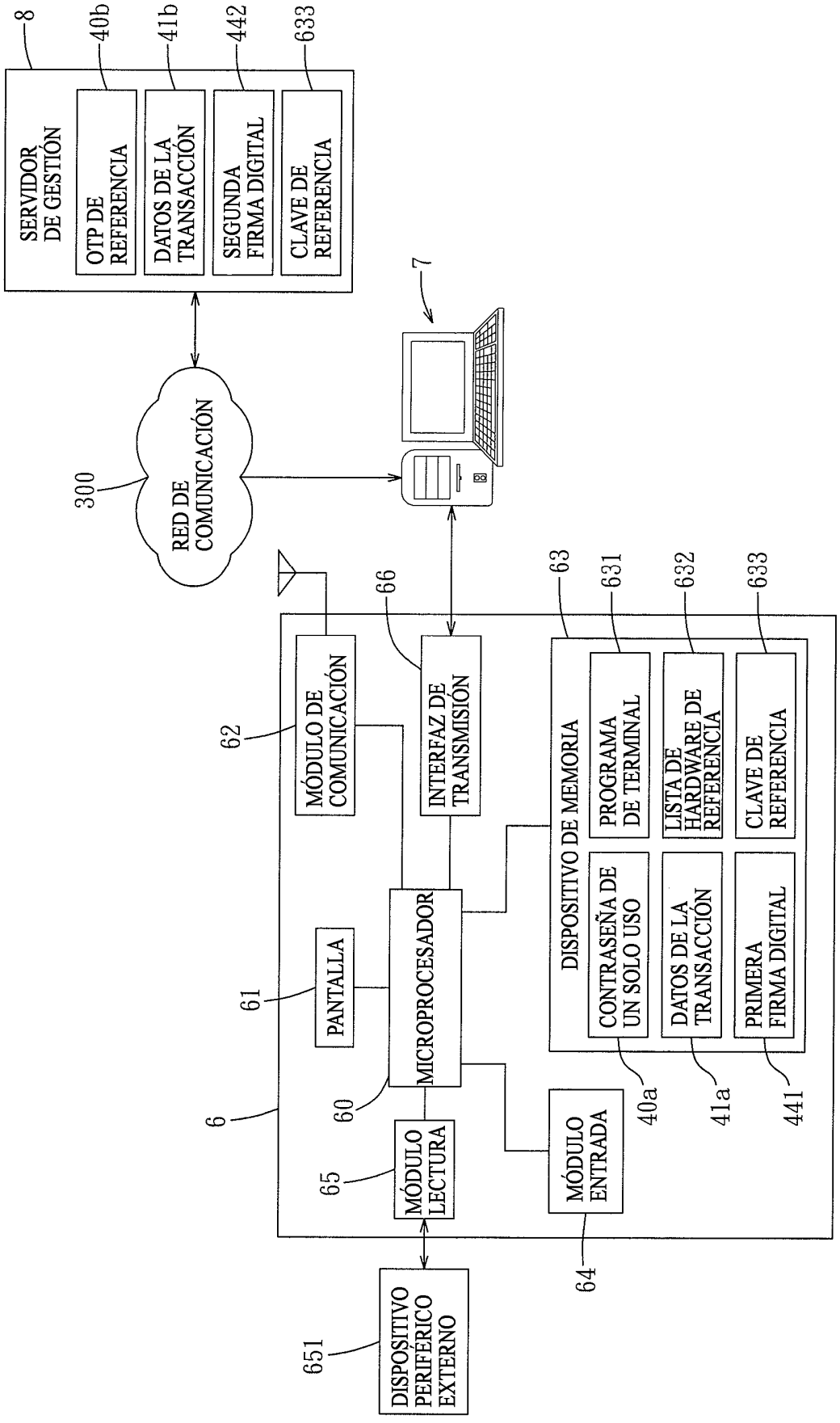
8
40b
41b
442
633
SERVIDOR DE GESTIÓN
OTP DE REFERENCIA
DATOS DE LA TRANSACCIÓN
SEGUNDA FIRMA DIGITAL
CLAVE DE REFERENCIA
7
300
RED DE COMUNICACIÓN
66
63
631
632
633
62
MÓDULO DE COMUNICACIÓN
INTERFAZ DE TRANSMISIÓN
DISPOSITIVO DE MEMORIA
PROGRAMA DE TERMINAL
LISTA DE HARDWARE DE REFERENCIA
CLAVE DE REFERENCIA
61
PANTALLA
MICROPROCESADOR
CONTRASEÑA DE UN SOLO USO
DATOS DE LA TRANSACCIÓN
PRIMERA FIRMA DIGITAL
6
60
40a
41a
441
65
MÓDULO LECTURA
MÓDULO ENTRADA
64
651
DISPOSITIVO PERIFÉRICO EXTERNO

FIG. 7

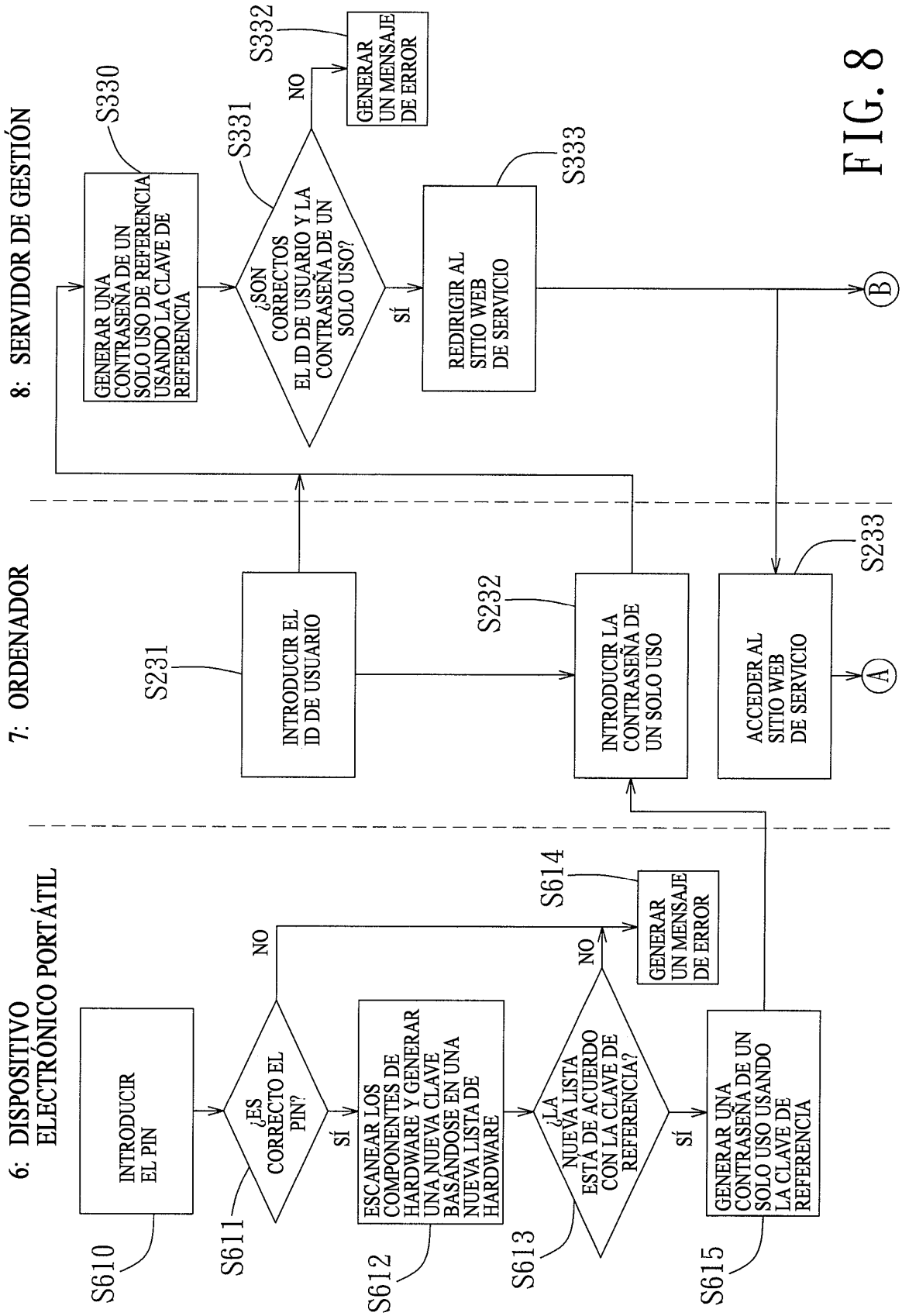
8: SERVIDOR DE GESTIÓN
7: ORDENADOR
6: DISPOSITIVO ELECTRÓNICO PORTÁTIL
S610
INTRODUCIR EL PIN
S611
¿ES CORRECTO EL PIN?
NO
SÍ
S612
ESCANEAR LOS COMPONENTES DE HARDWARE Y GENERAR UNA NUEVA CLAVE BASÁNDOSE EN UNA NUEVA LISTA DE HARDWARE
S613
¿LA NUEVA LISTA ESTÁ DE ACUERDO CON LA CLAVE DE REFERENCIA?
NO
SÍ
S614
GENERAR UN MENSAJE DE ERROR
S615
GENERAR UNA CONTRASEÑA DE UN SOLO USO USANDO LA CLAVE DE REFERENCIA
S231
INTRODUCIR EL ID DE USUARIO
S232
INTRODUCIR LA CONTRASEÑA DE UN SOLO USO
S233
ACCEDER AL SITIO WEB DE SERVICIO
A
B
S330
GENERAR UNA CONTRASEÑA DE UN SOLO USO DE REFERENCIA USANDO LA CLAVE DE REFERENCIA
S331
¿SON CORRECTOS EL ID DE USUARIO Y LA CONTRASEÑA DE UN SOLO USO?
NO
SÍ
S332
GENERAR UN MENSAJE DE ERROR
S333
REDIRIGIR AL SITIO WEB DE SERVICIO

FIG. 8

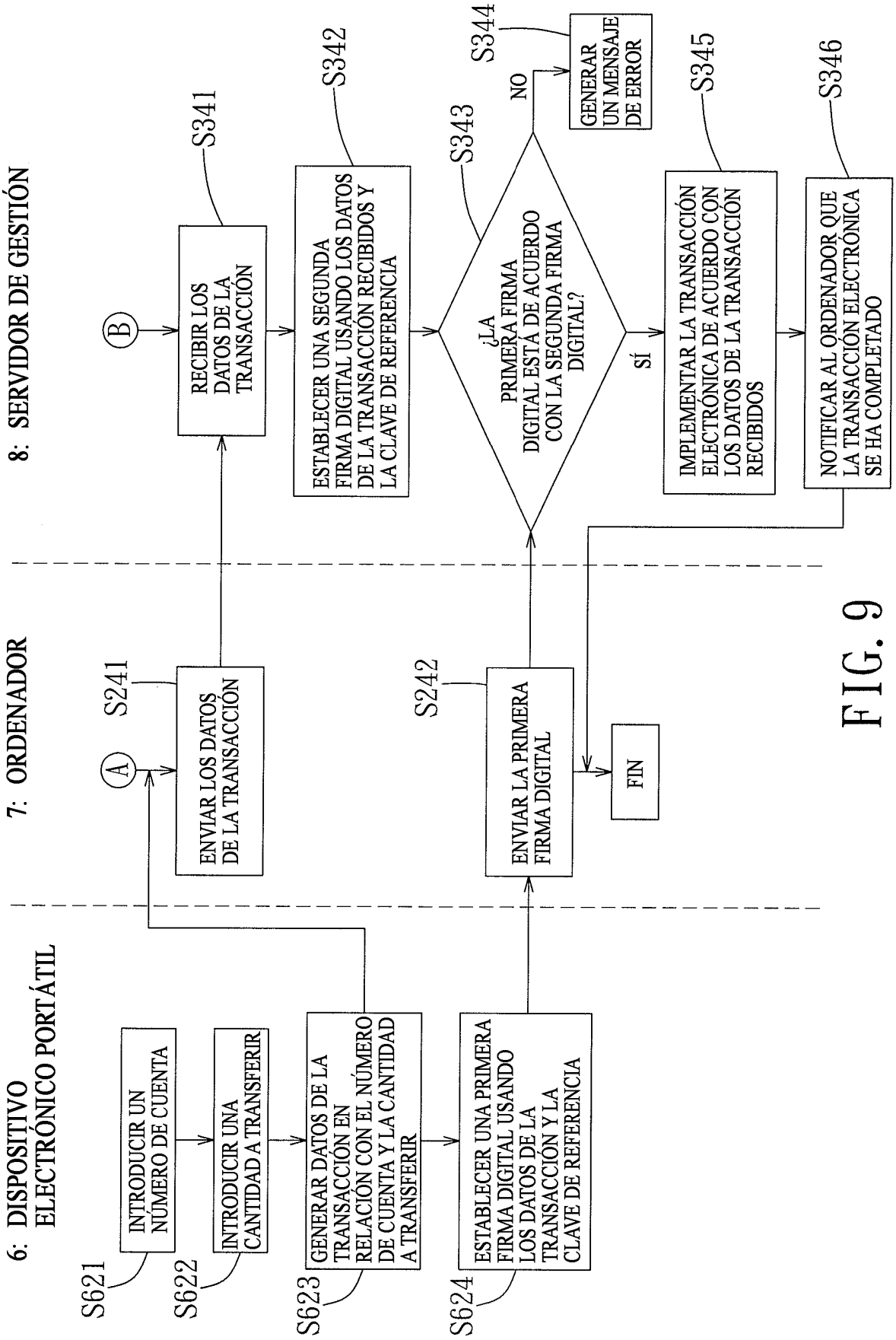
6: DISPOSITIVO ELECTRÓNICO PORTÁTIL
7: ORDENADOR
8: SERVIDOR DE GESTIÓN
INTRODUCIR UN NÚMERO DE CUENTA
INTRODUCIR UNA CANTIDAD A TRANSFERIR
GENERAR DATOS DE LA TRANSACCIÓN EN RELACIÓN CON EL NÚMERO DE CUENTA Y LA CANTIDAD A TRANSFERIR
ESTABLECER UNA PRIMERA FIRMA DIGITAL USANDO LOS DATOS DE LA TRANSACCIÓN Y LA CLAVE DE REFERENCIA
ENVIAR LOS DATOS DE LA TRANSACCIÓN
ENVIAR LA PRIMERA FIRMA DIGITAL
FIN
RECIBIR LOS DATOS DE LA TRANSACCIÓN
ESTABLECER UNA SEGUNDA FIRMA DIGITAL USANDO LOS DATOS DE LA TRANSACCIÓN RECIBIDOS Y LA CLAVE DE REFERENCIA
¿LA PRIMERA FIRMA DIGITAL ESTÁ DE ACUERDO CON LA SEGUNDA FIRMA DIGITAL?
NO
SÍ
GENERAR UN MENSAJE DE ERROR
IMPLEMENTAR LA TRANSACCIÓN ELECTRÓNICA DE ACUERDO CON LOS DATOS DE LA TRANSACCIÓN RECIBIDOS
NOTIFICAR AL ORDENADOR QUE LA TRANSACCIÓN ELECTRÓNICA SE HA COMPLETADO
S621
S622
S623
S624
S241
S242
S341
S342
S343
S344
S345
S346
A
B

FIG. 9