(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 599 985**

(51) Int. CI.:

G06F 21/34 (2013.01)
G06F 21/33 (2013.01)
H04L 9/32 (2006.01)
H04L 9/14 (2006.01)
G06Q 20/38 (2012.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **12.01.2011 E 15151322 (3)**

(97) Fecha y número de publicación de la concesión europea: **05.10.2016 EP 2927836**

(54) Título: **Validación en cualquier momento para los tokens de verificación**

(30) Prioridad:

12.01.2010 US 294338 P

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
06.02.2017

(73) Titular/es:

VISA INTERNATIONAL SERVICE ASSOCIATION (100.0%)
P.O. Box 8999 MS M1-11F
San Francisco, CA 94128, US

(72) Inventor/es:

HURRY, SIMON y
HAMMAD, AYMAN

(74) Agente/Representante:

SÁEZ MAESO, Ana

DESCRIPCIÓN

Validación en cualquier momento para los tokens de verificación

Referencias cruzadas a solicitudes relacionadas

Esta solicitud se basa y reivindica la prioridad a una Solicitud de Patente Provisional de Estados Unidos núm. 61/294,338, titulada "Anytime Reader Device Validation Service for Contactless Verification Tokens", presentada el 12 de enero del 2010, y también se relaciona con la Solicitud de Patente Provisional de Estados Unidos núm. 61/178,636 , titulada "Dynamic Data Authentication" presentada el 15 de mayo, 2009.

Antecedentes

A medida que aumentan los métodos y dispositivos para realizar transacciones financieras, persisten los viejos problemas como el fraude y la falsificación.

Una de las fuentes primarias de fraude, que es frecuente en la industria de tarjetas de crédito, es la duplicación. La duplicación se refiere a la copia electrónica de los datos almacenados electrónicamente de una tarjeta para crear tarjetas falsas. Una vez hecha la tarjeta falsa, existe la posibilidad de que pueda usarse con impunidad durante el tiempo que el usuario o la entidad emisora no se da cuenta o reporte que la información de la tarjeta de transacciones se ha visto comprometida. Este problema es particularmente frecuente en las transacciones sin presencia física de la tarjeta, como las compras y transacciones en línea, donde un falsificador no tiene por qué identificarse a través de una identificación con foto que coincide con la información impresa o almacenada en la tarjeta de transacción u otro dispositivo de consumo portátil.

Para combatir tal falsificación u otro uso no autorizado de las transacciones sin presencia física de tarjeta en línea o tradicionales de otro tipo, algunas entidades emisoras han comenzado a emitir tokens de verificación de tarjetas de contacto y sin contacto, también conocidos como tokens de verificación, para usarse junto con una computadora del usuario. El token de verificación de tarjeta puede verificar que el usuario que realiza la transacción está en posesión física de la tarjeta de transacción. Esto evita posibles fraudes en los que los estafadores obtienen solamente la información y no la tarjeta de transacción misma. Sin embargo, incluso el uso de unos tokens de verificación puede permitir diferentes formas de fraude.

Un método potencial de fraude tal es fabricar por los falsificadores o estafadores, su propia versión de los dispositivos lectores de tarjetas o tokens de verificación que son física y funcionalmente similares a las versiones autorizadas a fin de no levantar las sospechas de los usuarios finales. El estafador puede entonces distribuir estos dispositivos lectores de tarjetas fraudulentas o tokens de verificación a los usuarios que se configuran para duplicar los datos de usuario de las tarjetas de transacción siempre que se use en una transacción y que tenga los datos enviados a un sitio web o servidor operado por el falsificador. Como tal, existe una necesidad de verificar que los dispositivos de lectura de tarjeta o tokens de verificación son dispositivos autorizados fabricados por una fuente de confianza y no un dispositivo de duplicado fraudulento fabricado y distribuido por un falsificador o estafador.

La Patente de los Estados Unidos núm. 2009/0031131 describe un sistema para la gestión basada en token de un proceso de personalización PKI que incluye un sistema de petición y manejo de tokens (TRMS) configurado para recoger información de un solicitante; y un sistema de personalización de tokens (TPS) configurado para personalizar un token de hardware de manera que el uso del token de hardware se limita por la información solicitada. Un método para la gestión basada en tokens de un proceso de personalización de PKI incluye: solicitar un token de hardware; personalizar un token de hardware de manera que el token de hardware se limita a la operación dentro de los parámetros de limitación; vincular el token de hardware a una estación de trabajo que se configura para recibir el token de hardware y usar las credenciales dentro del token de hardware para solicitar y descargar los datos PKI desde un servidor PKI, la estación de trabajo que se configura, además, para personalizar un producto de usuario final mediante la carga de los datos de PKI en la memoria interna contenida dentro del producto de usuario final; y monitorear el uso del token de hardware y los datos PKI.

Las modalidades de la invención se dirigen a abordar estas y otras cuestiones.

Breve resumen

Las modalidades de la presente invención incluyen métodos para autenticar y registrar un fabricante de token de verificación que incluyen recibir una solicitud de registro de un fabricante de token de verificación en una computadora servidor y recuperar la información relacionada con el fabricante de token de verificación a partir de una base de datos y generar un par de claves específicas del fabricante mediante el uso de la computadora servidor. Otras modalidades pueden incluir realizar una revisión de riesgo con base en la información relacionada con el fabricante de token de verificación.

Otras modalidades de la presente invención, incluyen tanto métodos asimétricos como simétricos para validar, autenticar y registrar un fabricante de token de verificación que incluye generar un par de claves específicas del

fabricante para el fabricante de token de verificación (asimétricas) o generar una clave maestra (simétrica).El par de claves específicas del fabricante puede comprender un componente público y uno privado. Las modalidades también pueden incluir firmar el componente público del par de claves específicas del fabricante con el uso de la autoridad de certificación de régimen de pago (CA) y el envío del par de claves de fabricante de token de verificación con el componente público firmado al fabricante de token de verificación. Tales métodos también pueden incluir asociar el par de claves específicas de fabricante, la clave pública raíz de la CA y el componente público firmado del par de claves específica del fabricante con un identificador del fabricante de token de verificación y almacenar el identificador de fabricante del dispositivo lector asociado en una base de datos.

Otras diversas modalidades de la presente invención incluyen métodos para validar un token de verificación antes de que pueda usarse para iniciar una transacción. Tales métodos pueden incluir recibir una solicitud de validación a partir de un token de verificación y determinar un número de serie del token de verificación con base en la solicitud de validación. Tales modalidades pueden incluir determinar un estado de registro del número de serie del token verificación, determinar un identificador de fabricante de token de verificación con base en la solicitud de validación, y determinar un primer componente de un par de claves específicas del fabricante con base en el identificador de fabricante de token de verificación. Tales modalidades también pueden incluir recuperar un segundo componente de la clave específica de fabricante y una clave maestra de fabricante de token de verificación de una base de datos con base en el identificador del fabricante de token de verificación y realizar una autenticación mutua con el token de verificación. Las modalidades también pueden incluir realizar una autenticación mutua que comprende determinar una clave del token de verificación con base en el número de serie del token de verificación y la clave maestra del fabricante de token de verificación y establecer una sesión de clave del token de verificación con base en la clave del token de verificación. Establecer una sesión de clave del token de verificación también puede incluir generar un tercer componente de la clave específica de fabricante con base en el número de serie del token de verificación y una clave maestra asociada con la computadora servidor.

Otras modalidades de la presente invención incluyen métodos para producir un token de verificación auténtico. Tales métodos incluyen generar un número de serie para un token de verificación, generar un par de claves que incluye un componente público y un componente privado, firmar el componente público del par de claves con una clave privada específica del fabricante, almacenar el componente público firmado del par de claves en una memoria en el token de verificación junto con la clave raíz de la entidad emisora de certificados (CA) y asociar el número de serie con el par de claves, el componente público firmado. Tales modalidades pueden comprender además almacenar el número de serie, un identificador de fabricante, el código ejecutable en un procesador en la memoria del token de verificación. El código puede incluir instrucciones para que un procesador establezca una conexión con un servidor de verificación a través de una sesión de comunicación mediante el uso de una instalación de comunicación de una computadora a la que se conecta el token de verificación.

Breve descripción de los dibujos

La Fig. 1 es un esquema de un sistema que puede beneficiarse de diferentes modalidades de la presente invención en el contexto de una transacción de tarjeta de pago realizada en línea.

La Fig. 2 muestra una configuración ilustrativa que pueden implementar diversas modalidades de la presente invención.

La Fig. 3 es un esquema de un sistema para producir tokens de verificación de acuerdo con diversas modalidades de la presente invención.

La Fig. 4 es un diagrama de flujo de un método de validación y registro de un fabricante de token de verificación de acuerdo con una modalidad de la presente invención.

La Fig. 5 es un diagrama de flujo de un método para producir tokens de verificación de acuerdo con diversas modalidades de la presente invención.

La Fig. 6 es un esquema de un sistema para validar tokens de verificación de acuerdo con diversas modalidades de la presente invención.

La Fig. 7 es un diagrama de flujo de un método de validación de tokens de verificación de acuerdo con diversas modalidades de la presente invención.

La Fig. 8 es un esquema de un sistema para validar tokens de verificación de acuerdo con diversas modalidades de la presente invención.

La Fig. 9 es un diagrama de flujo de un método de validación de tokens de verificación de acuerdo con diversas modalidades de la presente invención.

La Fig. 10 es un diagrama de flujo de un método de validación de tokens de verificación de acuerdo con diversas modalidades de la presente invención.

La Fig. 11 es un sistema informático que se usa para implementar diversas modalidades de la presente invención.

Descripción detallada

Las modalidades de la presente invención se dirigen hacia dispositivos, sistemas y métodos para la autenticación de dispositivos de lectura de tarjetas de transacción o tokens de verificación para su uso en un sistema de transacciones. Como se usa en la presente descripción, los términos dispositivos de lectura de token de usuario, dispositivos de lectura de token y tokens de verificación, pueden usarse indistintamente para referirse a cualquier dispositivo que puede usarse para leer la información y verificar la presencia o autenticidad de los dispositivos portátiles de consumo, tokens de usuario, o tarjetas de transacción. Un token de verificación puede incluir cualquier combinación de hardware, firmware y software adecuado para leer, procesar o enviar datos hacia y desde un dispositivo portátil del consumidor. Los tokens de verificación pueden incluir dispositivos integrados, tales como componentes internos, circuitos integrados, y tarjetas de computadora en una computadora o dispositivo de comunicación o dispositivos periféricos, tales como los dispositivos USB o dispositivos de seguridad que se conectan o comunican con un dispositivo de computación o comunicación a través de una interfaz periférica. Un dispositivo de comunicación puede incluir cualquier dispositivo adecuado para enviar, recibir y procesar datos, que incluye pero no se limita a los teléfonos móviles, teléfonos inteligentes, PDAs, etc.

Los dispositivos portátiles de consumo, tokens de usuario o tarjetas de transacción comprenden dispositivos que contienen o almacenan información de identificación correspondiente a una cuenta mantenida por un usuario con otra entidad, que suele ser una entidad que mantiene, extiende, o acredita artículos de valor al usuario (*por ejemplo*, fondos monetarios, créditos, deudas, *etc*.). El término dispositivo portátil de consumo, token de usuario o tarjeta de transacción puede usarse indistintamente para referirse a diversos tipos de tarjetas de crédito, tarjetas de carga, tarjetas de débito, tarjetas bancarias, tarjetas de prepago, tarjetas de acceso, tarjetas de seguridad, y otras tarjetas que identifican una cuenta abierta por un usuario con otra entidad. Los dispositivos portátiles de consumo son capaces de existir tanto en forma pasiva (*por ejemplo*, tarjeta con una banda magnética o componentes RFID) y formas activas (*por ejemplo*, tarjetas de circuitos integrados, tarjetas inteligentes) y, además, incluyen los dispositivos electrónicos portátiles que, en su totalidad o en parte, funcionan como tales tarjetas. Tales dispositivos electrónicos portátiles pueden incluir tarjetas de memoria, tokens de cuenta, llaveros, dispositivos RFID, etiquetas engomadas, teléfonos celulares (que incluyen el teléfono de comunicaciones de campo cercano), y dispositivos de llavero (tal como el Speedpass™ disponible comercialmente de Exxon-Mobil Corp. o payWave™ comercialmente disponible de Visa, Inc.), asistentes digitales personales, otros dispositivos electrónicos móviles, transpondedores, soportes inteligente, y localizadores.

La información de identificación contenida por (*por ejemplo*, integrada en) un dispositivo de consumo portátil comprende, al menos, un número de cuenta u otro identificador, tal como un nombre de cuenta o un número de serie del dispositivo portátil de consumo. El número de cuenta puede comprender caracteres alfanuméricos. La información de identificación puede comprender, además, el nombre del titular de la cuenta (*por ejemplo*, el usuario), la fecha de caducidad de la tarjeta, los códigos de servicio, y los datos discrecionales. A modo de ejemplo, la información de identificación puede incluir los "datos de pago" convencionales almacenados en las pistas de la banda magnética de una tarjeta de crédito convencional (*por ejemplo*, Pista 1, Pista 2, y/o la Pista 3).

La información de identificación de un dispositivo de consumo portátil se lee por un lector, que es un componente eléctrico de un token de verificación que puede leer la información de identificación desde un dispositivo de consumo portátil y proporcionar la información de identificación a otro componente eléctrico. Un lector puede comprender uno o más de los siguientes: un lector de banda magnética, un lector de tarjeta de contacto, y un lector sin contacto, el último de los cuales se conoce comúnmente como un lector RFID (RFID que es un acrónimo de identificación por radio frecuencia).Los lectores se encuentran predominantemente en las ubicaciones de punto de venta de los comerciantes. Sin embargo, cada vez más, los lectores se incluyen como parte de un token de verificación dado a los usuarios para su uso en una computadora personal para usar en las transacciones en línea u otras actividades en las que un emisor, adquiriente, comerciante u otra entidad no puede comprobar personalmente la identidad del usuario autorizado o la autenticidad del dispositivo de consumo portátil. Esta tendencia representa una oportunidad para los estafadores y un correspondiente riesgo de un posible fraude a los usuarios, emisores y adquirentes.

La Fig. 1 ilustra un sistema ilustrativo que puede beneficiarse de diferentes aspectos de la invención y se describe en detalle para dar contexto a diversas modalidades, pero no debe considerarse limitante de ninguna manera. El sistema en la Fig. 1 se ilustra y describe en el contexto de una compra en línea.

Los sistemas de transacción, como el que se muestra en la Fig. 1, que usan dispositivos portátiles de consumo pueden ser susceptibles a los fabricantes fraudulentos que hacen e introducen tokens de verificación no autorizados en el flujo comercial para duplicar la información de usuario, tal como los números de tarjeta de crédito, de los usuarios desprevenidos. Para evitar la posibilidad de que un fabricante no autorizado duplique la información de usuario durante una transacción realizada con un token de verificación no autorizado, es deseable la previa autentificación o registro de un token de verificación antes de permitir su uso para completar cualquier transacción. Así, las modalidades proporcionan una mayor seguridad, y por lo tanto una mayor probabilidad, de que los usuarios hagan transacciones en línea mediante el uso de dispositivos portátiles de consumo.

En la Fig. 1 se muestran iconos para un usuario 1, un dispositivo de consumo portátil 5, un dispositivo de comunicación 7 (tal como un teléfono celular), una computadora 10, el sitio web de un comerciante 20, y una primera red de comunicaciones 31 que permite a la computadora del usuario y el sitio web del comerciante comunicarse entre sí. La primera red de comunicaciones 31 puede incluir Internet, una red de telecomunicaciones (*por ejemplo*, una red inalámbrica, red de telefonía celular, una red telefónica, una red por cable, o cualquier combinación de las mismas), una red de área extendida (WAN), una red de área local (LAN), un router o puerta de enlace acoplado a una de las redes anteriores, o cualquier combinación de lo anterior. También en la Fig. 1 se muestra un banco adquirente 50 para el comerciante, un banco emisor 60 para el dispositivo portátil de consumo 5, una red de procesamiento de pagos 70, y una segunda red de comunicaciones 32 que permite a la red de procesamiento de pagos 70 comunicarse con cada uno de los bancos 50 y 60.

La segunda red de comunicaciones 32 puede comprender Internet (y, por tanto, puede solaparse y compartir instalaciones con la primera red de comunicaciones 31), o puede comprender una o más redes privadas, o la combinación de una o más redes privadas con la Internet. Una red privada puede comprender una red de telecomunicaciones, una red de área extendida (WAN), una red de área local (LAN), o cualquier combinación de las mismas. En algunos casos, las primera y segunda redes de comunicaciones 31 y 32 pueden ser las mismas (tal como una red que usa la Internet como red principal).Una red de comunicaciones comprende, generalmente, una red de uno o más enlaces de comunicaciones y dos o más nodos que pasan mensajes de una parte de la red a la otra parte. Cada nodo comprende una o más piezas de maquinaria eléctrica, y cada enlace puede comprender uno o más de los siguientes: fibras ópticas, enlaces ópticos, enlaces de radio, y cables eléctricos. Los componentes descritos hasta ahora son, en su mayor parte, convencionales y se disponen de manera convencional.

Diversas modalidades de la presente invención pueden usarse para autenticar, registrar u opcionalmente actualizar un token de verificación integrado o periférico 40 antes de que se use por primera vez en un sistema de transacciones tal como el que se muestra en la Fig. 1. En algunas modalidades, el registro o autenticación previa de los tokens de verificación puede completarse sin necesidad de introducir, enviar, o de cualquier otra manera usar dispositivos portátiles de consumo de un usuario, tal como una tarjeta RFID, o liberar cualquier otra información del usuario. En algunas modalidades, un token de verificación puede autenticarse por tener el token de verificación en comunicación con un servidor host a través de cualquier medio de comunicación adecuado y la implementación de un esquema de autenticación mutua simétrico o asimétrico. En tales modalidades, sin embargo, es necesario asegurar que la tecnología del token de verificación o el esquema de autenticación no pueden fabricarse, reproducirse, o distribuirse por un fabricante no autorizado de manera que los token de verificación fraudulenta no pueden introducirse en el mercado para duplicar datos de usuario y transmitirlos a los estafadores. Puesto que es difícil mantener tales tecnología y esquemas sin ser hackeados o copiados, es ventajoso tomar precauciones adicionales. Otros aspectos de la Fig. 1 se describirán con más detalle a continuación en referencia a modalidades de la presente invención.

La Fig. 2 muestra una configuración de una computadora 10, varios tokens de verificación 40A, 40B, y 40C, y un dispositivo de consumo portátil 5 que puede usarse en implementaciones de diversas modalidades de la presente invención. La computadora 10 puede incluir dispositivos de interfaz de usuario, tales como el teclado 250 y la pantalla 260.Los tokens de verificación 40A, 40B, 40C pueden tener una interfaz USB u otra interfaz periférica que puede conectarse a una interfaz periférica 16 en la computadora 10.La interfaz periférica 16 en la computadora 10 puede implementarse como varios protocolos de interfaz periférica estándar o propietarios adecuados para conectar un token de verificación a la computadora 10.Mediante la autenticación o registro previo de los fabricantes del token de verificación y exigir prácticas y protocolos específicos para los fabricantes en la elaboración de tokens de verificación auténticos, diversas modalidades de la presente invención proporcionan niveles adicionales de seguridad contra posibles estafadores que duplican información personal o de cuenta de usuario sensible mediante tokens de verificación fraudulenta, falsificados o de cualquier otra manera no autorizados.

Los tokens de verificación 40A, 40B, y 40C pueden tener interfaces USB u otra interfaz periférica 46 que puede conectarse a una interfaz periférica 16 en la computadora 10.Como se muestra en la Fig. 2, la computadora 10 puede incluir una pantalla 260 y un dispositivo de entrada 250 como el teclado que se muestra.

La interfaz periférica 16 en la computadora 10 puede implementarse como varios protocolos de interfaz periférica estándar o propietarios adecuados para conectar un token de verificación a la computadora 10.Estas normas pueden incluir USB, USB 2.0, FireWire™ (IEEE 1394), puertos serie y paralelo, etc. Por ejemplo, el token de verificación 40A puede ser un lector de banda magnética de contacto basada en USB, el token de verificación 40B puede ser un lector RFID basado en USB o FireWire™, mientras el token de verificación 40C puede ser algún otro tipo de lector de dispositivo de consumo portátil inalámbrico que se integra dentro de la computadora de hardware 10 o se conecta internamente a la placa base o el bus interno.

El usuario puede entonces presentar el dispositivo de consumo portátil 5 a uno o más de los tokens de verificación compatibles para iniciar, procesar, o de cualquier otra manera completar una transacción mediante el uso de la computadora 10.Sin embargo, antes de usar el token de verificación en una solicitud de transacción o autenticación real, la entidad/servidor de autenticación o validación puede exigir que el token de verificación se autentifique mediante el uso de diversos sistemas y métodos de acuerdo con modalidades de la presente invención. La base de los sistemas y métodos para la autenticación de un token de verificación puede incluir los procesos, métodos y sistemas para el

registro o autenticación previa de un fabricante de token de verificación y la fabricación y programación actual de los tokens de verificación, que se describirá con más detalle abajo.

Como se muestra en la Fig. 1, la computadora 10 puede comprender una computadora de sobremesa, una computadora portátil, o cualquier dispositivo electrónico portátil que tiene una instalación de red y una interfaz periférica para la comunicación con uno o más dispositivos periféricos. La computadora 10 tiene uno o más procesadores 11, un medio legible por computadora tangible 12 acoplado al(los) procesador(es) 11 que almacena códigos de instrucción (software) que controla el(los) procesador(es) 11 y que almacena los datos usados por el(los) procesador(es) 11, y una interfaz de usuario 13 acoplada al(los) procesador(es) 11.La instalación de red 14 y la interfaz periférica 16 también pueden acoplarse al(los) procesador(es) 11, con la instalación de red 14 que también se acopla a la primera red de comunicaciones 31.La interfaz de usuario 13 comprende uno o más dispositivos de salida de vídeo (*por ejemplo*, pantallas, visualizadores) y uno o más dispositivos de entrada (*por ejemplo*, teclado, ratón, ratón de bola, etc.)para que el usuario 1 reciba información desde la computadora 10, y para proporcionar información a la computadora 10.

El medio legible por computadora 12 puede comprender una combinación de memoria de semiconductores y de almacenamiento no volátil, tal como una o más unidades de disco y/o la memoria no volátil. El medio legible por computadora 12 almacena un sistema operativo para la computadora 10, que permite que los procesos y aplicaciones se ejecuten por el(los) procesador(es) 11.El sistema operativo proporciona servicios a estos procesos y aplicaciones, y permite que estos procesos y aplicaciones accedan a los componentes de la interfaz de usuario 13, las porciones del medio legible por computadora 12, la instalación de red 14, la interfaz periférica 16, y otros componentes de la computadora 10.El sistema operativo puede ser complejo y completo, tal como se encuentra en las computadoras de sobremesa, o simplificado, tal como se encuentra en los teléfonos celulares, PDAs, y muchos otros tipos de dispositivos electrónicos portátiles.

El servicio de red 14 de la computadora 10 puede comprender software y hardware que permiten que un proceso que se ejecuta en la computadora 10 se comunique con una red de comunicaciones, tal como la red 31, para enviar y recibir mensajes, datos, y similares, a una o más entidades acopladas a la red de comunicaciones. El hardware de la instalación 14 puede comprender hardware dedicado separado del/de los procesador(es) 11, o el uso compartido del(de los) procesador(es) 11, o una combinación de los mismos. El software de la instalación 14 puede comprender firmware, software almacenado en un medio legible por computadora 12 u otro medio legible por computadora, porciones del sistema operativo, o una combinación de cualquiera de los elementos anteriores.

La instalación de red 14 es preferentemente un recurso no exclusivo, que permite el acceso a la red de comunicaciones por otros procesos y aplicaciones que se ejecutan por la computadora 10.La interfaz periférica 16 de la computadora 10 comprende una conexión por cable o inalámbrica que permite a un dispositivo periférico (separado de la computadora 10) comunicarse con la computadora. Las conexiones cableadas convencionales incluyen conectores de bus serie universal (USB) ("puertos USB"), puertos serie, puertos paralelos y puertos PCMCIA. Las conexiones inalámbricas convencionales incluyen estaciones de base de infrarrojos (IR) y estaciones de base Bluetooth™ que se incorporan en la computadora 10 o que se acoplan a una interfaz periférica de la computadora 10.

Además del lector 44 y la interfaz periférica 46, el token de verificación 40 comprende además un procesador 41, un medio legible por computadora tangible 42 acoplado al procesador 41 que almacena los datos y los códigos que dirigen el funcionamiento del procesador 41, un módulo de seguridad 43 acoplado al procesador 41 y adaptado para almacenar de manera segura una o más claves de encriptación y para encriptar y desencriptar los datos para el token de verificación 40, un lector 44 acoplado al procesador 41 y adaptado para leer los dispositivos portátiles de consumo 5, y una interfaz periférica 46 acoplada al procesador 41 y adaptada para comunicarse a la computadora 10 por medio de la interfaz periférica 16.

El procesador 41 puede comprender un microprocesador convencional, y el medio legible por computadora 42 puede comprender una combinación de memoria de semiconductores y de almacenamiento no volátil, tal como memoria no volátil. El medio legible por computadora 42 puede incluir el almacenamiento de varios elementos de datos, códigos de procesador que dirigen el funcionamiento del procesador 41 y la memoria del procesador que el procesador 41 puede usar en la realización de sus tareas. Con referencia de nuevo a la Fig. 1, el módulo de seguridad 43 puede comprender el circuito de encriptado y desencriptado (que puede incluir uno o más procesadores), y puede comprender una o más claves de encriptado almacenadas en una memoria protegida. El módulo de seguridad 43 también puede incluir un circuito de seguridad cortafuegos que protege el token de verificación 40 de ataques de piratas informáticos realizados a través de la interfaz periférica 16.

El lector 44 puede comprender un lector de convenciones. La interfaz periférica 46 puede comprender una conexión por cable o inalámbrica adaptada para comunicar con la interfaz periférica 16 de la computadora 10.Las conexiones cableadas convencionales incluyen conectores de bus serie universal ("puertos USB"), puertos serie, puertos paralelos y puertos PCMCIA. Las conexiones inalámbricas convencionales pueden incluir estaciones remotas de infrarrojos y Bluetooth™. Cuando se usa una conexión por cable convencional con interfaz periférica 46, el token de verificación 40 puede acoplarse de manera desmontable a la computadora 10 en la interfaz periférica 16, tal como en un conector de puerto USB.

El token de verificación 40 también puede incluir varios códigos integrados en el medio legible por computadora 42 que dirigen al procesador de datos 41 para llevar a cabo las acciones respectivas. Un primer código puede dirigir al procesador de datos 41 para comunicarse con la computadora 10 por medio de la interfaz periférica 46 a fin de obtener las instalaciones de redes de acceso 14 de computadora 10.El primer código puede comprender el código que dirige al procesador de datos 41 para enviar un controlador de dispositivo a la computadora 10 y una instrucción para instalar el controlador de dispositivo en el sistema operativo de la computadora, en donde el controlador de dispositivo es una colección de instrucciones a ejecutar por la computadora 10 que permite a la computadora 10 reconocer el token de verificación y comunicarse con el token de verificación 40, y permite al procesador de los datos del token 41 hacer llamadas de función a diferentes (API) del sistema operativo de la computadora, tales como las relacionadas con las redes y el acceso a la instalación de red 14.

Así los llamados controladores de "auto-instalación" se conocen en la técnica, y pueden usarse en la presente descripción. Ellos comprenden una o más llamadas de función a una interfaz de programación de aplicaciones (API) del sistema operativo de la computadora, tal como la API del administrador de dispositivos. El primer código puede configurarse para funcionar con un sistema operativo seleccionado, como Windows o Symbian OS, o puede configurarse para trabajar con varios sistemas operativos. En este último caso, el primer código puede incluir varios controladores de dispositivo para los diferentes sistemas operativos, y las instrucciones que consultan a la computadora 10 por su tipo de sistema operativo y seleccionan (e instalan) el controlador más apropiado para el sistema operativo de la computadora. Los controladores de dispositivos pueden almacenarse en una sección del medio legible por computadora 42.

Un segundo código de token de verificación 40 dirige al procesador 41 para recibir información de identificación que se lee desde el dispositivo portátil de consumo 5 por el lector 44.El segundo código puede incluir código que dirige al procesador 41 para recibir un identificador universal de recursos (URID) de una entidad/servidor de validación 80, como se lee desde el dispositivo portátil de consumo 5 por el lector 44.Estas instrucciones pueden incluir instrucciones de E/S convencionales que dirigen las comunicaciones con lector 44.El dispositivo portátil de consumo 5 diferente, puede almacenar y proporcionar URID diferentes a diferentes entidades de validación 80.Un identificador de recursos uniforme (URID) puede comprender un localizador de recursos uniforme (URL), una dirección de protocolo de Internet (dirección IP), o cualquier otro tipo de identificador que puede identificar una entidad en una red de comunicaciones.

Si un dispositivo de consumo portátil 5 no proporciona un URID para la entidad/servidor de validación 80, el token de verificación 40 puede almacenar un URID para una entidad/servidor de validación 80, específica o por defecto, de un fabricante. En algunas configuraciones, algunos tokens de verificación 40 pueden ser de marca compartida con los respectivos bancos emisores y solamente trabajan para los dispositivos portátiles de consumo que son de marca compartida con los mismos bancos emisores, y cada banco emisor puede tener su propia entidad/servidor de validación 80 con su URID propia. En tal configuración, estos tokens de verificación 40 pueden almacenar los URID para sus respectivas entidades de validación 80 de marca compartida. En lugar, o además de esta configuración, algunos tokens de verificación 40 pueden asociarse con las redes de procesamiento de pago 70 respectivas, y cada una de tales redes puede tener su propia entidad/servidor de validación 80.En tal configuración, estos tokens de verificación 40 pueden almacenar los URID para sus respectivas entidades de validación asociadas 80.

En consecuencia, el segundo código del token de verificación 40 puede configurarse además para dirigir el procesador de datos 41 a usar solamente un URID predeterminado almacenado por el token de verificación 40, o usar un URID predeterminado si el dispositivo de consumo portátil 5 no proporciona el token de verificación 40 con un URID para la entidad/servidor de validación 80.Como otra implementación, el token de verificación 40 puede incluir código que dirige al procesador 41 para seleccionar uno de una serie de URID almacenados en el token de verificación 40 con base en un número de banco proporcionado en la información de identificación o integrado en el número de cuenta. La dirección y los códigos más arriba pueden implementarse con las instrucciones convencionales de E/S, instrucciones de acceso a memoria, y las instrucciones lógicas y de control de la CPU. Uno o más URID para entidades de validación pueden almacenarse en la memoria legible por computadora 42.

Un tercer código de token de verificación 40 dirige al procesador de datos 41 para establecer la comunicación con la entidad/servidor de validación 80 mediante el uso de la instalación de red 14 de la computadora 10.El sistema operativo de la computadora 10 comprende uno o más módulos de software y programas de aplicación, genéricamente llamados "módulos de servicios de la red" en la presente descripción, que pueden acceder a la instalación de red 14 y establecer sesiones de comunicación con las entidades en la red de comunicaciones 31.Tales módulos de servicios de red incluyen Microsoft's Windows Communications Foundation (*por ejemplo*, .NET 3.0, .NET 4.0, *etc.*), Apple's CFNetwork Framework, la sección de redes de los núcleos de los sistemas operativos UNIX y Linux, la capa de servicios del sistema operativo y la capa base de servicios del sistema operativo Symbian, los navegadores de Internet, y similares. Cada uno de estos módulos de servicios de red es no exclusivo (*por ejemplo*, capaz de servir a más de un procesador, y más de un proceso/aplicación) y proporcionan una interfaz de programación de aplicaciones (API) para un conjunto de funciones que un procesador puede acceder mediante el llamado de función respectivo. Con estas prestaciones de la API, una colección de las llamadas de función puede construirse fácilmente para ejecutar por un procesador, que permiten al procesador establecer un canal de comunicación con una entidad en una red de comunicaciones acoplada a una instalación de red 14, y para el intercambio de mensajes y datos con la entidad.

El tercer código del token de verificación 40 comprende una colección tal de llamados de función a la API de un módulo de servicios de red de la computadora 10, que incluye una o más llamadas de función que proporcionan el identificador universal de recursos (URID) para la entidad/servidor de validación 80 y una instrucción para establecer una sesión con la entidad de validación. La sesión puede ser una sesión de capa de conexión segura (o capa de transporte seguro) (*por ejemplo*, una sesión SSL) con autenticación mutua. Como parte del establecimiento de la sesión en algunas implementaciones, el tercer código del token de verificación 40 puede incluir dirigir al procesador de datos 41 para proporcionar, o para que se proporcione, una dirección de red para el token al módulo de servicios de red de la computadora y a la entidad/servidor de validación 80.La dirección de red puede ser estática o dinámica, la última de las cuales puede obtenerse a través de la llamada de función de la API al módulo de servicios de red de la computadora. La dirección de red puede ser una dirección IP.

Si el token de verificación 40 se configura para usar un navegador de Internet para un módulo de servicios de red, este puede comprender, además, llamadas de función de la API para que el sistema operativo de la computadora inicie una instancia del navegador y lo proporcione con acceso a la instancia del navegador. En algunas implementaciones, tal como cuando la entidad de verificación 40 almacena el URID de la entidad/servidor de validación 80, el tercer código puede dirigir al procesador de datos 41 para establecer la comunicación con la entidad/servidor de validación 80 mucho antes de que el usuario 1 presente el dispositivo de consumo portátil 5 al lector 44.La verificación 40 y la validación 80 pueden mantener la sesión de comunicación activa hasta que el dispositivo 5 se presenta al lector 44, y en los intervalos que el dispositivo 5 se presenta al lector 44, mediante el intercambio de mensajes de "pulsación" de forma intermitente. Por ejemplo, el token de verificación 40 puede periódica, no periódica, o aleatoriamente enviar mensajes a la entidad/servidor de validación 80 que confirman su presencia en la sesión, y la entidad/servidor de validación 80 puede enviar un mensaje de respuesta que confirma su presencia en la sesión.

Un cuarto código del token de verificación 40 dirige al procesador de datos 41 para transmitir al menos una porción de la información de identificación a la entidad/servidor de validación 80 por medio de las prestaciones de red 14 de la computadora 10, en donde la información de identificación se transmite en forma encriptada. Si se establece una sesión SSL, el cuarto código puede dirigir al procesador de datos 41 para pasar la información de identificación al módulo de servicios de red de la computadora mediante el uso de la llamada de función apropiada a la API para el módulo de servicios de red y la información de identificación puede transmitirse en la sesión SSL, donde los datos transmitidos y recibidos se encriptan por una clave de sesión. Para una capa adicional de seguridad, el cuarto código puede comprender además un código que dirige al procesador 41 para cifrar la información de identificación con la ayuda del módulo de seguridad 43 mediante el uso de una clave de encriptación almacenada en el token 40 antes de proporcionarla a la instalación de red 14.Estas instrucciones pueden incluir instrucciones de E/S convencionales que dirigen las comunicaciones con el módulo de seguridad 43 para pasar la información de identificación al módulo 43 y para recibir de vuelta la información encriptada. Una clave de encriptación para esto puede almacenarse en un medio legible por computadora 42 o en el módulo de seguridad 43.

El uso de llamadas de función a diversas interfaces de programación de aplicaciones (API) del sistema operativo de la computadora 10 sus módulos de soporte, prestaciones, y sus aplicaciones se conocen bien en la técnica de software, y un experto en la técnica será capaz de construir instrucciones y la llamadas de función de la API para implementar los códigos y las tareas anteriormente descritos en vista de esta descripción sin la experimentación excesiva.

La Fig. 3 es un esquema de un sistema 300 para el registro y la autenticación de los fabricantes de token de verificación de acuerdo con una modalidad de la presente invención. El sistema 300 puede incluir una entidad/servidor de validación 80 conectada a una red de comunicación, tal como la primera red de comunicación 31.A través de la red de comunicación 31, la entidad/servidor de validación 80 también puede acoplarse a una base de datos 303, banco emisor 60, y un número de fabricantes de token de verificación 305, 307, y 309.La entidad/servidor de validación 80 puede operarse por el emisor, el adquirente, un comerciante o una red de procesamiento de pagos 70, tales como Visa Net™.

La entidad/servidor de validación 80 puede configurarse y/o programarse para requerir que un fabricante de token de verificación que desea fabricar tokens de verificación auténticos o de cualquier otra manera aprobados para presentar una solicitud de registro o validación. En algunas modalidades, la entidad/servidor de validación 80 puede alojar un sitio web u otra interfaz de usuario para que los fabricantes de tokens de verificación 305, 307, o 309 puedan descargar los formularios y/o especificaciones apropiadas respecto a la información que la entidad/servidor de validación 80 requiere para validar o registrar, en última instancia, un fabricante de token de verificación.

Los fabricantes de tokens de verificación pueden reunir toda la información necesaria y luego presentar una solicitud de registro o validación a la entidad/servidor de validación 80 en la acción 1.Los formularios, instrucciones o especificaciones proporcionadas por la entidad/servidor de validación 80 pueden exigir que las solicitudes de registro incluyan información específica del fabricante de token de verificación, tales como el nombre, ubicación, referencias comerciales del fabricante, o cualquier otra información que la entidad/servidor de validación 80 puede usar para acceder a la información respecto al fabricante de token de verificación solicitante o para evaluar la legitimidad del fabricante de token de verificación solicitante. La entidad/servidor de validación 80 puede usar la información presentada en la solicitud de registro para recopilar y evaluar la información respecto al fabricante de token de verificación solicitante para determinar si el fabricante de token de verificación solicitante es una entidad de confianza o legítima.

En algunas modalidades, la determinación en cuanto a la confiabilidad o la legitimidad de un fabricante de token de verificación solicitante puede basarse en protocolos de análisis de riesgos internos de la entidad que opera la entidad/servidor de validación 80 en la acción 2.Por ejemplo, una red de procesamiento de pagos, tal como una red de procesamiento de pagos de tarjetas de crédito, puede aplicar sus propios protocolos de gestión de riesgos y fraudes desarrollados internamente para evaluar cada fabricante de token de verificación solicitante. En algunas modalidades, cuando la entidad/servidor de validación 80 recibe una solicitud de registro de un fabricante de token de verificación, puede analizar la información de la solicitud de registro para construir consultas y/o solicitudes propias con el propósito de recopilar información de antecedentes respecto al fabricante de token de verificación solicitante. En algunas modalidades, la entidad/servidor de validación 80 puede consultar diversas bases de datos tales como la base de datos 303 para obtener información de antecedentes respecto al fabricante de token de verificación solicitante.

En modalidades en las que la entidad/servidor de validación 80 se opera por una entidad que no tenga su propio protocolo de gestión de riesgo o fraude, la entidad/servidor de validación 80 puede enviar las solicitudes de registro para la información de la solicitud de registro a un servicio o entidad de análisis externo, para determinar si se registra o valida el fabricante de token de verificación solicitante en la acción 2. Por ejemplo, la entidad/servidor de validación 80 puede enviar información de solicitud de registro, o una solicitud o consulta que contiene información de solicitud de registro, a la base de datos 303 para determinar si el fabricante de token de verificación solicitante aparece con un estado o denominación particular.

Específicamente, la base de datos 303 puede ser una base de datos de ejecución de la ley o la industria que enumera los estafadores o falsificadores conocidos con base en una conducta criminal, quejas de los consumidores o los informes de litigio civil. Como alternativa, la base de datos 303 también puede enumerar las entidades con base en su confiabilidad, calificación crediticia, clasificación o calificación en el sector u otros indicios reveladores de que el fabricante de token de verificación solicitante es probable que sea un fabricante confiable o legítima. En otras modalidades, la base de datos 303 puede construirse, operarse y mantenerse por la misma entidad que opera la entidad/servidor de validación 80.

Con base en los resultados de los protocolos de gestión de riesgos o fraude, internos o externos, la entidad/servidor de validación 80 puede determinar si el fabricante de token de verificación solicitante se considerará confiable y, en consecuencia, se registrará como un fabricante de token de verificación de confianza en la acción 3. Una vez que se hace la determinación de si el fabricante de token de verificación solicitante se registrará como un fabricante de confianza o legítimo, la entidad/servidor de validación 80 puede enviar un mensaje de respuesta o el mensaje de registro al fabricante de token de verificación solicitante en la acción 4. En el caso de que la entidad/servidor de validación 80 determina que el fabricante de token de verificación solicitante no representa un riesgo adecuado de acuerdo con las tolerancias al riesgo de la entidad/servidor de validación 80, el banco que opera, la red de procesamiento de pagos, el emisor etc., la entidad/servidor de validación 80 puede enviar un mensaje de respuesta que incluye una indicación de que la solicitud de registro se deniega.

En tales modalidades, el mensaje de respuesta que incluye una indicación de denegación también puede incluir una explicación u otra indicación de por qué se denegó la solicitud de registro. Además, la entidad/servidor de validación 80 puede registrar un identificador asociado con el fabricante de token de verificación denegado como un fabricante de token de verificación denegado anterior o actualmente. En tales modalidades, una lista fabricantes de tokens de verificación denegados puede almacenarse en una tabla o en la base de datos 303.Tales listas de los fabricantes de token de verificación denegados también pueden incluir las razones o deficiencias por las que se denegó al fabricante de token de verificación. Si un fabricante de token de verificación denegado presenta una nueva solicitud de validación, la entidad/servidor de validación 80 puede hacer referencia a la lista de los fabricantes de token de verificación denegados además o en sustitución de la aplicación de los protocolos de gestión de riesgos o fraude.

En el caso de que el mensaje de respuesta o de registro incluye una aprobación o validación del fabricante de token de verificación solicitante, el mensaje de respuesta o de registro también puede incluir información adicional respecto al fabricante, los estándares y la programación de los tokens de verificación registrados o validados. Por ejemplo, el mensaje de registro puede incluir un identificador del fabricante de token de verificación, una clave específica de token de verificación, la clave puede incluir un par de claves simétricas, un par de claves asimétricas, la clave o código semilla que debe usarse en la fabricación y configuración de los tokens de verificación. En algunas modalidades, los componentes del par de claves simétricas, el par de claves asimétricas, la clave o el código semilla pueden firmarse por un certificado de autenticación maestro a nombre de la entidad/servidor de validación 80, un banco emisor 60 u otra entidad que opera la entidad/servidor de validación 80. Por ejemplo, el fabricante de token de verificación 305 puede recibir un mensaje de respuesta de registro que indica un identificador específico del fabricante, un par de claves asimétricas de los cuales el componente público se firma por los certificados maestros a nombre de la entidad/servidor de validación 80.El mensaje de respuesta de registro también puede incluir un conjunto, intervalo, o algoritmo de números de serie aprobados que el fabricante de token de verificación puede asignar a los tokens de verificación que fabrica.

En otras modalidades, el mensaje de respuesta o registro puede incluir instrucciones, direcciones, URL u otras direcciones con las que el fabricante de token de verificación solicitante puede acceder u obtener los requisitos y especificaciones para la fabricación de tokens de verificación autorizados. Los requisitos, especificaciones, o

instrucciones pueden ser generales y aplicables a todos los fabricantes de tokens de verificación autorizados, o pueden ser específicos de un fabricante de token de verificación particular. En otras modalidades, los requisitos, las especificaciones y las instrucciones enviadas o de cualquier otra manera proporcionadas a un fabricante de token de verificación autorizado puede ser una combinación de requisitos, especificaciones e instrucciones generales y específicos.

Una vez que un fabricante de token de verificación autorizado recibe un mensaje de respuesta de registro aprobado y accede a los requisitos, especificaciones e instrucciones para producir tokens de verificación, puede comenzar a fabricar tokens de verificación. Por ejemplo el fabricante de token de verificación 305 puede producir tokens de verificación de lector de banda magnética basado en contacto 311 en la acción 5.Similarmente, los fabricantes de tokens de verificación 307 y 309 pueden producir tokens de verificación RFID sin contacto, así como también otros tokens de verificación inalámbricos 313 y 315 de acuerdo con los requisitos, especificaciones e instrucciones específicos proporcionados para cada fabricante de token de verificación individual.

Por ejemplo, puede exigirse a cada fabricante de token de verificación imprimir, grabar, almacenar, o de cualquier otra manera incluir un identificador específico del fabricante en cada token de verificación que produce. Además, cada token de verificación puede incluir un número de serie del que otra información, tal como la información de encriptado, puede derivarse, o determinarse. En algunas modalidades, el número de serie de un token de verificación en particular puede asociarse con un algoritmo criptográfico específico o par de claves. Los fabricantes de token de verificación pueden compartir dicha información con la entidad/servidor de validación 80.En tales modalidades, el token de verificación, como se produce por el fabricante de token de verificación y la entidad/servidor de validación 80 pueden compartir información secreta diversa para producir, determinar, cuestionar y responder uno al otro mediante el uso de la información criptográfica.

Cuando se fabrican los tokens de verificación, los tokens de verificación pueden distribuirse a los usuarios para usar con sus dispositivos portátiles de consumo compatibles, tales como tarjetas de crédito, tarjetas de débito, llaveros, etc.

Una vez distribuido a un usuario, el token de verificación puede requerirse para autenticarse por la entidad/servidor de validación 80 antes de que pueda usarse junto con un dispositivo de consumo portátil o en cualquier tipo de transacción sin validación. El código puede incluirse en el medio legible por computadora 42 para solicitar al usuario o instruir al procesador 11 para usar y autenticar el token de verificación. Las instrucciones, que pueden ser en soporte de papel o electrónico, pueden dirigir al usuario para acoplar el token de verificación al dispositivo de computación del usuario, tal como una computadora portátil o de sobremesa. Una vez que el token de verificación se acopla al dispositivo de computación personal del usuario, el código ejecutable que puede incluirse en un medio legible por computadora 42 en el token de verificación 40 puede ejecutarse por el procesador 11 de la computadora 10.En otras modalidades, el código ejecutable puede incluirse en un medio legible por computadora independiente, tal como una unidad basada en electromagnética, óptica, o flash, entregada junto con el token de verificación. En otras modalidades, el código ejecutable puede descargarse desde la entidad/servidor de validación 80 u otro servidor asociado con la entidad/servidor de validación 80.En algunas modalidades, el sitio de descarga puede proporcionarse por un sitio web alojado en la entidad/servidor de validación 80 u otro servidor asociado con la entidad/servidor de validación 80.

En algunas modalidades, el código ejecutable puede incluir instrucciones para las prestaciones de red 14 de la computadora 10 para conectar con la entidad/servidor de validación 80 sobre una o más redes de comunicación, tal como Internet. En tales modalidades, el código ejecutable puede ejecutarse de forma local en dispositivo de computación del usuario o en un servidor remoto, tal como la entidad/servidor de validación 80 para completar uno o más programas o protocolos de validación iniciales o posteriores. El código ejecutable puede incluir un protocolo de validación completamente automatizado o un protocolo que requiere varias entradas de usuario o la interacción.

Por ejemplo, el código ejecutable puede incluir instrucciones para proporcionar una interfaz de usuario que solicita al usuario que introduzca información específica del usuario o del token de verificación para su presentación a la entidad/servidor de validación 80.En otras modalidades, el token de verificación puede completar una validación automatizada en un segundo plano, sin la necesidad de interacción, interferencia, o entrada del usuario. En cualquiera de tales modalidades, los dispositivos de computación de los usuarios pueden enviar y recibir información o validación de acuerdo con los requisitos de la entidad/servidor de validación 80 para la validación del token de verificación.

La Fig. 4 es un diagrama de flujo de un método de acuerdo con una modalidad de la presente invención para el registro de un fabricante de token de verificación para reducir o eliminar la posibilidad de que un fabricante de token de verificación no autorizado duplique la información de la cuenta de usuario de un dispositivo de consumo portátil sin el conocimiento del usuario. Todos los fabricantes de tokens de verificación autorizados, independientemente de que el token de verificación se integra en un dispositivo informático o de comunicación o se añade como un dispositivo periférico, tal como un dispositivo USB, puede requerirse que se registren a sí mismos como fabricantes con una entidad/servidor de validación 80 que opera dentro o en cooperación con uno o más sistemas de transacción. Esta fase de configuración y proceso de registro puede incluir las acciones descritas anteriormente en referencia a la Fig. 3.

En la acción 410 del método 400 que se muestra en la Fig. 4, la entidad/servidor de validación 80 puede recibir una solicitud de un fabricante de token de verificación para registrarse en la entidad/servidor de validación 80 o el operador

de sistema de transacciones, tal como una red de procesamiento de pagos 70.A continuación, en la acción 420, la entidad/servidor de validación 80 o el operador del sistema de transacción puede realizar una revisión de riesgo de los fabricantes de acuerdo con varios protocolos de riesgo internos y externos. Estas revisiones pueden incluir referencias a ambas bases de datos internas y bases de datos externas o fuentes de datos tales como agencias de informes de crédito, de informes de fraude, y de orden público. Si la revisión de riesgo es satisfactoria para el operador del sistema de transacción o servidor principal, a continuación, un par de claves específicas del fabricante puede asignarse a cada fabricante en la acción 430.En algunas modalidades, el fabricante de token de verificación puede generar la clave específica del fabricante, mientras que en otras modalidades, el operador de la entidad/servidor de validación 80 o el sistema de transacción puede generar la clave específica del fabricante. La clave específica del fabricante puede ser o bien un par de claves simétricas o un par de claves asimétricas.

El operador de la entidad/servidor de validación 80 o el sistema de transacción puede crear la clave maestra del fabricante de token de verificación (KMC) que puede compartirse entre el fabricante y la entidad/servidor de verificación durante el registro en la acción 440.Las claves y los pares de claves descritas en la presente descripción pueden incluir claves simétricas, asimétricas, o de otro tipo de criptografía.

En la acción 450, la entidad/servidor de validación 80 puede firmar uno de los componentes del par de claves del fabricante de token de verificación para proporcionar un nivel adicional de verificación cuando se comunica con el token de verificación. El fabricante de token de verificación puede enviar una parte del par de claves específicas del fabricante, es decir, la mitad pública del par de claves a la entidad/servidor de validación 80 para obtener una clave específica del fabricante o el certificado de clave pública para vincular la clave o clave pública al fabricante de token de verificación. El certificado de clave o clave pública puede incluir información específica del fabricante diversa. Por ejemplo, el certificado de clave pública o clave puede incluir el nombre del fabricante o identificador, dirección, número de teléfono o cualquier otra información que puede usarse para verificar que la clave o clave pública pertenecen al fabricante.

En tales modalidades, la entidad/servidor de verificación 80 o el fabricante de token de verificación 305, 307, o 309 o el token de verificación comparten un secreto. La entidad/servidor de validación 80 puede entonces enviar la clave específica del fabricante de token de verificación, con o sin el componente firmado, al fabricante de token de verificación registrado/aprobado. Opcionalmente, la entidad/servidor de validación 80 puede enviar las especificaciones de fabricación, requisitos o números de serie a los fabricantes de token de verificación registrados de acuerdo con los cuales los fabricantes de token de verificación registrados pueden producir tokens de verificación.

Una vez que se registra un fabricante, puede empezar a crear tokens de verificación. La Fig. 5 es un diagrama de flujo de un método 500 para la fabricación de tokens de verificación de acuerdo con una modalidad de la presente invención. El método 500 puede realizarse por un fabricante de token de verificación que se registra o de cualquier otra manera se aprueba por una entidad/servidor de validación. Para cada token de verificación, el fabricante de token de verificación puede generar o producir un número de serie en la acción 510.En algunas modalidades, los números de serie pueden generarse o de cualquier otra manera seleccionar de un conjunto de números de serie asignados al fabricante de token de verificación. En tales modalidades, el conjunto de números de serie puede representarse por un conjunto finito de números, un algoritmo para la producción de números de serie al azar o casi al azar u otra metodología para la producción de números de serie que pueden o no, estar asociados con el fabricante de token de verificación. En modalidades en las que el conjunto de números de serie se asocian con el fabricante de token de verificación, la entidad/servidor de validación 80 puede usar el número de serie del token de verificación para determinar el fabricante de token de verificación y/o la información específica del token de verificación, tal como el par de claves específicas de token de verificación o la clave maestra del fabricante de token de verificación (KMC) o certificado que puede usarse para cifrar o descifrar la información enviada entre el fabricante de token de verificación y el token de verificación.

Algunas modalidades pueden usar un requisito de certificado estándar PKCS, el certificado/firma puede incluir (1) un número de serie de token de verificación y (2) un nombre de fabricante o identificador. Además, el fabricante puede derivar una clave con base en el KMC y el número de serie del token de verificación y estos pueden almacenarse en el medio legible por computadora 42 en el token de verificación. Los tokens de verificación pueden enviarse y distribuirse.

En la acción 520, el fabricante de token de verificación puede generar un par de claves para cada token de verificación, sus fabricantes o emisores. El par de claves puede incluir un componente público y uno privado. El par de claves puede ser un par de claves simétricas o asimétricas. El par de claves puede ser el token de verificación específico y único para el fabricante de token de verificación que hizo el token de verificación. En otras modalidades, el par de claves para un token de verificación en particular puede ser único en todos los tokens de verificación, independientemente del fabricante de token de verificación que hizo el token de verificación.

Para obtener un nivel adicional de seguridad, cada componente del par de claves del token de verificación escrita o almacenada en el token de verificación puede firmarse por un certificado CA o maestro o una clave privada en la acción 530 para crear el certificado público del token de verificación. Específicamente, la clave pública del token de verificación puede firmarse por la clave privada del fabricante de token de verificación. En tales modalidades, el certificado público del token de verificación puede incluir el número de serie del token de verificación u otro identificador.

En algunas modalidades, la clave raíz de CA o maestra se asocia con el fabricante de token de verificación, mientras

que en otras modalidades, la clave raíz de CA o maestra puede asociarse con una entidad/servidor de validación. En tales modalidades, la componte pública firmada de la clave raíz de CA o maestra del par de claves del token de verificación puede verificarse y/o desencriptarse por una entidad/servidor de validación.

Una vez que el par de claves, número de serie y/o el certificado de clave pública se generan para el token de verificación, todos o algunos componentes del par de claves, número de serie y/o el certificado público pueden almacenarse o escribirse en una memoria en el token de verificación en la acción 540.Similarmente, el certificado público del token de verificación y/o la clave pública del fabricante también pueden almacenarse en el token de verificación. En algunas modalidades, sólo un componente del par de claves se almacena o se escribe en el token de verificación. En tales modalidades, es ventajoso para escribir y/o almacenar el componente público o el componente público firmado del par de claves en el token de verificación, mientras se mantiene secreto el componente privado. El almacenamiento de los componentes del par de claves, u otra información, en el token de verificación puede incluir almacenar información en una memoria o memoria protegida.

Una vez que se genera el par de claves y se escribe o se almacena en el token de verificación, los componentes privados del par de claves pueden compartirse entre el fabricante de token de verificación, la entidad/servidor de validación u otra entidad de confianza. En algunas modalidades, la información compartida puede incluir una asociación del par de claves al número de serie, el fabricante de verificación o un identificador del fabricante de token de verificación.

Opcionalmente, el número de serie y un identificador del fabricante pueden almacenarse/ escribirse en la memoria en el token de verificación en la acción 550.Por último, en la acción 560, el fabricante de token de verificación puede también escribir/almacenar software de validación ejecutable y/o una dirección web para un servidor de validación de autenticación en la memoria o la memoria protegida del token de verificación. El código de software ejecutable puede incluir instrucciones para dirigir un procesador en una computadora en la que el token de verificación puede conectarse para iniciar cada sesión de comunicación sobre un medio de comunicación a través de las prestaciones de comunicación de la computadora para validar el token de verificación.

Cada vez que un usuario elige, pero sobre todo en la recepción de un nuevo token de verificación, él o ella pueden iniciar uno o más procesos para registrar y/o validar el token de verificación. La Fig. 6 es un esquema de un sistema 600 que puede usarse para validar y/o autenticar un token de verificación 40.Antes de que el dispositivo de consumo portátil 5 se presenta al token de verificación 40 para iniciar una transacción, el usuario puede obligarse, o elegir primero validar y/o autenticar el token de verificación 40 en la entidad/servidor de validación 80.

En algunas modalidades, para validar el token de verificación 40 el usuario puede (1) iniciar sesión en un sitio web operado por la entidad/servidor de validación 80; (2) usar HTTPS u otro protocolo de seguridad, el sitio web puede indicar al usuario que introduzca el token de verificación si el usuario no lo ha hecho ya; (3) el sitio web puede solicitar y validar la certificación del token de verificación o el par de claves/componentes del par de claves mediante el uso de las claves del fabricante; (4) a continuación, el sitio web puede generar un número aleatorio y solicitar el token de verificación para firmar este número; (5) el sitio web puede validar la firma y mostrar un mensaje al usuario de que el token de verificación es válido; y (6) el sitio web también puede mostrar el número de serie del token de verificación que puede grabarse en el propio token de verificación.

En otras modalidades, el usuario puede instruirse para ir a un sitio web de validación. La sugerencia puede venir en forma de una carta, un correo electrónico, un SMS o mediante un código ejecutable o archivo estático almacenado en el token de verificación. La instrucción puede o no incluir un hiperenlace a la web. Es ventajoso que la instrucción no incluya un hiperenlace o URL y simplemente un mensaje que indica al usuario iniciar sesión en un sitio web de confianza en el que el usuario ya puede tener una cuenta registrada. Este aspecto manual de navegar a la página web de validación ayuda a evitar que los estafadores o los fabricantes de tokens de verificación fraudulentos dirijan a los usuarios a una página web falsa o fraudulenta y engañen a los usuarios para "validar" el token de verificación fraudulento con el sitio web falso para duplicar la información confidencial del usuario. Mientras se visualiza el sitio web de validación, puede solicitarse al usuario que introduzca un número aleatorio o semialeatorio. El número aleatorio puede generarse por el servidor de validación, el sitio web, la computadora del usuario, el token de verificación o simplemente ser un número de elección del usuario.
El número aleatorio puede enviarse al lector de token de verificación y firmarse por una de las claves de token de verificación, es decir, la clave privada. Entonces, el lector puede devolver el número firmado, el certificado público del lector y el certificado de clave pública del fabricante a la entidad/servidor de 80.La entidad/servidor de validación 80 puede validar a continuación, el certificado de clave pública del fabricante mediante el uso de la clave maestra o raíz de la entidad/servidor de validación 80.La entidad/servidor de validación 80 también puede extraer y validar la clave pública del lector mediante el uso de la clave pública del fabricante. La entidad/servidor de validación 80 puede entonces validar el número de serie y el nombre o el identificador del fabricante contra el registro de los fabricantes de tokens de verificación autenticados o registrados. Finalmente, la entidad/servidor de validación 80 puede validar el número aleatorio firmado mediante el uso de la clave pública del token de verificación.

En otra modalidad, el usuario puede conectar el token de verificación 40 a la computadora 10 a través de una interfaz periférica. Una vez conectado a la computadora 10, el token de verificación 40 automáticamente o incitado por el

usuario puede iniciar uno o más segmentos de código ejecutable mediante el uso del procesador de la computadora 10 o un procesador incorporado en el token de verificación 40.En cualquiera de tales modalidades, la computadora 10 puede enviar una solicitud de validación a la entidad/servidor de validación 80 mediante el uso de sus prestaciones de comunicaciones sobre un medio de comunicación, tal como Internet, en la acción 1.La solicitud de validación puede incluir información pública y secreta diversa respecto al token de verificación 40.Por ejemplo, la solicitud de validación puede incluir el componente público del par de claves específicas del token de verificación 40, el número de serie del token de verificación 40, un número aleatorio generado y/o firmado por el token de verificación 40 la computadora 10 o una consulta de cuestionamiento.

La entidad/servidor de validación 80 puede recibir la solicitud de validación de la computadora 10 en la acción 2.La entidad/servidor de validación 80 puede recibir la solicitud de validación a través de cualquier medio de comunicación adecuado que conecta la computadora 10 a la entidad/servidor de validación 80.En algunas modalidades, la entidad/servidor de validación 80 puede analizar varias piezas de información a partir de la solicitud de validación. Por ejemplo, la entidad/servidor de validación 80 puede analizar el componente público del par de claves específicas del token de verificación 40, el número de serie del token de verificación 40, un número aleatorio generado y/o firmado por el token de verificación 40 o la computadora 10 o una consulta de cuestionamiento. Con base en la información analizada a partir de la solicitud de validación, la entidad/servidor de validación 80 puede recuperar o de cualquier otra manera producir la información asociada con el token de verificación 40.

Por ejemplo, la entidad/servidor de validación 80 puede usar el número de serie del token de validación 40 para producir, determinar y/o recuperar un componente privado de un par de claves asociadas con el token de verificación 40.En otras modalidades, la entidad/servidor de validación 80 puede usar un identificador de fabricante analizado a partir de la solicitud de validación para determinar si el número de serie en la solicitud de validación es consistente con los números de serie asignados y/o producidos por ese fabricante de token de verificación. La entidad/servidor de validación 80 puede usar cualquier y toda la información analizada a partir de la solicitud de validación para recuperar toda la información asociada a un token de verificación particular 40, el fabricante del token de verificación o un usuario asociado con el token de verificación 40.

En algunas modalidades, la entidad/servidor de validación 80 puede analizar un identificador de token de verificación o el número de serie para el token de verificación 40 a partir de la solicitud de validación en la acción 2.La entidad/servidor de validación 80 puede comprobar si el identificador de token de verificación o el número de serie analizado se valida previamente en la acción 3.En algunas modalidades, si el identificador de token de verificación o número de serie analizado se valida previamente, la entidad/servidor de validación 80 puede devolver un mensaje de validación a la computadora 10 en la acción 4, en cuyo punto, el usuario puede presentar un dispositivo de consumo portátil 5 a un token de verificación 40 para iniciar una transacción. En otras modalidades, la entidad/servidor de validación 80 puede, junto con el mensaje de validación, enviar la instrucción de actualización de información del token de verificación.

En algunas modalidades, la instrucción de actualización de información del token de verificación puede incluir el código legible por computadora para instruir al procesador de computadora 10 para volver a escribir una parte o toda la información almacenada en el token de verificación 40.Por ejemplo, uno o más componentes de la pareja de claves asociadas con el token de verificación 40 pueden reemplazarse con los nuevos componentes de un par de claves recién asociados con el token de verificación 40.Las actualizaciones de la información del token de verificación almacenada en el token de verificación 40 puede permitirse o limitarse solamente a la entidad/servidor de validación 80 cuando pueda establecer una sesión de comunicación de sesión de clave segura.

En algunas modalidades, en la acción 3, la entidad/servidor de validación 80 puede realizar una autenticación mutua y establecer una sesión de clave con la computadora 10.La clave de sesión entre la computadora 10 y la entidad/servidor de validación 80 puede establecerse por la entidad/servidor de validación 80 al generar un número aleatorio u otro mensaje de cuestionamiento, firmar ese número al azar o mensaje de cuestionamiento con el componente del par de claves asociado con el token de verificación 40 y enviar la información firmada de vuelta al token de verificación 40.El token de verificación 40 puede descifrar la información firmada y enviar de vuelta la respuesta correcta de acuerdo con la desencriptación mediante el uso del componente del par de claves almacenado en el token de verificación 40.
En algunas modalidades, el componente del par de claves almacenado en el token de verificación 40 se firma por una clave raíz de CA o maestra asociada con el fabricante de token de verificación o la entidad/servidor de validación 80. En tales modalidades, la respuesta desencriptada recibida del token de verificación 40 debe entonces desencriptarse mediante el uso de la clave raíz de CA o maestra para autenticar aún más la autenticidad del token de verificación 40. En cualquiera de estas modalidades, la entidad/servidor de validación 80 puede recibir la respuesta del token de verificación 40.Con base en la respuesta recibida del token de verificación 40, la entidad/servidor de validación 80 puede determinar si el token de verificación 40 es auténtico, válido o de cualquier otra manera producido por un fabricante de token de verificación de confianza que experimenta y recibe la autorización para producir tokens de verificación. Si se determina que el token de verificación 40 es válido, entonces puede usarse con el dispositivo portátil de consumo 5 para iniciar las transacciones. Un mensaje a este efecto puede enviarse a la computadora 10 desde la entidad/servidor de validación 80 para además activar el token de verificación 40 o instruir la computadora 10 para usar posteriormente el token de verificación 40 para iniciar una transacción, en la acción 4.

En los eventos que el token de verificación 40 se determina que es fraudulento o de cualquier otra manera inválido, ese

token de verificación, o cualquier información asociada a este, tales como el número de serie o identificación del token de verificación, puede enumerarse como un token de verificación potencialmente fraudulento y se bloquea para su uso para las transacciones.

En el caso de que el token de verificación 40 no se ha validado previamente por la entidad/servidor de validación 80, la entidad/servidor de validación 80 puede almacenar el número de serie o identificador del token de verificación recién validado en una base de datos 603 para su posterior recuperación y confirmación de la validación previa del token de verificación 40 en la acción 5.En algunas modalidades, la entidad/servidor de validación 80 puede informar a la entidad bancaria emisora 60 que el token de verificación 40 se ha validado exitosamente por la entidad/servidor de validación 80 para iniciar transacciones mediante el uso del dispositivo portátil de consumo 5 en la acción 6.Alternativamente, el banco emisor 60 puede informarse de que un token de verificación portátil potencialmente fraudulento intenta validarse.

Los métodos, sistemas y servidores de acuerdo con diversas modalidades de la presente invención incluyen ventajas sobre los medios existentes para disuadir o detener los estafadores de introducir tokens de verificación fraudulentos en el flujo comercial para duplicar la información sensible del usuario. Diversas modalidades de la presente invención incluyen los esquemas de validación de múltiples capas o de múltiples partes para impedir a los estafadores producir y validar tokens de verificación fraudulentos que podrían engañar a una entidad/servidor de validación, lo que reduce así, aún más, la posibilidad de duplicar la información del usuario. Por ejemplo, el certificado público del fabricante producido por la entidad/servidor de validación y almacenado en el token de verificación puede ayudar a asegurarse mejor de que la entidad/servidor de validación tiene una interacción de autenticación previa con el fabricante del token de verificación en particular. Entonces solamente la entidad/servidor de validación que tiene acceso a la clave raíz de CA o maestra específica del fabricante o el certificado raíz de CA puede recuperar, desencriptar o de cualquier otra manera extraer la clave pública del token de verificación del certificado público del token de verificación mediante el uso de la clave pública del fabricante recuperada/generada con base en la validación del certificado de clave pública del fabricante.

El certificado de clave pública del fabricante, o los medios para generar uno, es decir, la clave raíz de CA o maestra o el certificado de la entidad/servidor de validación, no estaría disponible para un fabricante de token de verificación no autenticado, y así, tal fabricante fraudulento no podría generar un certificado que podría usarse para generar/validar un certificado público de token de verificación auténtico o la clave pública de token de verificación que coincidiría con la clave privada almacenada en el token de verificación. Sin tal información, un usuario que visita un sitio web de confianza para validar un token de verificación no podría ser engañado en la validación de un token de verificación fraudulento, o de cualquier otra manera no auténtico. Estas características aumentan en gran medida la seguridad de los tokens de verificación usados para realizar transacciones financieras y de otro tipo mediante el uso de dispositivos portátiles de consumo, es decir, las tarjetas de crédito y de débito, iniciadas desde un terminal de usuario en un lugar separado de un establecimiento comercial u otra entidad que de cualquier otra manera podrían verificar la autenticidad del dispositivo de consumo portátil o usuario. Estas características pueden además mejorarse al requerir que el usuario manualmente o de cualquier otra manera navegue independientemente a un sitio web para iniciar el proceso de validación a fin de reducir la posibilidad de que un token de verificación fraudulento navegue automáticamente a un sitio web de validación fraudulento.

La Fig. 7 es un diagrama de flujo de un método 700 para realizar un primer uso o registro de un token de verificación. Durante el proceso descrito anteriormente, la entidad/servidor de validación puede comprobar si el token de verificación se valida previamente. Si el número de serie no está en una base de datos de tokens de verificación previamente validados, el siguiente procedimiento puede realizarse antes de usarlo por primera vez.

En la acción 710 la entidad/servidor de validación puede obtener la clave del token de verificación mediante el número de serie y la clave raíz de CA o maestra registrada en la entidad/servidor de validación para ese fabricante de token de verificación. En la acción 720, la entidad/servidor de validación puede realizar una autenticación mutua y establecer una clave de sesión mediante el uso ya sea de una clave de token de verificación derivada o un procedimiento estándar con base en Global Platform SCPOI o 02 o el estándar de personalización de tarjetas EMVCO.A continuación, en la acción 730, si la autenticación mutua es exitosa, entonces el token de verificación puede permitir el acceso de lectura, escritura y actualización.

En la acción 740, bajo la clave de sesión, la entidad/servidor de validación puede reemplazar el componente clave existente almacenado en el token de verificación con un nuevo componente clave derivado mediante el uso del número de serie del token de verificación y una clave maestra (MDK).Cualquier otro dato necesario puede escribirse en este punto y el usuario puede registrarse opcionalmente en este momento. En la acción 750, el token de verificación puede permitir el acceso de escritura/actualización si tiene lugar la autenticación mutua con el nuevo componente clave. Por último, en la acción 760, la entidad/servidor de validación puede registrar el número de serie del token de verificación en la base de datos de token de verificación.

La respuesta a una solicitud de validación inicial o primera puede ser una primera prueba de validación o registro para validar el token de verificación 40.Para iniciar la validación o solicitud de registro, el token de verificación 40 puede enviar su número de serie a la entidad/servidor de validación 80, junto con un mensaje o a solicitud de validación encriptada por una clave, con el mensaje y la clave que son un secreto compartido entre el token de verificación 40 y la entidad/servidor de validación 80 (es decir, no se conoce públicamente).En algunas modalidades, la clave puede

asociarse únicamente con el número de serie del token. La clave puede ser una clave de encriptación simétrica que incluye una o un par de claves asimétricas.

La entidad/servidor de validación 80 puede tener o tener acceso a una base de datos de números de serie y las claves asociadas correspondientes o algoritmos almacenados para generar las claves, y puede validar que el token de verificación 40 envía el mensaje correcto para el número de serie. Para ello, el token de verificación 40 puede comprender un número de serie y la clave única integrada en un medio legible por computadora o memoria, la clave única que es única para el token de verificación 40, y el código que dirige al procesador de datos 41 para enviar el número de serie y un mensaje encriptado por la clave única a la entidad/servidor de validación 80.

El mensaje puede almacenarse previamente en el medio legible por computadora, o derivable/determinable a partir de la información conocida tanto por el token de verificación 40 como por la entidad/servidor de validación 80, tal como un mensaje derivado a partir de un algoritmo aplicado a la fecha actual, el número de serie del token 40, y/o la clave de sesión de la sesión de comunicación entre el token 40 y la entidad/servidor de validación 80.De esta manera, el mensaje enviado por el token 40 a la entidad/servidor de validación 80 es verificable por la entidad/servidor de validación 80 mediante el uso de la información almacenada en la entidad de validación. El medio legible por computadora o memoria para las tareas anteriores pueden situarse en el medio legible por computadora 42 y/o el módulo de seguridad 43.Los códigos anteriores pueden incluir instrucciones de E/S en el módulo de seguridad 43, y las llamadas de función a la API del módulo de servicios de red de la computadora.

Opcionalmente, el token de verificación 40 puede enviar, de manera ocasional, una o más piezas de información única de máquina de la computadora 10 a la entidad/servidor de validación 80, que puede comprobar esta información contra una base de datos de información de computadora asociada con los estafadores conocidos. Dicha información única de máquina puede incluir los números de serie de los procesadores, las unidades de disco y los sistemas operativos de la computadora 10.El token de verificación 40 puede comprender código que dirige al procesador de datos 41 para obtener una o más piezas de información única de máquina de la computadora 10, y enviar la información específica de máquina a la entidad/servidor de validación 80.Este código puede incluir llamadas de función a la API del sistema operativo del equipo para obtener la información, y la llamada de función a la API del módulo de servicios de red de la computadora para enviar la información a la entidad/servidor de validación 80.

Como otra opción, el token de verificación 40 puede configurarse para solicitar al usuario 1 una contraseña para activar una o más características del token 40.La contraseña puede almacenarse en un medio legible por computadora situado en el módulo de seguridad 43 o en un medio legible por computadora 42.La contraseña puede proporcionarse al usuario 1 en un pedazo de papel por el fabricante del token de verificación, proveedor o vendedor del token 40. El token 40 puede enviarse al usuario 1 a través del correo, por o en nombre de un banco emisor, o puede comprarse por el usuario 1 en una tienda. El token 40 puede configurarse para requerir que se escriba la contraseña cada vez que el usuario desea presentar un dispositivo de consumo portátil 5, y/o cada vez que el token 40 se acopla a un computadora 10.Para ello, el token de verificación 40 puede comprender, además, código incorporado en el medio legible por computadora 42 que dirige al procesador de datos 41 para solicitar al usuario que introduzca una contraseña en un teclado de computadora 10, leer una contraseña introducida por el usuario, y comparar la contraseña introducida con una contraseña almacenada incorporada en el medio legible por computadora. Este código puede comprender las llamadas de función de la API a la interfaz gráfica de usuario del sistema operativo de la computadora 10 para abrir un cuadro de visualización en la interfaz de usuario 13 para solicitar y recibir una contraseña del usuario 1, las instrucciones de E/S, las instrucciones de acceso a memoria, y las instrucciones lógicas y de control de la CPU. El token de verificación 40 puede comprender además uno o más de los siguientes:

(1) el código incorporado en un medio legible por computadora 42 que dirige al procesador de datos 41 para iniciar y/o permitir la comunicaciones descritas anteriormente con la computadora 10 en respuesta a una contraseña introducida que coincide con la contraseña almacenada;
(2) el código incorporado en un medio legible por computadora 42 que dirige al procesador de datos 41 para iniciar y/o permitir las comunicaciones descritas anteriormente con la entidad/servidor de validación 80 en respuesta a una contraseña introducida que coincide con la contraseña almacenada;

(3) el código incorporado en un medio legible por computadora 42 que dirige al procesador de datos 41 para activar el lector 44 y/o para aceptar la información de identificación del lector 44 en respuesta a una contraseña introducida que coincide con la contraseña almacenada; y

(4) el código incorporado en un medio legible por computadora 42 que dirige al procesador de datos 41 para iniciar y/o permitir la transmisión descrita anteriormente de la información de identificación a la entidad/servidor de validación 80 en respuesta a la contraseña introducida que coincide con la contraseña almacenada.

Estos códigos pueden incluir instrucciones de E/S, instrucciones de acceso a memoria, y las instrucciones lógicas y de control de la CPU. Las instrucciones, solas o en combinación, evitan la transmisión de la información de identificación a la entidad/servidor de validación 80 cuando la contraseña introducida no es la misma que la contraseña almacenada, y de esta manera comprenden código incorporado en el medio legible por computadora que dirige al procesador de datos para hacerlo. Un experto en la técnica será capaz de construir las instrucciones y las llamadas de función de la API para

implementar los códigos descritos anteriormente en vista de esta descripción sin experimentación excesiva. Como protección adicional, el token de verificación 40 puede comprender además el código integrado en el medio legible por computadora 42 que dirige al procesador de datos 41 para establecer un nombre de usuario para el token mediante la presentación al usuario 1 de un cuadro de diálogo para recibir la entrada que designa un nombre de usuario, y mediante el almacenamiento del nombre de usuario en el medio legible por computadora 42.

Los códigos anteriores para el procesamiento de la contraseña pueden aumentarse aún más para incluir solicitar un nombre de usuario para el token y comparar el nombre de usuario recibido con el nombre de usuario almacenado para una coincidencia, y que incluye una coincidencia como una condición que debe cumplirse en cada uno de los cuatro códigos anteriores que inician o permiten que se realicen diversas acciones. Estos códigos pueden incluir instrucciones de E/S, instrucciones de acceso a memoria, y instrucciones lógicas y de control de la CPU.

En cada una de las modalidades descritas en la presente descripción relativo al token de verificación 40, el token de verificación 40 puede enviar la información de identificación correspondiente al dispositivo de consumo portátil 5 de la computadora 10 en un número de formas, que incluyen:(1) la forma inalterada ("forma clara"), (2) la forma encriptada, (3) formada con HASH (por ejemplo, codificada), (4) la forma firmada, (5) o cualquier combinación de estas formas. Estas formas pueden generarse por el dispositivo portátil de consumo 5, el token de verificación 40, la computadora 10, o cualquier combinación de los mismos. Además, el token de verificación 40 y la entidad/servidor de validación 80 pueden realizar un proceso de autenticación mutua antes de que el token de verificación 40 envíe la información de identificación.

En cada una de las modalidades descritas en la presente descripción relativas al token de verificación 40, los códigos anteriores del token 40 y la información de identificación leídos del dispositivo 5 por el token 40 pueden almacenarse independientemente de la computadora 10 y pueden protegerse de programas (como software espía y otros programas maliciosos) que se ejecutan en la computadora 10.En tales implementaciones, la información de identificación se pone en forma segura (por ejemplo, encriptada, con HASH, firmada, o combinación de las mismas) mediante el token de verificación 40 antes de que la información se proporcione a la computadora 10.

En consecuencia, proteger la información no depende de la seguridad de la computadora 10.Las claves simétricas o asimétricas pueden usarse para el encriptado y firma. Las claves para un token de verificación 40 pueden ser únicas con respecto a otros tokens de verificación (es decir, las claves para un token pueden ser únicas para ese token). Las claves para un token, y particularmente las claves simétricas, pueden basarse en un número de serie asignado únicamente para el token de verificación, que el token puede comunicar a la entidad/servidor de validación 80 en una comunicación inicial. Tanto el token de verificación como la entidad/servidor de validación pueden tener un secreto compartido sobre la manera de obtener una clave a partir del número de serie del token, tal como mediante la manipulación y/o el reemplazo de dígitos seleccionados del número de serie. Un número de claves puede derivarse del número de serie único mediante el uso de los respectivos secretos compartidos. Así, los mensajes de cuestionamiento y respuesta usados en un proceso de autenticación mutua entre un token de verificación y una entidad/servidor de validación pueden firmarse mediante el uso de las claves derivadas respectivas del número de serie del token de verificación.

La Fig. 8 es un esquema de un sistema para la actualización de la información almacenada en un medio legible por computadora o la memoria en el token de verificación 40. En la acción 1, token de verificación 40 puede conectarse a la computadora 10 a través de un usuario. Una vez que el token de verificación 40 se conecta a la computadora 10, a través de una interfaz periférica u otra interfaz de comunicación, el token de verificación 40 puede establecer un enlace de comunicaciones con la computadora 10.En algunas modalidades, la interfaz periférica puede incluir una interfaz USB o FireWire™, así como también cualquier otra interfaz de bus periférica o interna adecuada para el establecimiento de la comunicación y la transferencia de información entre el token de verificación 40 y la computadora 10.
Mediante el uso del enlace de comunicación entre el token de verificación 40 y la computadora 10, el token de verificación 40, o el procesador incluido ahí, puede instruir a la computadora 10 para establecer una sesión de comunicación entre el token de verificación y una entidad/servidor de validación mediante el uso de la interfaz de red de la computadora en la acción 920.En tales modalidades, la interfaz/instalación de red de la computadora 10 puede conectarse a través del medio de comunicación tal como una red informática privada o la Internet. En tales modalidades, el token de verificación 40 puede comprender el código ejecutable que incluye instrucciones para el procesador del token de verificación 40 o el procesador de la computadora 10 para establecer la comunicación mediante el uso de la interfaz de red de la computadora 10.En algunas modalidades, el código puede incluir una URL u otra dirección para ponerse en contacto con un sitio web u otro servicio operado por la entidad/servidor de validación 80.

Una vez que se establece el enlace de comunicación entre el token de verificación 40 y la entidad/servidor de validación 80, la computadora 10 puede descargar el código ejecutable desde la entidad/servidor de validación 80 que incluye instrucciones para proporcionar a un usuario diversas indicaciones que aparecen en la pantalla de la computadora 10 en la acción 930.El código ejecutable puede incluir HTML u otro código universalmente ejecutable en una computadora mediante el uso de un navegador web u otra aplicación de comunicación basada en la web. Las instrucciones para el usuario pueden incluir instrucciones para el usuario para iniciar, continuar o concluir una solicitud de validación del token de verificación 40.Ejemplo, la computadora 10 puede pedir al usuario que introduzca el número de serie del token de verificación 40 impreso en el exterior del token de verificación 40.En algunas modalidades, el número de serie impreso,

grabado o estampado en el token de verificación 40 es el mismo que un número de serie almacenado en el medio legible por computadora o la memoria en el token de verificación 40.En otras modalidades, el número de serie impreso, grabado o estampado en el token de verificación 40 es diferente o una variación de un número de serie almacenado en el medio legible por computadora o la memoria en el token de verificación 40.

Si el usuario entra la entrada apropiada para la(s) solicitud(es) y la entrada, o una versión cifrada de la entrada, coincide con la información almacenada en el token de verificación 40 y/o la entidad/servidor de validación 80, a continuación, una clave de sesión puede establecerse entre el token de verificación 40 y la entidad/servidor de validación 80.En algunas modalidades, la entrada en respuesta al pedido puede incluir una contraseña conocida sólo por el(los) usuario(s) autorizado(s) y la entidad/servidor de validación 80, mientras que en otras modalidades, la entrada en respuesta al pedido puede incluir algunos o todos los número de serie leídos desde el exterior o en la memoria del token de verificación 40.Una vez establecida la clave de sesión, la entidad/servidor de validación 80 puede iniciar el reemplazo de la clave existente u original derivada del número de serie del token de verificación y/o la clave maestra de la entidad/servidor de validación o el certificado en la acción 940.Si, bajo la sesión de clave, el token de verificación 40 y la entidad/servidor de validación 80 pueden realizar una autenticación mutua, entonces el token de verificación puede permitir a la entidad/servidor de validación 80 reemplazar la clave original con una nueva clave en la acción 950.En algunas modalidades, puede solicitarse al usuario que permita o deniegue el reemplazo de la clave existente en el token de verificación 40 con la nueva clave de la entidad/servidor de validación 80.Por último, la entidad/servidor de validación 80 puede registrar el número de serie del token de verificación 40 con la base de datos del token de verificación para la referencia futura y el token de verificación 40 enviar otra solicitud de validación de vez en cuando en la etapa 960.La base de datos del token de verificación puede incluir asociaciones entre el número de serie original, la clave original, y cada iteración o clave de reemplazo se asocia o se ha asociado al token de verificación 40.

La Fig. 10 es un diagrama de flujo de un método 1000 de un método para usar una entidad/servidor de validación 80 para validar un token de verificación 40 de acuerdo con diversas modalidades de la presente invención. El método 1000 comienza en la acción 1010, en la que la entidad/servidor de validación 80 establece un enlace de comunicación con un token de verificación mediante el uso de una instalación de red de la entidad/servidor de validación 80.En algunas modalidades, se establece el enlace de comunicación entre las entidades/servidores de validación 80 y la computadora 10 a la que se conecta el token de verificación 40.En otras modalidades, el token de verificación 40 y la entidad/servidor de validación 80 se conectan directamente a través de una conexión física o una conexión inalámbrica, tal como WiFi™, Bluetooth™, GSM, CDMA, 3G, 4G, u otros datos inalámbricos o protocolo de comunicación. En el enlace de comunicación establecido, la entidad/servidor de validación 80 puede recibir una información de identificación encriptada y/o la información del token de verificación enviada por un token de verificación 40 en la acción 1020.Como se describió anteriormente, la información de identificación encriptada o sin encriptar y/o la información del token de verificación puede incluir un número de serie, mensaje de autenticación, un identificador de fabricante de token de verificación y cualquier otra información que puede usarse por la entidad/servidor de validación 80 para realizar una autenticación mutua con el token de verificación 40.

En la acción 1030, la entidad/servidor de validación 80 puede analizar o desencriptar la información de identificación recibida y/o la información del token de verificación. Para analizar la información recibida, la entidad/servidor de validación 80 puede usar la información asociada al token de verificación del que se recibió la información. En algunas modalidades, la información asociada al token de verificación incluye una clave de delimitación que indica a la entidad/servidor de validación cómo analizar la información recibida en segmentos de datos constitutivos. Por ejemplo, la información asociada puede incluir una lista de segmentos de datos constitutivos, delimitadores, y la forma de los datos, es decir, una tabla de cadenas delimitado con coma. En otras modalidades, la información asociada al token de verificación puede incluir una clave simétrica o asimétrica correspondiente que se empareja con la clave asimétrica almacenada o enviada desde el token de verificación. La información asociada puede incluir también una clave maestra específica del fabricante que se usó para firmar el componente de clave almacenado en el token de verificación. La clave maestra puede usarse, en combinación con el componente clave correspondiente asociado con el token de verificación que no se almacena en el token de verificación, para descifrar la información firmada por el componente clave almacenado en el token de verificación.

La entidad/servidor de validación puede aplicar al menos una de las pruebas de validación descritas anteriormente para la información desencriptada en la etapa 1040.Con base en los resultados de la prueba o pruebas de validación, la entidad/servidor de validación puede comprobar el valor/mensaje para el token de verificación. Si se pasan las pruebas o de cualquier otra manera se consideran satisfactorias, entonces el valor/mensaje de verificación puede indicar al token de verificación que la entidad/servidor de validación es de confianza y debe permitirse el acceso de lectura, escritura o reemplazo de la información almacenada en el token de verificación. En otras modalidades, el valor/mensaje de verificación puede incluir información que puede usarse para añadir, modificar o reemplazar la información almacenada en el token de verificación. En diversas modalidades, un procesador incluido en el token de verificación o la computadora a la que se conecta puede iniciar la lectura, escritura o el reemplazo de la información almacenada en el token de verificación. En tales modalidades, la información puede incluir un reemplazo o un nuevo componente clave que se puede usar para futuras transacciones y la solicitud de validación enviada mediante el uso del token de verificación. En las modalidades correspondientes, el reemplazo o nuevo componente clave y el nuevo componente clave correspondiente, es decir, los pares de claves simétricas o asimétricas, pueden almacenarse para futuras referencias en las solicitudes de validación o de transacción.

Al tener diversas modalidades e implementaciones de token de verificación 40 descritas, se describen ahora diversas modalidades e implementaciones de la entidad/servidor de validación. La entidad/servidor de validación 80 comprende un sistema que tiene uno o más servidores acoplados a una red de comunicaciones que puede recibir una solicitud de un token de verificación 40 para procesar (*por ejemplo*, para validar) la información del token de verificación y la información que el token lee a partir de un dispositivo portátil 5, y para proporcionar un valor de verificación del dispositivo (dCVV2) al token y a la red de procesamiento de pagos 70 si la información de identificación pasa una o más pruebas de validación.

Un servidor ilustrativo de la entidad/servidor de validación 80 se muestra en la Fig. 1. El servidor comprende uno o más procesadores 81 acoplado a cada uno de un medio tangible legible por computadora 82, una interfaz de usuario 83, una o más bases de datos 86, y una instalación de red 84, el último de los cuales se acopla a las primera y segunda redes de comunicaciones 31 y 32. La interfaz de usuario 83 comprende uno o más dispositivos de salida de vídeo (por *ejemplo*, pantallas, visualizadores) y uno o más dispositivos de entrada (*por ejemplo*, teclado, ratón, ratón de bola, etc.), que permiten a un administrador de la entidad/servidor de validación 80 recibir información del servidor y para proporcionar entrada al servidor. El medio legible por computadora 82 puede comprender una combinación de memoria de semiconductores y de almacenamiento no volátil, tal como una o más unidades de disco y/o la memoria no volátil.

El medio legible por computadora 82 almacena un sistema operativo para el servidor, que permite que los procesos y aplicaciones se ejecuten por el(los) procesador(es) 81, y permite que se ejecuten los códigos para dirigir el funcionamiento del(los) procesador(es) 81.El sistema operativo proporciona servicios a estos procesos y aplicaciones, y permite que estos procesos y aplicaciones accedan a los componentes de interfaz de usuario 83, las porciones del medio legible por computadora 82, las prestaciones de red 84, y otros componentes de la entidad/servidor de validación 80.

El sistema operativo puede ser completo. Específicamente, el sistema operativo proporciona uno o más módulos de comunicaciones de E/S que permiten que el(los) procesador(es) 81 se comuniquen con la interfaz de usuario 83 y las bases de datos 86.Cada módulo de comunicaciones de E/S tiene una interfaz de programación de aplicaciones (API) con un conjunto de funciones que un procesador 81 puede llamar con el fin de acceder a los componentes. El sistema operativo de la entidad/servidor de validación 80 también puede comprender uno o más módulos de servicios de red que pueden acceder a la instalación de red 84 y establecer las sesiones de comunicación a las entidades en las redes de comunicación 31 y 32, y con el servidor de transmisión de SMS 35.

Tales módulos de servicios de red incluyen la Fundación de Microsoft's Windows Communications Foundation (*por ejemplo*, .NET 3.0, .NET 4.0, etc.), Apple's CFNetwork Framework, la sección de conexión en red de los núcleos del sistema operativo Unix y Linux, y la capa de servicios del sistema operativo y la capa de servicios base del sistema operativo Symbian™, y lo similar. Cada uno de estos módulos de servicios de red pueden ser no exclusivos (*por ejemplo*, capaz de servir a más de un procesador y más de un proceso/aplicación) y cada uno proporciona una interfaz de programación de aplicaciones (API), que tiene una colección de funciones que un procesador 81 puede llamar con el fin de gestionar las comunicaciones con otra entidad. Con estas prestaciones de la API, una colección de llamadas de función de la API puede construirse fácilmente para que ejecute un procesador, que permite al procesador establecer un canal de comunicación con una entidad en una red de comunicación acoplada a la instalación de red 84, y para el intercambio de mensajes y datos con la entidad. El sistema operativo anterior, los módulos y las API, todas incluyen instrucciones que dirigen el funcionamiento del(los) procesador(es) 81.

Una o más bases de datos 86 pueden configurarse como servidores de base de datos, que el(los) procesador(es) 81 puede(n) acceder a través de las prestaciones de red 84 a través de una red de comunicaciones privada 87, que se ilustra por la línea discontinua en la Fig. 1. La entidad/servidor de validación 80 tiene convencionalmente un reloj 88 para el seguimiento de tiempo y fechas para diversas aplicaciones. El reloj 88 puede ser un simple contador de segundos o fracciones de los mismos, que puede leerse por el procesador 81 por una operación de E/S, o puede comprender una disposición más compleja de hardware o firmware que puede proporcionar los diversos componentes de la fecha y tiempo actual (año, mes, día, hora, minuto y segundo) en diferentes registros que pueden leerse por el procesador 81 a través de la ejecución de una o más operaciones de E/S.

La entidad/servidor de validación 80 puede procesar información de identificación transmitida desde una pluralidad de diferentes tokens de verificación 40 (*por ejemplo*, millones de tokens), y puede procesar cualquier número de transmisiones por un token 40 particular. La entidad/servidor de validación 80 aplica una o más pruebas de validación al token de verificación 40.Para estas tareas, la entidad/servidor de validación 80 puede comprender código incorporado en un medio legible por computadora 82 que dirige al procesador de datos 81 para comunicarse con la computadora 10 y el token de verificación 40 mediante el uso de una instalación de red 84 sobre la red de comunicaciones 31.Este código puede incluir instrucciones que establecen una sesión de comunicaciones con la computadora 10, que incluye la opción de establecer una sesión SSL con autenticación mutua y encriptado con base en un algoritmo triple DES, e instrucciones para enviar y recibir mensajes al token de verificación 40 a través de la sesión de comunicaciones.

La entidad/servidor de validación 80 puede comprender además el código incorporado en un medio legible por computadora 82 que dirige al procesador de datos 81 para recibir información de identificación encriptada enviada por el token de verificación 40, y el código que dirige al procesador de datos 81 para desencriptar la información de

identificación encriptada. La información de identificación puede encriptarse por una clave de sesión de una sesión SSL o mediante una clave de encriptación almacenada en el token de verificación 40 y que se conoce para la entidad/servidor de validación 80, o puede encriptarse doblemente por ambas teclas. La última clave puede asignarse únicamente al token. La entidad/servidor de validación 80 puede comprender además el código incorporado en un medio legible por computadora 82 que dirige al procesador de datos 81 para aplicar una o más pruebas de validación como se describe anteriormente arriba. El procesador de datos 81 puede acceder a las bases de datos 86 en la realización de una o más pruebas de validación. Las pruebas de validación y los códigos, por lo tanto se describen a continuación en mayor detalle. Estos códigos y los códigos descritos a continuación para la entidad/servidor de validación 80 pueden implementarse en cualquier número de lenguajes de programación. Además, un experto en la técnica será fácilmente capaz de construir instrucciones para implementar estos códigos en vista de esta descripción sin excesiva experimentación.

Como se describe anteriormente, una primera prueba de validación que puede aplicar la entidad/servidor de validación 80 se refiere a la verificación de que el token de verificación 40 es auténtico. Para esto, el token de verificación 40 puede enviar su número de serie a la entidad/servidor de validación 80, junto con un mensaje de prueba encriptado por una clave de encriptación, con el mensaje de prueba y la clave de encriptación que se conocen para el token 40 y la entidad/servidor de validación 80 (pero no el público en general), y con la clave de encriptación que se asigna además únicamente al número de serie del token.

La entidad/servidor de validación 80 puede acceder a una base de datos de números de serie de tokens y las claves de encriptación correspondientes asociadas únicamente en una de las bases de datos 86, y puede determinar si el token de verificación 40 envía un mensaje de prueba correcto para el número de serie que el token proporcionado. El mensaje de prueba puede ser fijo o variable; en el último caso puede generarse sobre la base de información conocida por ambos el token 40 y la entidad/servidor de validación 80.El mensaje de prueba puede encriptarse y desencriptarse por un algoritmo triple DES, que puede implementarse por un número de conjuntos de instrucciones de computadora bien conocidos.

Si el mensaje de prueba enviado es correcto, puede considerarse que se pasa la primera prueba de validación. Para ello, la entidad/servidor de validación 80 puede comprender código integrado en el medio legible por computadora 82 que dirige al procesador de datos 81 para recibir uno o más mensajes del token de verificación 40 a través de la instalación de red 84 que tiene número de serie del token y el mensaje de prueba encriptado, el código que dirige al procesador de datos 81 para desencriptar el mensaje de prueba encriptado, el código que dirige al procesador de datos 81 para obtener uno o más mensajes aceptables que pueden aceptarse como el mensaje de prueba correcto de una de las bases de datos 86, y el código que dirige al procesador de datos 81 para comparar el mensaje de prueba desencriptado con uno o más mensajes aceptables para determinar si se pasa la primera prueba de validación (en el caso de una coincidencia entre el mensaje de prueba desencriptado y un mensaje aceptable), o se falla (en el caso de que no coincidan).Un mensaje aceptable puede obtenerse mediante el acceso directamente desde una de las bases de datos 86, o mediante la generación a partir de información almacenada en una o más de las bases de datos 86.Los códigos anteriores pueden implementarse con las instrucciones de E/S convencionales, las llamadas de función de la API para las bases de datos, las instrucciones de acceso a memoria, las instrucciones aritméticas y lógicas de la CPU, y las instrucciones de control de la CPU. En vista de esta descripción, los códigos pueden implementarse por un experto en la técnica sin experimentación excesiva.

En una segunda prueba de validación, la entidad/servidor de validación 80 puede tener una base de datos en las bases de datos 86 que realiza el seguimiento de los números de serie de los tokens de verificación que se usan en actividades fraudulentas, y la entidad/servidor de validación 80 puede comprobar el número de serie del token de verificación 40 contra esta base de datos. Si una comprobación de esta base de datos indica que el token de verificación 40 no se involucró en actividades fraudulentas, puede considerarse que se pasa la segunda prueba de validación.

Para implementar la segunda prueba de validación, la entidad/servidor de validación 80 puede comprender código incorporado en el medio legible por computadora 82 que dirige al procesador de datos 81 para recibir un mensaje del token de verificación 40 a través de la instalación de red 84 que tiene el número de serie del token, el código que dirige al procesador de datos 81 para tener el número de serie recibido comparado con los números de serie almacenados en una base de datos de las bases de datos 86 que almacena números de serie de tokens usados en transacciones fraudulentas para determinar si se pasa la segunda prueba de validación (sin actividad fraudulenta), o se falla (actividad fraudulenta).Los códigos anteriores pueden implementarse con las instrucciones de E/S convencionales, las llamadas de función de la API para las bases de datos, las instrucciones de acceso a memoria, las instrucciones lógicas de la CPU, y las instrucciones de control de la CPU. En vista de esta descripción, los códigos pueden implementarse por un experto en la técnica sin experimentación excesiva.

Como una tercera prueba de validación, la entidad/servidor de validación 80 puede enviar un mensaje al token de verificación 40 que solicita a ese token 40 enviar una o más piezas de información específica de computadora acerca de la computadora 10, tales como los números de serie de uno o más de los siguientes: el procesador de la computadora, una o más de las unidades de disco de la computadora, el sistema operativo de la computadora. La entidad/servidor de validación 80 puede recibir esta información y comprobarla contra una base de datos que almacena la información específica de computadora de las computadoras que se sabe se han involucrado en actividades fraudulentas. Si una

comprobación de esta base de datos indica que la computadora 10 usada por el token de verificación 40 no se ha involucrado en actividades fraudulentas, puede considerarse que pasa la tercera prueba de validación.

Para llevar a cabo la tercera prueba de validación, la entidad/servidor de validación 80 puede comprender código incorporado en un medio legible por computadora 82 que dirige al procesador de datos 81 para enviar un mensaje al token de verificación 40 que solicita información específica de la computadora (si el token de verificación 40 no ha enviado dicha información de antemano sin solicitarla), código que dirige al procesador de datos 81 para recibir uno o más mensajes de datos del token de verificación 40 a través de la instalación de red 84 que tiene el número de serie del token y la información específica de la computadora, y el código que dirige al procesador de datos 81 para tener la información específica de la computadora recibida en comparación con la información específica de la computadora almacenada en una base de datos (de las bases de datos 86) que almacena información específica de la computadora de computadoras usadas en transacciones fraudulentas para determinar si se pasa la tercera prueba de validación (sin actividad fraudulenta), o se falla (actividad fraudulenta).Los códigos anteriores pueden implementarse con las instrucciones de E/S convencionales, las llamadas de función de la API para bases de datos, instrucciones de acceso a memoria, instrucciones lógicas de la CPU, y las instrucciones de control de la CPU. En vista de esta descripción, los códigos pueden implementarse por un experto en la técnica sin experimentación excesiva.

La entidad/servidor de validación 80 puede comprender un sitio web accesible para el usuario 1 que permite al usuario:(1) crear una cuenta protegida por contraseña asociada con el número de serie del token, el último de los cuales puede proporcionarse en un pedazo de papel enviado originalmente con el token; (2) asociar una dirección de correo electrónico a usar por una o más de las alertas descritas anteriormente; (3) asociar un número de teléfono móvil y/o URID (*por ejemplo*, dirección de red) del dispositivo de comunicaciones del usuario 5 para usarse por una o más de las alertas descritas anteriormente; y (4) seleccionar una o más de las condiciones de alerta descritas anteriormente. El sitio web también puede permitir que el usuario proporcione y asocie los números de cuenta de uno o más de los dispositivos del usuario 5 con la cuenta protegida por contraseña, y puede además permitir al usuario asociar los mensajes de correo electrónico y números de teléfonos para las alertas a dispositivos 5 en particular, de acuerdo con sus números de cuenta. Una de las bases de datos 86 puede asignarse para mantener las cuentas protegidas por contraseña de los usuarios. Cuando la entidad/servidor de validación 80 recibe una solicitud de validación del token de verificación 40, puede consultarse esta base de datos para encontrar la cuenta protegida por contraseña del usuario (*por ejemplo*, identificar al usuario a partir del número de serie del token y/o el número de cuenta enviado en la información de identificación), y determinar qué alertas de mensaje de texto deben generarse y enviarse en base a los parámetros almacenados en la cuenta protegida por contraseña. Los códigos y las acciones anteriores pueden implementarse con los códigos HTML de la página (*por ejemplo*, páginas web), instrucciones de E/S convencionales, instrucciones de acceso a memoria, llamadas de función de la API de base de datos, instrucciones aritméticas de la CPU, instrucciones lógicas de la CPU, y las instrucciones de control de la CPU. En vista de esta descripción, los códigos pueden implementarse por un experto en la técnica sin experimentación excesiva.

Puede apreciarse que algunas implementaciones de token de verificación 40 pueden configurarse para trabajar con dispositivos de pago de consumo seleccionados 5, tales como los emitidos por un banco seleccionado, o configurarse para trabajar con un sitio Web del comerciante seleccionado 20.

Todavía en otras implementaciones, el token de verificación 40 puede contener el URID de la entidad/servidor de validación 80, que gestiona las solicitudes de validación para varios dispositivos portátiles de consumo 5 de marca compartida, diferentes. Además, cada uno de estos dispositivos 5 de marca compartida puede contener un URID para un comerciante de marca compartida. El URID de comerciante se lee por el token de verificación 40 y se proporciona a una entidad/servidor de validación junto con la información de identificación del dispositivo. La entidad/servidor de validación 80 puede enviar la información de identificación validada a la URID del comerciante.

Las modalidades de la invención no se limitan a sistemas de autenticación que implican transacciones. El mismo enfoque podría aplicarse a otros sistemas de autenticación. Por ejemplo, las modalidades podrían usarse para autenticar a un usuario mediante el uso de una aplicación de banca en línea. Un titular de la tarjeta puede introducir su ID de usuario en un sitio web bancario. El titular de la tarjeta puede entonces presentar su dispositivo de consumo portátil a un token de verificación. El sitio web bancario puede validar el ID de usuario y las credenciales del token mediante la comunicación con una entidad de validación.

Las modalidades de la invención no se limitan a las modalidades descritas anteriormente. Por ejemplo, aunque se muestran los bloques funcionales separados para un emisor, sistema de procesamiento de pago, y adquirente, algunas entidades realizan todas estas funciones y pueden incluirse en modalidades de la invención.

La Fig. 11 es un diagrama de bloques del sistema de computadora típico 1100 configurado para ejecutar código legible por computadora para implementar varias funciones y acciones de acuerdo con diversas modalidades de la presente invención.

El sistema 1100 es representativo de un sistema informático capaz de realizar la presente invención. El sistema informático puede estar presente o usarse para poner en práctica cualquiera de los métodos o las modalidades de computadora o computadora servidor en las Figs.1 a 10.Será fácilmente evidente para un experto en la técnica que

muchas otras configuraciones de hardware y software son adecuadas para usar con la presente invención. Por ejemplo, la computadora puede ser una configuración de escritorio, portátil, montada en bastidor o de tableta. Además, la computadora puede ser una serie de computadoras conectadas en red. Además, se contempla el uso de otros microprocesadores, tales como los microprocesadores Xeon™, Pentium™ o Core™; los microprocesadores Turion™ 64, Opteron™ o Athlon™ de Advanced Micro Devices, Inc; y similares. Además, se contemplan otros tipos de sistemas operativos, como Windows, WindowsXP®, WindowsNT®, o similar de Microsoft Corporation, Solaris de Sun Microsystems, Linux, Unix, y similares. Todavía en otras modalidades, las técnicas descritas anteriormente pueden implementarse en un chip o una placa de procesamiento auxiliar. Varias modalidades pueden basarse en sistemas proporcionados por daVinci, Pandora, Silicon Color, u otros proveedores.

En una modalidad, el sistema informático 1100 incluye típicamente una pantalla 1110, la computadora 1120, un teclado 1130, un dispositivo de entrada de usuario 1140, la comunicación o interfaz de red 1150, y similares. En diversas modalidades, la pantalla (monitor) 1110 puede llevarse a la práctica como una pantalla CRT, una pantalla LCD, una pantalla de plasma, una proyección directa o retroproyección DLP, una micropantalla, o similares. En diversas modalidades, la pantalla 1110 puede usarse para mostrar interfaces de usuario y las imágenes renderizadas.

En diversas modalidades, el dispositivo de entrada de usuario 1140 se lleva a la práctica típicamente como un ratón de computadora, un ratón de bola, un panel táctil, una palanca de mando, un mando a distancia inalámbrico, tableta de dibujo, el sistema de comando de voz, y similares. El dispositivo de entrada de usuario 1140 típicamente permite a un usuario seleccionar objetos, iconos, texto y similares que aparecen en la pantalla 1111 a través de un comando como un clic de un botón o similar. Un dispositivo de entrada de usuario especializado adicional 1145, tal como una banda magnética, transceptor RFID o lector de tarjetas inteligentes también puede proporcionarse en diversas modalidades. En otras modalidades, el dispositivo de entrada de usuario 1145 incluye pantallas del sistema informático adicionales (por ejemplo, monitores múltiples).Además el dispositivo de entrada de usuario 1145 puede implementarse como una o más interfaces de usuario gráficas en una pantalla tal.

Las modalidades de las interfaces de computadora 1150 incluyen típicamente una tarjeta Ethernet, un módem (teléfono, satélite, cable, ISDN), una unidad de línea de abonado digital (DSL) (asíncrona), la interfaz FireWire, la interfaz USB, y similares. Por ejemplo, las interfaces de computadora 1150 pueden acoplarse a una red informática, a un bus FireWire, o similares. En otras modalidades, las interfaces de computadora 1150 pueden integrarse físicamente en la placa base de la computadora 1120, pueden ser un programa de software, tal como el software de DSL, o similares.

La RAM 1170 y el disco duro 1180 son ejemplos de medios tangibles legibles por computadora configurados para almacenar datos tales como usuario, la cuenta y el nivel de transacción de datos, datos agregados calculados, súper claves, subclaves y otro código de computadora ejecutable, código legible por humanos, o similares. Otros tipos de medios tangibles incluyen medios de almacenamiento magnéticos, tal como disquetes, discos duros en red o discos duros extraíbles; medios de almacenamiento ópticos tal como CD-ROM, DVD, memorias holográficas, o códigos de barras; medios semiconductores tales como memorias flash, memorias de sólo lectura (ROM); memorias volátiles respaldada por batería; dispositivos de almacenamiento en red, y similares.

En la presente modalidad, el sistema de computadora 1100 también puede incluir software que permite comunicaciones a través de una red tal como los protocolos HTTP, TCP/IP, RTP/RTSP, y similares. En modalidades alternativas de la presente invención, también pueden usarse otros softwares de comunicaciones y protocolos de transferencia, por ejemplo IPX, UDP o similares.

En diversas modalidades, la computadora 1120 incluye típicamente componentes de computadora familiares, tales como un procesador 1160, y dispositivos de almacenamiento de memoria, tales como una memoria de acceso aleatorio (RAM) 1170, unidades de disco 1180, y el bus del sistema 1190 que interconectan los componentes anteriores.

En algunas modalidades, la computadora 1100 incluye uno o más microprocesadores Xeon de Intel. Además, en la presente modalidad, la computadora 1120 incluye típicamente un sistema operativo basado en UNIX.

Debe entenderse que las modalidades de la presente invención como se describe anteriormente pueden implementarse en forma de lógica de control mediante el uso de software de computadora de una manera modular o integrada. Sobre la base de la descripción y enseñanzas proporcionadas en la presente descripción, un experto en la técnica conocerá y apreciará otras formas y/o métodos para implementar la presente invención mediante el uso del hardware y una combinación de hardware y software

Cualquiera de los componentes de software o funciones descritas en esta solicitud, pueden implementarse como código de software para ejecutarse por un procesador mediante el uso de cualquier lenguaje de programación adecuado tal como, por ejemplo, Java, C ++ o Perl mediante el uso, por ejemplo, de técnicas orientadas a objetos o convencionales. El código de software puede almacenarse como una serie de instrucciones o comandos en un medio legible por computadora, tal como una memoria de acceso aleatorio (RAM), una memoria de sólo lectura (ROM), un medio magnético tal como una unidad de disco duro o un disquete, o un medio óptico, tal como un CD-ROM. Cualquier medio legible por computadora tal puede residir en o dentro de un único aparato computacional, y puede estar presente o dentro de diferentes aparatos computacionales dentro de un sistema o red.

La descripción anterior es ilustrativa y no es restrictiva. Muchas variaciones de la invención serán evidentes para los expertos en la técnica tras la revisión de la descripción. El alcance de la invención debe, por lo tanto, determinarse no con referencia a la descripción anterior, sino que debe determinarse con referencia a las reivindicaciones pendientes junto con todo su alcance, o equivalentes.

Una o más características de cualquier modalidad pueden combinarse con una o más características de cualquier otra modalidad sin apartarse del alcance de la invención.

Una relación de "uno", "un" o "la" se entiende que significa "uno o más" salvo que se indique específicamente lo contrario.

Reivindicaciones

1. Un método para generar un token de verificación por un fabricante de token de verificación, el método que comprende:
generar un número de serie para un token de verificación;
generar un par de claves específicas de token de verificación que incluye un componente público y un componente privado con base en una clave maestra del fabricante de token de verificación;
asociar el número de serie con el par de claves específicas de token de verificación; y
almacenar el componente privado del par de claves específicas de token de verificación a una memoria en el token de verificación,
validar el token de verificación por un servidor de validación, en donde el componente privado del par de claves específicas de token de verificación se usa por el token de verificación para generar una respuesta a un mensaje de cuestionamiento firmado desde el servidor de validación por desencriptar el mensaje de cuestionamiento firmado mediante el uso del componente privado, y la clave maestra del fabricante de token de verificación se usa por el servidor de validación para desencriptar aún más la respuesta recibida del token de verificación para determinar que el token de verificación es de un fabricante de token de verificación de confianza.

2. El método de la reivindicación 1 que comprende además almacenar el número de serie en la memoria en el token de verificación.

3. El método de la reivindicación 1 en donde generar el par de claves específicas del token de verificación comprende firmar el componente público del par de claves con la clave maestra específica del fabricante para generar un certificado público del token de verificación.

4. El método de la reivindicación 3 que comprende además el almacenamiento del certificado público del token de verificación en la memoria del token de verificación.

5. El método de la reivindicación 1 que comprende además almacenar un identificador de fabricante en la memoria del token de verificación.

6. El método de la reivindicación 1 que comprende además almacenar, en el token de verificación, el código ejecutable para establecer una conexión con un servidor de verificación a través de una sesión de comunicación mediante el uso de una instalación de comunicación de un dispositivo de computación al que se conecta el token de verificación.

7. El método de la reivindicación 1 que comprende además:
enviar una solicitud de registro a una computadora servidor; y
recibir la clave maestra del fabricante de token de verificación desde la computadora servidor.

8. El método de la reivindicación 7 en donde la computadora servidor lleva a cabo una revisión del riesgo con base en la información relacionada con el fabricante de token de verificación.

9. El método de la reivindicación 7, que comprende además la recepción de un certificado de clave de fabricante de token de verificación desde la computadora servidor.

10. Un equipo que comprende:
un procesador; y
un código que se almacena en memoria, que cuando se ejecuta por el procesador, provoca que el procesador realice el método de las reivindicaciones 1-9.

11. Un programa de computadora que comprende instrucciones legibles por máquina que cuando se ejecutan por un aparato de cálculo causa que éste realice el método de cualquiera de las reivindicaciones 1-9.

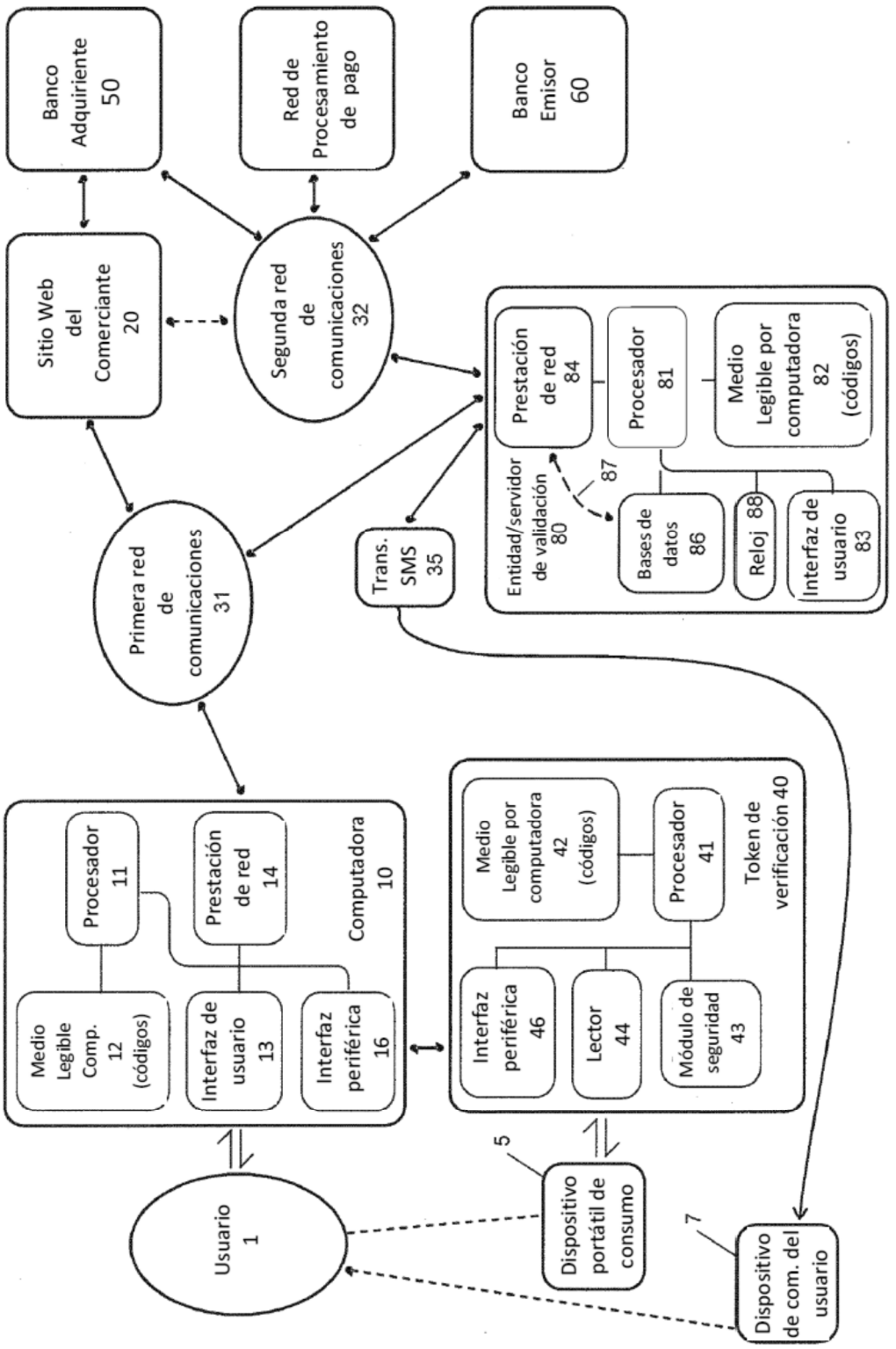
Banco Adquiriente 50
Red de Procesamiento de pago
Banco Emisor 60
Sitio Web del Comerciante 20
Segunda red de comunicaciones 32
Primera red de comunicaciones 31
Trans. SMS 35
Entidad/servidor de validación 80
Prestación de red 84
Procesador 81
Medio Legible por computadora 82 (códigos)
87
Bases de datos 86
Reloj 88
Interfaz de usuario 83
Computadora 10
Procesador 11
Prestación de red 14
Medio Legible Comp. 12 (códigos)
Interfaz de usuario 13
Interfaz periférica 16
Token de verificación 40
Medio Legible por computadora 42 (códigos)
Procesador 41
Interfaz periférica 46
Lector 44
Módulo de seguridad 43
Usuario 1
5
Dispositivo portátil de consumo
7
Dispositivo de com. del usuario

Fig. 1

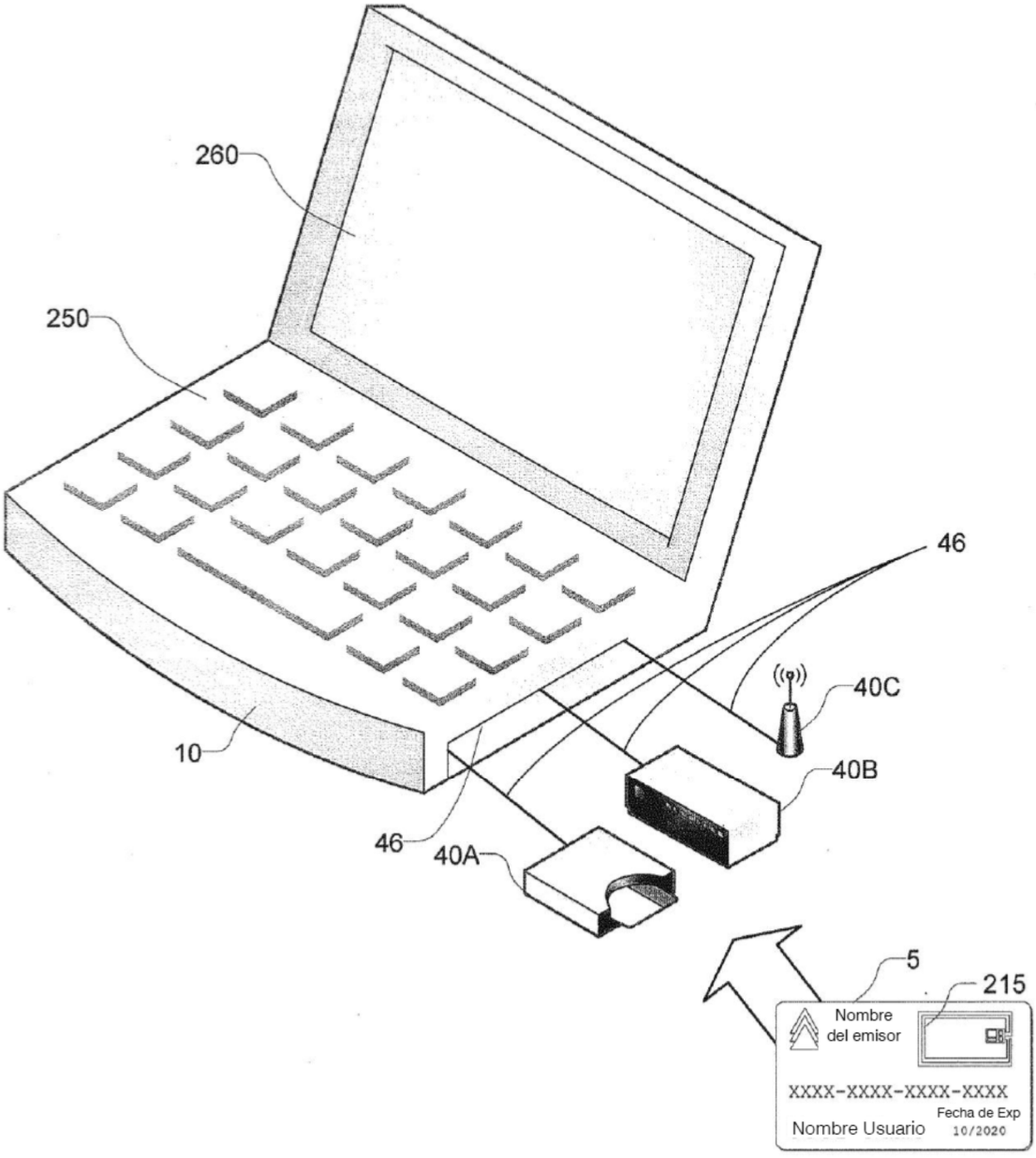
260
250
46
40C
40B
10
46
40A
5
215
Nombre
del emisor
XXXX-XXXX-XXXX-XXXX
Fecha de Exp
Nombre Usuario
10/2020

Fig. 2

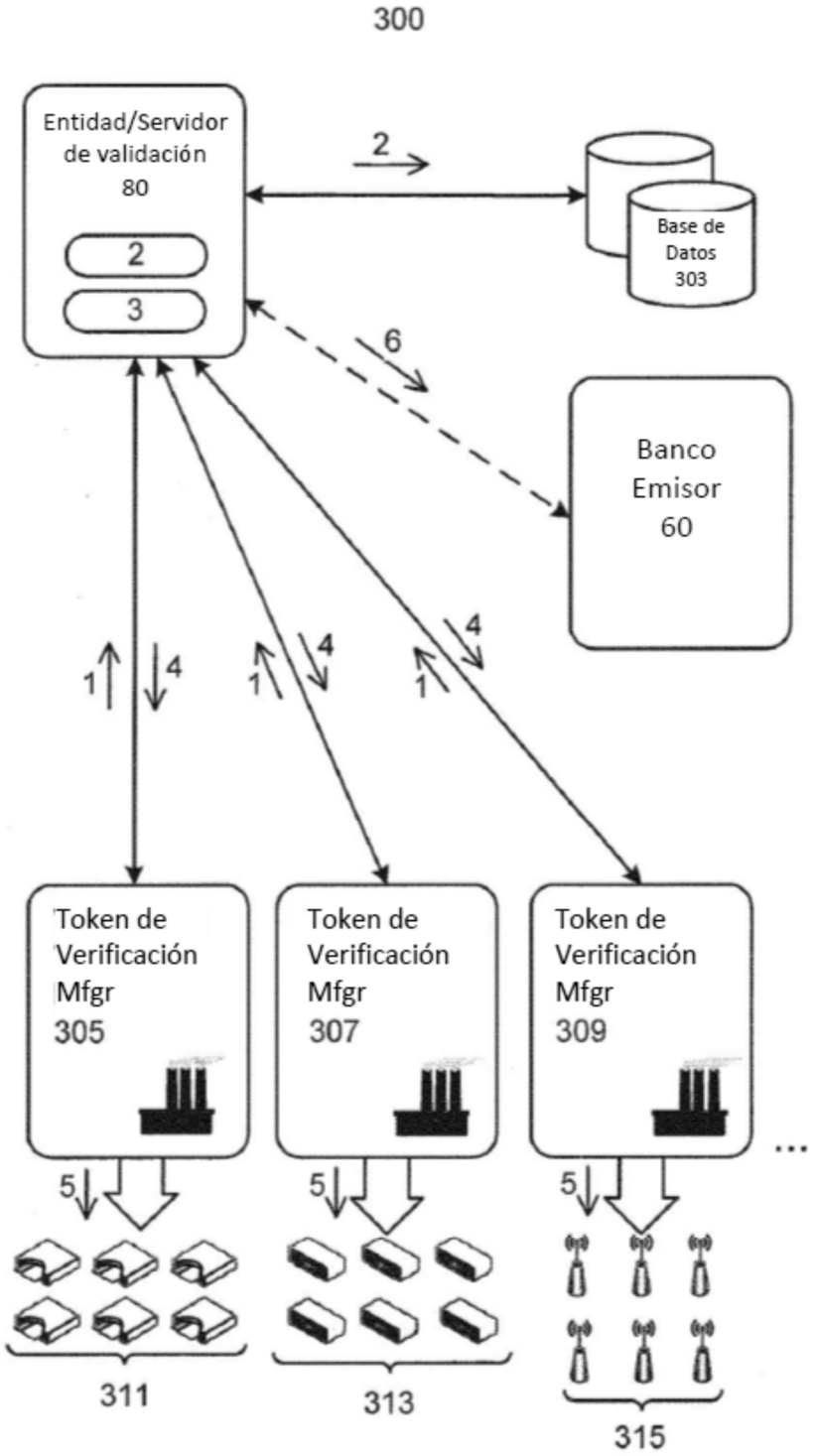
300
Entidad/Servidor de validación 80
2
3
2
Base de Datos 303
6
Banco Emisor 60
1
4
1
4
1
4
Token de Verificación Mfgr 305
Token de Verificación Mfgr 307
Token de Verificación Mfgr 309
...
5
5
5
311
313
315

Fig. 3

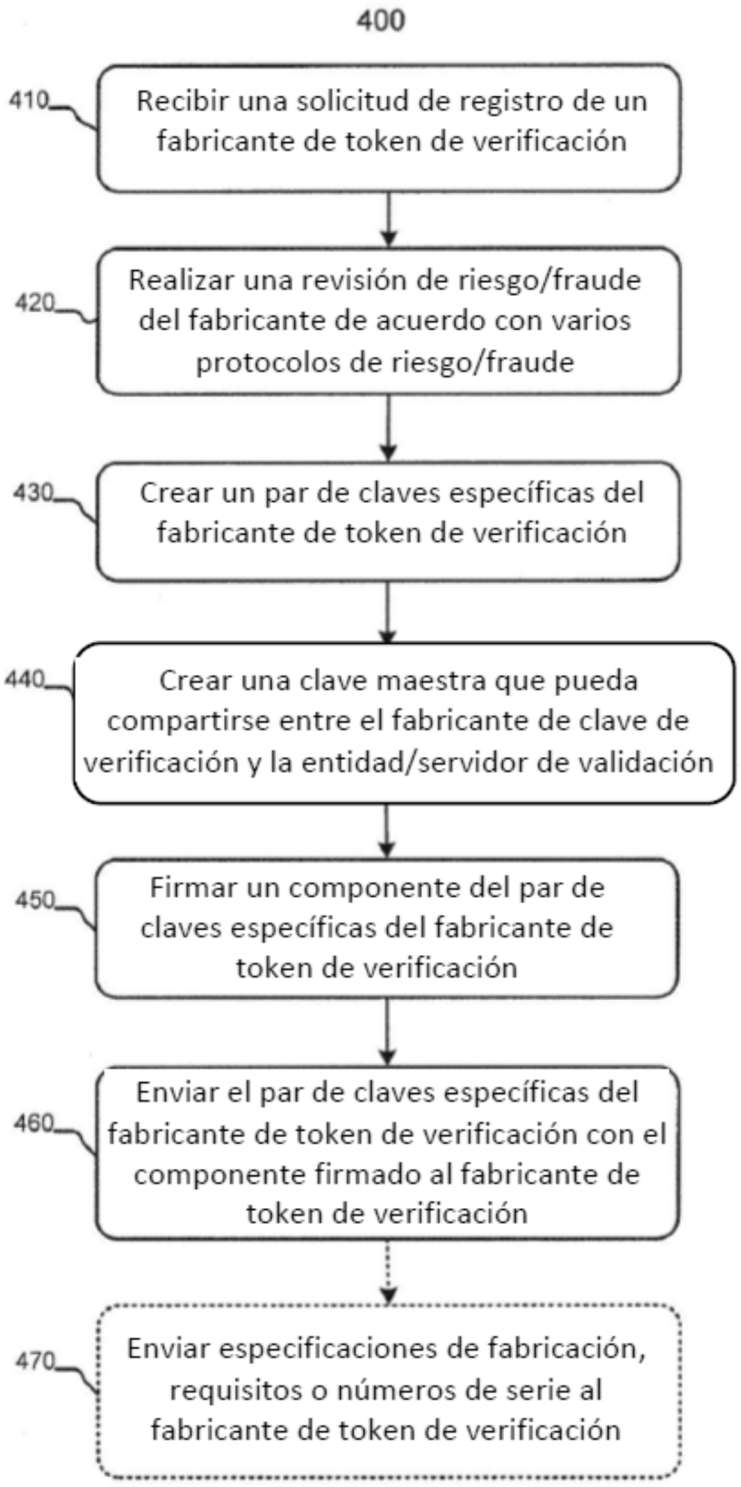
400
410
Recibir una solicitud de registro de un fabricante de token de verificación
420
Realizar una revisión de riesgo/fraude del fabricante de acuerdo con varios protocolos de riesgo/fraude
430
Crear un par de claves específicas del fabricante de token de verificación
440
Crear una clave maestra que pueda compartirse entre el fabricante de clave de verificación y la entidad/servidor de validación
450
Firmar un componente del par de claves específicas del fabricante de token de verificación
460
Enviar el par de claves específicas del fabricante de token de verificación con el componente firmado al fabricante de token de verificación
470
Enviar especificaciones de fabricación, requisitos o números de serie al fabricante de token de verificación

Fig. 4

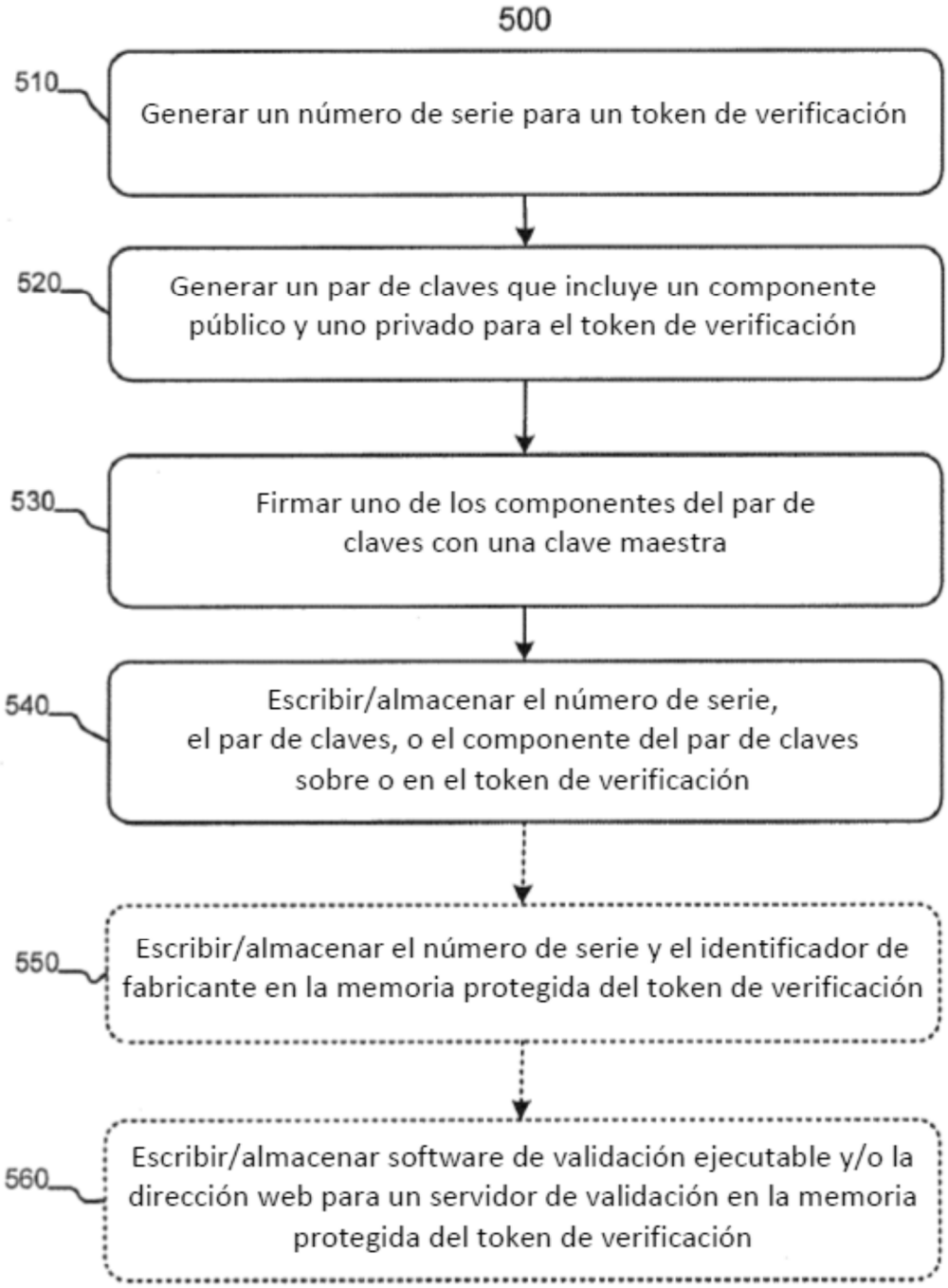
500
510
Generar un número de serie para un token de verificación
520
Generar un par de claves que incluye un componente público y uno privado para el token de verificación
530
Firmar uno de los componentes del par de claves con una clave maestra
540
Escribir/almacenar el número de serie, el par de claves, o el componente del par de claves sobre o en el token de verificación
550
Escribir/almacenar el número de serie y el identificador de fabricante en la memoria protegida del token de verificación
560
Escribir/almacenar software de validación ejecutable y/o la dirección web para un servidor de validación en la memoria protegida del token de verificación

Fig. 5

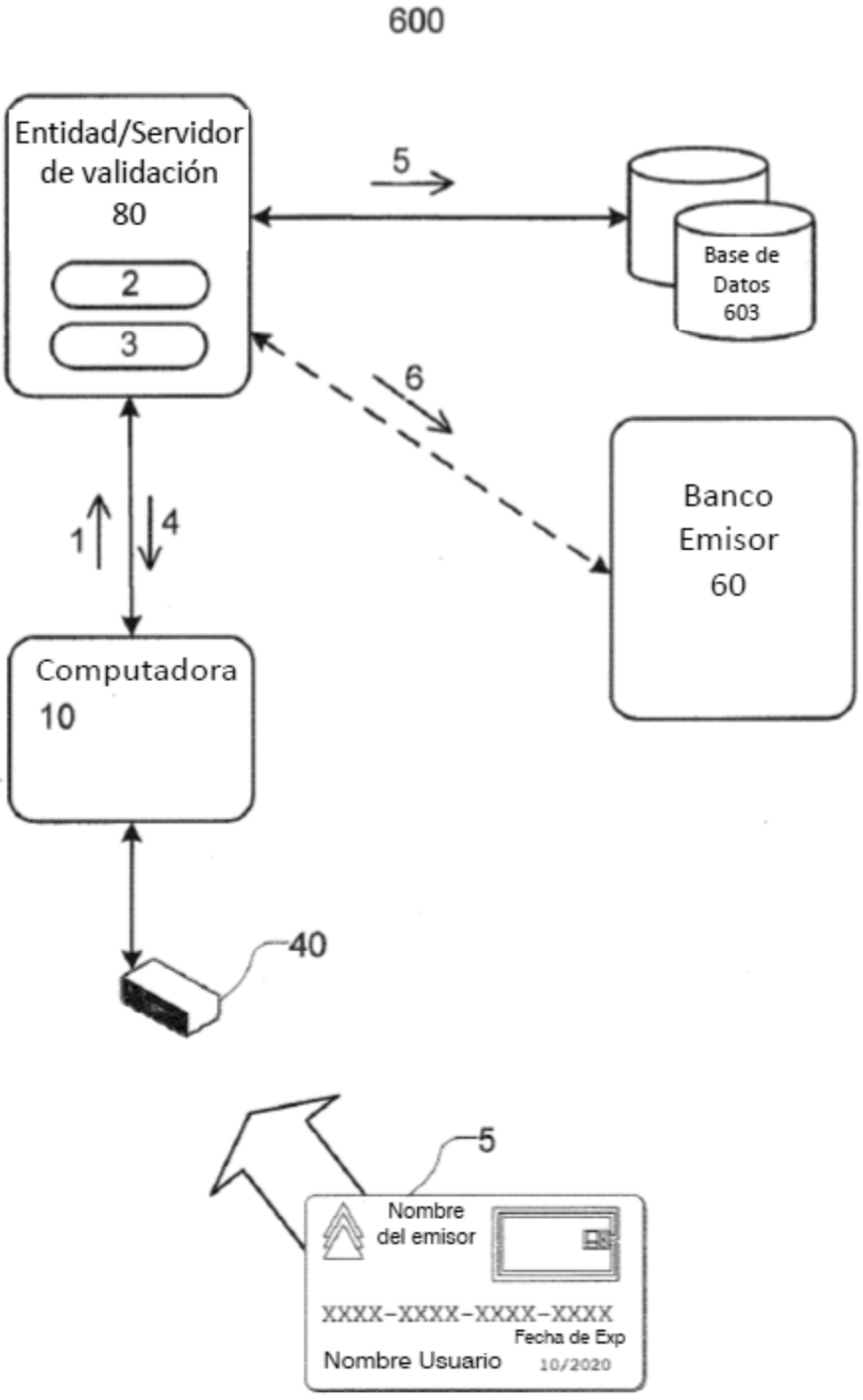
600
Entidad/Servidor de validación 80
2
3
5
Base de Datos 603
6
Banco Emisor 60
1
4
Computadora 10
40
5
Nombre del emisor
XXXX-XXXX-XXXX-XXXX
Fecha de Exp
Nombre Usuario
10/2020

Fig. 6

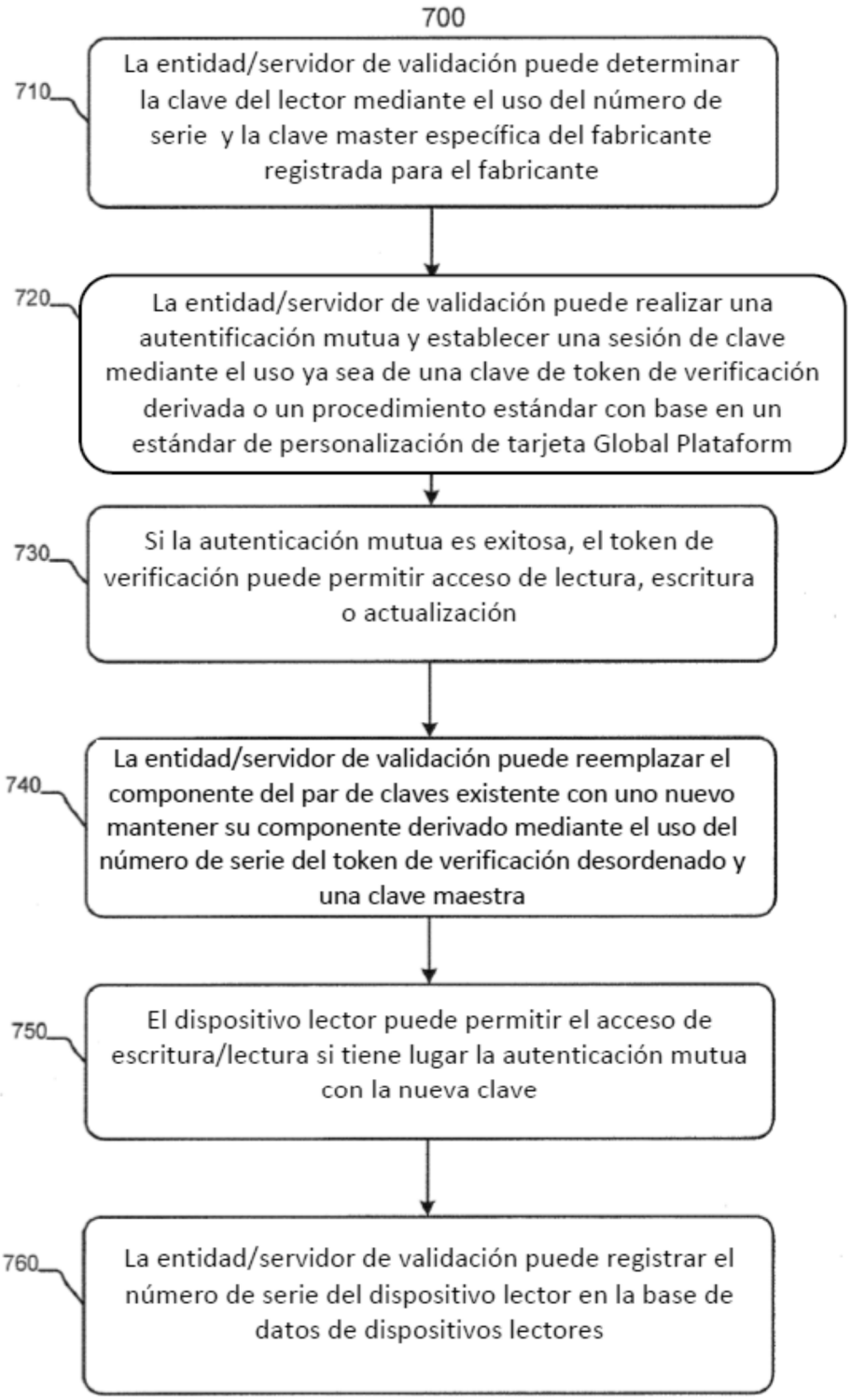
700
710
La entidad/servidor de validación puede determinar la clave del lector mediante el uso del número de serie y la clave master específica del fabricante registrada para el fabricante
720
La entidad/servidor de validación puede realizar una autentificación mutua y establecer una sesión de clave mediante el uso ya sea de una clave de token de verificación derivada o un procedimiento estándar con base en un estándar de personalización de tarjeta Global Plataform
730
Si la autenticación mutua es exitosa, el token de verificación puede permitir acceso de lectura, escritura o actualización
740
La entidad/servidor de validación puede reemplazar el componente del par de claves existente con uno nuevo mantener su componente derivado mediante el uso del número de serie del token de verificación desordenado y una clave maestra
750
El dispositivo lector puede permitir el acceso de escritura/lectura si tiene lugar la autenticación mutua con la nueva clave
760
La entidad/servidor de validación puede registrar el número de serie del dispositivo lector en la base de datos de dispositivos lectores

Fig. 7

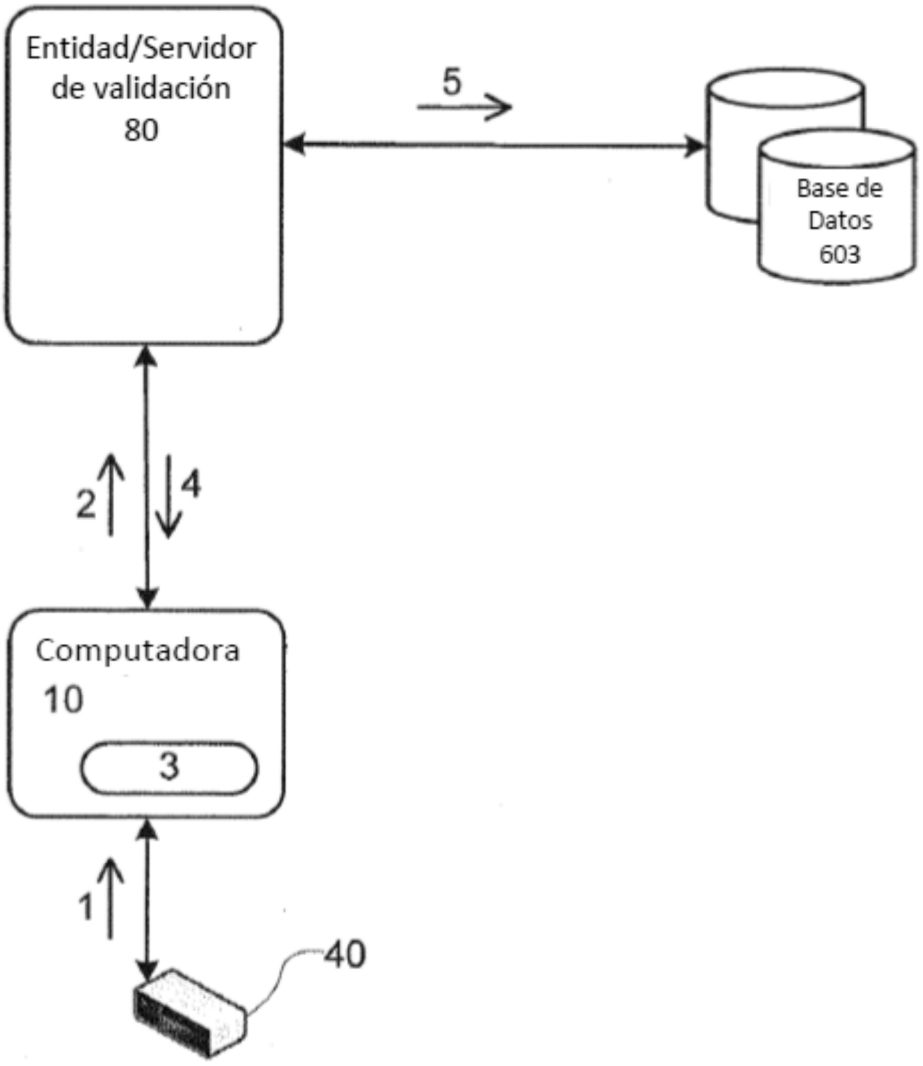
Entidad/Servidor
de validación
80
5
Base de
Datos
603
2
4
Computadora
10
3
1
40

Fig. 8

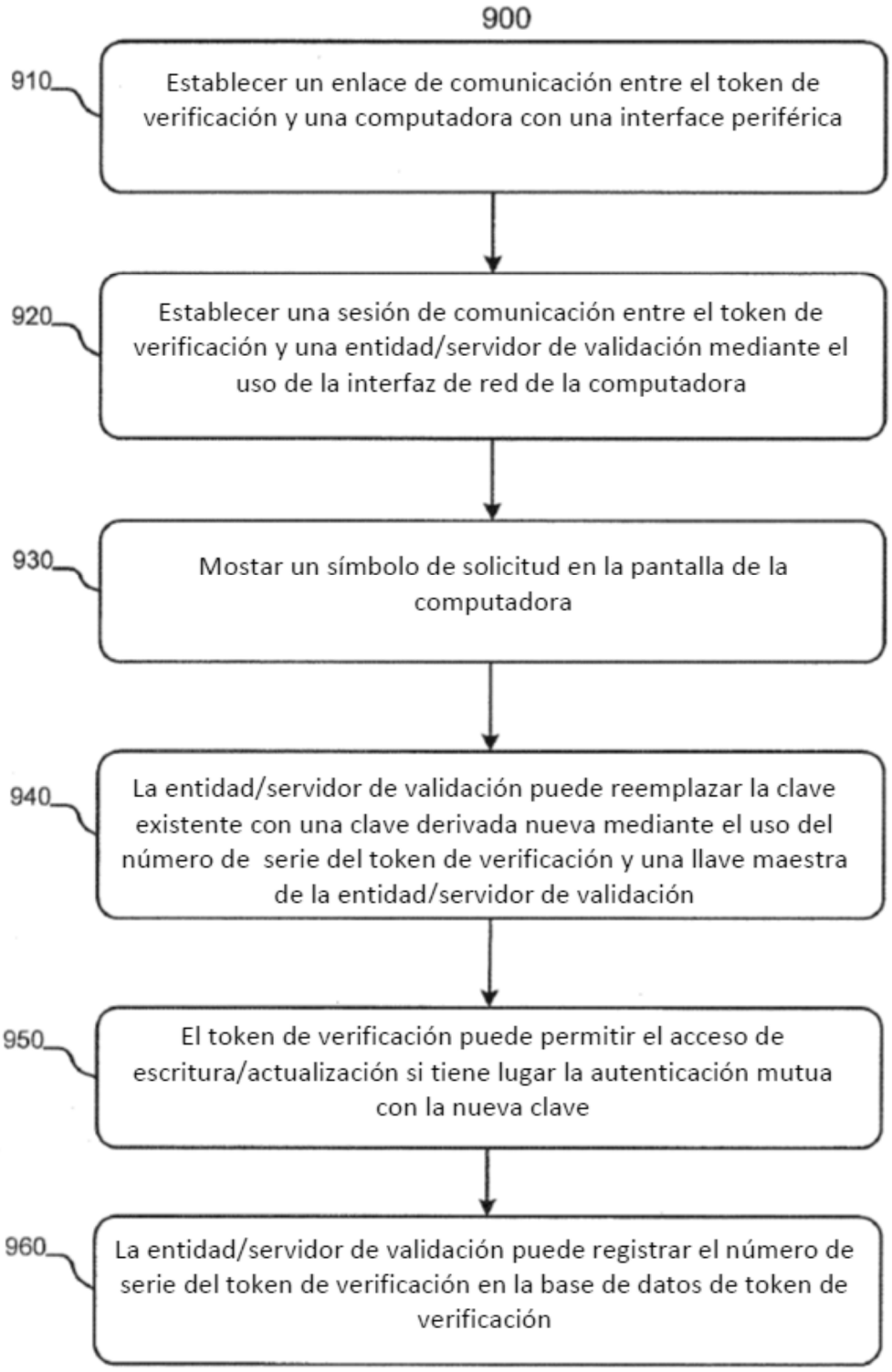
900
910
Establecer un enlace de comunicación entre el token de verificación y una computadora con una interface periférica
920
Establecer una sesión de comunicación entre el token de verificación y una entidad/servidor de validación mediante el uso de la interfaz de red de la computadora
930
Mostar un símbolo de solicitud en la pantalla de la computadora
940
La entidad/servidor de validación puede reemplazar la clave existente con una clave derivada nueva mediante el uso del número de serie del token de verificación y una llave maestra de la entidad/servidor de validación
950
El token de verificación puede permitir el acceso de escritura/actualización si tiene lugar la autenticación mutua con la nueva clave
960
La entidad/servidor de validación puede registrar el número de serie del token de verificación en la base de datos de token de verificación

Fig. 9

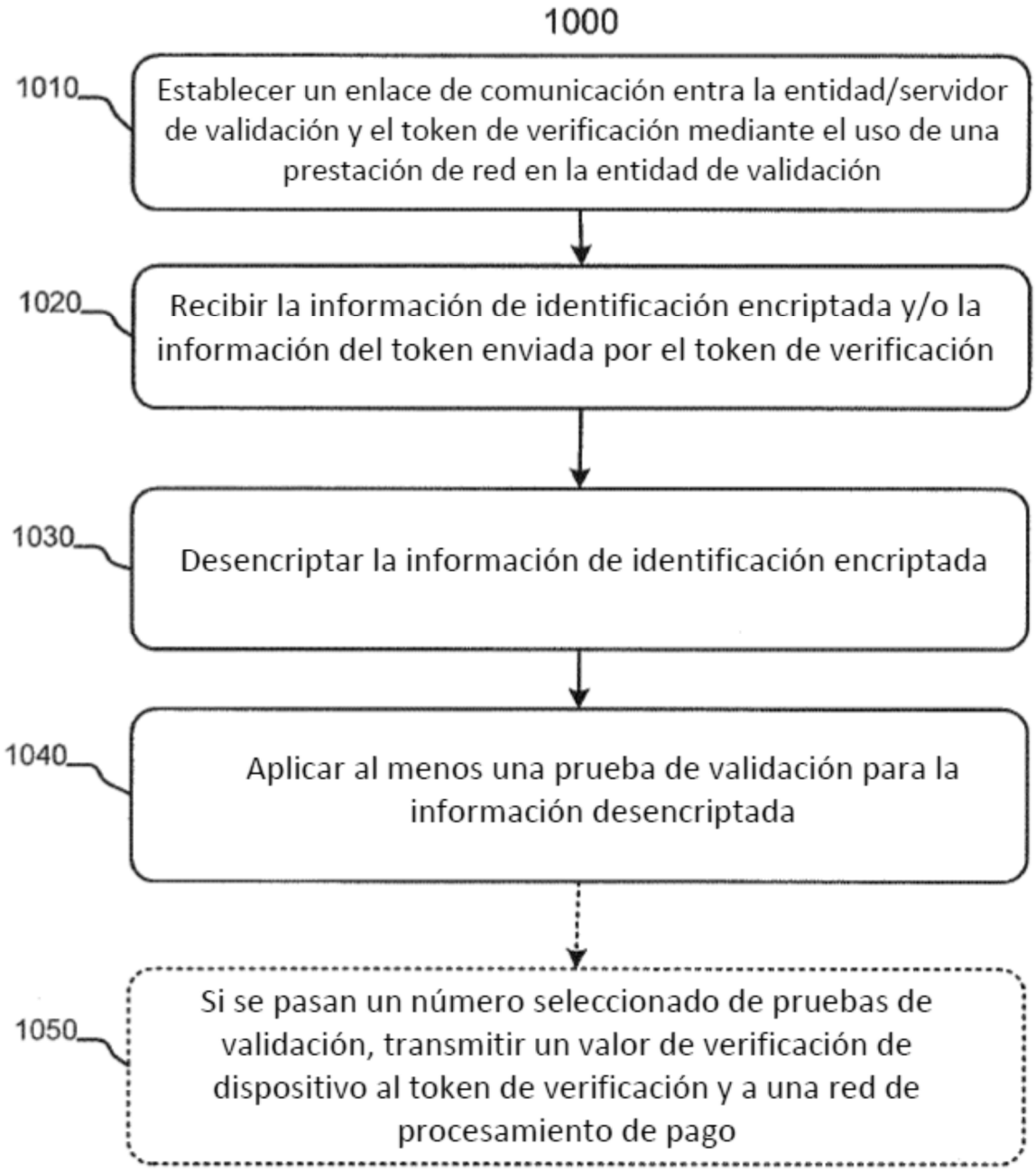
1000
1010
Establecer un enlace de comunicación entra la entidad/servidor de validación y el token de verificación mediante el uso de una prestación de red en la entidad de validación
1020
Recibir la información de identificación encriptada y/o la información del token enviada por el token de verificación
1030
Desencriptar la información de identificación encriptada
1040
Aplicar al menos una prueba de validación para la información desencriptada
1050
Si se pasan un número seleccionado de pruebas de validación, transmitir un valor de verificación de dispositivo al token de verificación y a una red de procesamiento de pago

Fig. 10

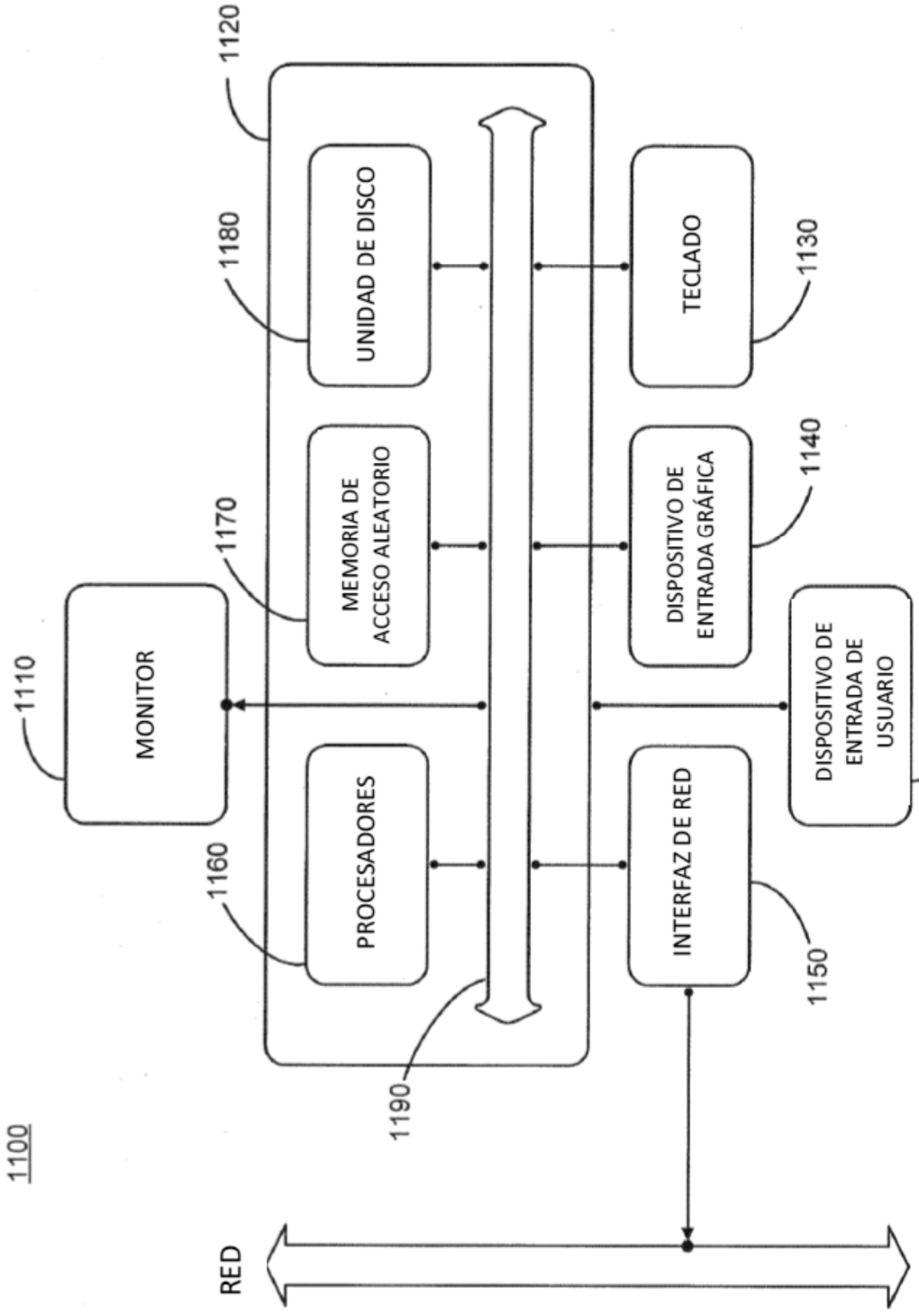
1100
1120
1180
UNIDAD DE DISCO
TECLADO
1130
1170
MEMORIA DE ACCESO ALEATORIO
1140
DISPOSITIVO DE ENTRADA GRÁFICA
1110
MONITOR
DISPOSITIVO DE ENTRADA DE USUARIO
1145
1160
PROCESADORES
INTERFAZ DE RED
1150
1190
RED

Fig. 11