(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 797 111**

(51) Int. CI.:

G06Q 20/20 (2012.01)
G06Q 20/36 (2012.01)
G06Q 20/32 (2012.01)
G06Q 20/38 (2012.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **18.05.2017 E 17000854 (4)**

(97) Fecha y número de publicación de la concesión europea: **18.03.2020 EP 3246866**

(54) Título: **Intercambio seguro de unos datos sensibles a través de una red basada en códigos de barras y testigos**

(30) Prioridad:

18.05.2016 FR 1654400
18.05.2016 US 201615158130

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
01.12.2020

(73) Titular/es:

AMADEUS S.A.S. (100.0%)
485 route du Pin Montard Sophia Antipolis
06410 Biot, FR

(72) Inventor/es:

APARICIO RUIZ, PABLO;
TAHON, MATHIEU y
ESPEJO MALAGON, DANIEL

(74) Agente/Representante:

SUGRAÑES MOLINÉ, Pedro

DESCRIPCIÓN

Intercambio seguro de unos datos sensibles a través de una red basada en códigos de barras y testigos

Campo técnico

La invención se refiere en general a ordenadores y software informático, y en particular a métodos, sistemas, y productos de programa informático para intercambiar de manera segura datos sensibles a través de una red.

Antecedentes

Puesto que existen muchas oportunidades para que los datos sensibles se vean comprometidos durante el pago, tales como datos de tarjeta de crédito, es obligatorio para pagos de tarjeta de crédito cara a cara que utilicen dispositivos que están de acuerdo con la Norma de Seguridad de Datos de la Industria de Tarjeta de Pago (PCI-DSS), que ayuda a aliviar las vulnerabilidades y protege los datos del titular de la tarjeta. Sin embargo, en ocasiones estar conforme con PCI-DSS puede ser extraordinariamente difícil y costoso. En un enfoque para proteger datos sensibles, puede usarse el uso de sustitución de datos con un testigo o alias como una sustitución para los datos de tarjeta de crédito reales. El testigo puede usarse en lugar de una tarjeta de crédito real del individuo durante una transacción de pago. Por ejemplo, un usuario puede utilizar su teléfono inteligente u otro dispositivo electrónico portátil para pagar un producto. Específicamente, el usuario puede descargar una aplicación a un teléfono inteligente. El usuario puede a continuación introducir información que pertenece a una tarjeta de crédito, y envía la información a través de una red a un grupo de servidores. En respuesta a recibir una información de tarjeta de crédito del usuario, los servidores pueden generar en testigos la información de tarjeta de crédito del usuario. Los expertos en la materia apreciarán fácilmente que los testigos no tienen significado por sí mismos, y por lo tanto no pueden usarse en solitario. Adicionalmente, la generación de testigos puede ser menos costosa y más segura que la encriptación de extremo a extremo.

Por ejemplo, los agentes de reserva de terceros (es decir, agentes de viajes) o viajeros pueden utilizar dispositivos informáticos para crear una reserva de viaje, que presenta oportunidades para que los datos de la tarjeta de crédito del viajero se vean comprometidos durante el pago. En ocasiones un viajero puede necesitar pagar la reserva de viaje por sí mismo o por otros imprevistos relacionados, tales como cargos por equipaje, durante el tránsito. Es decir, el viajero puede necesitar pagar por gastos relacionados con el viaje en un aeropuerto u otra ubicación, tal como una estación de tren.

Además de los desafíos anteriormente mencionados para proteger los datos del titular de la tarjeta, debería apreciarse también que los viajeros pueden encontrar también otros problemas cuando intentan pagar una reserva de viaje en un aeropuerto u otra ubicación similar. Por ejemplo, si un viajero desea pagar una reserva de viaje usando su teléfono inteligente, esto puede volverse problemático si el viajero está visitando un país extranjero. Esto es debido a que muchos proveedores celulares pueden no ofrecer servicio en otro país, o pueden cobrar tasas muy altas para itinerancia de datos puesto que el viajero está abordo. Por lo tanto, existe una necesidad para aceptar pagos de viajeros incluso si el teléfono inteligente del viajero no tiene conectividad de red. Adicionalmente, debería apreciarse también que puede ser problemático e inconveniente que un viajero retire su monedero de su bolsillo para recuperar su tarjeta de crédito, especialmente si el viajero tiene prisa o tiene muchas maletas que llevar en tránsito. De manera similar, puede ser también inconveniente que un viajero busque en su bolso su billetera para recuperar su tarjeta de crédito, especialmente si sus manos están ya llenas de maletas que necesitan llevarse en tránsito.

Por lo tanto, son necesarios métodos, sistemas, y productos de programa informático mejorados que permitan el intercambio seguro de datos sensibles a través de una red.

El documento GB 2 478 712 A se refiere a un sistema de autorización. El sistema de autorización comprende un terminal de procesamiento de transacción para procesar transacciones; y un dispositivo de usuario móvil. El dispositivo de usuario comprende medios para recibir información relacionada con una transacción particular del terminal de procesamiento, y medios para generar un código de usuario para autorizar una transacción dependiendo de la información recibida, en el que el código de usuario está adaptado para recibirse por el terminal de procesamiento para posibilitar de esta manera que el terminal de procesamiento procese la transacción.

El documento EP 2 819 080 A1 se refiere a un sistema de telecomunicación. El sistema de telecomunicación comprende un servidor de autorización para permitir una autorización rápida por medio de un dispositivo de telecomunicación móvil también en un entorno donde no está disponible conexión de red móvil estable. De acuerdo con dicho sistema, el dispositivo móvil está configurado para solicitar automáticamente un testigo de autorización del servidor de autorización mucho antes del evento de autorización real. Si no hay disponible conexión de red móvil, la solicitud se reenvía automática y repetitivamente al servidor de autorización hasta que se restablezca la conexión de red móvil y se reciba el código de autorización solicitado. El servidor de autorización está configurado para transmitir el testigo de autorización solicitado al dispositivo móvil y para recibir el testigo de autorización e información relacionada con un producto o servicio de un terminal. El servidor de autorización valida el testigo de autorización y autoriza o deniega la compra del producto o servicio dependiendo de una cuenta de recursos asociada con el usuario del dispositivo móvil. El servidor de autorización transmite la autorización o denegación al terminal).

Sumario

La invención se define en las reivindicaciones independientes. Las reivindicaciones dependientes definen realizaciones de la misma.

De aquí en adelante, se desvelan ejemplos de un sistema para intercambiar de manera segura un testigo de tarjeta de crédito entre un primer ordenador y un ordenador externo para comprar un producto. El primer ordenador incluye uno o más procesadores, una memoria, y una cámara acoplados a al menos un procesador. El primer ordenador explora un primer código de barras por la cámara. El primer código de barras se publica después de una visualización del ordenador externo e indica una pluralidad de parámetros de pago para el pago del producto. El primer ordenador decodifica el primer código de barras para extraer los parámetros de pago. El primer ordenador publica los parámetros de pago para su visualización a un usuario. El primer ordenador recibe una primera entrada, donde la primera entrada indica un número de tarjeta de crédito para comprar el producto, y un testigo de tarjeta de crédito que corresponde al número de tarjeta de crédito se graba en la memoria. En respuesta a la recepción de la primera entrada, el primer ordenador genera un segundo código de barras que tiene una primera carga útil encriptada. La primera carga útil encriptada incluye el testigo de tarjeta de crédito. El primer ordenador publica el segundo código de barras para su visualización, donde el segundo código de barras es legible por un dispositivo óptico del ordenador externo.

En algunas realizaciones, el sistema comprende adicionalmente un tercer ordenador y una bóveda de testigos en comunicación con el ordenador externo. El ordenador externo envía el segundo código de barras al tercer ordenador. En una realización, el tercer ordenador decodifica el segundo código de barras, valida contenido de la primera carga útil encriptada para obtener el testigo de tarjeta de crédito, y recupera un número de tarjeta de crédito original de la bóveda de testigos basándose en el testigo de tarjeta de crédito. En algunas realizaciones, el tercer ordenador se comunica con una red de pagos para determinar si es válido el número de tarjeta de crédito original, y en respuesta a que el número de tarjeta de crédito original sea válido, la red de pagos autoriza el pago para el producto y envía una aprobación al tercer ordenador. En algunas realizaciones, el ordenador externo recibe la aprobación del tercer ordenador para el pago del producto, genera un tercer código de barras que contiene una recepción de pago para el producto, y publica el tercer código de barras para su visualización. El tercer código de barras se explora por la cámara.

En algunas realizaciones, la pluralidad de parámetros de pago incluye al menos una cantidad monetaria, un tipo específico de divisa en la que está basada la cantidad monetaria, una descripción del producto, y una identificación (ID) de referencia de pago.

En algunas realizaciones, antes de explorar el primer código de barras por la cámara, el primer ordenador y un tercer ordenador están conectados a una red, el primer ordenador recibe una segunda entrada que indica el número de tarjeta de crédito, y en respuesta a la recepción de la segunda entrada, el primer ordenador genera una segunda carga útil encriptada que contiene el número de tarjeta de crédito. En algunas realizaciones, el primer ordenador transmite una solicitud de aprovisionamiento de tarjeta que incluye la segunda carga útil encriptada a través de la red, el tercer ordenador recibe la solicitud de aprovisionamiento de tarjeta a través de la red, y en respuesta a la recepción de la solicitud de aprovisionamiento de tarjeta el tercer ordenador desencripta la segunda carga útil encriptada para obtener el número de tarjeta de crédito. En algunas realizaciones, el tercer ordenador envía el número de tarjeta de crédito a una aplicación de generación de testigos, y en respuesta a la recepción del número de tarjeta de crédito, la aplicación de generación de testigos genera el testigo de tarjeta de crédito. En algunas realizaciones, el testigo de tarjeta de crédito se graba en una bóveda de testigos y también se transmite a través de la red del tercer ordenador de vuelta al primer ordenador, y el primer ordenador almacena el testigo de tarjeta de crédito como una función de troceo en la memoria. En algunas realizaciones, los procesadores son parte de un dispositivo electrónico portátil.

De acuerdo con otro aspecto, se desvela un método para intercambiar de manera segura un testigo de tarjeta de crédito entre un primer ordenador de sistema y un ordenador externo para comprar un producto. El método incluye explorar un primer código de barras por una cámara de un primer ordenador, donde el primer código de barras se publica después de la visualización del ordenador externo y el primer código de barras indica una pluralidad de parámetros de pago del producto. El método comprende adicionalmente la decodificación del primer código de barras, por el primer ordenador, para extraer los parámetros de pago. El método también incluye publicar los parámetros de pago para su visualización a un usuario por el primer ordenador. El método incluye adicionalmente la recepción de una primera entrada por el primer ordenador, donde la primera entrada indica un número de tarjeta de crédito para comprar el producto, y un testigo de tarjeta de crédito se graba en una memoria del primer ordenador que corresponde al número de tarjeta de crédito. En respuesta a la recepción de la primera entrada, el método incluye generar, por el primer ordenador, un segundo código de barras que contiene una primera carga útil encriptada, donde la primera carga útil encriptada incluye el testigo de tarjeta de crédito. Finalmente, el método incluye publicar el segundo código de barras para su visualización por el primer ordenador, donde el segundo código de barras es legible por un dispositivo óptico del ordenador externo.

En algunas realizaciones, el ordenador externo envía el segundo código de barras a través de una red a un tercer ordenador. El tercer ordenador decodifica el segundo código de barras, valida contenido de la primera carga útil encriptada para obtener el testigo de tarjeta de crédito, y recupera un número de tarjeta de crédito original de una

bóveda de testigos basándose en el testigo de tarjeta de crédito. En algunas realizaciones, el tercer ordenador envía una comunicación a una red de pagos. En respuesta a la recepción de la comunicación, la red de pagos determina si es válido el número de tarjeta de crédito original. En respuesta a que el número de tarjeta de crédito original sea válido, la red de pagos autoriza el pago para el producto por la red de pagos y envía una aprobación al tercer ordenador. En algunas realizaciones, el tercer ordenador recibe la aprobación del pago para el producto, envía la aprobación a través de la red al ordenador externo, genera un tercer código de barras que contiene una recepción de pago para el producto, y publica el tercer código de barras para su visualización por el ordenador externo, en el que el tercer código de barras se explora por la cámara del primer ordenador.

En algunas realizaciones, antes de la exploración del primer código de barras por el primer ordenador, el primer ordenador y el tercer ordenador están conectados a una red. El primer ordenador recibe una segunda entrada que indica el número de tarjeta de crédito y genera, en respuesta a la recepción de la segunda entrada, una segunda carga útil encriptada que contiene el número de tarjeta de crédito. El primer ordenador transmite una solicitud de aprovisionamiento de tarjeta que incluye la segunda carga útil encriptada a través de la red. El tercer ordenador recibe la solicitud de aprovisionamiento de tarjeta a través de la red, y en respuesta a la recepción de la solicitud de aprovisionamiento de tarjeta, desencripta la segunda carga útil encriptada para obtener el número de tarjeta de crédito. El tercer ordenador envía el número de tarjeta de crédito a una aplicación de generación de testigos del tercer ordenador y, en respuesta a la recepción del número de tarjeta de crédito, genera el testigo de tarjeta de crédito por la aplicación de generación de testigos. En algunas realizaciones, el tercer ordenador graba el testigo de tarjeta de crédito en una bóveda de testigos y transmite el testigo de tarjeta de crédito a través de la red. El primer ordenador recibe el testigo de tarjeta de crédito por el sistema a través de la red y almacena el testigo de tarjeta de crédito como una función de troceo en la memoria del sistema. En algunas realizaciones, el primer ordenador es un dispositivo electrónico portátil.

De acuerdo con otro aspecto más, se proporciona un producto de programa informático para intercambiar de manera segura un testigo de tarjeta de crédito con un ordenador externo para comprar un producto. El producto de programa informático comprende un medio de almacenamiento legible por ordenador no transitorio y código de programa almacenado en el medio de almacenamiento legible por ordenador no transitorio que, cuando se ejecuta por uno o más procesadores, provoca que el uno o más procesadores exploren un primer código de barras por una cámara, donde el primer código de barras se publica después de una visualización del ordenador externo y el primer código de barras indica una pluralidad de parámetros de pago del producto. Se provoca adicionalmente que los procesadores decodifiquen el primer código de barras para extraer los parámetros de pago. Se provoca adicionalmente que los procesadores publiquen los parámetros de pago para su visualización a un usuario. Se provoca adicionalmente que los procesadores reciban una primera entrada, donde la primera entrada indica un número de tarjeta de crédito para comprar el producto, y un testigo de tarjeta de crédito que corresponde al número de tarjeta de crédito se graba en la memoria. En respuesta a la recepción de la primera entrada, se provoca adicionalmente que los procesadores generen un segundo código de barras que contiene una primera carga útil encriptada, donde la primera carga útil encriptada incluye el testigo de tarjeta de crédito. Se provoca adicionalmente que los procesadores publiquen el segundo código de barras para su visualización. El segundo código de barras es legible por un dispositivo óptico del ordenador externo.

El sumario anterior presenta un sumario simplificado para proporcionar un entendimiento básico de algunos aspectos de los sistemas y/o métodos analizados en el presente documento. Este sumario no es una vista general extensiva de los sistemas y/o métodos analizados en el presente documento. No se pretende para identificar elementos clave/críticos o para delinear el alcance de tales sistemas y/o métodos. Su único propósito es presentar algunos conceptos de una forma simplificada como un preludio a una descripción más detallada que se presenta más adelante.

Breve descripción de los dibujos

Los dibujos adjuntos, que se incorporan en y constituyen una parte de esta memoria descriptiva, ilustran diversas realizaciones de la invención y, junto con la descripción general de la invención proporcionada anteriormente, y la descripción detallada de las realizaciones proporcionadas a continuación, sirven para explicar las realizaciones de la invención.

La Figura 1 es una vista esquemática de un entorno de operación ejemplar para intercambiar un testigo de tarjeta de crédito para comprar un producto, donde el entorno de operación incluye un dispositivo cliente, un sistema de comercio, y un servidor.
La Figura 2 es una vista esquemática de un sistema informático ilustrativo de la Figura 1.
La Figura 3 es una vista esquemática del dispositivo de cliente mostrado en la Figura 1 que descarga una aplicación.
La Figura 4 es una vista esquemática del dispositivo de cliente y el sistema de comercio mostrado en la Figura 1, donde tanto el dispositivo de cliente como el sistema de comercio pueden visualizar códigos de barras únicos.

Descripción detallada

Haciendo referencia ahora a la Figura 1, un entorno de operación 10 de acuerdo con una realización de la invención puede incluir un dispositivo cliente 12, un sistema de comercio 14, y uno o más servidores 16. Como se explica en

mayor detalle a continuación, el servidor 16 puede estar en comunicación con una bóveda de testigos 18 así como con un servidor de pagos 20. Los expertos en la materia apreciarán fácilmente que la bóveda de testigos 18 es un servidor seguro donde se almacenan de manera segura los testigos y un correspondiente número de cuenta primaria (PAN). El PAN, que se encuentra típicamente entre catorce a dieciséis números de longitud, es un número de tarjeta de crédito asociada con una tarjeta de crédito del titular de la cuenta. La bóveda de testigos 18 es la única ubicación en el entorno de operación 10 en la que puede mapearse el testigo de vuelta al PAN. Además, debería apreciarse también que la bóveda de testigos 18 cumple con las especificaciones de la Norma de Seguridad de Datos de la Industria de Tarjeta de Pago (PCI-DSS). Cada uno del dispositivo de cliente 12, el sistema de comercio 14, y el servidor 16 pueden comunicarse a través de una red 26. La red 26 puede incluir una o más redes privadas o públicas (por ejemplo, la Internet) que habilitan el intercambio de datos.

El dispositivo de cliente 12 puede ser, por ejemplo, un ordenador de tableta, teléfono inteligente, o cualquier otro dispositivo informático adecuado. Se ha de apreciar que puesto que un usuario final puede eventualmente utilizar el dispositivo de cliente 12 durante el tránsito mientras está viajando, el dispositivo cliente 12 puede ser un dispositivo electrónico portátil. Es decir, el dispositivo de cliente 12 puede dimensionarse de manera que el dispositivo de cliente 12 puede llevarse en el bolso de un viajero, equipaje de mano, billetera o incluso en un bolsillo del viajero. Como se explica en mayor detalle a continuación, un usuario final puede usar el dispositivo de cliente 12 para reservar y pagar por una reserva de viaje accediendo al sistema de comercio 14. Por ejemplo, el viajero puede lanzar una aplicación de explorador, y usar la aplicación de explorador para pagar unas reservas de viajes. Se ha de apreciar que el viajero puede descargar en primer lugar una aplicación 27 a la memoria del dispositivo de cliente 12 en primer lugar antes de que pueda usarse el dispositivo de cliente 12 para reservar y pagar una reserva de viaje.

El dispositivo de cliente 12 puede incluir una cámara 22 así como una pantalla 24. La cámara 22 puede capturar imágenes. Adicionalmente, debería apreciarse también que el dispositivo de cliente 12 puede reconocer y decodificar códigos de barras que se capturan por la cámara 22. Algunos ejemplos de códigos de barras que pueden capturarse por la cámara 22 y decodificarse por el dispositivo de cliente 12 incluyen, pero sin limitación, códigos de respuesta rápida (códigos QR). La pantalla 24 del dispositivo de cliente 12 puede ser, por ejemplo, una pantalla de cristal líquido (LCD) que visualiza electrónicamente gráficos como texto, imágenes, e imágenes en movimiento.

El sistema de comercio 14 puede estar asociado con proveedor o proveedores de viajes específicos. En una realización, el sistema de comercio 14 puede incluir una aplicación 28 de comercio, un dispositivo óptico 30, y una pantalla 32. Como se explica mayor detalle a continuación, la aplicación 28 de comercio puede usarse en conjunto con el dispositivo de cliente 12 para intercambiar de manera segura un testigo de tarjeta de crédito para la compra de un producto. Se ha de apreciar que el sistema de comercio 14 puede ser móvil también. En una realización no limitante, el producto puede ser un producto de viaje tal como, por ejemplo, viaje de línea aérea, viaje de tren, viaje de ferry, habitaciones de hotel, alquiler de coches, turismo y otras actividades relacionadas con el viaje. El producto puede abarcar también no únicamente productos de viajes, sino también otros gastos relacionados con el viaje tales como, por ejemplo, cuotas de equipaje que pueden incurrirse durante el tránsito, o la mejora de una reserva de viaje existente. El dispositivo óptico 30 puede ser cualquier tipo de dispositivo para capturar imágenes tal como, por ejemplo, un escáner o una cámara web. Específicamente, el sistema de comercio 14 puede reconocer y decodificar códigos de barras que se publican en la pantalla 24 del dispositivo de cliente 12. La pantalla 32 del sistema de comercio 14 puede ser, por ejemplo, un LCD que visualiza electrónicamente gráficos como texto, imágenes, e imágenes en movimiento.

El servidor 16 puede estar en comunicación con la bóveda de testigos 18 así como con el servidor de pago 20 a través de la red 26. El servidor de pagos 20 puede estar en comunicación con una red de pagos 34 y un proveedor de servicio de pago (PSP) 36 mediante el servidor de pagos 20. Como se explica en mayor detalle a continuación, el servidor 16 puede recuperar un número de tarjeta de crédito original de la bóveda de testigos 18 basándose en el testigo de tarjeta de crédito. El servidor 16 puede recibir la autorización de la red de pagos 34 que el número de tarjeta de crédito original es válido, y confirma con el PSP 36 que el sistema de comercio 14 está de hecho autorizado a realizar un pago para comprar un producto particular.

Haciendo referencia ahora a la Figura 2, el dispositivo de cliente 12, el sistema de comercio 14, y el servidor 16 del entorno de operación 10 pueden implementarse en uno o más dispositivos o sistemas informáticos, tales como el sistema informático 40 ejemplar. El sistema informático 40 puede incluir un procesador 42, una memoria 44, un dispositivo de memoria de almacenamiento masivo 46, una interfaz de entrada/salida (E/S) 48, y una Interfaz de Hombre a Máquina (HMI) 50. El sistema informático 40 también puede acoplarse operativamente a uno o más recursos externos 52 a través de la red 26 o interfaz de E/S 48. Los recursos externos pueden incluir, pero sin limitación, servidores, bases de datos, dispositivos de almacenamiento masivo, dispositivos periféricos, servicios de red basados en la nube o cualquier otro recurso informático adecuado que puede usarse por el sistema informático 40.

El procesador 42 puede incluir uno o más dispositivos seleccionados a partir de microprocesadores, microcontroladores, procesadores de señales digitales, microordenadores, unidades de procesamiento central, campo de matrices de puertas programables, dispositivos lógicos programables, máquinas de estado, circuitos lógicos, circuitos analógicos, circuitos digitales o cualquier otro dispositivo que manipula señales (analógicas o digitales) basándose en instrucciones operacionales que se almacenan en la memoria 44. La memoria 44 puede incluir un dispositivo de una sola memoria o una pluralidad de dispositivos de memoria incluyendo, pero sin limitación, memoria

de sólo lectura (ROM), memoria de acceso aleatorio (RAM), memoria volátil, memoria no volátil, memoria de acceso aleatorio estática (SRAM), memoria de acceso aleatorio dinámica (DRAM), memoria flash, memoria caché o cualquier otro dispositivo capaz de almacenar información. El dispositivo de memoria de almacenamiento masivo 46 puede incluir dispositivos de almacenamiento de datos tal como un disco duro, unidad óptica, unidad de cinta, dispositivo de estado sólido volátil o no volátil, o cualquier otro dispositivo capaz de almacenar información.

El procesador 42 puede operar bajo el control de un sistema operativo 56 que reside en la memoria 44. El sistema operativo 56 puede gestionar recursos informáticos de modo que código de programa informático incorporado como una o más aplicaciones de software informáticas, tal como una aplicación 58 que reside en la memoria 44, puede tener instrucciones ejecutadas por el procesador 42. En una realización alternativa, el procesador 42 puede ejecutar la aplicación 58 directamente, en cuyo caso el sistema operativo 56 puede omitirse. Una o más estructuras de datos 60 también pueden residir en la memoria 44, y pueden usarse por el procesador 42, el sistema operativo 56 o la aplicación 58 para almacenar o manipular datos.

La interfaz de E/S 48 puede proporcionar una interfaz de máquina que acopla operativamente el procesador 42 a otros dispositivos y sistemas, tal como la red 26 o recurso externo 52. La aplicación 58 puede, de este modo, trabajar cooperativamente con la red 26 o el recurso externo 52 comunicando a través de la interfaz de E/S 48 para proporcionar las diversas características, funciones, aplicaciones, procesos o módulos que comprenden realizaciones de la invención. La aplicación 58 también puede tener código de programa que se ejecuta por uno o más recursos externos 52, o de otra manera basarse en funciones o señales proporcionadas por otro sistema o componentes de red externos al sistema informático 40. De hecho, dada las casi infinitas configuraciones posibles de hardware y software, los expertos en la materia entenderán que realizaciones de la invención pueden incluir aplicaciones que se ubican externamente al sistema informático 40, se distribuyen entre múltiples ordenadores u otros recursos externos 52 o se proporcionan por recursos informáticos (hardware y software) que se proporcionan como un servicio a través de la red 26, tal como un servicio de informática en la nube.

La HMI 50 puede acoplarse operativamente a el procesador 42 de sistema informático 40 de una manera conocida para permitir que un usuario interactúe directamente con el sistema informático 40. La HMI 50 puede incluir visualizadores de vídeo o alfanuméricos, una pantalla táctil, un altavoz y cualquier otro identificador de audio o visual adecuado capaz de proporcionar datos al usuario. La HMI 50 también puede incluir dispositivos de entrada y controles tal como un teclado alfanumérico, un dispositivo apuntador, teclados numéricos, botones de pulsación, botones de control, micrófonos, etc., capaces de aceptar comandos o entradas del usuario y transmitir la entrada introducida al procesador 42.

Una base de datos 54 puede residir en el dispositivo de memoria de almacenamiento masivo 46, y puede usarse para recopilar y organizar datos usados por los varios sistemas y módulos descritos en este documento. La base de datos 54 puede incluir datos y soportar estructuras de datos que almacenan y organizan los datos. En particular, la base de datos 54 puede disponerse con cualquier organización o estructura de base de datos incluyendo, pero sin limitación, una base de datos relacional, una base de datos jerárquica, una base de datos de red o combinaciones de las mismas. Puede usarse un sistema de gestión de base de datos en forma de una aplicación de software informática, que se ejecuta como instrucciones en el procesador 42, para acceder a la información o datos almacenados en registros de la base de datos 54 en respuesta a una consulta, en el que una consulta puede determinarse dinámicamente y ejecutarse por el sistema operativo 56, otras aplicaciones 58 o uno o más módulos.

Volviendo a hacer referencia ahora a la Figura 3, el dispositivo de cliente 12 puede descargar la aplicación 27 a su memoria. Específicamente, el dispositivo de cliente 12 puede conectarse a un servidor de aplicación 70 a través de la red 26, y descargar la aplicación 27 a la memoria del dispositivo de cliente 12. Como se observa en la Figura 3 un certificado público (certificado PubA) puede estar asociado con la aplicación 27. Una vez que se ha descargado satisfactoriamente la aplicación 27, un usuario final, tal como un viajero, puede crear un código de paso. El código de paso puede requerirse para conseguir acceso a la aplicación 27. En una realización, el código de paso puede introducirse manualmente en el dispositivo de cliente 12 usando un teclado (no ilustrado). Sin embargo, los expertos en la materia apreciarán que pueden usarse también otros enfoques para introducir el código de paso también. En una realización, el código de paso puede ser necesario que se introduzca dos veces para evitar escritura incorrecta accidental. Una vez que se crea el código de paso, al código de paso puede aplicarse una función de troceo y almacenarse en la memoria del dispositivo de cliente 12 para uso futuro. Los expertos en la materia apreciarán que aplicar función de troceo a contraseñas toma una contraseña de longitud variable y crea una contraseña de longitud fija críptica basada en la contraseña de longitud variable original.

El dispositivo de cliente 12 puede generar también un par de claves asimétricas, (PubP, PrivP). PubP representa la clave pública, y PrivP representa una clave privada. La criptografía asimétrica, que también se denomina como criptografía de clave pública, es un sistema criptográfico que usa un par de claves. En concreto, la clave pública PubP puede diseminarse de manera amplia, y la clave privada (PrivP), puede tener acceso controlado usando el código de paso. Las claves asimétricas se almacenan en la memoria del dispositivo de cliente 12.

Una vez que se almacena la aplicación 27 y las claves asimétricas en la memoria del dispositivo de cliente 12, el usuario final puede registrarse en la aplicación 27. Específicamente, el usuario final puede registrarse en la aplicación

27 e introducir el código de paso. Si el código de paso troceado introducido por el usuario coincide con el troceo previamente almacenado grabado en la memoria del dispositivo de cliente 12, a continuación se concede el acceso a la clave privada PrivP, y se concede el acceso a operaciones adicionales. Específicamente, el usuario final puede registrar ahora una o más tarjetas de crédito que pueden usarse para comprar un producto tal como, por ejemplo, tique de línea aérea usando la aplicación 27. Las tarjetas de crédito está cada una asociada con un número de tarjeta de crédito único.

Haciendo referencia de vuelta a la Figura 1, se ha de apreciar que el dispositivo de cliente 12 debe tener conectividad a la red 26 antes de que pueda registrarse la tarjeta de crédito. El registro de una tarjeta de crédito única usando la aplicación 27 del dispositivo de cliente 12 deberá ahora explicarse. En primer lugar, el usuario final puede seleccionar una opción para registrar un nuevo número de tarjeta de crédito usando el dispositivo de cliente 12. Por ejemplo, el usuario final puede seleccionar una opción tal como, por ejemplo, "Registrar tarjeta" en un menú que se visualiza en la pantalla 24 del dispositivo de cliente 12. El usuario final puede a continuación introducir el número de tarjeta de crédito y otros detalles de tarjeta de crédito usando un teclado u otra interfaz de usuario del dispositivo de cliente 12. Sin embargo, se ha de apreciar que pueden usarse otros enfoques también para introducir información de tarjeta de crédito tal como, por ejemplo, tomar una foto de la tarjeta de crédito real y analizar a continuación la foto a través de tecnología de Reconocimiento Óptico de Caracteres (OCR). Algunos ejemplos de otros detalles de tarjeta de crédito incluyen, pero sin limitación, una fecha de caducidad asociada con la tarjeta, el nombre del titular de la tarjeta primaria, la dirección del titular de la tarjeta primaria, y el valor de verificación de tarjeta (CVV) asociado con la tarjeta de crédito. Una vez que el usuario final ha introducido el número de tarjeta de crédito y los detalles de tarjeta de crédito asociados, puede ejecutarse una comprobación de tarjeta de crédito por la aplicación 27 para confirmar la fecha de caducidad. La aplicación 27 puede ejecutar también un algoritmo de Luhn, que es una fórmula de suma de comprobación usada para validar el número de tarjeta de crédito para números de tarjeta de crédito escritos incorrectamente.

Una vez que se verifica el número de tarjeta de crédito y los detalles de tarjeta de crédito asociados, la aplicación 27 del dispositivo de cliente 12 puede crear una carga útil encriptada, que se denomina como la carga útil de aprovisionamiento de tarjeta. Específicamente, la aplicación 27 del dispositivo de cliente 12 puede obtener el certificado público PubA. La aplicación 27 puede a continuación generar una clave simétrica S1 y su vector inicial asociado I1. La clave simétrica S1 y el vector inicial I1 pueden concatenarse, y a continuación firmarse por la clave privada (PrivP) para obtener $(S1, I1)^*_P$, donde "*" indica que el valor está firmado. La aplicación 27 puede a continuación concatenar la clave simétrica S1, el vector inicial I1, y $(S1, I1)^*_P$, y a continuación encriptar estos valores usando el certificado público PubA basándose en el esquema de relleno de Relleno de Encriptación Asimétrico Óptico (OAEP) para obtener $(S1, I1, (S1, I1)^*_P)'_A$, donde "'" indica que el valor está encriptado.

La aplicación 27 del dispositivo de cliente 12 puede a continuación firmar el número de tarjeta de crédito, que se indica en el presente documento como N, con la clave privada PrivP para obtener la firma N^*_P. El número de tarjeta de crédito N puede a continuación concatenarse con la firma N^*_P y encriptarse con la clave simétrica S1 para obtener $(N, N^*_P)'_{S1}$. Finalmente, la aplicación 27 del dispositivo de cliente 12 puede concatenar el certificado de la clave pública PubP, el resultado del cual se denomina certP, junto con $(S1, I1, (S1, I1)^*_P)'_A$ y $(N, N^*_P)'_{S1}$. El resultado es la carga útil de aprovisionamiento de tarjeta. El dispositivo de cliente 12 puede enviar la carga útil de aprovisionamiento de tarjeta al servidor 16 a través de la red 26 como parte de una solicitud de aprovisionamiento de tarjeta.

En respuesta a la recepción de la solicitud de aprovisionamiento de tarjeta, el servidor 16 puede extraer la carga útil de aprovisionamiento de tarjeta y a continuación desencriptar la carga útil de aprovisionamiento de tarjeta para obtener el número de tarjeta de crédito N. Específicamente, el servidor 16 puede a continuación obtener la clave simétrica S1, el vector inicial I1, y $(S1, I1)^*_P$ y desencriptar cada uno de estos valores con un certificado privado PrivA. El certificado privado PrivA es la clave privada asociada con el certificado público PubA, y el certificado público PubA y el certificado privado PrivA se generan antes de que se grabe la aplicación 27 en el servidor de aplicación 70. El servidor 16 puede a continuación verificar la firma de $(S1, I1)^*_P$ de la clave simétrica S1 y el vector inicial I1 usando el certificado concatenado de la clave pública certP. El servidor 16 puede a continuación obtener el número de tarjeta de crédito N y N^*_P y desencriptar ambos de estos valores usando la clave simétrica S1. La firma N^*_P del número de tarjeta de crédito N puede a continuación verificarse usando el certificado concatenado de la clave pública certP.

El servidor 16 puede a continuación enviar el número de tarjeta de crédito N a una aplicación de generación de testigos 74. La aplicación de generación de testigos 74 puede a continuación generar el testigo de tarjeta de crédito T basándose en el número de tarjeta de crédito único N. Los expertos en la materia apreciarán fácilmente que los testigos pueden no usarse fuera del contexto de una transacción única específica con un comerciante particular. La aplicación de testigo 74 puede a continuación enviar el testigo de tarjeta de crédito T de vuelta al servidor 16. La aplicación de testigo 74 puede enviar también el testigo T así como el número de tarjeta de crédito único N a la bóveda de testigos 18. La bóveda de testigos 18 es la única ubicación en el entorno de operación 10 en la que el testigo de tarjeta de crédito T se mapea de vuelta al número de tarjeta de crédito único N.

En respuesta a la recepción del testigo de tarjeta de crédito T de la aplicación de generación de testigos 74, el servidor 16 puede a continuación generar una clave simétrica S2 y su vector inicial I2. En una realización, la clave simétrica S2 está basada en la norma de encriptación avanzada de 128 bits usando el modo de encadenamiento de bloque de cifrado de encriptación (AES 128 CBC). El servidor 16 puede a continuación concatenar la clave simétrica S2 y el

vector inicial I2, y a continuación firmar el valor con el certificado privado PrivA para obtener $(S2, I2)^*_A$. El servidor 16 puede a continuación concatenar la clave simétrica S2, el vector inicial I2, y $(S2, I2)^*_A$ encriptarlos con la clave pública PubP basándose en el esquema de relleno de OAEP para obtener $(S2, I2, (S2, I2)^*_A)'_P$. El servidor 16 puede a continuación firmar el testigo de tarjeta de crédito T con el certificado privado PrivA para obtener un testigo firmado T^*_A. El servidor 16 puede a continuación concatenar el testigo T con el testigo firmado T^*_A, y encripta ambos valores con la clave simétrica S2 para obtener $(T, T^*_A)'_{S2}$. Finalmente, el servidor 16 puede concatenar a continuación $(S2, I2, (S2, I2)^*_a)'_p$ y $(T, T^*_A)'_{S2}$. La carga útil resultante se envía en una respuesta de aprovisionamiento de tarjeta 76 de vuelta a través de la red 26 al dispositivo de cliente 12.

En respuesta a la recepción de la respuesta de aprovisionamiento de tarjeta 76, la aplicación 27 del dispositivo de cliente 12 puede verificar un certificado concatenado del certificado privado PrivA, que se denomina como certA, con claves ancladas. Los expertos en la materia apreciarán que las claves ancladas son un mecanismo de seguridad para resistir la suplantación por atacantes que usan certificados fraudulentos. La aplicación 27 del dispositivo de cliente 12 puede a continuación obtener la clave simétrica S2, el vector inicial I2, y la firma $(S2, I2)^*_A$, y desencripta estos valores con la clave privada PrivP. La aplicación del dispositivo de cliente 12 puede a continuación verificar la firma $(S2, I2)^*_A$ de la clave simétrica S2 y el vector inicial I2 con el certificado concatenado del certificado privado certA. La aplicación 27 del dispositivo de cliente 12 puede a continuación obtener el testigo de tarjeta de crédito T así como el testigo firmado T^*_A, y desencripta estos valores usando la clave simétrica S2. La aplicación 27 del dispositivo de cliente 12 puede a continuación verificar el testigo firmado T^*_A del testigo de tarjeta de crédito T con el certificado concatenado del certificado privado certA. Finalmente, después se verifica el testigo firmado T^*_A, el testigo de tarjeta de crédito T puede almacenarse en la memoria del dispositivo de cliente 12.

Se ha de apreciar que el dispositivo de cliente 12 almacena el testigo de tarjeta de crédito T en su respectiva memoria, y ese testigo de tarjeta de crédito puede usarse un momento posterior durante una transacción de pago. Si el usuario final está viajando y está situado en un país extranjero u otra ubicación donde el servicio celular no está disponible o es costoso debido a cobros de itinerancia, el usuario final no necesita conectividad de red para pagar por una reserva de viaje específica, puesto que el testigo de tarjeta de crédito del usuario final T ya se ha almacenado en memoria. Adicionalmente, debería apreciarse también que puede grabarse más de un testigo de tarjeta de crédito en la memoria del dispositivo de cliente 12, donde cada testigo de tarjeta de crédito corresponde a una tarjeta de crédito única. Por ejemplo, volviendo ahora a la Figura 4, el dispositivo de cliente 12 tiene dos números de tarjeta de crédito 80 visualizados en la pantalla 24. Se ha de apreciar que únicamente los últimos cuatro dígitos del número de tarjeta de créditos 80 son visibles para el usuario final, y el número de tarjeta de crédito completo no se almacena en la memoria del dispositivo de cliente 12.

Durante el viaje, el usuario final puede necesitar pagar por una reserva de viaje y/u otros imprevistos relacionados tales como, por ejemplo, cargos por exceso de equipaje. En la realización ejemplar como se muestra en la Figura 4, el usuario final puede necesitar pagar cargos por exceso de equipaje, que cuestan cincuenta euros. Sin embargo, se ha de apreciar que la realización como se muestra en la Figura 4 es simplemente ejemplar en su naturaleza y que pueden comprarse también diversos otros productos y cargos. Haciendo referencia ahora a ambas de las Figuras 1 y 4, un agente puede a continuación verificar que el usuario final desea pagar por el producto (por ejemplo, los cincuenta euros por los cargos por exceso de equipaje) usando una de las tarjetas de crédito que tiene su correspondiente testigo de tarjeta de crédito T grabado en la memoria del dispositivo de cliente 12. Una vez que se confirma esto, el agente puede usar a continuación un teclado u otro dispositivo de entrada del sistema de comercio 14 (no ilustrado) para indicar que el usuario final desea pagar por el producto usando su dispositivo cliente 12.

En respuesta a la recepción de la indicación del agente, la aplicación de comercio 28 del sistema de comercio 14 puede enviar una solicitud al servidor 16 a través de la red 26. La solicitud enviada al servidor 16 es para un código de barras 82, o una carga útil de código de barras, que indica una pluralidad de parámetros de pago con respecto al producto. En la realización ejemplar como se muestra en la Figura 4 el código de barras 82 es un código de QR; sin embargo, se ha de apreciar que pueden generarse también otros tipos de códigos de barras. En una realización, los parámetros de pago pueden incluir, pero sin limitación, una cantidad monetaria de propiedad (por ejemplo, cincuenta euros), un tipo específico de divisa en la que esté basada la cantidad monetaria (por ejemplo, euros), una descripción del producto (por ejemplo, cargos por exceso de equipaje), y una identificación (ID) de referencia de pago.

En respuesta a la recepción de la solicitud del sistema de comercio 14, el servidor 16 puede a continuación confirmar con el PSP 36 que el sistema de comercio 14 está de hecho autorizado a realizar un pago usando el código de barras 82. Si el sistema de comercio 14 está autorizado a realizar un pago usando el código de barras 82, a continuación el PSP 36 puede generar el código de barras 82. El código de barras 82 puede codificarse con un par de claves asimétricas temporales. El PSP 36 puede a continuación enviar una autorización al servidor 16. La autorización incluye el código de barras 82. En respuesta a la recepción de la autorización del PSP 36, el servidor 16 puede a continuación enviar el código de barras 82 a través de la red 26 al sistema de comercio 14. En respuesta a la recepción del código de barras 82, la aplicación 28 del sistema de comercio 14 puede publicar el código de barras 82 en su correspondiente pantalla 24.

Una vez que se publica el código de barras 82 en la pantalla 24 del sistema de comercio 14, el usuario final puede a continuación situar el dispositivo de cliente 12 de manera que la cámara 22 pueda explorar el código de barras 82. Se

ha de apreciar que el usuario final ya se ha registrado en la aplicación 27 del dispositivo de cliente 12, y ha introducido satisfactoriamente el código de paso. El dispositivo de cliente 12 puede a continuación decodificar el código de barras 82 para extraer los parámetros de pago. El dispositivo de cliente 12 puede a continuación publicar los parámetros de pago en su pantalla 24. Por ejemplo, como se observa en la Figura 4, los parámetros de pago indican que se requieren cincuenta euros para el pago de cargos por exceso de equipaje. El dispositivo de cliente 12 puede publicar también los dos números de tarjeta de crédito 80 que tienen sus correspondientes testigos de tarjeta de crédito T grabados en la memoria del dispositivo de cliente 12.

El usuario final puede a continuación seleccionar o introducir qué número de tarjeta de crédito 80 debe usarse para comprar el producto usando el dispositivo de cliente 12. En una realización, el usuario final puede usar también un número de tarjeta de crédito 80 por defecto que está preseleccionado en el momento del pago, o pueden utilizarse reglas más complejas para la selección automática de un número de tarjeta de crédito particular. En el caso de que únicamente un único número de tarjeta de crédito 80 tenga un correspondiente testigo de tarjeta de crédito T grabado en memoria, entonces el usuario final puede simplemente necesitar confirmar que debe usarse el único número de tarjeta de crédito 80. En respuesta a la recepción de una confirmación del usuario final, la aplicación 17 del dispositivo de cliente 12 puede a continuación generar otro código de barras 84. En la realización ejemplar como se muestra en la Figura 4, el código de barras 84 es también un código de QR; sin embargo se ha de entender que pueden usarse también otros tipos de códigos de barras. El código de barras 84 incluye una carga útil encriptada. La generación de la carga útil encriptada se describe a continuación.

La aplicación 27 del dispositivo de cliente 12 puede generar en primer lugar una clave simétrica S3 y su vector inicial 13. La aplicación 27 del dispositivo de cliente 12 puede a continuación concatenar tanto la clave simétrica S3 como el vector inicial 13 y firmar el resultado con la clave privada PrivP para obtener $(S3, I3)^*_P$. La clave simétrica S3, el vector inicial 13, y $(S3, I3)^*_p$ pueden a continuación encriptarse con el certificado público PubA basándose en el esquema de relleno de OAEP para obtener $(S3, I3, (S3, I3)^*_P)'_A$. La aplicación 27 del dispositivo de cliente 12 puede a continuación crear una carga útil L. Específicamente, la carga útil L puede incluir $(S3, I3, (S3, I3)^*_P)'_A$ y el testigo de tarjeta de crédito T. La carga útil L se firma a continuación con la clave privada PrivP para obtener L^*_P. La carga útil L y la carga útil firmada L^*_P se firman a continuación con la clave simétrica S3 para obtener $(L, L^*_P)'_{S3}$. Finalmente, el certificado concatenado de la clave pública certP, $(S3, I3, (S3, I3)^*_P)'_A$ y $(L, L^*_P)'_{S3}$ se concatenan para crear la carga útil encriptada.

La aplicación 27 del dispositivo de cliente 12 puede a continuación publicar el código de QR 84 en su pantalla 24. Una vez que el usuario final observa que el código de QR 84 ha publicado en la pantalla 24 del dispositivo de cliente 12, el usuario final puede a continuación ubicar el dispositivo de cliente 12 de manera que el código de QR 84 puede leerse por el dispositivo óptico 30 del sistema de comercio 14 usando comunicación de luz visible. El sistema de comercio 14 puede a continuación enviar el código de QR 84, o la carga útil del código de QR, a través de la red 26 al servidor 16. El servidor 16 puede a continuación decodificar y validar la carga útil encriptada contenida por el código de QR 84. Específicamente, el servidor 16 puede validar la carga útil encriptada para obtener el testigo de tarjeta de crédito T. Se ha de apreciar que antes de la validación, puede cancelarse la transacción. Por lo tanto, no puede realizarse pago usando la tarjeta de crédito del usuario final.

El servidor 16 puede validar la carga útil encriptada obteniendo la clave simétrica S3, el vector inicial I3, y $(S3, I3)^*_P$, y desencripta estos valores usando el certificado privado PrivA. El servidor 16 puede a continuación verificar la firma $(S3, I3)^*_P$ de la clave simétrica S3 y el vector inicial I3 usando el certificado concatenado de la clave pública certP para obtener la carga útil L y la carga útil firmada L^*_P. La carga útil firmada L^*_P se verifica a continuación por el certificado concatenado de la clave pública certP. Validar la carga útil encriptada permite que el servidor 16 recupere el número de tarjeta de crédito original N de la bóveda de testigos 18.

Una vez que se ha recibido el número de tarjeta de crédito original N, el servidor 16 puede a continuación realizar una autorización de pago para obtener la aprobación del emisor de la tarjeta de crédito. Específicamente, el servidor 16 puede enviar una consulta a través de la red 26 a la red de pagos 34 para determinar si el número de tarjeta de crédito N es válido y se concede la aprobación del emisor de la tarjeta de crédito para hacer un pago. La red de pagos 34 puede enviar una autorización a través de la red 26 y de vuelta al servidor 16. En respuesta a la recepción de la autorización de pago de la red de pagos, el servidor 16 puede a continuación enviar una respuesta a través de la red 26 al sistema de comercio 14. La respuesta indica que el número de tarjeta de crédito N es válido y que se ha confirmado el pago por el emisor de la tarjeta de crédito.

En respuesta a la recepción de la respuesta del servidor 16, el sistema de comercio 14 puede a continuación generar una recepción de pago. En particular, la aplicación 28 de comercio del sistema de comercio 14 puede a continuación generar una recepción de pago que está contenida en un código de barras (no ilustrado). El código de barras puede publicarse en la pantalla 32 del sistema de comercio 14. El usuario final puede a continuación ubicar el dispositivo de cliente 12 de manera que la cámara 22 puede explorar el código de barras publicado en la pantalla 32 del sistema de comercio 14.

Haciendo referencia en general a las figuras, el sistema desvelado proporciona un enfoque conveniente fácil de usar para que el dispositivo de cliente se comunique con el sistema de comercio, incluso cuando el dispositivo de cliente

tiene conectividad de red limitada o ninguna. Se ha de apreciar que un viajero puede no poder conectarse a Internet durante el tránsito, especialmente cuando él o ella pueden estar visitando países o áreas extranjeras del mundo donde la conectividad de red es limitada o no existente. De hecho, el sistema desvelado utiliza el hardware existente en un dispositivo cliente (por ejemplo, la cámara) para explorar y decodificar un código de barras que se publica en la pantalla del sistema de comercio. El sistema desvelado proporciona un enfoque más eficaz para que un viajero pague una reserva de viaje sin la necesidad de su tarjeta de crédito física. En otras palabras, los viajeros pueden ya no necesitar ubicar su tarjeta de crédito física, que puede ser difícil de ubicar especialmente si un viajero está llevando numerosas maletas en tránsito. Finalmente, las tarjetas corporativas, pueden usarse también tarjetas compartidas, millas de viajero frecuente, o incluso tarjetas de crédito virtuales.

En general, las rutinas ejecutadas para implementar las realizaciones de la invención, ya se implementen como parte de un sistema operativo o una aplicación, componente, programa, objeto, módulo o secuencia de instrucciones específico, o incluso un subconjunto de los mismos, se pueden denominar en el presente documento "código de programa informático" o simplemente "código de programa". Código de programa habitualmente comprende instrucciones legibles por ordenador que están residentes en diversas veces en diversos dispositivos de memoria y de almacenamiento en un ordenador y que, cuando se leen y ejecutan por uno o más procesadores en un ordenador, provocan que ese ordenador realice las operaciones necesarias para ejecutar operaciones y/o elementos que incorporan los diversos aspectos de las realizaciones de la invención. Instrucciones de programa legibles por ordenador para efectuar operaciones de las realizaciones de la invención pueden ser, por ejemplo, lenguaje de ensamblaje o bien código fuente o bien código objeto escrito en cualquier combinación de uno o más lenguajes de programación.

Diverso código de programa descrito en este documento puede identificarse basándose en la aplicación dentro de la que se implementa en realizaciones específicas de la invención. Sin embargo, debería apreciarse que cualquier nomenclatura de programa particular a continuación se usa meramente para conveniencia y, por lo tanto, la invención no debería limitarse a usar solamente en cualquier aplicación especificada identificada y/o implícita por tal nomenclatura. Adicionalmente, dado el número generalmente infinito de maneras en las que pueden organizarse programas informáticos en rutinas, procedimientos, métodos, módulos, objetos y similares, así como las diversas maneras en las que la funcionalidad de programa puede asignarse entre diversas capas de software que están residentes dentro de un ordenador típico (por ejemplo, sistemas operativos, librerías, API, aplicaciones, subprogramas, etc.), debería apreciarse que las realizaciones de la invención no se limitan a la organización específica y asignación de funcionalidad de programa descritas en este documento.

El código de programa incorporado en cualquiera de las aplicaciones/módulos descritos en este documento se puede distribuir individual o colectivamente como un producto de programa en una diversidad de diferentes formas. En particular, el código de programa puede distribuirse usando un medio de almacenamiento legible por ordenador que tienen instrucciones de programa legibles por ordenador en el mismo para provocar que un procesador efectúe aspectos de las realizaciones de la invención.

Medio de almacenamiento legible por ordenador, que es inherentemente no transitorio, puede incluir medio tangible volátil y no volátil y extraíble y no extraíble implementado en cualquier método o tecnología para almacenamiento de información, tal como instrucciones legibles por ordenador, estructuras de datos, módulos de programa, u otros datos. Medio de almacenamiento legible por ordenador puede incluir adicionalmente RAM, ROM, memoria de sólo lectura borrable y programable (EPROM), memoria de sólo lectura eléctricamente programable borrable (EEPROM), memoria flash u otra tecnología de memoria de estado sólido, memoria de sólo lectura de disco compacto portátil (CD-ROM), u otro almacenamiento óptico, cintas magnéticas, cinta magnética, almacenamiento de disco magnético u otros dispositivos de almacenamiento magnético, o cualquier otro medio que puede usarse para almacenar la información deseada y que puede leerse por un ordenador. Un medio de almacenamiento legible por ordenador no debería interpretarse como señales transitorias en sí (por ejemplo, ondas de radio u otras ondas electromagnéticas que se propagan, ondas electromagnéticas que se propagan a través de un medio de transmisión tal como una guía de ondas, o señales eléctricas transmitidas a través de un alambre). Instrucciones de programa legibles por ordenador pueden descargarse a un ordenador, otro tipo de aparato de procesamiento de datos programable, u otro dispositivo desde un medio de almacenamiento legible por ordenador o a un ordenador externo o dispositivo de almacenamiento externo a través de una red.

Pueden usarse instrucciones de programa legibles por ordenador almacenadas en un medio legible por ordenador para dirigir un ordenador, otros tipos de aparato de procesamiento de datos programable, u otros dispositivos para funcionar de una manera particular, de manera que las instrucciones almacenadas en el medio legible por ordenador producen un artículo de fabricación que incluye instrucciones que implementan las funciones, actos y/u operaciones especificadas en los diagramas de flujo, diagramas de secuencia y/o diagramas de bloques. Las instrucciones de programa informáticas pueden proporcionarse a uno o más procesadores de un ordenador de fin general, un ordenador de fin especial, u otro aparato de procesamiento de datos programable para producir una máquina, de tal forma que las instrucciones, que se ejecutan a través del uno o más procesadores, provocan que se realicen una serie de cálculos para implementar las funciones, actos y/u operaciones especificados en el diagrama de flujos, diagrama de secuencias y/o diagramas de bloque.

En ciertas realizaciones alternativas, las funciones, actos y/u operaciones especificados en el diagrama de flujos, diagrama de secuencias y/o diagramas de bloque pueden reordenarse, procesarse en serie y/o procesarse simultáneamente consistentes con realizaciones de la invención. Además, cualquiera del diagrama de flujos, diagrama de secuencias y/o diagramas de bloque puede incluir más o menos bloques que los ilustrados consistentes con realizaciones de la invención.

La terminología usada en este documento es para el propósito de describir únicamente realizaciones particulares y no se pretende que sea limitante de las realizaciones de la invención. Como se usa en el presente documento, las formas singulares "un", "una" y "el", "la" se pretende que incluyan las formas plurales también, a menos que el contexto lo indique claramente lo contrario. Se entenderá adicionalmente que los términos "comprende" y/o "que comprende", cuando se usan en esta memoria descriptiva, especifican la presencia de características establecidas, elementos integrantes, etapas, operaciones, elementos, y/o componentes, pero no excluyen la presencia o adición de una o más otras características, elementos integrantes, etapas, operaciones, elementos, componentes, y/o grupos de los mismos. Asimismo, en la medida en la que las expresiones "incluye", "teniendo/que tiene", "tiene", "con", "compuesto por" o variantes de las mismas se usan o bien en la descripción detallada o bien en las reivindicaciones, se pretende que tales expresiones sean inclusivas de una manera similar a la expresión "comprendiendo/que comprende".

Mientras toda la invención se ha ilustrado mediante una descripción de diversas realizaciones y mientras estas realizaciones se han descrito en considerable detalle, no es la intención del solicitante restringir o de cualquier forma limitar el alcance de las reivindicaciones adjuntas a tal detalle. A los expertos en la materia se les ocurrirán fácilmente ventajas y modificaciones adicionales. Por lo tanto, la invención no está limitada, en sus aspectos más amplios, a los detalles específicos, aparato y método representativos y ejemplos ilustrativos mostrados y descritos. Por consiguiente, pueden hacerse desviaciones de tales detalles sin alejarse del espíritu o alcance del concepto inventivo general del solicitante.

REIVINDICACIONES

1. Un sistema (10) para intercambiar de manera segura un testigo de tarjeta de crédito (T) entre un primer ordenador (12) y un ordenador externo (14) para comprar un producto, comprendiendo el sistema (10):

el ordenador externo (14);
el primer ordenador (12) con uno o más procesadores, una cámara (22) acoplada al uno o más procesadores, y una memoria acoplada al uno o más procesadores, almacenando la memoria datos que comprenden una base de datos y código de programa que, cuando se ejecuta por el uno o más procesadores, provoca al sistema (10):

explorar un primer código de barras (82) por la cámara (22), en el que el primer código de barras (82) se publica en un visor (24) del ordenador externo (14) y el primer código de barras (82) indica una pluralidad de parámetros de pago del producto;
decodificar el primer código de barras (82) para extraer los parámetros de pago;
publicar los parámetros de pago para visualizar a un usuario;
recibir una primera entrada, en el que la primera entrada indica un número de tarjeta de crédito (80) para comprar el producto;
en respuesta a la recepción de la primera entrada, generar un segundo código de barras (84) que contiene una primera carga útil encriptada, en el que la primera carga útil encriptada incluye un testigo de tarjeta de crédito (T) que corresponde al número de tarjeta de crédito (80), en el que el testigo de tarjeta de crédito (T) se almacena en la memoria;
y publicar el segundo código de barras (84) para su visualización, en el que el segundo código de barras (84) es legible por un dispositivo óptico (30) del ordenador externo (14),

en el que antes de la exploración del primer código de barras (82) por la cámara (22), el primer ordenador (12) y un tercer ordenador (16) están conectados a una red (26), en el que el primer ordenador (12) está dispuesto para:

recibir una segunda entrada que indica el número de tarjeta de crédito (80);
generar una segunda carga útil encriptada que contiene el número de tarjeta de crédito (80) en respuesta a la recepción de la segunda entrada;
transmitir una solicitud de aprovisionamiento de tarjeta que incluye la segunda carga útil encriptada a través de la red (26),

en el que el tercer ordenador (16) está dispuesto para:

recibir la solicitud de aprovisionamiento de tarjeta a través de la red (26);
desencriptar, en respuesta a la recepción de la solicitud de aprovisionamiento de tarjeta, la segunda carga útil encriptada para obtener el número de tarjeta de crédito (80), enviar el número de tarjeta de crédito (80) a una aplicación de generación de testigos (74),

en el que, en respuesta a la recepción del número de tarjeta de crédito (80), la aplicación de generación de testigos (74) genera el testigo de tarjeta de crédito (T),
en el que el testigo de tarjeta de crédito (T) se graba en una bóveda de testigos (18) y también se transmite a través de la red (26) desde el tercer ordenador (16) de vuelta al primer ordenador (12), y
en el que el primer ordenador (12) está dispuesto para almacenar el testigo de tarjeta de crédito (T) en la memoria.

2. El sistema (10) de la reivindicación 1, que comprende adicionalmente:

el tercer ordenador (16) en comunicación con el ordenador externo (14), en el que el ordenador externo (14) está dispuesto para enviar el segundo código de barras (82) al tercer ordenador (16); y
la bóveda de testigos (18) en comunicación con el tercer ordenador (16);
en el que el tercer ordenador (16) está dispuesto para decodificar el segundo código de barras (82), para validar contenido de la primera carga útil encriptada para obtener el testigo de tarjeta de crédito (T), y para recuperar un número de tarjeta de crédito original (N) de la bóveda de testigos (18) basándose en el testigo de tarjeta de crédito (T).

3. El sistema (10) de la reivindicación 2, en el que el tercer ordenador (16) está dispuesto para comunicarse con una red de pagos (34) para determinar si el número de tarjeta de crédito original (N) es válido, y en respuesta a que el número de tarjeta de crédito original (N) sea válido, la red de pagos (34) autoriza un pago para el producto y envía una aprobación al tercer ordenador (16).

4. El sistema (10) de la reivindicación 3, en el que el ordenador externo (14) está dispuesto para recibir la aprobación del tercer ordenador (16) para el pago para el producto, para generar un tercer código de barras que contiene una recepción de pago para el producto, y para publicar el tercer código de barras para su visualización, en el que el tercer código de barras se explora por la cámara (22).

5. El sistema (10) de cualquiera de las reivindicaciones 1 a 4, en el que el uno o más procesadores son parte de un dispositivo electrónico portátil.

6. Un método para intercambiar de manera segura un testigo de tarjeta de crédito (T) entre un primer ordenador (12) y un ordenador externo (14) para comprar un producto, comprendiendo el método:

explorar un primer código de barras (82) por una cámara (22) de un primer ordenador (12), en el que el primer código de barras (82) se publica en un visor (24) del ordenador externo (14) y el primer código de barras (82) indica una pluralidad de parámetros de pago del producto;
decodificar el primer código de barras (82), por el primer ordenador (12), para extraer los parámetros de pago;
publicar los parámetros de pago para su visualización por un usuario por el primer ordenador (12);
recibir una primera entrada por el primer ordenador (12), en el que la primera entrada indica un número de tarjeta de crédito (80) para comprar el producto;
en respuesta a la recepción de la primera entrada, generar, por el primer ordenador (12), un segundo código de barras (84) que contiene una primera carga útil encriptada, en el que la primera carga útil encriptada incluye un testigo de tarjeta de crédito (T) que corresponde al número de tarjeta de crédito (80), en el que el testigo de tarjeta de crédito (T) se almacena en una memoria del primer ordenador (12); y
publicar el segundo código de barras (84) para su visualización por el primer ordenador (12), en el que el segundo código de barras (84) es legible por un dispositivo óptico (30) del ordenador externo (14),
en el que el método comprende adicionalmente:

antes de la exploración del primer código de barras (82) por el primer ordenador (12), conectar el primer ordenador (12) y un tercer ordenador (16) a una red (26);
recibir, por el primer ordenador (12), una segunda entrada que indica el número de tarjeta de crédito (80);
en respuesta a la recepción de la segunda entrada, generar, por el primer ordenador (12), una segunda carga útil encriptada que contiene el número de tarjeta de crédito (80);
transmitir, por el primer ordenador (12), una solicitud de aprovisionamiento de tarjeta que incluye la segunda carga útil encriptada a través de la red (26);
recibir la solicitud de aprovisionamiento de tarjeta, por el tercer ordenador (16), a través de la red (26);
en respuesta a la recepción de la solicitud de aprovisionamiento de tarjeta, desencriptar la segunda carga útil encriptada para obtener el número de tarjeta de crédito (80) por el tercer ordenador (16);
enviar el número de tarjeta de crédito (16) a una aplicación de generación de testigos (74) por el tercer ordenador (16); y
en respuesta a la recepción del número de tarjeta de crédito (80), generar el testigo de tarjeta de crédito (T) por la aplicación de generación de testigos (74),

en el que el método comprende adicionalmente:

grabar el testigo de tarjeta de crédito (T) en una bóveda de testigos (18) por el tercer ordenador (16);
transmitir, por el tercer ordenador (16), el testigo de tarjeta de crédito (T) a través de la red (26);
recibir el testigo de tarjeta de crédito (T) por el primer ordenador (12) a través de la red (26); y
almacenar el testigo de tarjeta de crédito (T) en la memoria del primer ordenador (12).

7. El método de la reivindicación 6, que comprende adicionalmente:

enviar, por el ordenador externo (14), el segundo código de barras (84) a través de la red (26) al tercer ordenador (16);
decodificar, por el tercer ordenador (16), el segundo código de barras (84);
validar contenido de la primera carga útil encriptada, por el tercer ordenador (16), para obtener el testigo de tarjeta de crédito (T); y
recuperar, por el tercer ordenador (16), un número de tarjeta de crédito original (N) de la bóveda de testigos (18) basándose en el testigo de tarjeta de crédito (T).

8. El método de la reivindicación 7, que comprende adicionalmente:

enviar una comunicación a una red de pagos (34) por el tercer ordenador (16);
en respuesta a la recepción de la comunicación, determinar si el número de tarjeta de crédito original (N) es válido por la red de pagos (34);
en respuesta a que el número de tarjeta de crédito original (N) sea válido, autorizar un pago para el producto por la red de pagos (34); y
enviar una aprobación al tercer ordenador (16) por la red de pagos (34).

9. El método de la reivindicación 8, que comprende adicionalmente:

recibir, por el tercer ordenador (16), la aprobación para el pago para el producto;
enviar la aprobación a través de la red (26) al ordenador externo (14);

generar, por el ordenador externo (14), un tercer código de barras que contiene una recepción de pago para el producto; y
publicar el tercer código de barras para su visualización por el ordenador externo (14), en el que el tercer código de barras se explora por la cámara (22) del primer ordenador (12).

10. El método de cualquiera de las reivindicaciones 6 a 9, en el que el primer ordenador (12) es un dispositivo electrónico portátil.

11. Un producto de programa informático para intercambiar de manera segura un testigo de tarjeta de crédito (T) con un ordenador externo (14) para comprar un producto, comprendiendo el producto de programa informático:
instrucciones de código de programa almacenadas en un medio legible por ordenador para ejecutar las etapas de proceso de acuerdo con las reivindicaciones 6 a 10 cuando dicho programa se ejecuta en un ordenador.

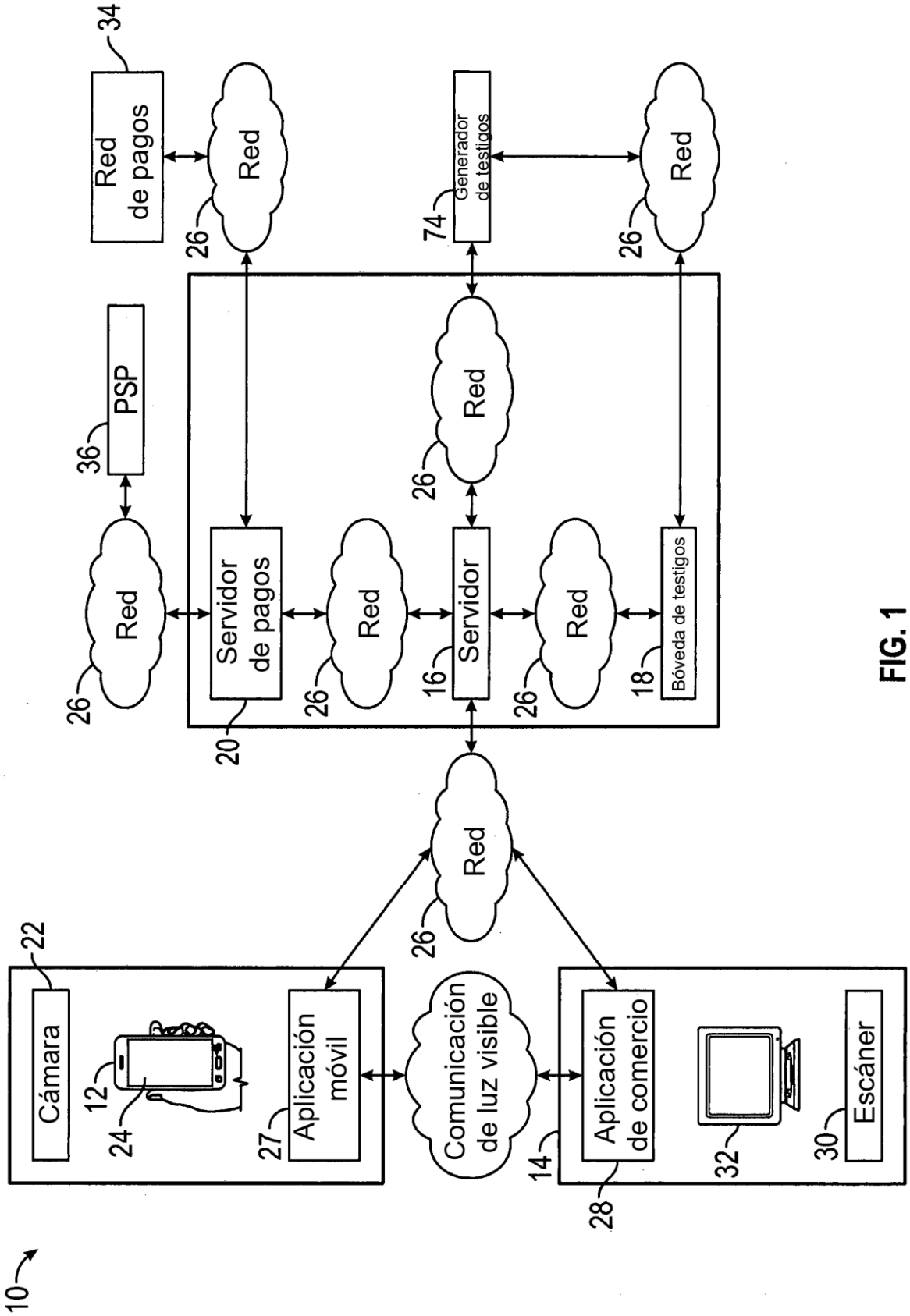
10
22
Cámara
12
24
27
Aplicación móvil
Comunicación de luz visible
14
Aplicación de comercio
28
32
30
Escáner
Red
26
20
Servidor de pagos
16
Servidor
18
Bóveda de testigos
36
PSP
34
Red de pagos
74
Generador de testigos

FIG. 1

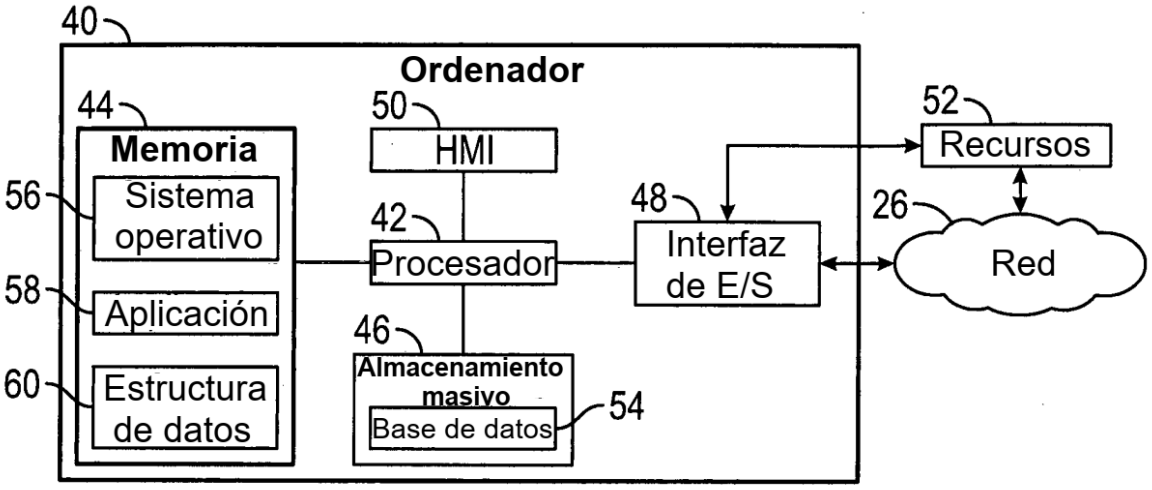
40
Ordenador
44
Memoria
56
Sistema operativo
58
Aplicación
60
Estructura de datos
50
HMI
42
Procesador
46
Almacenamiento masivo
Base de datos
54
48
Interfaz de E/S
52
Recursos
26
Red

FIG. 2

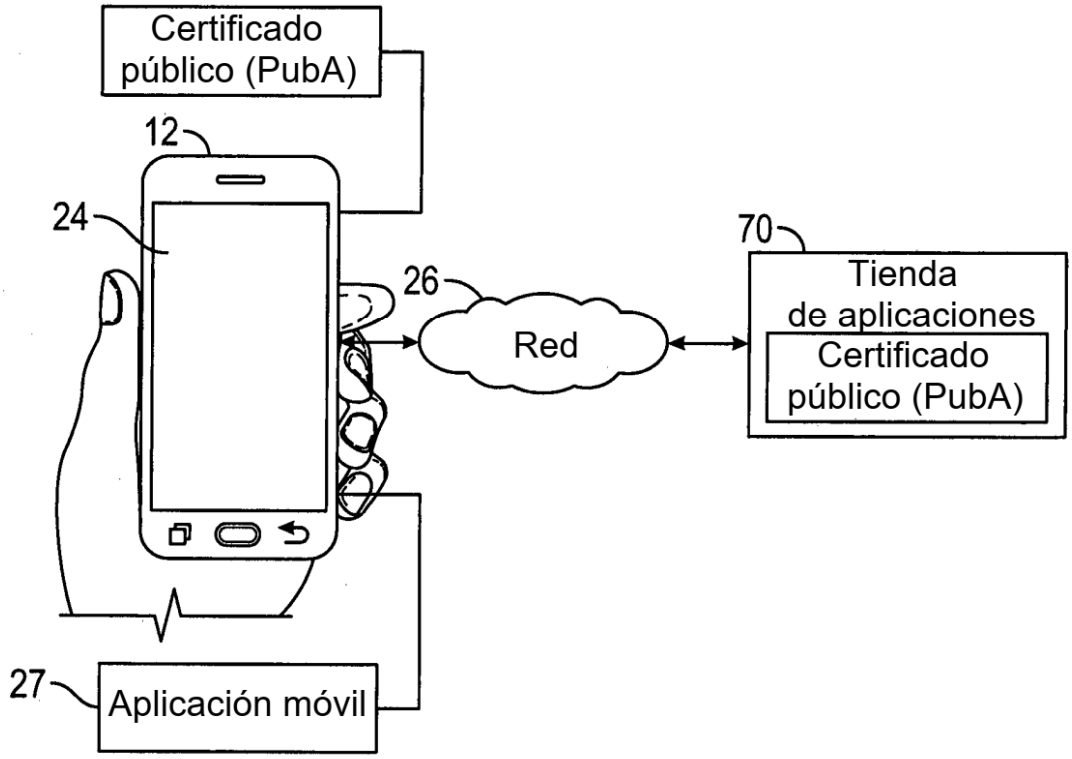
Certificado público (PubA)
12
24
26
Red
70
Tienda de aplicaciones
Certificado público (PubA)
27
Aplicación móvil

FIG. 3

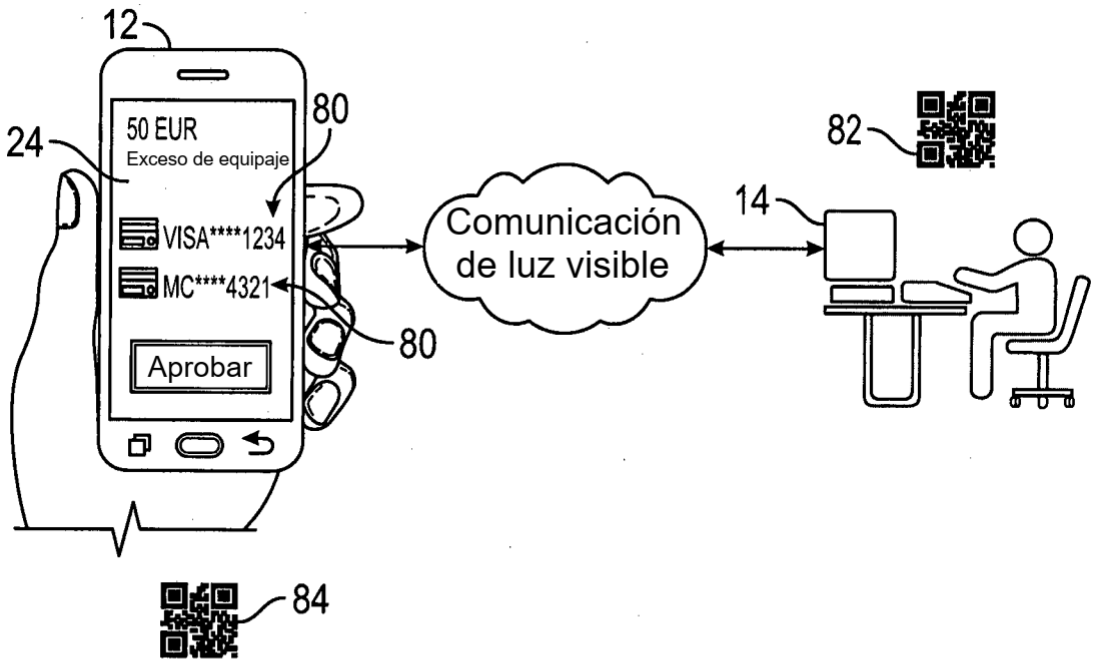
12
50 EUR
Exceso de equipaje
24
80
VISA****1234
MC****4321
Aprobar
80
Comunicación
de luz visible
82
14
84

FIG. 4