(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 626 064**

(51) Int. CI.:

H04L 29/06 (2006.01)
H04W 12/06 (2009.01)
G06Q 20/32 (2012.01)
G06Q 20/18 (2012.01)
G06Q 20/38 (2012.01)
G06Q 20/40 (2012.01)
G06Q 20/42 (2012.01)
H04L 29/08 (2006.01)
H04L 9/32 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **06.12.2013 PCT/HU2013/000118**

(87) Fecha y número de publicación internacional: **12.06.2014 WO14087179**

(96) Fecha de presentación y número de la solicitud europea: **06.12.2013 E 13826744 (8)**

(97) Fecha y número de publicación de la concesión europea: **22.02.2017 EP 2929671**

(54) Título: **Procedimiento y sistema para autenticar a un usuario que utiliza un dispositivo móvil y por medio de certificados**

(30) Prioridad:

07.12.2012 HU P1200715

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
21.07.2017

(73) Titular/es:

MICROSEC SZAMITASTECHNIKAI FEJLESZTÖ ZRT. (100.0%)
Záhony u. 7 D. ép.
1031 Budapest, HU

(72) Inventor/es:

VANCZÁK, GERGELY

(74) Agente/Representante:

DURÁN MOYA, Luis Alfonso

DESCRIPCIÓN

Procedimiento y sistema para autenticar a un usuario que utiliza un dispositivo móvil y por medio de certificados

SECTOR TÉCNICO

La invención se refiere a un procedimiento y un sistema adaptados para autenticar a un usuario que posee un dispositivo móvil en una entidad, en particular en un banco.

ANTECEDENTES DE LA TÉCNICA

En la actualidad, el volumen de transacciones bancarias en línea está aumentando extraordinariamente. El número de fraudes relacionados con datos de tarjetas bancarias también está aumentando, lo que plantea un serio reto para preservar la integridad de los sistemas de pago en línea.

Estos fenómenos generan una gran demanda para la mejora continua de sistemas de pago y otros sistemas que requieren autenticación de usuario de alto nivel. Por lo tanto, la técnica anterior contiene diversas soluciones para mejorar la seguridad de dichos sistemas.

En el documento US 2011/0270751 A1 se da a conocer un sistema y un procedimiento de autenticación para autenticación de dos factores. El sistema según el documento comprende un servidor de provisión de servicios, un terminal adaptado para utilizar el servidor, un dispositivo móvil, y, de forma opcional, un servidor, adaptado para almacenar varios datos de identificación, que se conecta tanto al dispositivo móvil como al servidor de provisión de servicios. Según el documento US 2011/0270751 A1 el código QR que se muestra en el terminal y se escanea por medio del dispositivo móvil comprende un denominado identificador de la transacción o ID de sesión, así como la dirección del servidor de provisión de servicios. La denominada "petición de autenticación" que se muestra en el código QR, puede ser recibida por el usuario mediante capturar una imagen de la pantalla del terminal utilizando la cámara del dispositivo móvil, o en un mensaje de correo electrónico. Para conseguir la identificación mediante el servidor de provisión de servicios, el dispositivo móvil pasa datos de identificación al servidor de provisión de servicios directamente o desde el servidor que almacena datos de identificación.

En el documento US 2012/0240204 A1 se da a conocer un sistema para autenticar a un usuario en el que el usuario recibe los datos necesarios para la autenticación por medio del escaneo de un código QR, u otro código de barras apropiado, con su dispositivo móvil desde un terminal conectado a un servidor de provisión de servicios, en el que el servidor de provisión de servicios utiliza asimismo los datos recibidos del usuario para generar el código QR. Los datos son enviados al dispositivo móvil de forma cifrada y son descodificados por el dispositivo. El usuario utiliza estos datos para la autenticación en el servidor de autenticación conectado al servidor de provisión de servicios. El servidor de autenticación verifica los datos recibidos aplicando una base de datos de datos de identificación, y, dependiendo del resultado de la verificación, autentica o rechaza al usuario.

En el documento US 2012/0166309 A1 se da a conocer un sistema en el que se utiliza un terminal y un dispositivo móvil para transacciones bancarias. El terminal y el dispositivo móvil se comunican utilizando códigos de barras, por ejemplo, códigos QR. La solución dada a conocer en el documento US 2012/0166309 A tiene la desventaja de que no se aplica comunicación de datos cifrados para transferir datos, y que en los códigos QR se incluyen datos confidenciales. Por consiguiente, el código QR incluye los datos de la transacción (número de tarjeta, importe a transferir, número de cuenta, etc.) en cada ocasión. Dado que cualquiera que use una aplicación apropiada puede leer los códigos QR, los datos confidenciales incluidos en los mismos también son accesibles para cualquiera.

Según el documento US 2012/0166309 A1, los datos a confirmar (que constituyen información confidencial) se transfieren por medio de la pantalla de un primer dispositivo a un segundo dispositivo (por ejemplo, a un dispositivo móvil desde un terminal), lo que significa que se pueden pasar datos falsos al segundo dispositivo en caso de que el primer dispositivo se vea comprometido. Si el usuario tiene prisa, confirmando de forma rutinaria la transacción en el dispositivo móvil, puede confirmar a ciegas el proceso en el que están implicados los datos falsos. Sin comunicación de datos cifrados se puede acceder a y obtener toda la información confidencial sobre la red, y la información puede utilizarse posteriormente para fraudes (por ejemplo, para cometer un fraude CNP (tarjeta no presente, Card Not Present)) sin conocimiento del usuario.

Una grave desventaja de las soluciones citadas anteriormente es que implican la transferencia de datos confidenciales (aunque a veces en forma cifrada) entre los componentes individuales del sistema de autenticación. Por lo tanto es posible que los datos sean capturados en la red por un atacante, que puede a continuación falsificar los datos capturados.

Se describe un proveedor de firmas conectado a un dispositivo móvil y a un proveedor de servicios en el documento titulado "3.2 Using mobile devices for digital signatures" ("3.2 Utilización de dispositivos móviles para firmas digitales") por Zoltán Faigl, Sándor Imre, and Balázs Budai (Az m-kormányzat biztonsági kérdései és leheto˝ségei, Híradástechnika, vol. LX., no. 3, pág. 30-31, 2005.) Según el documento, la clave de firma y el algoritmo son

almacenados por el proveedor de firmas, y el propio dispositivo móvil se identifica en el proveedor de firmas, por ejemplo utilizando un código PIN.

Se dan a conocer sistemas de autenticación basados en el escaneo de códigos QR en los documentos US 2012/0005076 A1, US 2012/0066501 A1 y US 2012/0203646 A1. Según el documento US 2012/0066501 A1 el sistema se compone de un dispositivo móvil adaptado para escanear un código QR, un terminal y un sistema de provisión de servicios, la autenticación basada en códigos QR se aplica en un sistema para firmas digitales según el documento US 2012/0203646 A1. En el documento US 2012/0116972 A1 se da a conocer un sistema de pago electrónico que comprende un sistema de gestión de firmas.

En el documento US 2007/0130463 se da a conocer un sistema de autenticación que, además del dispositivo móvil y el sistema de provisión de servicios, comprende un denominado "sistema de autenticación y claves" capaz por ejemplo de sincronizar claves. En los documentos US 2011/0296191 A1 y US 2011/0314371 A1 se dan a conocer sistemas que permiten la firma digital mediante múltiples partes. Asimismo, en los documentos WO 2005/067402 A2, WO 2009/080999 A2 y US 2011/219427 A1 se dan a conocer sistemas para firma digital. En el documento WO 2010/056969 A2 se da a conocer un sistema que utiliza mensajes cortos (SMS) para transacciones en línea. Se describe una utilización a modo de ejemplo del protocolo MQTT en J. M. Robinson, J. G. Frey, A. J. Stanford-Clark, A. D. Reynolds, B. V. Bedi: Sensor Networks and Grid Middleware for Laboratory Monitoring (Redes de sensores y software intermedio de red para monitorización de laboratorios), actas de la primera conferencia internacional de ciencia virtual y computación de red (e-Science'05), Computer Society, IEEE.

En vista de las soluciones conocidas, existe una demanda para la mejora de procedimientos y sistemas de autenticación conocidos, con el fin de aumentar la protección y seguridad de dichos procedimientos y sistemas.

DESCRIPCIÓN DE LA INVENCIÓN

El objetivo principal de la invención es proporcionar un procedimiento, según la reivindicación 1, y un sistema, según la reivindicación 13, que carezcan de las desventajas de las soluciones de la técnica anterior en el mayor grado posible.

Un objetivo adicional de la invención es proporcionar un procedimiento y un sistema que puedan autenticar a un usuario con mayor seguridad, y de proteger los datos confidenciales en mayor medida en comparación con soluciones conocidas.

Según la invención, los inventores han reconocido la ventaja del hecho de que los dispositivos móviles disponibles comercialmente son capaces de ejecutar aplicaciones (por ejemplo, navegadores) que permiten al dispositivo móvil llevar a cabo una autenticación basada en certificados por ejemplo, de tipo X.509. Por lo tanto es posible aplicar la tecnología PKI (infraestructura de claves públicas, Public Key Infraestructure) para iniciar sesión de forma segura en páginas web que requieren autenticación bidireccional (preferentemente de tipo SSL (Secure Sockets Layer, capa de conexiones seguras)), en las que el dispositivo móvil y la página web se identifican mutuamente utilizando sus certificados X.509 respectivos. PKI es una tecnología criptográfica que permite la comunicación segura sobre redes públicas no seguras y proporciona identificación de usuario fiable. Tal como se define mediante el protocolo de criptografía de SSL, se deberían aplicar certificados de clave pública que cumplan el estándar X.509, para cifrar las claves simétricas utilizadas durante el establecimiento del canal SSL; los certificados basados en otros estándares no se pueden aplicar.

Basándose en la posibilidad de realizar la autenticación utilizando los denominados dispositivos móviles inteligentes por medio de estos certificados, el procedimiento y el sistema según la presente invención ofrecen soluciones que hacen más económicos, más seguros y más eficientes los procesos empresariales que requieren autenticación de dos factores. El sistema y el procedimiento según la invención ofrecen asimismo una solución para la firma digital auténtica de contratos en línea, utilizando el dispositivo móvil de la parte firmante de una manera directa o indirecta para autorizar los documentos.

Por medio del procedimiento y el sistema según la invención, aplicando un proceso de autenticación basado en certificados residentes en dispositivos móviles, se puede implementar una autenticación basada en PKI muy potente, que es una de las soluciones de autenticación más seguras y más eficientes de hoy en día.

Según la invención se puede conseguir el nivel máximo de seguridad cuando la clave privada perteneciente al certificado residente en el dispositivo móvil existe solamente en una única instancia, es decir, se genera preferentemente en el propio dispositivo móvil. La forma en que se generan y gestionan las claves es muy importante para el nivel de seguridad alcanzable mediante procesos basados en claves. Los dispositivos que ejecutan iOS (sistema operativo de iPhone) tienen una herramienta integrada, el SCEP (protocolo de inscripción de certificados simple), que es perfectamente capaz de generar claves, y de enviar las peticiones de certificados al proveedor de certificación autenticado utilizando una contraseña negociada previamente. Para conseguir el máximo nivel de seguridad posible, las funciones del SCEP se deben implementar preferentemente en plataformas móviles que ejecuten otros sistemas operativos.

En el procedimiento y el sistema, según la invención, un certificado de autenticación (preferentemente de tipo X.509) emitido por un proveedor de certificación registrado al propietario del dispositivo móvil está disponible en el dispositivo móvil, perteneciendo la clave privada al certificado que se ha generado preferentemente en el propio dispositivo móvil.

El procedimiento y el sistema, según la invención, se basan en la autenticación aplicando certificados residentes en los dispositivos móviles. La autenticación se lleva a cabo aplicando el protocolo de transferencia de datos HTTP, preferentemente por medio de un canal SSL. Las características del protocolo SSL están reguladas mediante el estándar RFC 6101.

La solución, según la invención, reduce de forma significativa la posibilidad de fraudes en línea, y reduce los riesgos de la utilización no autorizada de tarjetas bancarias. La utilización de dispositivos móviles inteligentes de la manera especificada por la invención reduce los costes de los procedimientos existentes de autenticación de dos factores (SMS, autentificador). La aplicación del procedimiento y el sistema, según la invención, alivia la desconfianza de los usuarios hacia la banca en línea, y disminuye de forma significativa las pérdidas financieras derivadas de los fraudes.

Dado que la solución, según la invención, no implica en modo alguno la manipulación y el almacenamiento de datos de tarjetas bancarias durante el proceso de autenticación de transacciones (de tarjetas) bancarias en línea, el estándar de la industria PCI DSS (estándar de seguridad de datos para la industria de tarjetas de pago) no es relevante para la misma. Sin embargo, la solución, según la invención, cumple los requisitos de seguridad bancarios determinados en PCI DSS.

Los objetivos de la invención se pueden conseguir mediante el procedimiento según la reivindicación 1 y el sistema según la reivindicación 13. Se definen realizaciones preferentes de la invención en las reivindicaciones dependientes.

BREVE DESCRIPCIÓN DE LOS DIBUJOS

Se describen a continuación realizaciones preferentes de la invención a modo de ejemplo, haciendo referencia a los siguientes dibujos, en los que

la figura 1 es un diagrama de bloques que muestra una realización del procedimiento y el sistema, según la invención,

la figura 2 es un diagrama de bloques que muestra otra realización del procedimiento y el sistema, según la invención,

la figura 3 es un diagrama de bloques de otra realización más del procedimiento y el sistema, según la invención, y

la figura 4 muestra los componentes de la realización del procedimiento y el sistema mostrados en la figura 3.

MODOS PARA LLEVAR A CABO LA INVENCIÓN

Los dibujos adjuntos muestran componentes tanto del procedimiento como del sistema, según la invención. En lo que sigue, se describirá en primer lugar el procedimiento según la invención, haciendo referencia a algunos componentes del sistema. El sistema, según la invención, se describirá asimismo en una sección posterior.

La figura 1 muestra una realización del procedimiento, según la invención, por medio de un diagrama de bloques. El procedimiento, según la invención, está adaptado para autenticar a un usuario -10- en una entidad -16-. En el contexto de la presente memoria descriptiva, el término "entidad" se utiliza para hacer referencia a una empresa, organización, institución financiera, estado, o individuo. Tal como se mostrará más adelante en relación con las realizaciones, la autenticación puede tener muchos objetivos. La autenticación puede requerirse para confirmar un inicio de sesión del usuario en una entidad, para autorizar una transacción bancaria, o para identificar a un usuario para generar una firma digital. Por supuesto, el procedimiento de autenticación según la invención puede aplicarse para otros objetivos.

En el transcurso del procedimiento según la invención, un contacto del usuario -10- realizado en un navegador de un terminal -12- es detectado por medio de un módulo de contacto -20- de la entidad -16- (un módulo que permite ponerse en contacto con la entidad -16-), y una dirección de red del módulo de autenticación -24- de la entidad -16- se envía por medio del módulo de contacto -20- a un dispositivo móvil -14- del usuario -10- en un mensaje de autenticación. Basándose en la dirección de red, el dispositivo móvil -14- es capaz de ponerse en contacto con el módulo de autenticación -24-. Dado que el dispositivo móvil -14- se asigna a un usuario específico, la entidad -16- puede enviar el mensaje de autenticación al usuario dado -10-.

El dispositivo móvil -14- es preferentemente un dispositivo móvil inteligente, por ejemplo un teléfono inteligente o una tableta. Un certificado, emitido por un proveedor -18- de certificación aceptado por la entidad -16- está disponible en el dispositivo móvil -14-. El certificado tiene una clave privada de usuario de una longitud, por lo menos, de 1024 bits, preferentemente una longitud de 2048 bits, e identifica inequívocamente al usuario -10-. La clave privada se genera preferentemente en el dispositivo móvil -14-, lo que implica que no existe ninguna copia de la clave.

Después de que el mensaje de autenticación ha sido enviado, se ejecutan las siguientes etapas en el procedimiento según la invención. La aceptabilidad de un certificado de entidad del módulo de autenticación -24- se verifica por medio del dispositivo móvil -14- basándose en la dirección de red, y la aceptabilidad de un certificado de usuario del dispositivo móvil -14- se verifica por medio del módulo de autenticación -24-, y en caso de que el certificado de entidad y el certificado de usuario sean aceptables, el usuario -10- se autentica en la entidad -16- estableciendo un canal de comunicación entre el dispositivo móvil -14- y el módulo de autenticación -24-, mientras que en caso de que el certificado de entidad o el certificado de usuario no sean aceptables, el usuario -10- es rechazado en la entidad -16-.

En la realización del procedimiento, según la invención, que se muestra en la figura 1, la etapa de verificar la aceptabilidad del certificado de entidad comprende verificar por medio del dispositivo móvil -14- la validez del certificado de entidad en un proveedor de certificación de entidad, y la fiabilidad del proveedor de certificación de entidad se verifica por medio del dispositivo móvil -14-. En caso de que el certificado del módulo de autenticación -24- se haya emitido por un proveedor de certificación que el dispositivo móvil -14- considera "no fiable", el dispositivo móvil -14- interrumpe el contacto con el módulo de autenticación -24-. En esta realización del procedimiento, la etapa de verificar la aceptabilidad del certificado de usuario comprende verificar por medio del módulo de autenticación -24- la validez del certificado de usuario en el proveedor de certificación de usuario, y la fiabilidad del proveedor de certificación de usuario. En la realización, según la figura 1, tanto el proveedor de certificación de usuario como el proveedor de certificación de entidad están implementados como el proveedor -18- de certificación. En la realización de la figura 1, el módulo de autenticación -24- y el proveedor -18- de certificación se conectan mediante un canal de comunicación -116- que, a modo de ejemplo, se implementa mediante internet. No es necesario que los certificados del dispositivo móvil -14- y el módulo de autenticación -24- estén emitidos por el mismo proveedor de certificación. En caso de que el proveedor de certificación de usuario sea diferente del proveedor de certificación de entidad, a continuación el dispositivo móvil -14- y el módulo de autenticación -24- comprueban mutuamente la fiabilidad del proveedor de certificación del otro.

En la realización mostrada en la figura 1, el proveedor de certificación de entidad corresponde a la clave privada de la entidad del módulo de autenticación -24-, y el certificado de entidad es firmado por el proveedor de certificación de entidad, el proveedor de certificación de usuario corresponde a la clave privada del usuario del dispositivo móvil -14-, y el certificado de usuario es firmado por el proveedor de certificación de usuario.

En caso de que tanto el certificado de entidad como el certificado de usuario sean aceptables, se establece una conexión bidireccional basada en certificados, preferentemente un canal de comunicación de tipo SSL bidireccional, entre el dispositivo móvil y el módulo de autenticación. Antes de establecer el canal de comunicación, los certificados se verifican mutuamente (comprobación de fiabilidad y revocación utilizando los protocolos OCSP (protocolo de estado de certificados en línea) o CRL (lista de revocación de certificados)), a lo que sigue una denominada operación de mutuo acuerdo. Entre el dispositivo móvil y el módulo de autenticación no tiene lugar ningún intercambio de datos relacionado con datos confidenciales antes de verificar los certificados.

Habitualmente se crea un canal de comunicación SSL unidireccional entre el terminal -12- y el módulo de contacto -20-, lo que significa que solo el módulo de contacto -20- se identifica en el dispositivo móvil -14- con su certificado cuando se establece el canal. La razón por la que el módulo de contacto -20- y el módulo de autenticación -24- no están combinados en un único módulo, según la invención, es que un único módulo dado -es decir, la página web correspondiente al módulo- es capaz de establecer una conexión (canal de comunicación) SSL unidireccional o bien bidireccional. Dado que los módulos conocidos (páginas web) que requieren autenticación establecen una conexión SSL unidireccional con el usuario, -lo que implica que no se requiere que los usuarios se autentiquen por sí mismos utilizando un certificado de usuario, ya que esto haría imposible utilizar un PC o terminal arbitrario para realizar las tareas diarias-, la manera más conveniente de extender las soluciones existentes es implementar una autenticación basada en certificados utilizando un módulo independiente, el módulo de autenticación, que se integra en sistemas conocidos. Al contrario de los terminales utilizados para realizar tareas administrativas diarias, el dispositivo móvil del usuario es un dispositivo de utilización privada, y por lo tanto el certificado que se puede asignar a éste se puede aplicar para una autenticación SSL bidireccional.

Se crea una conexión SSL unidireccional cuando se establece una conexión HTTPS entre un cliente (navegador) y un servidor web, se requiere que solo el servidor web debe identificarse utilizando su certificado, que es preferentemente un certificado de servidor web SSL de tipo X.509 de clave pública emitido al propio dominio del servidor web, y se firma preferentemente mediante un proveedor de certificación fiable por ambas partes. El cliente se conectará al servidor web solo si el certificado del servidor web se puede atribuir a un certificado del proveedor de certificación fiable, y el certificado del servidor web es válido (no ha caducado, no se ha revocado ni se ha suspendido).

Se crea una conexión SSL bidireccional cuando se establece una conexión HTTPS entre un cliente (navegador) y un servidor web, se requiere que ambas partes (cliente y servidor web) se identifiquen utilizando sus propios certificados, que son preferentemente certificados de servidor web, así como certificados X.509 de clave pública. El cliente se conectará al servidor web solo si el certificado del servidor web se puede atribuir a un certificado de un proveedor de certificación fiable, y el certificado del servidor web es válido (no ha caducado, no se ha revocado ni se ha suspendido). Asimismo, el servidor web solo permite al cliente conectarse si el certificado de autenticación del cliente ha sido emitido por una parte fiable, y es válido (no ha caducado, no se ha revocado ni se ha suspendido).

Según la invención, la conexión entre el dispositivo móvil -14- y el módulo de autenticación -24- se crea solamente después de que los certificados del dispositivo móvil -14- y el módulo de autenticación -24- se han verificado mutuamente. Según soluciones de la técnica anterior, la creación del canal de comunicación requiere como mucho la verificación del certificado del módulo de autenticación correspondiente mediante el dispositivo móvil. Sin embargo, para establecer un canal de comunicación suficientemente seguro entre el dispositivo móvil y el módulo de autenticación no es suficiente verificar la fiabilidad del servidor de autenticación mediante el dispositivo móvil. Además de eso, también se debe verificar la fiabilidad del cliente mediante el servidor de autenticación. Hasta hace poco, los dispositivos móviles en funcionamiento no estaban preparados para esta verificación, es decir, los dispositivos móviles no admitían conexiones basadas en certificados. Tal como se ha mencionado anteriormente, los dispositivos que ejecutan iOS soportan la utilización de certificados, pero en dispositivos móviles que ejecutan otros sistemas operativos, tales como Android, es necesario instalar una aplicación dedicada. La solución que actualmente está más extendida en el mundo de la banca implica la utilización de contraseñas de una solo utilización.

Según el documento US 2012/0240204 A1, el canal de comunicación entre el dispositivo móvil y el servidor de autenticación se establece después de que el servidor de autenticación ha sido verificado por el cliente. Después de eso, los datos de autorización reales que otorgan el permiso al usuario se intercambian a través del canal, y estos datos se aplican para identificar al cliente y para confirmar la transacción.

Frente a esto, en el procedimiento según la invención, la autenticación se lleva a cabo como una consecuencia del establecimiento del canal de comunicación, es decir, el proceso de establecimiento del canal de comunicación comprende la autenticación.

El procedimiento de autenticación, según la invención, es más ventajoso que la solución de la técnica anterior según el documento US 2012/0240204 A1, ya que la solución descrita en el mismo no incluye la verificación del cliente mediante el servidor de autenticación del banco antes de que se establezca el canal de comunicación. Esta deficiencia de la solución, según el documento US 2012/0240204 A1, puede ser explotada por un atacante como sigue.

Al tomar el control del PC del cliente, o introduciéndose a través de la red entre el PC y el servidor del proveedor de servicios (que es equivalente al módulo de contacto de la invención), según el documento, un atacante puede sustituir el URL (localizador uniforme de recursos), es decir, la dirección de red del servidor de autenticación que tiene un certificado SSL válido y fiable que está comprendido en el código QR, por su propia dirección de red que puede parecerse en gran medida al URL real del servidor de autenticación. Por lo tanto, según la solución descrita en el documento, el dispositivo móvil considerará el servidor de autenticación falso (el servidor del atacante) como fiable, ya que puede tener un certificado válido (cualquiera puede obtener un certificado SSL para su propio dominio). Después de establecer satisfactoriamente el canal de comunicación HTTPS unidireccional con el servidor falso, el cliente envía los datos de autorización (OTP, PIN, datos firmados con clave, etc.) al servidor del atacante. El atacante puede establecer a continuación la conexión SSL unidireccional con el servidor de autenticación real, y puede enviar los datos de autorización especificados por el cliente, aprovechándose por lo tanto de los mismos.

Por el contrario, en el procedimiento según la invención, el dispositivo móvil -14- también tiene que presentar un certificado válido al módulo de autenticación -24- para que se establezca el canal de comunicación. Es decir, se tiene que establecer una conexión SSL bidireccional entre el dispositivo móvil y el módulo de autenticación, que impide el ataque "de intermediario" descrito anteriormente como sigue. En caso de que, de la manera descrita anteriormente, el atacante envíe una dirección de red falsa al dispositivo móvil -14- en un mensaje de autenticación como la dirección de red del módulo de autenticación, acepta del dispositivo móvil los certificados de autenticación emitidos por el mismo proveedor de certificación fiable, por ejemplo para establecer una conexión, por ejemplo, un canal de comunicación HTTPS, y el atacante puede obtener los datos de autorización indirectos del usuario después de que se ha establecido el canal del comunicación. Sin embargo, el atacante no puede aprovecharse de los datos de autorización obtenidos, dado que no se puede conectar al módulo de autenticación real suplantando al usuario (es decir, utilizando la clave privada del usuario y el certificado almacenado en el dispositivo móvil), puesto que no posee la clave privada del usuario.

Por lo tanto, en el proceso descrito en el documento US 2012/0240204 A1 es suficiente sabotear un PC, por ejemplo un terminal (que puede estar situado, por ejemplo, en un cibercafé) para que un atacante adquiera la capacidad de atacar de forma relativamente fácil el proceso de autorización. Sin embargo, en la solución según la invención, el atacante no puede aprovecharse de los datos obtenidos en caso de que solo se vea comprometida una de las

partes.

En la realización mostrada en la figura 1, se inicia un contacto de inicio de sesión en el módulo de contacto -20- a través de un canal de comunicación -100-, y de este modo el terminal -12- muestra una interfaz de inicio de sesión de la entidad -16-. El canal de comunicación -100- se puede establecer por ejemplo utilizando una red de internet.

En el procedimiento según la invención, tanto el terminal -12- como el dispositivo móvil -14- se conectan a internet de uno u otro modo (Wi-Fi, 3G, GPRS, etc.). Los procedimientos (servicios de entidad), según las realizaciones de la invención, se pueden llevar a cabo de tal modo que los usuarios y clientes accedan a módulos individuales de la entidad -16- sobre internet.

Según la presente realización, el usuario -10- (que posee un dispositivo móvil -14-) inicia sesión en primer lugar utilizando el navegador del terminal -12- en una página web principal de la entidad -16- (es decir, en el módulo de contacto -20-) que requiere una autenticación sencilla basada en nombre/contraseña de inicio de sesión utilizando una conexión -preferentemente unidireccional- que utiliza el protocolo de transferencia de datos HTTPS.

Tras la autenticación satisfactoria basada en nombre/contraseña de inicio de sesión la entidad -16- todavía no concede al usuario -10- acceso al módulo de contacto -20-. En lugar de ello, la entidad -16- devuelve la dirección de red, es decir, el URL del módulo de autenticación -24-. Por consiguiente, tanto el módulo de contacto -20- como el módulo de autenticación -24- se pueden implementar como una página web respectiva. El usuario abre a continuación la página en la dirección de red del módulo de autenticación -24- utilizando su dispositivo móvil -14-. La conexión al módulo de autenticación -24- requiere una clave privada -por ejemplo, de tipo RSA- y un certificado de autenticación correspondiente -por ejemplo, de tipo X.509- emitido a nombre del usuario. Tanto la clave privada como el certificado se almacenan en el dispositivo móvil. Tal como se presenta a continuación, el enlace enviado por el módulo de contacto -20- comprende la dirección de red del módulo de autenticación -24- (el URL de la página web del mismo: https://<sitioweb-secundario>), y preferentemente el valor del identificador de la transacción perteneciente al inicio de sesión basado en nombre/contraseña de inicio de sesión realizado utilizando el módulo de contacto.

Por lo tanto, el URL requerido para autorizar la autenticación se construye como: https://<sitio-web-secundario>/?idtr=ϕ(idtr)

donde

- ϕ es una clave simétrica del banco/organización

- idtr es un identificador de la transacción, y

- ϕ(idtr) es el idtr cifrado utilizando ϕ.

El cifrado del identificador de la transacción se hace necesario solo en caso de que también se prevea ocultar el identificador de la transacción (que puede ser un número aleatorio).

El URL puede ser transferido al dispositivo móvil -14- de maneras diferentes según un ejemplo que no forma parte de la invención. Por lo tanto, el URL se puede integrar en un mensaje de autenticación como sigue.

Según un ejemplo, el mensaje de autenticación puede ser un código QR, en cuyo caso la dirección de red se envía al dispositivo móvil -14- llevando a cabo las siguientes etapas: después de que se ha especificado el par nombre de usuario/contraseña, el URL del módulo de autenticación de la entidad -16- que está solicitando la autenticación basada en certificados del cliente SSL, así como el identificador de la transacción actual, se ponen a disposición del usuario mediante el módulo de contacto -20- en un código QR mostrado en la pantalla del terminal -12-. Por lo tanto, el código QR se pasa al terminal -12- mediante el módulo de contacto -20-; y a continuación el código se muestra en la pantalla del terminal y se captura mediante el dispositivo de formación de imágenes del dispositivo móvil -14-, y, por lo tanto, se transfiere al dispositivo móvil -14-. De este modo, el mensaje de autenticación es enviado al dispositivo móvil -14- mediante el módulo de contacto -20-. Según la figura 1, el código QR se envía al terminal -12- a través de un canal de comunicación -102-, por ejemplo sobre internet, y se transfiere a continuación utilizando un canal de comunicación -104-, es decir, tal como se ha descrito anteriormente, sacando una fotografía del código QR.

El mensaje del módulo de contacto -20- llega al dispositivo móvil -14- como un mensaje de tipo MQ (Message Queue, cola de mensajes), preferentemente de tipo MQ-TT (transporte de telemetría MQ). Las colas de mensajes implementan un protocolo de comunicación asíncrono, lo que significa que el emisor y el receptor del mensaje no tienen que conectarse necesariamente a la cola de mensajes simultáneamente. El mensaje es enviado por el emisor a la cola de mensajes, donde se almacena y espera para la entrega hasta que el receptor lo recibe desde la cola de mensajes. Los mensajes recibidos mediante la cola de mensajes pueden estar limitados en tamaño, y el tiempo de almacenamiento de un mensaje dado en la cola también puede estar limitado. Hay múltiples tipos de protocolos MQ

(por ejemplo, AMQP, MQTT, STOMP), teniendo todos una serie de implementaciones diferentes (tales como IBM webSphere MQ, Apache ActiveMQ, RabbitMQ), pero la funcionalidad básica, en otras palabras, el almacenamiento de mensajes en una cola de entrega, es la misma.

MQTT es un denominado protocolo "peso pluma". Sus características más importantes son que se puede implementar utilizando una cantidad mínima de código y que tiene una demanda de ancho de banda extremadamente baja. Estas características lo hacen ideal para la comunicación continua con dispositivos móviles.

El protocolo MQTT es utilizado por plataformas de mensajería para comunicarse con servidores y recibir mensajes de los mismos, pero se aplica asimismo en marcapasos para la monitorización remota de la circulación y la actividad cardíaca, para la monitorización y control de oleoductos, y para la monitorización automatizada del nivel de los ríos. El protocolo MQTT funciona asimismo sobre un canal SSL cifrado.

En ese caso, el dispositivo móvil inteligente aplica una aplicación de cliente apropiada para conectarse -por medio de un protocolo MQ implementado utilizando canales de comunicación de direcciones diferentes -108-, -110- mostrados en la figura 1- a un módulo -26- de cola de mensajes de la entidad -16-. La conexión al módulo -26- de cola de mensajes normalmente se lleva a cabo aplicando alguna clase de autenticación (tal como una autenticación basada en nombre de usuario/contraseña). Los servidores utilizados para dar servicio al módulo de contacto -20- y al módulo de autenticación -24- de la entidad -26- son capaces de enviar mensajes por medio del módulo -26- de cola de mensajes a los dispositivos móviles conectados -14-. La figura 1 muestra los canales de comunicación bidireccional -106-, -112- utilizados para conectar el módulo de contacto -20- y el módulo -26- de cola de mensajes. En la realización mostrada en la figura 1, el módulo de autenticación -24- es capaz indirectamente de enviar mensajes de tipo cola de mensajes (en lo que sigue: mensajes MQ) a través del canal de comunicación -118-.

Una característica ventajosa de la invención que aplica mensajes de tipo cola de mensajes como mensajes de autenticación es que los dispositivos móviles -14- pueden enviar una respuesta firmada de forma electrónica (acuse de recibo), firmada con la clave de firma de los mismos, al módulo de contacto -20- después de que es recibido (o leído por el cliente) un mensaje de autenticación enviado por la entidad. Esta solución contempla que la entidad -16- siempre posee una prueba firmada de forma electrónica (firmada utilizando la clave de usuario almacenada en el dispositivo móvil) respecto de que el mensaje de autenticación ha sido enviado. Por lo tanto, la entidad siempre tiene una prueba fehaciente que ayuda a evitar futuras disputas. El envío automático de acuses de recibo del mensaje de autenticación no se resuelve según soluciones conocidas.

Aplicando el módulo -26- de cola de mensajes, la entidad -16- se puede poner en contacto con los usuarios directamente, sin implicar a una tercera parte en el proceso -siempre que los usuarios inicien sesión en la aplicación apropiada de la entidad utilizando sus dispositivos móviles. De este modo, puede hacerse necesario que el usuario/cliente envíe acuses de recibo para los mensajes enviados por la entidad -16-. La aplicación de la entidad se puede configurar de tal modo que el dispositivo móvil deba enviar un acuse de recibo firmado de forma electrónica al servidor de la entidad -16- que prueba de manera irrefutable que el mensaje ha sido recibido.

En un ejemplo que no forma parte de la invención, el mensaje de autenticación y el URL del módulo de autenticación integrado en el mismo, se pueden transferir al dispositivo móvil -14- utilizando un SMS (mensaje corto de texto). Los proveedores de servicios de SMS no garantizan el envío y la entrega inmediata de los mensajes.

En un ejemplo que no forma parte de la invención, el mensaje de autenticación se puede transferir asimismo en un denominado "mensaje de envío automatizado". Los proveedores de servicios tampoco garantizan el envío y entrega inmediatos de los mensajes en el caso de los mensajes de envío automatizado. En un ejemplo que no forma parte de la invención, se pueden utilizar asimismo mensajes de correo electrónico para transferir el mensaje de autenticación.

Se puede concebir asimismo una estructura de emergencia para la mensajería, que significa que cuando un canal de mensajería no está disponible, se sustituirá por el canal de mensajería de preferencia secundaria. Para mostrar la estructura de emergencia, la figura 1 muestra los canales de comunicación -102-, -104- adaptados para transferir el código QR, y también los canales de comunicación -108-, -110-, -106- y -112- adaptados para transferir el mensaje MQ.

Después de que se recibe el mensaje de autenticación enviado en un mensaje MQ, el dispositivo móvil -14- se conecta a la dirección de red recibida, en otras palabras, a la dirección de red del módulo de autenticación -24- utilizando su clave privada y el certificado de autenticación de tipo X.509 correspondiente. Según la figura 1, esta conexión -la apertura de la dirección de red del módulo de autenticación -24--, se implementa utilizando un canal de comunicación -114-. El canal de comunicación -114- puede establecerse por ejemplo utilizando una red internet.

El módulo de autenticación -24- realiza a continuación una comprobación de revocación del certificado del cliente en el proveedor -18- de certificación utilizando preferentemente OCSP o CRL. En caso de que el certificado perteneciente al dispositivo móvil -14- sea inválido (se haya suspendido, revocado, o la comprobación haya fallado), se devuelve un mensaje de error al dispositivo móvil -14- a través del canal de comunicación -120-, y al módulo de

contacto -20- a través del canal de comunicación -118-.

En caso de que la entidad -16- se comunique con el dispositivo móvil por medio de una conexión MQ, también se puede notificar al dispositivo móvil la autenticación fallida en un mensaje MQ enviado por medio de los canales de comunicación -106-, -108-.

En caso de que el certificado residente en el dispositivo móvil sea válido, y preferentemente si los datos incluidos en el mismo se han aceptado y el identificador de la transacción indica una autenticación satisfactoria mediante el módulo de contacto -20-, el módulo de autenticación -24- envía al dispositivo móvil -14- a través del canal de comunicación -120- un mensaje que indica una autenticación satisfactoria. Al igual que el canal de comunicación -114-, el canal de comunicación -120- se implementa preferentemente utilizando la red internet. En caso de que la entidad -16- se comunique con el dispositivo móvil -14- por medio de una conexión MQ, se notifica asimismo al dispositivo móvil la autenticación satisfactoria en un mensaje MQ. Como una última etapa después de la autenticación satisfactoria, el usuario inicia sesión mediante el módulo de contacto -20- de la entidad -16-.

La figura 1 puede mostrar asimismo una realización de este tipo del procedimiento de autenticación según la invención en el que es necesaria la autenticación del usuario para aprobar una transacción (por ejemplo, una transferencia bancaria). La realización de la invención aplicada para esto se describe a continuación.

En un estado inicial de la etapa de aprobación de la transacción, el usuario -10- que tiene el dispositivo móvil -14- inicia sesión en el módulo de contacto -20- de la entidad -16- en el navegador del terminal -12-. En la presente realización, la entidad -16- es preferentemente un banco. Se puede acceder a la interfaz en línea del módulo de contacto -20- utilizando un canal de comunicación HTTPS unidireccional. El usuario -10- que ha iniciado sesión, inicia una transacción (por ejemplo, una transferencia de dinero), y rellena el formulario de la transacción. En la siguiente página, el banco muestra la información sobre la transacción a aprobar, y el usuario confirma los datos de la transacción en el navegador de su ordenador.

A continuación, el banco envía al dispositivo móvil -14- la dirección de red del módulo de autenticación en un mensaje de autenticación, y el usuario abre el mensaje utilizando su dispositivo móvil -14-. De manera análoga a lo que se ha descrito anteriormente, se requiere la clave privada y el certificado perteneciente a la misma (almacenados en el dispositivo móvil -14-) para conectarse al módulo de autenticación -24- (la diferencia es que en esta realización el objetivo de la autenticación que solicita el módulo de autenticación -24- es la aprobación de la transacción). Análogamente a lo expuesto anteriormente, el enlace enviado por el módulo de contacto -20- comprende el URL (https://<sitio-web-secundario>) del módulo de autenticación -24-, así como el valor del identificador de la transacción perteneciente a la transacción.

No se puede descifrar en absoluto ningún dato confidencial relacionado con la transacción a partir del enlace enviado al dispositivo móvil -14-, ya que éste solo comprende el identificador de la transacción, que incluso se puede cifrar utilizando la clave simétrica del banco.

También en esta realización, el mensaje de autenticación se transfiere al dispositivo móvil -14- por medio del canal descrito anteriormente (mensaje MQ).

A continuación, también de una manera similar a la anterior, el dispositivo móvil -14- utiliza su clave privada y el certificado perteneciente a la misma para conectarse al módulo de autenticación -24-, que lleva a cabo a continuación una comprobación de revocación en el certificado del cliente. En caso de que el certificado sea inválido (se haya suspendido, revocado, o la comprobación haya fallado), se devuelve un mensaje de error al dispositivo móvil -14- y al módulo de contacto -20-.

En caso de que el certificado sea válido, y preferentemente en caso de que el módulo de contacto -20- haya aceptado la autenticación basándose en los datos comprendidos en el certificado y en el identificador de la transacción (idtr), el módulo de autenticación -24- devuelve al dispositivo móvil -14- los datos de la transacción en la siguiente etapa. En esta fase la transacción todavía no ha sido aprobada en el dispositivo móvil -14-.

En este momento el usuario puede revisar los datos de la transacción. Según una realización, el banco requiere que el cliente, preferentemente por medio de los módulos de autenticación -24-, confirme algunos de los datos de la transacción volviendo a introducirlos (por ejemplo, en caso de una transferencia bancaria, puede ser necesario tener que volver a introducir el importe a transferir y/o el número de cuenta de destino). Si el cliente omite esta etapa en el dispositivo móvil -14-, o introduce datos incorrectos, la transacción fallará. En esta realización del procedimiento según la invención, se elimina el problema de la "aprobación a ciegas", es decir, la posibilidad de que el cliente apruebe los datos de la transacción sin comprobarlos realmente. El denominado ataque "de intermediario" se puede impedir asimismo aplicando esta realización del procedimiento: en caso de que el terminal -12- pase a estar controlado por un atacante, y los datos de la transacción se falsifiquen utilizando la técnica "de intermediario", el usuario no puede entonces confirmar ni siquiera accidentalmente la transacción falsa por medio del enlace de aprobación enviado por el banco. Éste no es el caso para la introducción de contraseñas de una sola utilización enviadas en mensajes SMS, o contraseñas generadas utilizando autentificadores. (En el primer caso, no hay manera

de "forzar" al cliente a verificar los datos, dado que la solución que implica SMS es pasiva).

En caso de que el banco se comunique con el dispositivo móvil -14- a través de una conexión MQ, el dispositivo móvil es notificado asimismo de la aprobación de la transacción en un mensaje MQ.

En la etapa descrita anteriormente también es posible rechazar completamente la transacción. Cuando se aplica una comunicación basada en MQ, se envía un mensaje al dispositivo móvil -14- que indica que la transacción ha sido cancelada por el cliente.

En caso de una aprobación satisfactoria, un rechazo, o si se ha alcanzado el límite de tiempo para la aprobación, el módulo de contacto -20- muestra un mensaje en el navegador del terminal -12- en el área de la interfaz de usuario correspondiente al módulo de contacto -20-.

En una realización, un usuario -10- solicita un servicio en el módulo de contacto -20- de la entidad -16- por medio del navegador del terminal -12- rellenando un formulario electrónico, donde se requiere la firma mutua de un contrato por la entidad -16- y el usuario -10-. El contrato puede prepararse de forma dinámica en el módulo de contacto -20- de la entidad -16- o puede ser un contrato preparado previamente. Utilizando su propia clave de firma, el módulo de contacto -20- de la entidad -16- firma de forma electrónica el contrato cumplimentado utilizando los datos introducidos por el usuario (cliente), y opcionalmente le proporciona una marca de tiempo certificada.

A continuación, en caso de que el usuario -10- haya sido ya autenticado y haya iniciado sesión aplicando el procedimiento, según la invención, tal como se ha descrito anteriormente, el certificado de usuario es introducido por la entidad -16- en el documento producido de este modo, donde el certificado de usuario dispone de la clave de firma del usuario, y se obtiene en segundo plano desde el módulo -28- de provisión de claves conectado a la entidad -16- utilizando información que identifica inequívocamente al usuario en el módulo -28- de provisión de claves. Para conseguir esto, la entidad -16- debería saber qué proveedor de claves proporciona la clave de firma aplicada actualmente del usuario -10- (el usuario -10- puede especificar esto previamente).

Por lo tanto, en esta realización se prepara un contrato a firmar por el usuario -10- y la entidad -16- utilizando los datos solicitados al usuario después del inicio de sesión, y a continuación el contrato se firma utilizando la clave de firma de la entidad -16- y la clave de firma del usuario -10-, estando ésta última almacenada en el módulo -28- de provisión de claves. La operación de firma, realizada en el módulo -28- de provisión de claves, es aprobada por el usuario -10- aplicando un certificado de autenticación residente en el dispositivo móvil -14-.

La figura 2 muestra una realización del procedimiento según la invención en la que se requiere la autenticación llevada a cabo utilizando el procedimiento inventivo para preparar la firma digital del usuario. En esta realización la función del módulo de autenticación es desempeñada por el módulo -28- de provisión de claves.

Según la figura 2, es posible seleccionar el certificado de firmante del usuario -10- incluso cuando el usuario -10- accede de forma anónima al módulo de provisión de claves -20- de la entidad -16- o después de una autenticación que no está basada en certificados. En ese caso, el certificado de firmante es solicitado al módulo de provisión de claves -26- no por la entidad -16- sino por el dispositivo móvil -14- del usuario -10-.

En esta realización el módulo de contacto -20- se aplica para enviar la dirección de red (URL) del módulo -28- de provisión de claves al dispositivo móvil -14- en un mensaje de autenticación de tal manera que se pueda realizar la operación de firma. El parámetro de dirección de red comprende la dirección de la entidad -16- donde el módulo de provisión de claves -26- debe enviar el certificado de firmante del usuario -10-. A continuación, el dispositivo móvil -14- se redirige al módulo de contacto -20- de la entidad -16-, donde continúa la operación de firma.

La entidad -16- genera a continuación un resumen criptográfico del documento que se ha complementado con su certificado de firmante y preparado para ser firmado por el usuario -10-. El tipo del algoritmo de resumen criptográfico aplicado (sha1, sha256, sha384, sha512) se debería indicar preferentemente al inicio del valor del resumen criptográfico generado. Por lo tanto, el documento a firmar que se identifica mediante el resumen criptográfico ya comprende el certificado de firmante de la entidad -16-.

En la presente realización la función del módulo de autenticación se lleva a cabo por el módulo -28- de provisión de claves. Por consiguiente, el enlace a enviar al dispositivo móvil -14- en el mensaje de autenticación es generado por el módulo de contacto -20- como sigue. El enlace comprende la dirección del sitio web del módulo -28- de provisión de claves que solicita el certificado de autenticación (es decir, la dirección de red).

Los siguientes parámetros GET se especifican en el URL:

- id: un identificador único de la entidad -16- que conoce el módulo de provisión de claves.
- par: los parámetros que se cifran utilizando una clave simétrica (ϕ) conocida por la entidad -16- y por el módulo -28-

de provisión de claves.

○ resumen criptográfico: resumen criptográfico del documento a firmar

○ idtr: identificador de la transacción

○ idusuario: un identificador único del usuario -10-, que es conocido por la entidad -16- y por el módulo -28- de provisión de claves, y

○ de forma opcional, se pueden especificar asimismo parámetros adicionales

https://<dirección del proveedor de claves>/?id=<id>&par=ϕ(par)

Se debe destacar en este caso que los datos confidenciales, tales como el resumen criptográfico, son enviados de forma cifrada. Se debe observar que la longitud del enlace generado no puede ser mayor de la que se podría contener en el mensaje de autenticación.

De manera similar a lo descrito anteriormente, el módulo de contacto -20- pone a disposición del usuario -10- el enlace generado (la dirección de red) en un mensaje MQ. En caso de que se apliquen mensajes de tipo cola de mensajes, se utilizan los canales de comunicación -100-, -102-, -104-, -106-, -108-, -110-, -112- mencionados anteriormente.

El usuario abre (por ejemplo en un navegador u otra aplicación) el enlace recibido en un mensaje de tipo cola de mensajes. El enlace es recibido por el dispositivo móvil en un mensaje MQ, y éste envía un acuse de recibo firmado relacionado con el mensaje MQ recibido por medio del módulo -26- de cola de mensajes, utilizando la clave de firma almacenada preferentemente en el dispositivo móvil -14-.

El enlace transferido de este modo al dispositivo móvil -14- se abre en una aplicación, habitualmente en un navegador -que admite autenticación basada en certificados. La página web que aparece es la página web del módulo -28- de provisión de claves que solicita la autenticación basada en certificados.

A continuación se lleva a cabo la autenticación en el dispositivo móvil -14- de la manera descrita anteriormente, utilizando un certificado, el módulo -28- de provisión de claves, y también un canal de comunicación -126- entre el módulo -28- de provisión de claves y el proveedor -18- de certificación. El módulo -28- de provisión de claves realiza por lo tanto una comprobación de revocación en el certificado de usuario utilizando OCSP (protocolo de estado de certificados en línea) o una CRL (lista de revocación de certificados) en colaboración con el proveedor -18- de certificación. En caso de que el certificado sea inválido (se haya suspendido, revocado, o la comprobación haya fallado), o si es válido pero no existe una clave de firma o una clave de cifrado correspondiente en el módulo -28- de provisión de claves, el módulo -28- de provisión de claves devuelve un mensaje de error al dispositivo móvil -14- y al módulo de contacto -20-.

Si la autenticación es satisfactoria, es decir, la verificación del certificado bidireccional se ha realizado satisfactoriamente, la clave de firma del usuario -10- (almacenada en el módulo de almacenamiento de claves conectado al módulo -28- de provisión de claves) es identificada de manera inequívoca por el módulo de provisión de claves -28- aplicando el certificado de usuario. El módulo de almacenamiento de claves se implementa preferentemente como un denominado HSM (módulo de seguridad hardware). En la siguiente etapa el módulo -28- de provisión de claves lee de su base de datos la clave o la contraseña de cifrado simétrica que es común con la entidad -16- utilizando el parámetro "id" no cifrado que se envió previamente junto con el enlace, descifra el parámetro GET cifrado, y lo utiliza para generar los otros parámetros requeridos.

Utilizando la clave almacenada en el módulo HSM especificado y aplicando la autenticación basada en certificados, el módulo de provisión de claves firma el resumen criptográfico desciframiento del parámetro GET cifrado. A continuación, el módulo -28- de provisión de claves notifica a la entidad -16- especificada en el parámetro GET a través de una conexión HTTPS que posee un resumen criptográfico para trasferirle, y que el resumen criptográfico ha sido firmado por el usuario -10- de la entidad -16-.

Con el fin de poder recibir los datos firmados por el usuario, la entidad -16- tiene que demostrar al módulo -28- de provisión de claves que la propia entidad -16- había solicitado al usuario -10- que firmase el documento perteneciente al resumen criptográfico.

Para ello, envía el resumen criptográfico perteneciente al documento dado al módulo -28- de provisión de claves incorporado en un documento (archivo txt, etc.) firmado con su propia clave. Es preferible especificar en el documento firmado de este modo la transacción del usuario a la que pertenece el resumen criptográfico dado.

El documento que comprende el resumen criptográfico firmado por la entidad -16- es verificado por el módulo -28- de provisión de claves. En caso de que se compruebe que la firma es válida y el resumen criptográfico comprendido en

el documento firmado sea el mismo que el resumen criptográfico pasado por el usuario -10- en el parámetro GET, se demuestra que la firma del resumen criptográfico había sido solicitada por la entidad -16-, y por lo tanto el resumen criptográfico no fue falsificado con ésta. A continuación, el módulo -28- de provisión de claves pasa el resumen criptográfico firmado por el usuario -10- a la entidad -16-. El resumen criptográfico firmado de forma electrónica por la entidad -16- es archivado por el módulo de provisión de claves como evidencia. Utilizando este documento, en una ocasión posterior el módulo -28- de provisión de claves puede probar que firmó utilizando la clave del usuario -10- un resumen criptográfico perteneciente a un documento cuya firma se había solicitado por una tercera parte, la entidad -16-.

A continuación el usuario -10- es informado de la operación de firma satisfactoria o fallida mediante el módulo de contacto -20- preferentemente tanto por medio del terminal -12- como del módulo -26- de cola de mensajes (si existe un canal de comunicación de ese tipo entre el banco/organización y el dispositivo móvil del cliente).

Las etapas llevadas a cabo aplicando la presente realización se pueden resumir como sigue: se detecta un contacto para la firma de un documento por medio del módulo de contacto -20-; se prepara un contrato firmado por la entidad -16- y para firmar por el usuario -10- utilizando datos solicitados al usuario -10-; y se genera un resumen criptográfico del contrato. En la presente realización, el módulo de autenticación es el módulo -28- de provisión de claves. Según la presente realización, la dirección de red del módulo de provisión de claves -24- se envía a continuación al dispositivo móvil -14- del usuario -10- en un mensaje de autenticación por medio del módulo de contacto -20-, y el resumen criptográfico cifrado se envía asimismo en el mensaje de autenticación. A continuación, en caso de que el canal de comunicación entre el dispositivo móvil -14- y el módulo -28- de provisión de claves se establezca satisfactoriamente (es decir, en caso de una autenticación satisfactoria), el resumen criptográfico cifrado y un identificador de la entidad -16- se envían al módulo -28- de provisión de claves, la entidad -16- se identifica mediante el módulo -28- de provisión de claves y el resumen criptográfico cifrado se descifra por medio de la clave asignada a la entidad -16-, y el resumen criptográfico se firma a continuación utilizando la clave del usuario -10- disponible en el módulo -28- de provisión de claves, y, verificando con la entidad -16- que el resumen criptográfico se recibió desde la entidad -16-, el resumen criptográfico se envía desde el módulo -28- de provisión de claves a la entidad -16-.

Según otra realización, el proceso de firma también se puede llevar a cabo firmando el resumen criptográfico utilizando la clave de firma residente en el dispositivo móvil inteligente del cliente. En este caso no es necesario un proveedor de claves externo, aunque el módulo de contacto -20- de la entidad -16- sigue siendo responsable de generar el documento a firmar en un formato apropiado apto para firma, de generar el resumen criptográfico, y de insertar el resumen criptográfico firmado y cerrar el documento cumplimentado.

En esta realización, el dispositivo móvil -14- comunica con el módulo -28- de provisión de claves por medio de canales de comunicación -122- y -124-; estando dirigido el canal de comunicación -122- desde el dispositivo móvil -14- hacia el módulo -28- de provisión de claves, y el canal de comunicación -124- en el sentido inverso. El módulo -28- de provisión de claves se conecta al módulo de contacto -20- por medio de canales de comunicación -128- y -130-; estando dirigido el canal de comunicación -128- desde el módulo -28- de provisión de claves hacia el módulo de contacto -20-, y el canal de comunicación -130- en el sentido inverso.

La realización detallada anteriormente implementa una funcionalidad de firma digital distribuida que permite tanto al usuario como a la entidad firmar los documentos (por ejemplo, contratos) que poseen. La característica más importante de un esquema de firma digital distribuido es que la entidad nunca posee la clave de firma privada del cliente que el cliente almacenó bien en un dispositivo móvil inteligente o en una tercera parte fiable (en la realización descrita anteriormente, el módulo de provisión de claves). Durante la operación de creación de la firma, el documento a firmar es preparado por la entidad en un formato que cumple un estándar de firma digital (por ejemplo, XAdES, PAdES). La propia operación de firma es realizada no por la entidad sino por el dispositivo móvil del usuario, o por una tercera parte fiable (el módulo de provisión de claves), después de la autenticación utilizando un certificado residente en el dispositivo móvil. El dispositivo móvil del usuario recibe solamente el resumen criptográfico del documento a firmar que es generado por la entidad. El resumen criptográfico se firma bien utilizando la clave privada del firmante almacenada en el dispositivo móvil, o, después de pasarla al módulo de provisión de claves, utilizando la clave del hardware protegido HSM almacenada en el mismo. Dado que solo recibe el resumen criptográfico, el módulo de provisión de claves nunca estará en posesión del contenido de los documentos a firmar. El resumen criptográfico firmado se devuelve a la entidad bien desde el dispositivo móvil o desde el módulo de provisión de claves, insertándolo la entidad en el documento sin finalizar que se ha preparado para la firma. La operación de firma del cliente se completa de este modo, y la entidad puede insertar otras firmas o marcas de tiempo. Para cada etapa del proceso de firma, la entidad solicita una autenticación basada en certificados a todas las partes. Además de proporcionar una identificación segura del usuario, la aplicación de la funcionalidad de firma de la entidad permite llevar a cabo una administración fiable en base a la firma electrónica remota.

El procedimiento, según la invención, se puede aplicar asimismo al desciframiento/descodificación de documentos. En ese caso la operación de desciframiento/descodificación se reduce a una autenticación realizada con el procedimiento según la invención.

En la presente realización, el usuario/cliente posee un documento cifrado, que recibió por ejemplo adjunto en un

mensaje de correo electrónico, o de algún otro modo. En primer lugar, como etapa de contacto del proceso de desciframiento del documento, el usuario pasa (carga) el documento que se tiene que descifrar al módulo de contacto, es decir, por ejemplo, lo envía en un mensaje de correo electrónico. A continuación, el módulo de contacto extrae del documento cifrado cargado la clave simétrica aplicada para cifrar el documento. La clave simétrica ha sido cifrada utilizando el certificado de cifrado del usuario. El enlace que se va a enviar al dispositivo móvil del usuario es generado por el módulo de contacto. De manera análoga al caso descrito anteriormente, el módulo de autenticación es el módulo de provisión de claves. El enlace comprende la dirección de red del módulo de autenticación. Los siguientes parámetros GET se especifican en el URL:

- id: un identificador de la entidad
- par: parámetros que se cifran utilizando una clave simétrica (ϕ) conocida por la entidad y el proveedor de claves:
  - clavecifrada: una clave simétrica cifrada utilizando el certificado de usuario
  - idtr: un identificador de la transacción
  - idusuario: un identificador único del usuario (por ejemplo, la dirección de correo)

https://<dirección del proveedor de claves>/?id=<id>&par=ϕ(par)

El módulo de contacto envía el enlace generado al usuario en un mensaje de autenticación. Abriendo el enlace utilizando su dispositivo móvil, el usuario inicia una conexión con el módulo de provisión de claves.

La autenticación se lleva a cabo por medio de una conexión de internet utilizando el certificado de autenticación residente en el dispositivo móvil, así como el certificado de entidad. En caso de una autenticación satisfactoria, el módulo de provisión de claves utiliza el certificado de usuario para identificar inequívocamente la clave de desciframiento del usuario, que preferentemente se almacena en un módulo HSM. En la siguiente etapa el módulo de provisión de claves lee de su base de datos la clave simétrica o, de forma opcional, la contraseña compartida con la entidad utilizando el parámetro "id" no cifrado que identifica al módulo de contacto, descifra el parámetro GET cifrado, y lo utiliza para generar los otros parámetros requeridos. La clave simétrica cifrada, obtenida del parámetro GET cifrado, se descifra utilizando la clave de desciframiento almacenada en el módulo HSM.

La clave simétrica descifrada se envía posteriormente por medio de una conexión HTTPS desde el módulo de provisión de claves al módulo de contacto especificado en el parámetro GET.

El módulo de contacto utiliza a continuación la clave simétrica recibida del módulo de provisión de claves para descifrar el documento del usuario, y hace que el documento se pueda descargar por medio de un enlace HTTPS. El enlace se envía al usuario bien por medio del terminal o en un mensaje de correo electrónico. De este modo, el documento desciframiento se pone a disposición del usuario.

Se muestra otra realización más de la invención en la figura 3. Según esta realización la entidad -16- es un banco -25- emisor de tarjetas, y un contacto de un usuario -10- que presenta datos de una tarjeta de crédito por medio del terminal -12- en una interfaz de pago de una tienda web, es detectado por medio del módulo de contacto -20- del banco -25- emisor de tarjetas a través de un servidor -30- de la tienda web, un servidor -32- del proveedor de servicios bancarios de la tienda web, y un servidor -34- de una empresa de tarjetas de crédito. En esta realización, se aplica un mensaje de tipo cola de mensajes como mensaje de autenticación. La presente realización excluye la aplicación de códigos QR como mensaje de autenticación, ya que se aplica el terminal -12- para mostrar la interfaz de pago de la tienda web que no es capaz de mostrar un código QR.

Por lo tanto, en esta realización el usuario (cliente) -10- que posee el dispositivo móvil -14- inicia una transacción de pago con tarjeta en el navegador del terminal -12-. La información de la transacción del pago con tarjeta introducida por el usuario en la interfaz de la tienda web se pasa por medio del servidor -32- del banco proveedor de servicios bancarios de la tienda web, y el servidor -34- de la empresa de tarjetas de crédito, llegando finalmente al banco emisor de la tarjeta -25-.

El banco emisor de la tarjeta -25- verifica los datos relacionados con el pago con tarjeta: se asegura de que la tarjeta existe y tiene fondos, y que no se ha bloqueado. Si la verificación es positiva, entonces antes de confirmar la transacción, se envía un mensaje de autenticación al usuario, notificándole que confirme el pago con tarjeta. El mensaje de autenticación se puede enviar utilizando el protocolo MQ. En caso de que se envíe un mensaje MQ, el dispositivo móvil inteligente del titular de la tarjeta debe conectarse al módulo -26- de cola de mensajes del banco emisor de la tarjeta -25-.

El mensaje de autenticación se aplica para enviar la dirección de red del módulo de autenticación -24- al dispositivo móvil -14-. El URL transferido no comprende ninguna información sobre el contenido de la transacción con tarjeta, solo un identificador de la transacción compuesto por números aleatorios, que puede ser utilizado para leer los datos

relacionados con la transacción con tarjeta en el dispositivo móvil -14- solo en caso de una autenticación satisfactoria basada en certificados.

El URL de autenticación que se envía en el mensaje de autenticación y se aplica para confirmar la transacción se construye como sigue: https://<sitioweb-secundario>/?idtr=ϕ(idtr)

donde

ϕ es una clave simétrica del banco emisor

idtr es un identificador de la transacción (tal como el identificador de una transacción de pago con tarjeta) ϕ(idtr) es el idtr cifrado utilizando ϕ.

Después de enviar el mensaje de autenticación el dispositivo móvil -14- utiliza su clave privada y el certificado que le pertenece para conectarse al módulo de autenticación -24- del banco emisor de la tarjeta -25- que solicita la autenticación basada en certificados, y que puede encontrarse en la ubicación de red enviada en un mensaje MQ.

De manera similar a lo descrito anteriormente, el módulo de autenticación -24- del banco emisor de la tarjeta -25- realiza una comprobación de revocación en el certificado del cliente (residente en su dispositivo móvil -14-) utilizando OC-SP o CRL. Además, el dispositivo móvil -14- verifica el certificado del módulo de autenticación -24-. En caso de que el certificado del dispositivo móvil sea inválido (se haya suspendido, revocado, o la comprobación haya fallado), se devuelve un mensaje de error al dispositivo móvil inteligente. En caso de que el banco emisor de la tarjeta -25- se comunique con el dispositivo móvil del cliente por medio de una conexión MQ, la autenticación fallida se notifica asimismo al dispositivo móvil en un mensaje MQ.

Si la confirmación falla por algún motivo (debido a un certificado inválido, rechazo, o un límite de tiempo), el mensaje de rechazo es enviado por el banco emisor al servidor -30- de la tienda web por medio del servidor -34- de la empresa de tarjetas de crédito y el servidor -32- del proveedor de servicios bancarios. El resultado de la transacción de pago con tarjeta aparece en la pantalla de visualización del terminal -12-.

En caso de que la autenticación sea satisfactoria, y en caso de que los datos comprendidos en el certificado, y -en base al identificador de la transacción con tarjeta- la autenticación haya sido aceptada por el módulo de contacto -20- del banco emisor de la tarjeta -25-, el módulo de autenticación -24- del banco emisor de la tarjeta -25- devuelve los datos de la transacción con tarjeta al dispositivo móvil -14-. En esta etapa la transacción todavía no se ha aprobado en el dispositivo móvil.

Después de revisar la información relacionada con la transacción de pago con tarjeta, el cliente puede confirmar o rechazar la transacción de pago con tarjeta por medio del módulo de autenticación -24- utilizando el dispositivo móvil -14- (por ejemplo, el navegador del mismo).

En caso de que el banco emisor de la tarjeta -25- se comunique con el dispositivo móvil por medio de una conexión MQ, también se notifica al dispositivo móvil en un mensaje MQ la aprobación satisfactoria de la transacción, o que la transacción ha fallado (debido a un rechazo).

El banco emisor de la tarjeta envía un aviso del evento de confirmación o rechazo de la transacción de pago con tarjeta del cliente al servidor del comerciante por medio de los sistemas de información de la empresa -34- de tarjetas de crédito y del banco -32- proveedor de servicios. El resultado de la transacción de pago con tarjeta aparece en la interfaz de usuario de la tienda web.

Según la presente realización, en caso de que se establezca un canal de comunicación entre el dispositivo móvil -14- y el módulo de autenticación -24-, los datos de pago de la tienda web se envían al dispositivo móvil -14-, y se recibe la información sobre la autorización o rechazo de los datos de pago del usuario -10-.

La realización de la figura 3 se muestra asimismo en la figura 4. Según soluciones de la técnica anterior el banco emisor de la tarjeta verifica los datos de la tarjeta y el estado de los fondos, y, en caso de una verificación positiva, confirma la transacción sin solicitar una confirmación del titular de la tarjeta. Debido a la naturaleza del proceso de pago en línea, en caso de que se vean comprometidos los datos de la tarjeta del cliente, el atacante puede hacer una utilización fraudulenta de la tarjeta sin que el cliente lo advierta, ya que la tarjeta sigue estando en poder del cliente.

El procedimiento de autenticación según la invención permite que el cliente confirme el pago utilizando un canal alternativo, disponiendo al mismo tiempo que, de los participantes del proceso de pago con tarjeta, solamente los servidores del banco emisor de la tarjeta -25- y el dispositivo móvil del cliente se tienen que involucrar en el proceso de autenticación. Otros componentes de la cadena no perciben que se está llevando a cabo un segundo proceso de autenticación en segundo plano. La cuestión clave es la manera en que el servidor del banco emisor de la tarjeta

establece la conexión con el dispositivo móvil inteligente del cliente después de que el servidor ha recibido los datos relacionados con la transacción de pago en línea dada, ya que el límite de tiempo para la confirmación es extremadamente corto. Las técnicas de mensajería que implican SMS o mensajes de envío automatizado pueden parecer una solución obvia, pero ambas tienen las siguientes desventajas:

• Por su naturaleza, estas técnicas no garantizan que el mensaje se envíe inmediatamente, y que el dispositivo móvil del cliente lo recibirá en un tiempo corto. Ningún proveedor de SMS lo garantiza.

• En ambos casos, se requiere una tercera parte externa (tal como un proveedor de SMS) para transmitir los mensajes, lo que hace que el banco emisor dependa en gran medida de estas partes.

• Ninguna de estas soluciones proporciona ninguna prueba a la parte emisora (el banco emisor de la tarjeta) de que el mensaje solicitando confirmación de la autorización se ha enviado realmente al cliente. Esto puede causar graves dificultades al banco emisor si se produce una disputa.

• La aplicación de mensajes SMS puede causar importantes costes adicionales de las transacciones.

La invención en la que el mensaje de autenticación se transfiere en un mensaje MQ elimina estas desventajas. El banco emisor de la tarjeta -25- puede enviar un mensaje de manera síncrona al dispositivo móvil conectado a través del módulo -26- de cola de mensajes sin implicar a un proveedor de servicios externo. De manera análoga a una transacción de transferencia bancaria, el mensaje comprende la dirección de red del módulo de autenticación -24-, incluyéndose como un parámetro el identificador correspondiente a la transacción con tarjeta en el mensaje. El mensaje MQ no comprende ningún dato sensible. La transacción puede ser consultada, confirmada o rechazada en el dispositivo móvil solamente después de una autenticación satisfactoria. La clave de firma residente en el dispositivo móvil se puede aplicar al envío de un acuse de recibo del mensaje MQ recibido del banco emisor de la tarjeta. El acuse de recibo puede ser archivado por el sistema del banco emisor como una prueba de la transacción.

Además de la banca en línea, la solución según la presente invención puede ser aplicada para eliminar completamente los fraudes relacionados con la retirada de efectivo de ATM que son capaces de mostrar códigos QR.

En caso de pérdida o robo del dispositivo móvil, el proceso de bloqueo del dispositivo es el mismo que el proceso de bloqueo de tarjetas bancarias perdidas/robadas. En cuanto el usuario informa de la pérdida o robo de su dispositivo móvil, los certificados residentes en el dispositivo se revocan inmediatamente, de tal modo que no se puede confirmar ninguna transacción adicional usándolos.

La solución según la invención puede acelerar de forma significativa los procesos bancarios para los clientes. Los clientes que poseen dispositivos móviles involucrados en el procedimiento pueden autorizar contratos bancarios en el hogar, utilizando sus firmas digitales. Los certificados de autenticación instalados en el dispositivo móvil se pueden aplicar asimismo para la conexión a redes VPN. La solución, según la invención, admite la confirmación de transacciones que requieren múltiples autorizadores.

Una realización de la invención se refiere a un sistema para autenticar un usuario en una entidad. El sistema según la invención comprende un módulo de contacto -20- adaptado para detectar un contacto de un usuario -10- con la entidad -16-, un terminal -12- adaptado para recibir el contacto iniciado por el usuario -10- con el módulo de contacto -20-, un módulo de autenticación -24- adaptado para autenticar al usuario -10-, y un dispositivo móvil -14- adaptado para recibir una dirección de red del módulo de autenticación -24- en un mensaje de autenticación desde el módulo de contacto -20-. En el sistema, según la invención, el dispositivo móvil está adaptado para verificar la aceptabilidad de un certificado de entidad del módulo de autenticación -24- en base a la dirección de red, y el módulo de autenticación -24- está adaptado para verificar la aceptabilidad de un certificado del dispositivo móvil -14-, y en caso de que el certificado de entidad y el certificado de usuario sean aceptables, el usuario -10- es autenticado en la entidad -16- mediante el sistema estableciendo un canal de comunicación entre el dispositivo móvil -14- y el módulo de autenticación -24-, mientras que en caso de que el certificado de entidad o el certificado de usuario no sean aceptables, el usuario -10- es rechazado en la entidad -16-.

Por supuesto, la invención no se limita a las realizaciones preferentes descritas en detalle anteriormente, sino que son posibles otras variantes, modificaciones, cambios y desarrollos dentro del alcance de protección definido por las reivindicaciones.

REIVINDICACIONES

1. Procedimiento para autenticar a un usuario (10) en una entidad (16), que comprende las etapas de

- detectar, por medio de un módulo de contacto (20) de la entidad (16), un contacto del usuario (10) realizado en un navegador de un terminal (12), y

- enviar, por medio del módulo de contacto (20), una dirección de red de un módulo de autenticación (24) de la entidad (16) a un dispositivo móvil (14) del usuario (10) en un mensaje de autenticación,

caracterizado por

- utilizar un mensaje de tipo cola de mensajes como el mensaje de autenticación, dicho mensaje se envía por medio de un módulo (26) de cola de mensajes correspondiente a la entidad (16), y un acuse de recibo firmado con una clave del usuario (10) se envía desde el dispositivo móvil (14) al módulo de contacto (20) después de que el mensaje de tipo cola de mensajes es recibido por el dispositivo móvil (14) que está conectado al módulo (26) de cola de mensaje,

- verificar la aceptabilidad de un certificado de entidad del módulo de autenticación (24) por medio del dispositivo móvil (14) en base a la dirección de red, y verificar la aceptabilidad de un certificado de usuario del dispositivo móvil (14) por medio del módulo de autenticación (24), y

- en caso de que el certificado de entidad y el certificado de usuario sean aceptables, autenticar al usuario (10) en la entidad (16) estableciendo un canal de comunicación (114, 120, 122, 124) entre el dispositivo móvil (14) y el módulo de autenticación (24), mientras que en caso de que el certificado de entidad o el certificado de usuario no sean aceptables, rechazar al usuario (10) en la entidad (16).

2. Procedimiento, según la reivindicación 1, **caracterizado por que**

- la etapa de verificar la aceptabilidad del certificado de entidad comprende verificar por medio del dispositivo móvil (14)

- la validez del certificado de entidad en un proveedor de certificación de entidad (18), y

- la fiabilidad del proveedor de certificación de entidad (18),

- la etapa de verificar la aceptabilidad del certificado de usuario comprende verificar por medio del módulo de autenticación (24),

- la validez del certificado de usuario en el proveedor de certificación de usuario (18), y

- la fiabilidad del proveedor de certificación de usuario (18).

3. Procedimiento, según la reivindicación 2, **caracterizado por que**

- el proveedor de certificación de entidad (18) corresponde a una clave privada de la entidad del módulo de autenticación (24), y el certificado de entidad es firmado por el proveedor de certificación de entidad (18), y

- el proveedor de certificación de usuario (18) corresponde a una clave privada de usuario del dispositivo móvil (14), y el certificado de usuario es firmado por el proveedor de certificación de usuario (18).

4. Procedimiento, según la reivindicación 3, **caracterizado por que** la clave privada de usuario se genera en el dispositivo móvil (14).

5. Procedimiento, según las reivindicaciones 1 a 4, **caracterizado por que** la entidad (16) es un banco emisor de las tarjetas (25), y un contacto de un usuario (10) mediante el envío de datos de una tarjeta de crédito por medio del terminal (12) en una interfaz de pago de una tienda web se detecta por medio de un módulo de contacto (20) del banco emisor de la tarjeta (25) por medio de un servidor (30) de la tienda web, por medio de un servidor (32) de un proveedor de servicios bancarios de la tienda web, y por medio de un servidor (34) de una empresa de tarjetas de crédito.

6. Procedimiento, según la reivindicación 5, **caracterizado por que**, en caso de que se establezca un canal de comunicación entre el dispositivo móvil (14) y el módulo de autenticación (24), los datos de pago de la tienda web son enviados al dispositivo móvil (14), y se recibe la información sobre la autorización o rechazo de los datos de pago por el usuario (10).

7. Procedimiento, según cualquiera de las reivindicaciones 1 a 6, **caracterizado por** detectar, por medio del módulo de contacto (20), un contacto de inicio de sesión en el terminal (12) que muestra una interfaz de inicio de sesión de la entidad (16), y aceptar el inicio de sesión del usuario (10) en la entidad (16) en caso de que se establezca el canal de comunicación (114, 120, 122, 124) entre el módulo de autenticación (24) y el dispositivo móvil (14).

8. Procedimiento, según la reivindicación 7, **caracterizado por que**, después de que se ha llevado a cabo el inicio de sesión,

- se prepara un contrato a firmar por el usuario (10) y la entidad (16) utilizando los datos solicitados al usuario (10), y

- el contrato se firma con una clave de firma de la entidad (16) y con una clave de firma del usuario (10) extraída de un módulo de provisión de claves (28).

9. Procedimiento, según cualquiera de las reivindicaciones 1 a 6, **caracterizado por que**

- se detecta un contacto para una firma de un documento por medio del módulo de contacto (20),

- se prepara un contrato firmado por la entidad (16) y para firmar por el usuario (10) utilizando datos solicitados al usuario (10), y se genera un resumen criptográfico del contrato,

- el módulo de autenticación es un módulo de provisión de claves (28), y se envía una dirección de red del módulo de provisión de claves (28) al dispositivo móvil (14) del usuario (10) en un mensaje de autenticación por medio del módulo de contacto (20), y el resumen criptográfico se envía cifrado en el mensaje de autenticación,

- en caso de establecimiento del canal de comunicación entre el dispositivo móvil (14) y el módulo de provisión de claves (28)

- el resumen criptográfico cifrado y un identificador de la entidad (16) se envían al módulo de provisión de claves (28),

- la entidad (16) se identifica por medio del módulo de provisión de claves (28), y el resumen criptográfico cifrado se descifra por medio de una clave asignada a la entidad (16), y a continuación el resumen criptográfico se firma con una clave del usuario (10) que está en poder del módulo de provisión de claves (28), y

- el resumen criptográfico se envía a la entidad (16) desde el módulo de provisión de claves (28) verificando con la entidad (16) que el resumen criptográfico ha recibido de la entidad (16).

10. Procedimiento, según cualquiera de las reivindicaciones 1 a 6, **caracterizado por que**

- el módulo de contacto (20) detecta un contacto para el desciframiento de un documento, durante lo cual el usuario (10) envía un documento a descifrar al módulo de contacto (20),

- el módulo de autenticación es un módulo de provisión de claves (28), y se envía una dirección de red del módulo de provisión de claves (28) al dispositivo móvil (14) del usuario (10) en un mensaje de autenticación por medio del módulo de contacto (20), que comprende una clave simétrica cifrada que se cifra mediante una clave simétrica que es común con la entidad (16),

- en caso de establecerse un canal de comunicación entre el dispositivo móvil (14) y el módulo de provisión de claves (28), el módulo de provisión de claves (28)

- identifica una clave de desciframiento del usuario (10) por medio del certificado de usuario,

- por medio de un parámetro que identifica el módulo de contacto (20), recupera de su base de datos la clave simétrica que es común con la entidad (16), y genera la clave simétrica cifrada mediante el desciframiento por medio de la clave simétrica que es común con la entidad (16),

- descifra la clave simétrica cifrada por medio de la clave de desciframiento, y

- envía la clave simétrica descifrada al módulo de contacto (20), y

- el módulo de contacto (20) descifra el documento a decifrar por medio de la clave simétrica.

11. Procedimiento, según cualquiera de las reivindicaciones 1 a 10, **caracterizado por que** el certificado es un certificado de tipo X.509.

12. Procedimiento, según cualquiera de las reivindicaciones 1 a 11, **caracterizado por que** el canal de

comunicación es un canal de comunicación SSL bidireccional.

13. Sistema para autenticar a un usuario (10) en una entidad (16), que comprende

- un módulo de contacto (20) adaptado para detectar un contacto del usuario (10) con la entidad (16),

- un terminal (12) adaptado para recibir el contacto iniciado por el usuario (10) con el módulo de contacto (20),

- un módulo de autenticación (24) adaptado para autenticar al usuario (10), y

- un dispositivo móvil (14) adaptado para recibir una dirección de red del módulo de autenticación (24) en un mensaje de autenticación desde el módulo de contacto (20),

caracterizado por que

- el sistema comprende además un módulo (26) de cola de mensajes correspondiente a la entidad (16), el mensaje de autenticación es un mensaje de tipo cola de mensajes enviado por medio del módulo (26) de cola de mensajes, y el dispositivo móvil (14) está adaptado para enviar un acuse de recibo firmado con una clave del usuario (10) al módulo de contacto (20) después de recibir el mensaje de tipo cola de mensajes, en el que el dispositivo móvil (14) está conectado al módulo (26) de cola de mensajes,

- el dispositivo móvil (14) está adaptado para verificar la aceptabilidad de un certificado de entidad del módulo de autenticación (24) en base a la dirección de red,

- el módulo de autenticación (24) está adaptado para verificar la aceptabilidad de un certificado de usuario del dispositivo móvil (14), y

- en caso de que el certificado de entidad y el certificado de usuario sean aceptables, el sistema autentica al usuario (10) en la entidad (16) estableciendo un canal de comunicación (114, 120, 122, 124) entre el dispositivo móvil (14) y el módulo de autenticación (24), mientras que en caso de que el certificado de entidad o el certificado de usuario no sean aceptables, el usuario (10) es rechazado en la entidad (16).

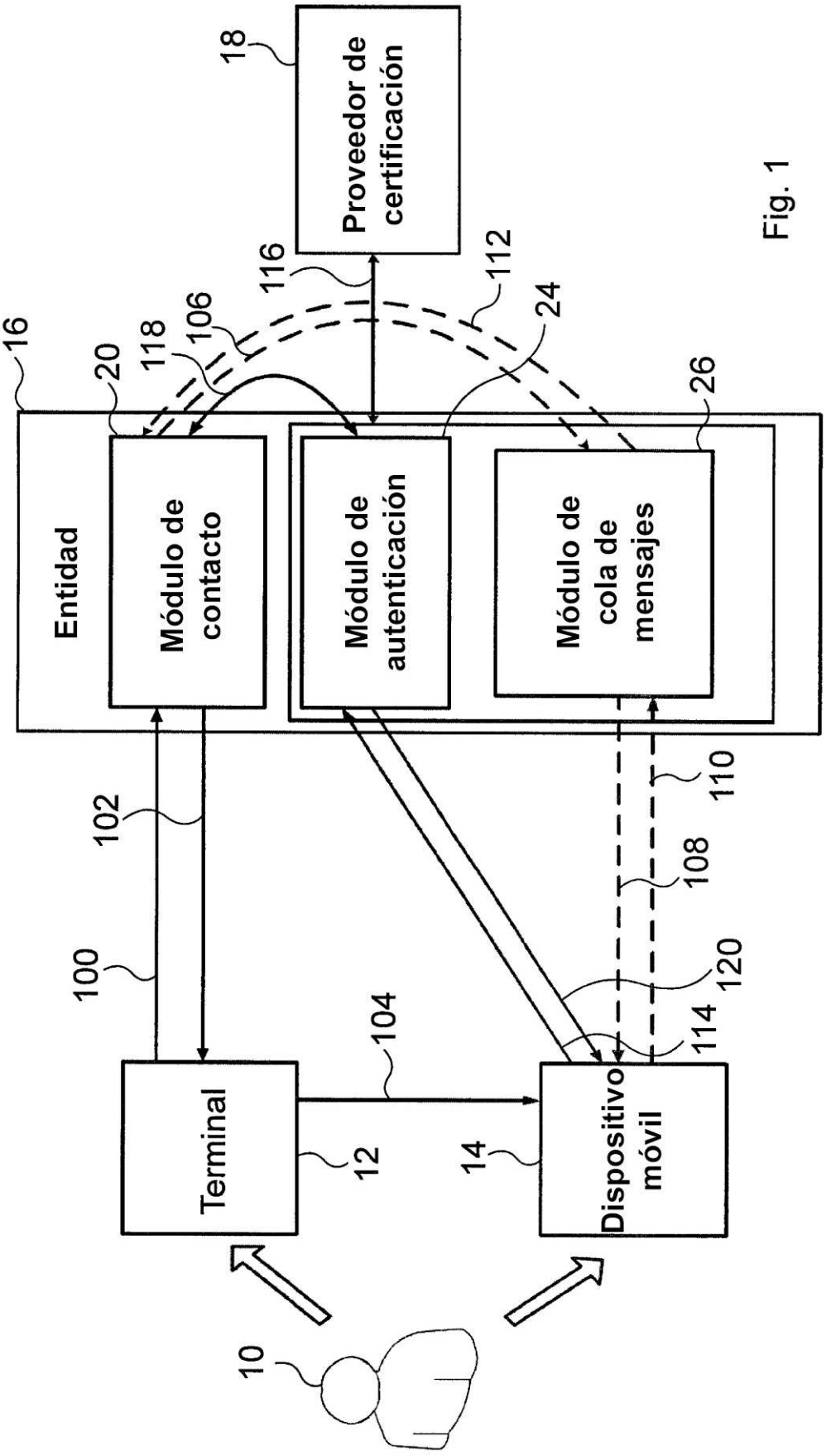
18
Proveedor de certificación
116
112
24
106
118
20
16
26
Entidad
Módulo de contacto
Módulo de autenticación
Módulo de cola de mensajes
110
102
108
100
120
104
114
Terminal
12
14
Dispositivo móvil
10

Fig. 1

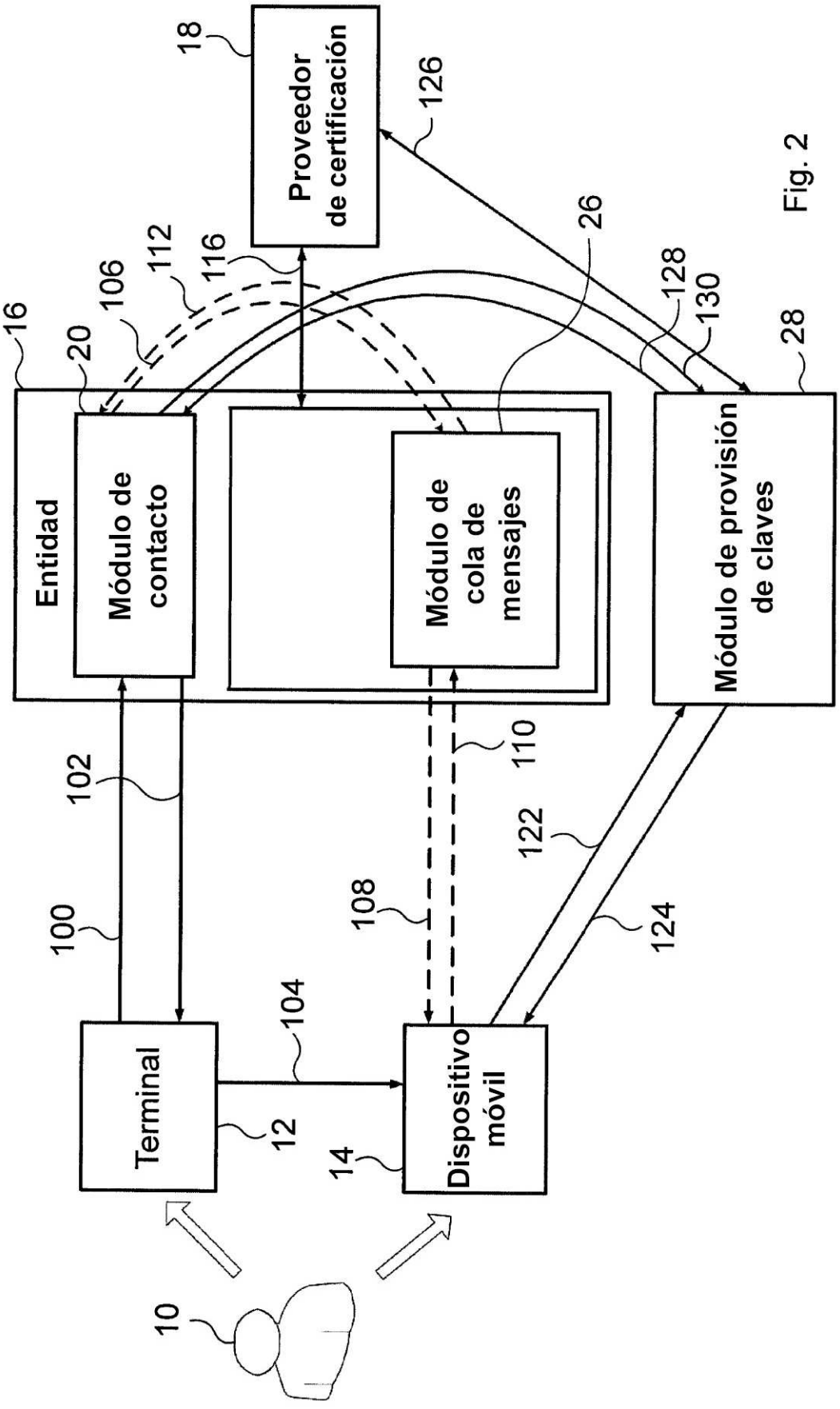
18
Proveedor de certificación
126
26
112
116
106
16
20
128
130
28
Entidad
Módulo de contacto
Módulo de cola de mensajes
Módulo de provisión de claves
102
110
122
100
108
124
104
Terminal
12
Dispositivo móvil
14
10

Fig. 2

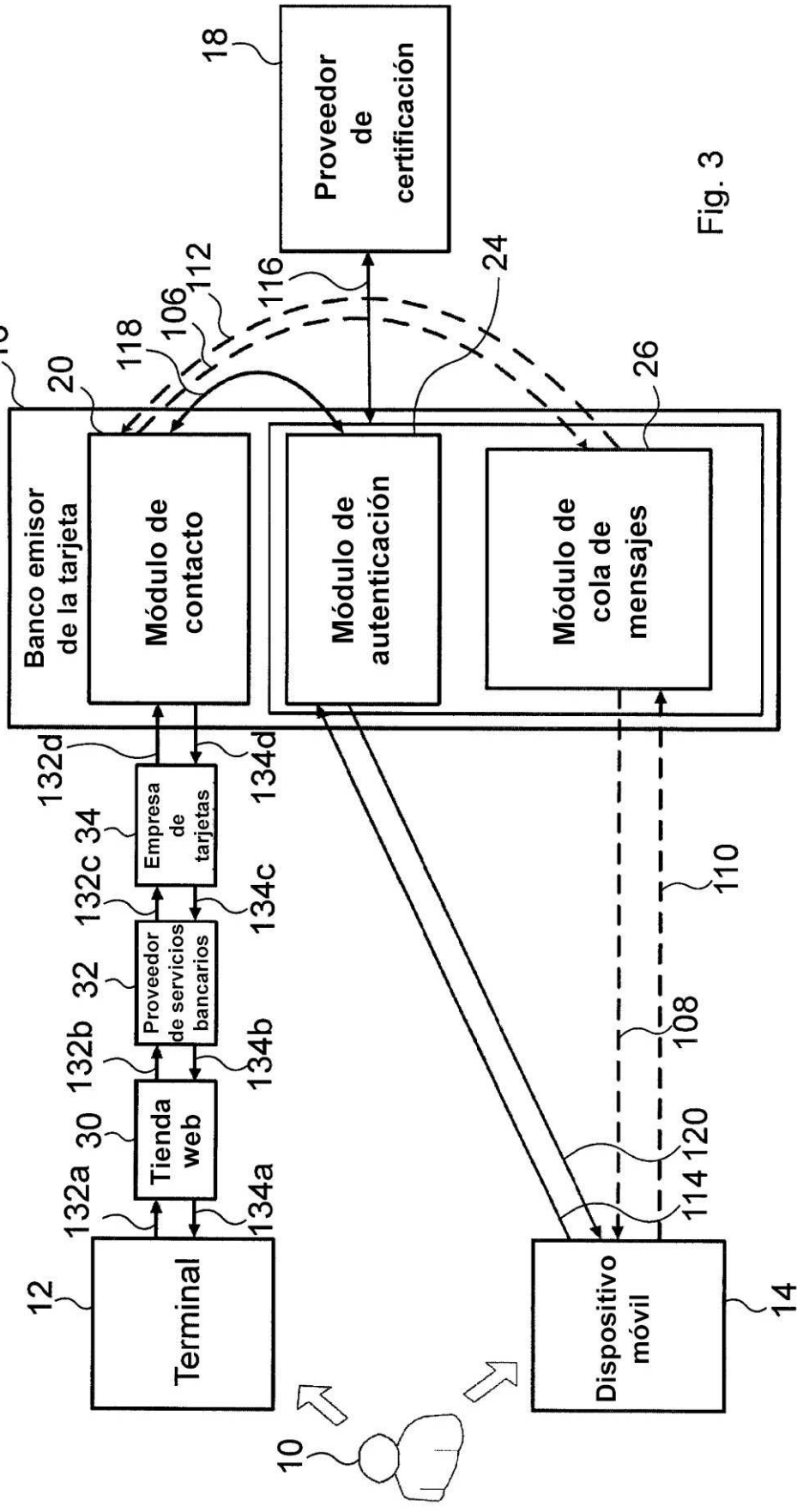
18
Proveedor de certificación
112
116
24
106
118
16
20
26
Banco emisor de la tarjeta
Módulo de contacto
Módulo de autenticación
Módulo de cola de mensajes
132d
134d
34
Empresa de tarjetas
132c
134c
32
Proveedor de servicios bancarios
132b
134b
30
Tienda web
132a
134a
110
108
120
114
12
Terminal
Dispositivo móvil
14
10

Fig. 3

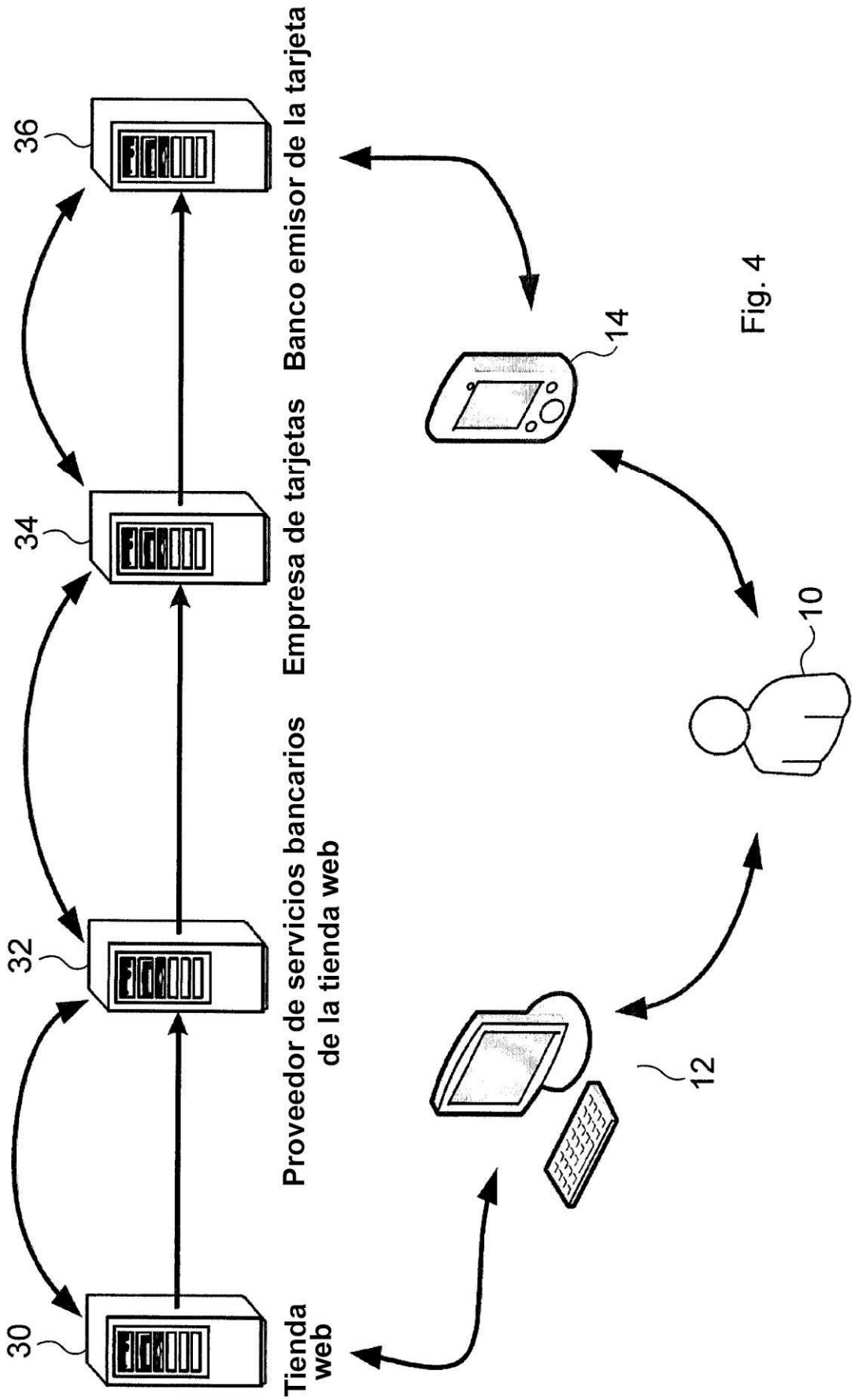
Tienda web
Proveedor de servicios bancarios de la tienda web
Empresa de tarjetas
Banco emisor de la tarjeta
30
32
34
36
12
14
10

Fig. 4