(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 601 505**

(51) Int. CI.:

H04L 9/08 (2006.01)
H04L 9/32 (2006.01)
H04L 29/06 (2006.01)
H04W 12/04 (2009.01)
H04W 12/06 (2009.01)
H04W 88/02 (2009.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **30.09.2011 PCT/IB2011/002305**

(87) Fecha y número de publicación internacional: **05.04.2012 WO12042367**

(96) Fecha de presentación y número de la solicitud europea: **30.09.2011 E 11828215 (1)**

(97) Fecha y número de publicación de la concesión europea: **03.08.2016 EP 2622786**

(54) Título: **Identificación de teléfono móvil y autenticación de comunicación**

(30) Prioridad:

07.01.2011 ZA 201100198
30.09.2010 ZA 201006995

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
15.02.2017

(73) Titular/es:

ENTERSEKT INTERNATIONAL LIMITED (100.0%)
Level 3, Alexander House, 35 Cybercity
Ebene , MU

(72) Inventor/es:

BRAND, CHRISTIAAN, JOHANNES, PETRUS;
VAN TONDER, ALBERTUS, STEFANUS y
MULLER, DANIEL, JACOBUS

(74) Agente/Representante:

CARPINTERO LÓPEZ, Mario

DESCRIPCIÓN

Identificación de teléfono móvil y autenticación de comunicación

Campo de la invención

Esta invención se refiere a la identificación de teléfonos móviles y a la autenticación y a la seguridad de los canales de comunicaciones entre teléfonos móviles y los servidores de aplicaciones. En particular, la invención se refiere a un sistema y procedimiento para autenticar y asegurar los canales de comunicaciones en línea entre los teléfonos móviles y los servidores de aplicaciones en línea de una manera que permita al servidor de aplicaciones validar la identidad del teléfono móvil y viceversa.

Antecedentes de la invención

En los negocios de módem de hoy en día, un número cada vez mayor de las transacciones se realizan electrónicamente a través de los servidores de aplicaciones en línea, por medio de comunicaciones a través de redes tales como, la más común, Internet. Mientras que tradicionalmente se realizaban desde ordenadores personales y otros dispositivos que normalmente tenían una considerable capacidad de procesamiento, cada vez más transacciones se realizan desde teléfonos móviles con acceso a Internet y otros dispositivos de mano móviles que no necesariamente tienen las mismas capacidades de procesamiento.

En el resto de esta memoria descriptiva, la expresión “teléfono móvil” debe interpretarse que incluye cualquier dispositivo de comunicaciones móvil capaz de comunicarse a través de una red de comunicaciones, tal como una red móvil, y tener al menos una cantidad limitada de capacidad de procesamiento. La expresión debería interpretarse para incluir específicamente todos los teléfonos móviles o celulares, pero también puede incluir ordenadores portables tales como los ordenadores portátiles, los ordenadores personales de mano y similares.

Un problema con las transacciones en línea convencionales es, sin embargo, el riesgo de seguridad inherente asociado con las comunicaciones en línea. Los operadores sin escrúpulos están desarrollando constantemente nuevas técnicas para interceptar la información transaccional y usar esta para estafar a las partes involucradas. Ejemplos de este tipo de amenazas a la seguridad incluyen el robo de identidad, ataques de hombre en el medio (MITM), pharming, phishing, examen de SMS/datos sobre el aire, secuestro de infraestructuras de terceras partes, troyanos, registradores de claves, así como varias combinaciones de estas amenazas.

En un intento de hacer transacciones en línea más seguras, se han desarrollado numerosas técnicas de seguridad. Una de estas técnicas, un ejemplo de la cual se conoce como autenticación de factor dos, utiliza el teléfono móvil del usuario como un dispositivo desacoplado de la transacción para proporcionar una capa adicional de seguridad. Debido a una relación de uno a uno que se supone que existe entre un usuario y su teléfono móvil, para la que esta tecnología se usa, se supone que el teléfono está siempre en posesión del usuario. Los mensajes del servicio de mensajes cortos (SMS) son actualmente el mecanismo preferido para los mensajes de seguridad y por lo general toman la forma de un mensaje de texto enviado por el proveedor de servicios (por ejemplo, una institución bancaria) al teléfono móvil del usuario. El mensaje incluye normalmente un solo pin único de una sola vez (OTP), que a continuación el usuario tiene que introducir manualmente en el entorno seguro al que desea acceder o antes de realizar una transacción segura, junto con los detalles normales de su inicio de sesión.

Si bien esta tecnología añade una capa adicional de seguridad, todavía es susceptible al abuso, ya que es posible interceptar los mensajes SMS a través de, por ejemplo, técnicas tales como la clonación de la tarjeta SIM. También requiere todavía que el usuario introduzca un código de 8 dígitos (o más) desde el teléfono móvil en el sitio web o de otra manera de la transacción segura que desea realizar. Otra desventaja de esta tecnología es el coste relativamente elevado que supone para la institución alojar la transacción segura, ya que tiene que enviar un mensaje SMS a través de un proveedor de red GSM cada vez que un usuario necesita autenticarse. La autenticación puede realizarse un número de veces durante cualquier sesión específica y cada uno los mensajes de este tipo serán facturados normalmente de manera individual por el proveedor de red GSM.

En esencia, este tipo de autenticación de factor dos no está completamente “fuera de banda” en el verdadero sentido de la palabra. Mientras que el OTP puede llegar al teléfono del usuario “fuera de banda”, el usuario tiene de nuevo que introducirle y transmitirle a través de la misma banda de comunicaciones, haciendo de este modo que sea susceptible a la interceptación una vez más. Si el navegador u otro canal de comunicaciones que se usa se han visto comprometidos, la transmisión del OTP se habrá visto igualmente comprometida.

Otro gran inconveniente de esta tecnología solo se ha hecho evidente ya que los teléfonos móviles se usan cada vez más como dispositivos para navegar por Internet y para las transacciones en línea. Un gran número de teléfonos móviles no permiten a los usuarios tener múltiples aplicaciones ejecutándose al mismo tiempo. Como resultado, el usuario no puede recibir un SMS con un OTP, mientras que navega por Internet en el teléfono a través de una aplicación de navegador de web. Esto requerirá que el usuario cierre el navegador antes de leer el SMS y el OTP, solo para a continuación tener que volver a iniciar el navegador con el fin de introducir el OTP en el sitio. Incluso en los casos en los que es posible tener múltiples aplicaciones activas en un momento dado, el cambio entre aplicaciones puede ser difícil e incómodo.

Además de lo que se ha dicho anteriormente, la mayoría de los protocolos de seguridad que se han desarrollado requieren una cantidad sustancial de capacidad de procesamiento con el fin de ser viables. Una de las medidas de seguridad más comunes usadas en las transacciones en línea de hoy en día es la seguridad de la capa de transporte (TLS) o su predecesor, la capa de conexión segura (SSL). SSL y TLS son ambas lo que se conoce como protocolos de cifrado y se usan para cifrar los segmentos de conexiones de red en la capa de aplicación para garantizar la seguridad del tránsito de extremo a extremo en la capa de transporte. SSL es, sin embargo, problemático para los teléfonos móviles por una variedad de razones, una de las cuales es el hecho de que los teléfonos generalmente no tienen la capacidad de procesamiento para calcular sus propios pares de claves de cifrado pública y privada que pueden usarse para una comunicación segura. Aparte de que en algunos casos potencialmente sea imposible para los teléfonos móviles solicitar los certificados, en otros casos el procedimiento será todavía complejo y tedioso. Además, la mayoría de los teléfonos móviles simplemente no tienen suficientes certificados raíz pre-instalados para permitirles aceptar cualquier subconjunto normal de certificados expedidos por las autoridades de certificación (CA) convencionales.

Como resultado de las limitaciones y dificultades anteriores con los teléfonos móviles, los operadores de los servidores de aplicaciones en línea, por ejemplo, los bancos, optan normalmente por evitar las complicaciones, limitando drásticamente el número y el alcance de las transacciones en línea que pueden realizarse desde el teléfono móvil de un usuario. Esto inhibe en gran medida el uso de la tecnología por los usuarios que todavía tienen que tener acceso a los ordenadores personales con el fin de usar la completa variedad de servicios ofrecidos por la mayoría de los servidores de aplicaciones en línea.

El documento US 2009/249074 describe un procedimiento de uso de certificados compactos para autentificar dispositivos inalámbricos y establecer conexiones seguras entre tales dispositivos.

El documento WO 02/15523 describe un procedimiento de autenticación de un cliente y un servidor entre sí usando certificados digitales en los que el cliente usa un primer protocolo de cifrado entre él mismo y una pasarela y el servidor usa un segundo protocolo de cifrado entre él mismo y la pasarela.

El documento US 2008/072039 describe un procedimiento para generar dinámicamente un certificado y un par de claves privada y pública asociadas para permitir a un cliente enviar un mensaje con seguridad a un cliente receptor, a través de un servidor de directorios, en el caso de que el cliente receptor no pueda estar localizado en el directorio.

El documento WO 99/49612 describe un procedimiento para generar una clave pública y un certificado implícito dentro de un sistema de cifrado de certificados implícitos basados en la identidad.

Los aspectos de la invención se exponen en las reivindicaciones adjuntas.

Breve descripción de los dibujos

La invención se describirá ahora a modo de solamente un ejemplo y con referencia a los dibujos adjuntos. En los dibujos:

la figura 1: es una ilustración esquemática de un sistema de autenticación de acuerdo con la invención; y
la figura 2: es un diseño esquemático de un certificado digital de acuerdo con la invención.

Descripción detallada con referencia a los dibujos

Un sistema (1) para autentificar un canal (3) de comunicaciones entre un teléfono (5) móvil, en este ejemplo un teléfono móvil, asociado a un usuario (7) y un servidor (9) de aplicaciones se muestra en la figura 1. El sistema (1) incluye una autoridad (11) de certificación, así como una aplicación (13) de software del lado del usuario instalada en el teléfono (5) móvil, y una aplicación (15) de software del lado del servidor instalada en el servidor (9) de aplicaciones. Además, el teléfono (5) móvil y el servidor (9) de aplicaciones incluyen cada uno un módulo de cifrado (no mostrado) proporcionado por la autoridad (11) de certificación que proporciona una funcionalidad de cifrado para el usuario y las aplicaciones (13, 15) del lado del servidor. Debería ser evidente que los módulos de cifrado pueden compilarse como parte de las aplicaciones de software del lado del servidor y del lado del usuario, respectivamente. Cuando, en el resto de esta descripción se hace referencia a la funcionalidad de cualquier aplicación de software del lado del servidor y del lado del usuario, se apreciará que tal funcionalidad puede proporcionarse, en efecto, por los módulos de cifrado del lado del servidor o del lado del usuario o viceversa.

La primera vez que la aplicación de software del lado del usuario requiere un cifrado o una identificación de usuario única, se constata que no hay ningún certificado (17) de usuario digital instalado actualmente en el teléfono (5) móvil. En este punto, la aplicación se conecta automáticamente a un servidor en línea de la autoridad (11) de certificación (“CA”) e intenta solicitar un certificado (17) de usuario digital desde el servidor (11). La aplicación (13) del lado del usuario valida en primer lugar que el servidor con el que está comunicándose es de hecho el de la CA (11), y no un servidor pirata. Esto se hace validando una firma (21) de certificado de CA enviada al teléfono (5) móvil por la CA (11), contra un certificado (23) de CA que viene distribuido como parte de la aplicación (13) de software del lado del usuario o el módulo de cifrado. Sin embargo, debería ser evidente que la validación de la CA podría ser inherente si la aplicación de software del lado del usuario es capaz de descifrar la comunicación de la CA que se ha

cifrado con una clave privada de CA. Si la aplicación de software del lado del usuario es capaz de descifrar la comunicación de CA cifrada de CA usando la clave pública de CA resulta que la CA es quien pretende ser.

Tras la validación exitosa del servidor (11) de CA, la CA crea y emite un certificado (17) de usuario digital para el teléfono móvil. El certificado (17) de usuario es un certificado digital X.509 firmado que puede usarse para identificar en primer lugar el teléfono (5) móvil en el que está instalado el certificado y también para intercambiar las claves (25) de cifrado simétricas con el servidor (9) de aplicaciones. Las claves de cifrado simétricas pueden, a su vez, usarse para el cifrado de datos entre el teléfono (5) y el servidor (9) de aplicaciones. Esta característica se elaborará con más detalle a continuación. El certificado (17) se firma con una clave (27) privada asociada con la CA (11), una clave (29) pública correspondiente de la CA (11) que se conoce tanto para las aplicaciones de software del lado del usuario como del lado del servidor o los módulos de cifrado, como sea el caso, que les permite descifrar la firma y verificar que se haya firmado por la clave (27) privada de CA y en consecuencia es auténtico.

Cuando se emite el teléfono (5) con el certificado (17) de usuario digital firmado, el servidor (11) calcula un par de claves de cifrado privada (31) y pública (33) de usuario en representación del teléfono (5). Esto sucederá principalmente en los casos en que el propio teléfono (5) no tenga suficiente capacidad de procesamiento para calcular por sí mismo el par de claves. A continuación, el servidor (11) intenta establecer un canal de comunicaciones seguro entre él mismo y el teléfono (5) por medio de un intercambio de claves Diffie-Hellman (DH) o un protocolo similar. Si el intercambio de claves DH tiene éxito, envía a su través la clave (31) privada de usuario a lo largo del canal seguro al teléfono (5), donde se recibe por la aplicación (13) de software del lado del usuario. La clave (33) pública de usuario asociada puede entonces incluirse en el certificado (17) de usuario y transmitirse al teléfono (5) por separado. Tras la recepción del par de claves de usuario, y el certificado (17), la aplicación (13) de software del lado del usuario los almacena en una parte cifrada (un recinto de seguridad) de la memoria del teléfono (5) desde donde solo las aplicaciones autorizadas, incluyendo la aplicación (13) de software del lado del usuario y/o el módulo de cifrado del lado del usuario, serán capaces de acceder a la misma. Debería apreciarse que si el teléfono (5) tiene suficiente capacidad de procesamiento, puede calcular por sí mismo el par (31, 33) de claves de usuario. En este caso la clave (31) privada de usuario no tiene que transmitirse entre el servidor (11) y el teléfono (5) y puede permanecer oculta en la memoria del teléfono. La aplicación (13) de software del lado del usuario puede entonces simplemente transmitir la clave (33) pública de usuario al servidor (11) de aplicaciones, junto con la solicitud del certificado (17) de usuario digital. El servidor (11) incluirá entonces la clave (33) pública de usuario en el certificado (17) y lo firmará con su propia clave privada (27) como anteriormente.

Un diseño típico de un certificado (17) de usuario digital se muestra en la figura 2. Además de la clave (33) pública de usuario y la firma (35) de CA, el certificado también contiene un identificador (37) que está asociado de forma única con el teléfono (5) móvil. El identificador (37) puede ser cualquier clave única que se emita por la CA. En la realización actual de la invención, el identificador (37) es un número secuencial generado por la CA (11). Debería apreciarse que debido a la naturaleza secuencial del identificador (37), existe una relación uno a uno entre cada certificado emitido por la CA (11) y un teléfono móvil. Además de lo anterior, el certificado (17) también puede incluir otra información tal como, por ejemplo, un número (39) de teléfono móvil asociado con la tarjeta SIM del teléfono (5), el IMEI (41) del teléfono y/o los números IMSI (43), así como una fecha (44) de caducidad del certificado.

Debería apreciarse que en el ejemplo descrito anteriormente la emisión y el almacenamiento del certificado (17) de usuario pueden ocurrir completamente en segundo plano y automáticamente, sin necesidad de ninguna intervención del usuario. Una vez que el certificado (17) de usuario digital se ha emitido por la CA (11) y se ha almacenado en la localización segura en el teléfono (5) móvil, puede usarse por la aplicación (13) de software del lado del usuario y/o el módulo de cifrado para identificar el teléfono (5), para autenticar los canales de comunicaciones entre el teléfono (5) y los servidores de aplicaciones (9) y para cifrar las comunicaciones entre el teléfono (5) y el servidor (9) de aplicaciones.

También se emite un certificado (45) de servidor digital por el CA (11) para el servidor (9) de aplicaciones. La emisión del certificado (45) de servidor puede ocurrir en cualquier momento, pero normalmente tras la solicitud del servidor (9) de aplicaciones. Esta solicitud también vendrá directamente desde la aplicación (15) de software del lado del servidor o el módulo de cifrado del lado del servidor, normalmente cuando la aplicación (15) se instala primero en el servidor (9) de aplicaciones. El formato del certificado (45) de servidor es similar al del certificado (17) de usuario descrito con referencia a la figura 2 e incluye su propia clave (47) pública de servidor. Una clave (49) privada de servidor correspondiente se guarda en una localización segura en el servidor (9), en donde solo es accesible por el servidor (9). A diferencia de en el caso del par (31, 33) de claves de usuario, el par (47, 49) de claves de servidor se calcula normalmente por el propio servidor (9), que generalmente tiene suficiente capacidad de procesamiento para hacerlo. Por lo tanto, el servidor (9) enviará su clave (47) pública a la CA (11) cuando se solicite el certificado (45) de servidor y la CA (11), a su vez, emitirá el certificado (45) de servidor, incluyendo la clave (47) pública de servidor, y lo firmará con su clave (27) privada.

Si se han emitido con certificados digitales tanto el teléfono (5) como el servidor (9) de aplicaciones, los certificados (17, 45) pueden usarse para autenticar los canales de comunicaciones entre los mismos, para identificar el teléfono y/o el servidor de aplicaciones y también para cifrar las comunicaciones entre los mismos. Cada vez que el teléfono (5) móvil se conecta a un servidor (9) de aplicaciones, se iniciará un procedimiento de intercambio de certificados, con lo que su certificado (17) se envía al servidor (9), y el certificado (45) del servidor se envía al teléfono (5). A

continuación, ambas partes validarán el contenido de los certificados (17, 45) recibidos, y la firma digital, para asegurarse de que los detalles de los certificados (17, 45) no se han manipulado. Esta validación se realiza usando un certificado (51) digital de CA que es parte tanto de la aplicación (13) de software del lado del usuario como de la aplicación (15) del lado del servidor o sus respectivos módulos de cifrado. El conocimiento de la clave (29) pública de CA puede, sin embargo, ser suficiente para permitir la validación de los certificados respectivos a realizarse. Debería apreciarse que el certificado (51) digital de CA incluirá la clave (29) pública de CA y que por lo tanto las aplicaciones del lado del usuario y del servidor usarán la clave (29) pública de CA para descifrar los certificados (17, 45) firmados. Si no se pueden descifrar los certificados con la clave (29) pública de CA, será evidente que no se han firmado con la clave (27) privada de CA, y por lo tanto no son auténticos.

En este punto, ambas partes pueden estar seguras de que están hablando con los destinatarios. Ahora, el teléfono (5) y el servidor (9) pueden compartir las claves (25) de cifrado por medio de las que puede hacerse un cifrado adicional de sus comunicaciones. Las claves (25) de cifrado compartidas son normalmente las claves de cifrado simétricas. Debería apreciarse que, después del intercambio de certificados, el teléfono (5) estará en posesión de la clave (47) pública del servidor de aplicaciones y el servidor (9) de aplicaciones estará en posesión de la clave (33) pública del teléfono. Por lo tanto, las claves de cifrado pueden cifrarse por el teléfono usando la clave (47) pública de servidor, y por el servidor usando la clave (33) pública del teléfono, garantizando de este modo que solo las partes receptoras serán capaces de descifrar las comunicaciones usando sus claves (31, 49) privadas respectivas.

El identificador (37) de teléfono incluido en el certificado (17) de usuario también puede usarse por el servidor (9) de aplicaciones para identificar de forma única el teléfono (5) y, en consecuencia, al usuario (7). El servidor de aplicaciones puede tener una base de datos de todos los identificadores emitidos por la CA (11) para los clientes del servidor de aplicaciones, y puede elegir comunicarse solo con los teléfonos incluidos en la base de datos. Los identificadores (37) también pueden estar unidos por el servidor (9) de aplicaciones a otra información relacionada con el usuario (7). Por lo tanto, cuando el servidor (9) de aplicaciones recibe un certificado (17) de usuario desde el teléfono (5), puede validarse en primer lugar que el certificado sea auténtico y que se ha emitido por la CA (11), y en segundo lugar que el teléfono (5) está de hecho asociado con un usuario registrado. Por lo tanto, el certificado (17) de usuario digital se usa no solo para autenticar el canal (3) de comunicaciones entre el teléfono (5) y el servidor (9) de aplicaciones, sino también para identificar de forma única al teléfono (5) que está intentando realizar transacciones con el servidor (9) de aplicaciones. De este modo, el servidor (9) de aplicaciones puede basarse en las comunicaciones recibidas desde el teléfono y estar seguro de que la comunicación a través del canal (3) de comunicaciones es segura.

Debería apreciarse que la aplicación de software del lado del usuario también puede validar que el servidor de aplicaciones es el legítimo propietario del certificado que envió, simplemente en virtud del hecho de que la aplicación de software del lado del usuario es capaz de descifrar la comunicación enviada al mismo por el servidor de aplicaciones y que se ha cifrado con la clave privada del servidor de aplicaciones. Solo las comunicaciones cifradas con la clave privada del servidor de aplicaciones serán capaces de descifrarse con la clave pública del servidor de aplicaciones.

En una realización alternativa de la invención, el teléfono móvil y el servidor de aplicaciones pueden incluir unos módulos de software adicionales y a medida, distribuidos por el propietario del servidor de aplicaciones. En esta realización, los módulos de software a medida se comunicarán con las aplicaciones de software del lado del usuario y del lado del servidor y/o los módulos de cifrado del lado del usuario y del servidor con el fin de invocar la funcionalidad de la invención.

Es previsible que la CA pueda emitir periódicamente nuevos certificados a todos los teléfonos y/o servidores de aplicaciones a los que ha emitido previamente certificados. Esto se puede hacer con la frecuencia necesaria, pero preferentemente sobre una base anual. La emisión de nuevos certificados de usuario puede incluir también a continuación el cálculo y la emisión de nuevos pares de claves privada/pública de usuario en los casos donde la CA calcula los mismos en representación del teléfono móvil.

También es previsible que el sistema sea capaz de emitir certificados que incluyan unas claves con tamaños de bit cada vez más grandes. En el momento de escribir, el estándar de la industria para las claves públicas y privadas es de 1024 bits. Sin embargo, el sistema puede adaptarse fácilmente para emitir pares de claves de 2048, 3072 y más bits.

La primera vez que la CA recibe una solicitud de un certificado de usuario de un teléfono nuevo, se apreciará que la CA puede emitir un teléfono de este tipo con un certificado autofirmado. A continuación, la CA puede comunicar la solicitud del certificado, junto con la identidad supuesta del teléfono nuevo al servidor de aplicaciones que, a su vez, puede decidir si puede emitirse un certificado de usuario legítimo al teléfono. Si el servidor de aplicaciones decide que el teléfono debería emitir un certificado de usuario legítimo comunicará esta decisión a la CA que, a su vez; emitirá un certificado de usuario legítimo, totalmente firmado al teléfono, como se ha descrito anteriormente. De este modo, el servidor de aplicaciones puede mantener un registro de las identidades y el número de certificados legítimos emitidos a sus usuarios por la CA.

La descripción anterior es solo a modo de ejemplo y se apreciará que pueden hacerse numerosas modificaciones a las realizaciones descritas sin apartarse del ámbito de la invención. En particular, la arquitectura del sistema y el flujo de datos como se ha descrito puede realizarse de cualquier número de maneras diferentes y en cualquier orden trabajable.

El sistema y procedimiento de la invención proporciona una forma de autenticar un canal de comunicaciones entre un teléfono móvil, en particular, un teléfono móvil, y un servidor de aplicaciones en línea, así como una manera de identificar de forma única el teléfono de transacción y cifrar las comunicaciones adicionales entre el servidor de aplicaciones y el teléfono.

Por lo tanto, la invención proporciona una forma segura de realizar transacciones desde teléfonos móviles con los servidores de aplicaciones en línea, haciendo de este modo posible y seguro para los proveedores de servicios, tales como los bancos, permitir el pleno uso de las funcionalidades de sus servicios en línea desde los teléfonos móviles y otros teléfonos móviles.

El sistema de la invención también puede usarse en otros dispositivos de comunicaciones móviles tales como los ordenadores portátiles. Con la tecnología SSL estándar usada en la mayoría de los casos, el ordenador portátil del usuario no se emite normalmente con su propio certificado digital. Por lo tanto, normalmente no hay confirmación desde el lado del usuario porque el usuario de transacción es, de hecho, el que pretende ser.

Por lo tanto, la invención proporciona una forma más fuerte de autenticación y una comunicación más segura que la proporcionada por los sistemas disponibles en la actualidad. El módulo de cifrado proporcionado por la CA de acuerdo con la invención, permite que las aplicaciones de software disponibles en la actualidad utilicen la invención.

REIVINDICACIONES

1. Un sistema (1) para autentificar un canal (3) de comunicaciones entre un teléfono (5) móvil asociado a un usuario (7) y un servidor (9) de aplicaciones, para identificar de forma única el teléfono (5) móvil y para cifrar las comunicaciones entre el teléfono (5) móvil y el servidor (9) de aplicaciones por el canal de comunicaciones, incluyendo el sistema una autoridad (11) de certificación, una aplicación (13) de software del lado del usuario instalada en el teléfono (5) móvil y un aplicación (15) de software del lado del servidor instalada en el servidor (9) de aplicaciones, en el que:

la aplicación (13) de software del lado del usuario está configurada para utilizar un módulo de cifrado del lado del usuario proporcionado por la autoridad (11) de certificación y para solicitar automáticamente un certificado (17) de usuario digital de la autoridad (11) de certificación;
la autoridad (11) de certificación está adaptada para, tras recibir la solicitud, calcular un par (31, 33) de claves privada y pública de usuario en representación del teléfono (5) móvil si el teléfono (5) móvil no tiene suficiente capacidad de procesamiento para hacerlo por sí mismo, para crear y emitir el certificado (17) de usuario al teléfono (5) móvil, incluyendo el certificado (17) de usuario al menos un identificador que se asocia de forma única con el teléfono (5) móvil y la clave (33) pública de usuario, y para transmitir la clave (31) privada de usuario al teléfono (5) móvil por un canal de comunicaciones seguro establecido entre la autoridad (11) de certificación y el teléfono (5) móvil por medio de un protocolo de intercambio de claves adecuado;
la aplicación (15) de software del lado del servidor está configurada para utilizar un módulo de cifrado del lado del servidor proporcionado por la autoridad (11) de certificación y para solicitar y recibir el certificado (17) de usuario desde el teléfono (5) móvil, para validarlo como procedente de la autoridad (11) de certificación usando el módulo (15) de cifrado del lado del servidor, para identificar de forma única el teléfono (5) móvil a partir del identificador con el certificado (17) de usuario, y para transmitir un certificado (45) de servidor digital emitido para el mismo por la autoridad (11) de certificación al teléfono (5) móvil donde se recibe por la aplicación (13) de software del lado del usuario y se valida como procedente de la autoridad (11) de certificación usando el módulo de cifrado del lado del usuario; y
tras la validación satisfactoria del certificado (17) de usuario por la aplicación (15) de software del lado del servidor y del certificado (45) de servidor por la aplicación (13) de software del lado del usuario, la aplicación (13) de software del lado del usuario y la aplicación (15) de software del lado del servidor se configuran adicionalmente para compartir las claves de cifrado que utilizan sus respectivos certificados para proporcionar el cifrado, siendo las claves de cifrado útiles para más cifrados de datos entre el teléfono (5) móvil y el servidor (9) de aplicaciones.

2. Un sistema (1) de acuerdo con la reivindicación 1, en el que la aplicación (13) de software del lado del usuario está configurada para solicitar automáticamente el certificado (17) de usuario digital de la autoridad (11) de certificación cuando el teléfono (5) móvil intenta realizar transacciones con el servidor (9) de aplicaciones por primera vez.

3. Un sistema (1) de acuerdo con la reivindicación 1 o la reivindicación 2, en el que la aplicación (13) de software del lado del usuario y la aplicación (15) de software del lado del servidor están configuradas adicionalmente para compartir las claves de cifrado que utilizan los pares (31, 33; 47,49) de claves pública y privada asociadas con sus respectivos certificados.

4. Un sistema (1) de acuerdo con una cualquiera de las reivindicaciones anteriores, en el que el identificador es una clave digital única emitida y asignada al teléfono móvil por la autoridad (11) de certificación.

5. Un sistema (1) de acuerdo con una cualquiera de las reivindicaciones anteriores, en el que el certificado (45) de servidor incluye un identificador de servidor asociado de forma única con el servidor (9) de aplicaciones y por medio del cual el teléfono (5) móvil puede identificar de forma única el servidor (9) de aplicaciones.

6. Un sistema (1) de acuerdo con una cualquiera de las reivindicaciones anteriores, en el que los certificados (17, 45) de usuario y de servidor incluyen una firma de autoridad de certificación generada con una clave privada de autoridad de certificación, una clave (29) pública de autoridad de certificación correspondiente por medio de la cual puede verificarse la firma que se conoce para las aplicaciones (13, 15) de software y/o los módulos de cifrado tanto del lado del usuario como del lado del servidor.

7. Un sistema (1) de acuerdo con una cualquiera de las reivindicaciones anteriores, en el que la autoridad (11) de certificación está configurada para incluir la clave (33) pública de usuario en el certificado (17) de usuario y la clave (47) pública de servidor en el certificado (45) de servidor.

8. Un sistema (1) de acuerdo con una cualquiera de las reivindicaciones anteriores, en el que la aplicación (13) de software del lado del usuario o el módulo de cifrado están configurados adicionalmente para dar instrucciones al teléfono (5) móvil para calcular por sí mismo el par (31, 33) de claves criptográficas privada y pública de usuario.

9. Un sistema (1) de acuerdo con una cualquiera de las reivindicaciones anteriores, en el que la aplicación (15) de software del lado del servidor o el módulo de cifrado están configurados para dar instrucciones al servidor (9) de aplicaciones para calcular un par (49 , 47) de claves privada y pública de servidor.

10. Un sistema (1) de acuerdo con una cualquiera de las reivindicaciones anteriores, en el que la aplicación (13) de software del lado del usuario o el módulo de cifrado están configurados adicionalmente para dar instrucciones al teléfono (5) móvil para almacenar el certificado (17) de usuario recibido y el par (31, 33) de claves privada y pública de usuario en una localización segura en una memoria de teléfono móvil desde la que solo puede recuperarse por las aplicaciones autorizadas.

11. Un sistema (1) de acuerdo con una cualquiera de las reivindicaciones anteriores, en el que la autoridad (11) de certificación está configurada para emitir periódicamente un nuevo certificado a uno o ambos del teléfono (5) móvil y el servidor (9) de aplicaciones.

12. Un procedimiento para permitir la autenticación de un canal (3) de comunicaciones entre un teléfono (5) móvil asociado a un usuario (7) y un servidor (9) de aplicaciones y una identificación única del teléfono (5) móvil por el servidor (9) de aplicaciones, realizándose el procedimiento en una autoridad (11) de certificación e incluyéndose las etapas de;
recibir una solicitud de un certificado (17) de usuario digital desde el teléfono (5) móvil, habiéndose enviado la solicitud desde una aplicación (13) de software del lado del usuario instalada en el teléfono (5) móvil;
calcular un par de claves asimétricas únicas, incluyendo las claves (31, 33) privada y pública de usuario en representación del teléfono (5) móvil si el teléfono (5) móvil no tiene suficiente capacidad de procesamiento para hacerlo por sí mismo, crear y emitir el certificado (17) de usuario para el teléfono (5) móvil, incluyendo el certificado (17) de usuario al menos un identificador asociado de forma única con el teléfono (5) móvil por medio del cual puede identificarse de forma única el teléfono (5) móvil y la clave (33) pública de usuario, transmitir la clave (31) privada de usuario al teléfono móvil por un canal de comunicaciones seguro establecido entre la autoridad (11) de certificación y el teléfono (5) móvil por medio de un protocolo de intercambio de claves adecuado;
emitir un certificado (45) de servidor digital para el servidor (9) de aplicaciones; e incluir una firma digital tanto en el certificado (17) de usuario como en el certificado (45) de servidor que permita a la aplicación (13) de software del lado del usuario y a una aplicación (15) de software del lado del servidor intercambiar certificados y validar los certificados (17, 45) respectivos usando al menos la firma digital y un módulo de cifrado proporcionado por la autoridad (11) de certificación.

13. Un procedimiento de acuerdo con la reivindicación 12, que incluye la etapa de, tras recibir la solicitud, asegurar el canal (3) de comunicaciones con el teléfono (5) móvil por medio de un protocolo de intercambio de claves adecuado.

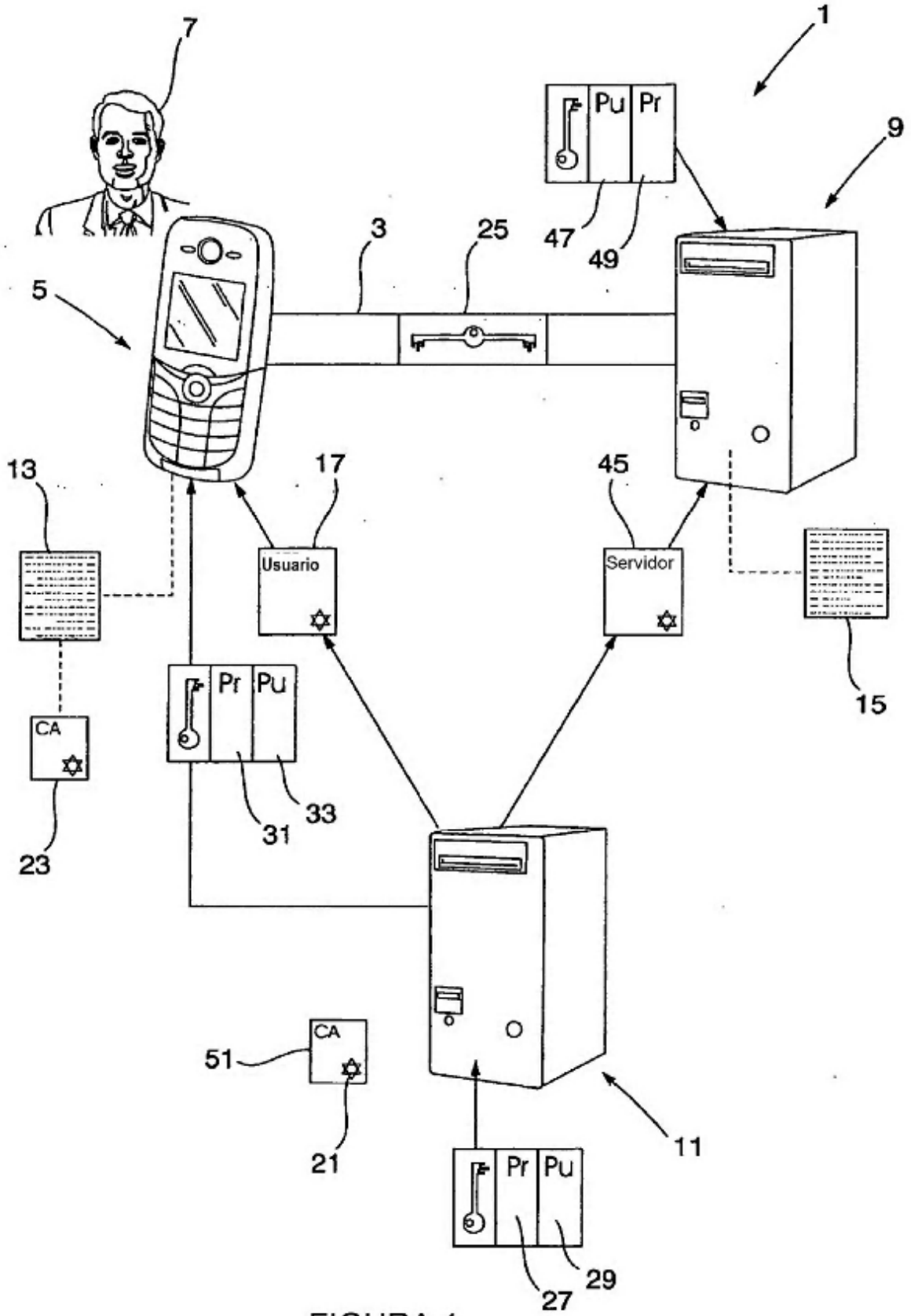
1
7
9
Pu
Pr
47
49
3
25
5
13
17
45
Usuario
Servidor
15
Pr
Pu
CA
31
33
23
CA
51
21
11
Pr
Pu
27
29

FIGURA 1

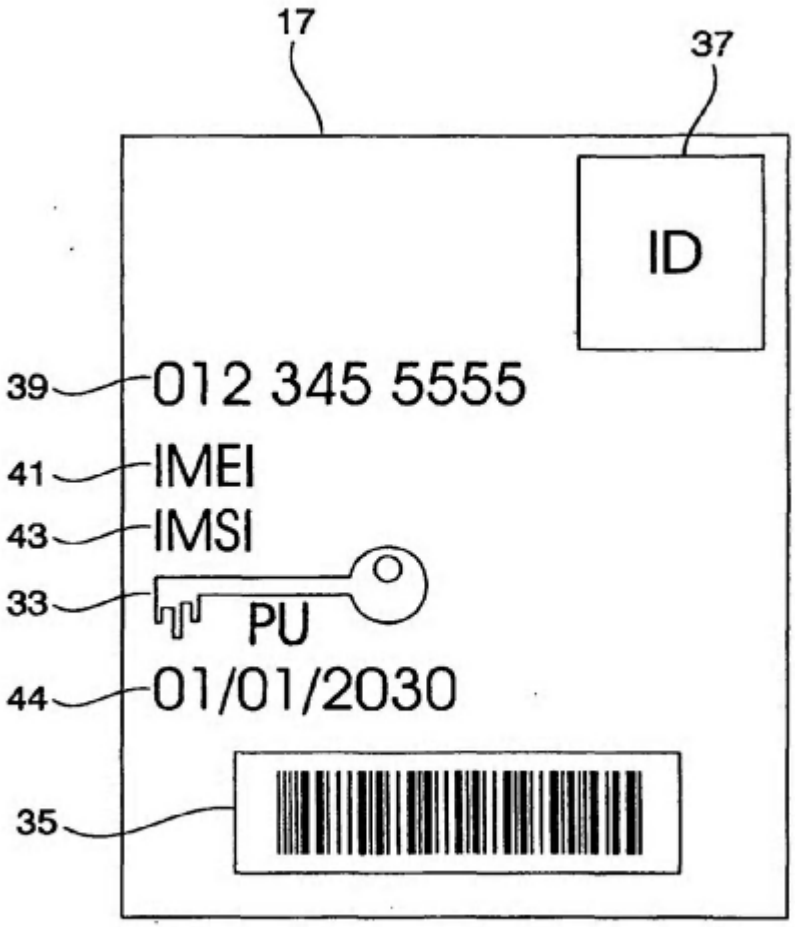

FIGURA 2