(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 644 739**

(51) Int. CI.:

H04L 9/30 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **22.02.2002 PCT/IB2002/02033**

(87) Fecha y número de publicación internacional: **28.08.2003 WO03071734**

(96) Fecha de presentación y número de la solicitud europea: **22.02.2002 E 02735717 (7)**

(97) Fecha y número de publicación de la concesión europea: **13.09.2017 EP 1476980**

(54) Título: **Solicitud de certificados digitales**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
30.11.2017

(73) Titular/es:

NOKIA TECHNOLOGIES OY (100.0%)
KEILALAHDENTIE 4
02150 ESPOO, FI

(72) Inventor/es:

ASOKAN, NADARAJAH;
GINZBOORG, PHILIP y
NIEMI, VALTTERI

(74) Agente/Representante:

VALLEJO LÓPEZ, Juan Pedro

DESCRIPCIÓN

Solicitud de certificados digitales

La presente invención se refiere a la solicitud y a la emisión de certificados digitales.

Cada vez se está volviendo más común que las transacciones sean llevadas a cabo por medios electrónicos. En las transacciones financieras, y en muchas otras transacciones, existe una necesidad de establecer un nivel de confianza entre las partes de la transacción. Por ejemplo, si un comprador desea comprar bienes en línea, entonces se ha dar garantía al proveedor de los bienes de que el comprador proporcionará el pago de los bienes. El comprador también puede desear que se le dé garantía de que su pago se va a transferir de hecho al proveedor.

Un medio para que se establezca tal confianza es mediante un sistema de clave pública/privada. En un sistema de este tipo, cada usuario tiene un par de claves. Una clave es una clave pública, que se puede facilitar a otros usuarios. La otra clave es una clave privada, que es mantenida en secreto por el usuario del cual es la clave. Las claves públicas y privadas están relacionadas por medio de algoritmos de tal modo que, a pesar de que es extremadamente difícil generar la clave privada a partir del conocimiento de la clave pública, la clave privada y la clave pública se pueden usar para la realización de firmas digitales. En la realización de firmas digitales, un primer algoritmo es aplicado por un usuario a su clave privada y a sus datos de origen, para formar datos de resultado; entonces, los datos de resultado se transmiten a otro usuario. El otro usuario aplica un segundo algoritmo a la clave pública del primer usuario, los datos de resultado, y, dependiendo del esquema de firma, otra entrada, para formar unos datos de verificación. La clave pública y privada y el primer y el segundo algoritmos están relacionados de tal modo que los datos de verificación indican, con un alto nivel de probabilidad, si la clave privada del primer usuario se usó para generar los datos de resultado. Con la condición de que la clave privada del primer usuario sea secreta salvo para él mismo, y que el segundo usuario pueda confiar en que la clave pública pertenece en realidad a el primer usuario, esto autentica al primer usuario con un alto nivel de probabilidad. Un ejemplo de un sistema de este tipo es el sistema de clave pública/privada de Privacidad Bastante Buena (PGP, *Pretty Good Privacy*).

Un certificado digital se usa normalmente para vincular una identidad de un sujeto a una clave pública. Los certificados son, en sí mismos, declaraciones firmadas que son emitidas por una autoridad de certificación. Si un usuario tiene la clave pública de la autoridad, este puede verificar los certificados que son emitidos por esa autoridad. Si un usuario (verificador) tiene acceso a un certificado que es emitido para la clave pública de otro usuario (firmante) por una autoridad en la que confía el verificador, entonces el verificador puede confiar realmente en que la clave pública pertenece al firmante. Este tipo de certificado se conoce como certificado de identidad. Los certificados de identidad no son suficientes para las transacciones que requieren autorización. Por ejemplo, en el caso de una compra en línea, puede que el vendedor desee verificar no solo la identidad del comprador sino también que el comprador tiene el dinero para pagar la compra. Además, la parte que emite el certificado tiene, por lo general, responsabilidades legales y empresariales en lo que respecta a cómo se usan sus certificados. Por estas razones, cada certificado contiene normalmente unos parámetros que definen cómo se debería usar ese certificado. Son ejemplos de esos parámetros el fin para el cual se ha emitido el certificado, el tiempo de expiración del certificado y el límite sobre la cantidad de dinero que se permite en una única transacción usando el certificado. Los certificados se pueden referir a una única transacción o se pueden usar para autorizar un número de transacciones, cada una dentro de un límite de valores que se especifica en el certificado.

Durante la emisión de un certificado digital a través de una conexión de red, se han de intercambiar al menos dos mensajes entre las partes solicitante y emisora. Esos dos mensajes son la solicitud de certificación que es enviada por la parte solicitante y una respuesta correspondiente que es enviada por la parte emisora. Hay normas para el procedimiento de emisión, por ejemplo, la norma PKCS10 de RSA (véase, en especial, PKCS n.º 10, v1.7: *Certification Request Syntax Standard* (norma de sintaxis de solicitudes de certificación), RSA Laboratories, 26 de mayo de 2000) y la norma RFC 2511 [CRMF] del grupo de trabajo de pkix de IETF (*Internet X.509 Certificate Request Message Format*, formato de mensajes de solicitud de certificados X.509 de Internet, RFC 2511).

La emisión de certificados a través de una red se puede asegurar de un número de formas. Por ejemplo, la solicitud de patente de los Estados Unidos "*System and method of boot-strapping a temporary public key infrastructure from a cellular telecommunication authentication and billing infrastructure*", de Nokia, US 09/659-781, 11 de septiembre 2000, (y las solicitudes correspondientes) describe un sistema en el que la seguridad de los mensajes de solicitud y de respuesta de certificado se basa en un secreto que es conocido tanto por el terminal móvil como por la red celular. En general, la solicitud de certificado se puede asegurar al adjuntar un campo autenticador a la misma, que puede ser, por ejemplo, un código de autenticación de mensaje que se computa usando un secreto compartido, o una firma digital que se computa usando una clave privada diferente de aquella cuya clave pública se está certificando.

Lo siguiente es un ejemplo de un campo autenticador que se computa usando un secreto compartido. En el sistema universal de telecomunicaciones móviles (UMTS, *Universal Mobile Telecommunications System*) el USIM (*Universal Subscriber Identity Module*, módulo universal de identidad de abonado) computa una clave de integridad IK de sesión durante el proceso de autenticación y de acuerdo de claves entre el teléfono (equipo de usuario) y la red celular. El USIM se puede encontrar en la forma de una tarjeta inteligente. El USIM exporta la IK al soporte lógico del

teléfono, que usa la IK para proteger la integridad de todos los mensajes de señalización. En el caso de los certificados de abonado de UMTS, la clave de integridad (IK, *integrity key*) de UMTS se puede usar para autenticar la solicitud de certificado, tal como se analiza en la solicitud de EE. UU. con número de serie 09/659.781 a la que se ha hecho referencia en lo que antecede. Una forma de hacer esto sería proteger de forma individual todas las solicitudes y respuestas de certificado por medio de la IK. Otra forma sería enviar todas las solicitudes y respuestas de certificado como mensajes de señalización, debido a que en UMTS (por ejemplo) el plano de señalización se protege por IK de forma automática.

Lo siguiente es un ejemplo de un autenticador en la forma de firmas digitales. La tarjeta inteligente se fabrica de tal modo que la misma contiene un par de claves de gestión antes de que la misma salga de la fábrica. El fabricante conoce la clave pública de gestión de cada tarjeta. El usuario puede, cuando obtiene la tarjeta, desencadenar que la tarjeta genere un nuevo par de claves. Este nuevo par de claves se podría usar, por ejemplo, para generar y, más adelante, verificar firmas para autorizar transacciones. El usuario puede obtener del fabricante un certificado para la nueva clave pública. Un certificado de este tipo se denomina normalmente certificado de dispositivo. Entonces, el certificado de dispositivo es una garantía de calidad de un par de claves (en concreto, de que las claves se generaron usando unos algoritmos correctos y de que la clave privada se encuentra en una ubicación segura). El autenticador para esta solicitud de certificado será una firma digital que se realiza usando la clave privada de gestión.

Cuando un usuario usa un dispositivo tal como un ordenador portátil, un teléfono móvil o un asistente personal digital (PDA, *Personal Digital Assistant*) para solicitar un certificado para una clave pública, esa clave pública se puede originar a partir del dispositivo desde el cual se realiza la solicitud o a partir de otro dispositivo.

Es deseable que, además de comprobar el derecho del usuario a realizar la solicitud, el emisor del certificado también tenga en cuenta la procedencia del par de claves, con el fin de inhibir el fraude. Por ejemplo, con el fin de que el emisor del certificado se proteja a sí mismo y proteja al propietario de la clave frente a un potencial fraude, puede ser deseable que el emisor del certificado emita un certificado en respuesta a una solicitud si la clave pública que es especificada por la solicitud se origina en otro dispositivo que no sea el que ha realizado la solicitud. Sin embargo, las presentes normas de emisión de certificados y otras descripciones públicamente disponibles de emisión de certificados no tienen en cuenta el origen de la clave pública para permitir que se realice esto.

El documento US 5.745.574 divulga un sistema de certificación que comprende una pluralidad de autoridades de certificación. Se proporciona un conjunto común de funciones de certificación para facilitar servicios de seguridad dentro del sistema.

De acuerdo con un aspecto de la presente invención, se proporciona un método para solicitar, de un emisor de certificados digitales, un certificado digital para una clave pública que está asociada a una clave privada correspondiente que es almacenada por una entidad de almacenamiento, comprendiendo el método: generar, por medio de una entidad de generación, un mensaje de solicitud de certificado indicativo de una solicitud para un certificado; y transmitir el mensaje de certificado del emisor de certificados digitales; incluyendo el mensaje de solicitud de certificado una indicación de la relación entre la entidad de almacenamiento y la entidad de generación.

De acuerdo con un segundo aspecto de la presente invención, se proporciona una entidad de generación para generar un mensaje de solicitud de certificado para solicitar, de un usuario de certificados digitales, un certificado digital para una clave pública que está asociada a una clave privada correspondiente que es almacenada por una entidad de almacenamiento, estando dispuesta la entidad de generación para generar el mensaje de solicitud de certificado que incluye una indicación de la relación entre la entidad de almacenamiento y la entidad de generación.

De acuerdo con un tercer aspecto de la presente invención, se proporciona un emisor de certificados digitales para procesar mensajes de solicitud de certificado que son generados por una entidad de generación, estando dispuesto el emisor de certificados digitales para analizar el mensaje de solicitud para determinar si este es una solicitud aceptable; y, si se determina que la solicitud es aceptable, emitir un certificado digital en respuesta a la solicitud, siendo dicho certificado para una clave pública que está asociada a una clave privada correspondiente que es almacenada por una entidad de almacenamiento, y estando dispuesto para limitar el certificado digital dependiendo de una indicación de una relación entre la entidad de generación y la entidad de almacenamiento que se incluye en el mensaje de solicitud de certificado.

De acuerdo con un cuarto aspecto de la presente invención, se proporciona un sistema de comunicación que comprende una entidad de generación de este tipo y un emisor de certificados digitales de este tipo.

Preferiblemente, la indicación es de una relación física entre la entidad de almacenamiento y la entidad de generación. Como alternativa, o además, la indicación puede ser de una relación de seguridad entre la entidad de almacenamiento y la entidad de generación.

Preferiblemente, la indicación puede adoptar una de un conjunto previamente determinado de formas. Una de las formas puede indicar que la entidad de almacenamiento está físicamente comprendida en la entidad de generación y

que la entidad de almacenamiento es físicamente segura, por ejemplo, resistente a manipulación indebida. Una de las formas puede indicar que la entidad de almacenamiento está físicamente comprendida en la entidad de generación y que la entidad de almacenamiento no es físicamente segura. Una de las formas puede indicar que la entidad de almacenamiento no está físicamente comprendida en la entidad de generación. Una de las formas puede indicar que la clave pública se ha proporcionado a la entidad de generación mediante una entrada de usuario. La entidad de generación se dispone preferiblemente para determinar la relación entre la misma y la entidad de almacenamiento y para proporcionar la indicación de acuerdo con el resultado de esa determinación.

Preferiblemente, el emisor de certificados digitales: analiza el mensaje de solicitud para determinar si este es una solicitud aceptable; y, si se determina que la solicitud es aceptable, emite un certificado digital en respuesta a la solicitud.

El mensaje de solicitud de certificado preferiblemente comprende unos datos que son una función de la clave privada, con lo que el mensaje de solicitud de certificado puede ser autenticado por el emisor de certificados digitales. El emisor de certificados digitales puede autenticar el mensaje de solicitud por medio de la clave pública o por medio de una clave simétrica compartida, que también puede ser almacenada por un almacén que está asociado al emisor de certificados digitales.

Preferiblemente, el emisor de certificados digitales se dispone para limitar el certificado digital a un nivel previamente determinado si no se autentica el mensaje de solicitud. Ese nivel puede ser nulo, caso en el cual podría ser que no se emitiera certificado alguno.

Preferiblemente, el emisor de certificados digitales se dispone para limitar el certificado digital dependiendo de la indicación de la relación que se incluye en el mensaje de solicitud de certificado. El emisor de certificados digitales puede almacenar una pluralidad de niveles de uso, correspondiéndose uno con cada valor disponible de la indicación de la relación, y puede aplicar esos niveles como límites sobre el certificado que se puede emitir en respuesta a una solicitud de acuerdo con la indicación en el mensaje.

La limitación del certificado es preferiblemente una limitación de las capacidades o el uso previsto del certificado. La indicación de la relación entre el elemento de almacenamiento y el elemento de generación de equipo en el interior de la solicitud de certificado puede influir en la decisión acerca de qué tipo de certificado producirá el emisor. La propia indicación se puede dejar fuera del certificado emitido, o esta se puede registrar de forma explícita en el interior del certificado, caso en el cual la misma es visible a la entidad que maneja el certificado.

La entidad de generación puede ser un elemento de equipo de usuario (UI, *user equipment*) de una red celular de comunicaciones, por ejemplo, un teléfono móvil de UMTS. La entidad de almacenamiento puede ser una tarjeta universal de circuito integrado (UICC, *universal integrated Circuit Card*) o un módulo inalámbrico de identidad (WIM, *Wireless identity Module*) que se instala en el elemento de equipo de usuario, por ejemplo, en la forma de una tarjeta inteligente. La entidad de generación y la entidad de almacenamiento pueden ser la misma, por ejemplo, estas se pueden encontrar, ambas, en una tarjeta inteligente.
El emisor de certificados puede ser parte de la red celular de comunicaciones, o puede ser externo a la red celular. La red puede, por ejemplo, ser una red de GSM (*Global System for Mobile Communications*, sistema global para comunicaciones móviles), o su sucesora, una red de 3G (tercera generación), o una derivada de la misma.

La presente invención se describirá a continuación a modo de ejemplo con referencia a los dibujos adjuntos.

En los dibujos:

la figura 1 ilustra la arquitectura de un sistema de comunicación;
la figura 2 ilustra un método para emitir un certificado digital;
las figuras 3 a 6 ilustran ejemplos de un equipo que implementa aspectos de la presente invención.

En el presente sistema, los dispositivos en una red de comunicación pueden solicitar, de un emisor de certificados, certificados para su uso en los aspectos de autenticación y de autorización de las transacciones. Cada certificado se solicita y se emite con respecto a una clave pública para la cual existe una clave privada correspondiente. La solicitud de un certificado se realiza de acuerdo con un método en el que la solicitud para el certificado incluye una indicación del origen o procedencia de la clave con respecto a la cual se solicita un certificado.

La figura 1 muestra un sistema de comunicación. El sistema incluye una red de conmutación y de transferencia de datos que se muestra en general en 1. Esta podría incluir una o más redes de telefonía e Internet. Se proporciona un número de puntos de acceso 2 por medio de los cuales los dispositivos pueden acceder a la red 1. Estos puntos de acceso podrían ser (sin limitación) estaciones de base inalámbricas, puntos de acceso de red cableados, etc. Los dispositivos podrían ser cualquier dispositivo con capacidades de red tal como un ordenador portátil 3, un PDA 4, un teléfono de línea fija 5, un teléfono móvil 6 o una televisión con capacidades multimedia interactivas 7. Los dispositivos se pueden comunicar a través de la red 1. Los dispositivos se pueden comunicar con un emisor de certificados 8 y un servidor de transacciones 9 a través de la red 1 y, normalmente, los dispositivos pueden ser

capaces de comunicarse entre sí a través de la red.

Al menos algunos de los dispositivos tienen pares asociados de clave pública/privada. Tales dispositivos almacenan su clave privada en secreto, pero pueden facilitar la clave pública a otros dispositivos para fines de cifrado y de autenticación. Al menos algunos de los dispositivos son capaces de soportar aplicaciones que pueden solicitar certificados con respecto a una clave pública. Por ejemplo, el ordenador portátil 3 incluye una memoria 10 (tal como una unidad de disco duro) que almacena claves públicas y privadas que están asociadas al ordenador portátil. La memoria 10 también almacena un soporte lógico que es capaz de solicitar y de usar un certificado, tal como se describirá con más detalle en lo sucesivo. El ordenador portátil incluye unos medios de procesamiento (de forma conveniente, al menos un procesador 11 con una memoria asociada) para ejecutar el soporte lógico. El soporte lógico se dispone preferiblemente para inhibir la transmisión de la clave privada fuera del dispositivo.

Cuando un dispositivo tal como el ordenador portátil 3 va a solicitar un certificado para una clave pública, el mismo transmite un mensaje de solicitud a través de la red 1 al emisor de certificados 8. Ese mensaje incluye una indicación de la clave pública para la cual se solicita el certificado. Si la red incluye un directorio de claves públicas 12, que almacena una lista de identificadores de usuario o de dispositivo y las claves públicas asociadas, entonces el mensaje puede incluir un identificador que está asociado a la clave pública y el emisor de certificados puede entonces, si es necesario, recuperar, del directorio, la clave pública asociada por medio de una consulta que se realiza sobre el identificador. Como alternativa, el mensaje de solicitud puede incluir la propia clave pública. A la recepción del mensaje de solicitud, el emisor de certificados realiza un proceso de verificación, que se describe con más detalle en lo sucesivo y, si es apropiado, emite un certificado. En el caso de un certificado para autorizar una transacción financiera, el certificado se puede asociar a una cantidad monetaria que limita el valor para el cual se puede depender del certificado en una única transacción.

Además del autenticador de solicitudes de certificado que se ha descrito anteriormente, la solicitud de certificado también se puede autenticar por medio de la clave privada que está asociada a la clave pública para la cual se realiza la solicitud. Esto solo se puede realizar si esa clave privada se encuentra disponible para el dispositivo que forma la solicitud. Este método se denomina prueba de posesión.

En el presente sistema, el mensaje de solicitud incluye un parámetro que indica la relación entre:

(a) la unidad que ha iniciado la solicitud, normalmente, la unidad en la que se genera la solicitud, (se hará referencia a la misma como la "unidad A"); y
(b) la unidad que está asociada a la clave pública para la cual se solicita el certificado, normalmente, la unidad que almacena la clave privada asociada, (se hará referencia a la misma como la "unidad B").

Se puede hacer referencia a este parámetro como parámetro de procedencia o Key_origin. Algunos ejemplos no limitantes de las relaciones que se pueden indicar mediante el parámetro Key_origin son:

1. que la unidad B sea un elemento o módulo de seguridad *específico* en el interior de la unidad A, por ejemplo, una tarjeta universal de circuito integrado (UICC, *Universal Integrated Circuit Card*) en el interior del teléfono de UMTS;
2. que la unidad B sea un elemento o módulo de seguridad que se incorpora en la unidad A;
3. que la unidad B sea una memoria interna no asegurada de la unidad A;
4. que la unidad B sea un dispositivo externo a la unidad A; y
5. que la clave pública se haya identificado directamente a partir de una entrada de usuario.

En general, el parámetro Key_origin indica el grado del conocimiento del equipo solicitante de cómo de bien está protegida la clave privada. Por ejemplo, si el parámetro Key_origin tiene unos valores de 1 o 2 en lo que antecede, entonces se puede asumir razonablemente que la clave privada se encuentra en una ubicación segura.

Algunos ejemplos del uso del parámetro Key_origin se darán a continuación.

En la figura 3, el número de referencia 6 designa un terminal de teléfono móvil o un dispositivo de equipo de usuario (UE, *user equipment*). El UE incluye un elemento o módulo de seguridad 16, en la forma de una tarjeta inteligente asegurada específica, por ejemplo, en una UICC 16. Si el UE solicita un certificado con respecto a una clave pública cuya clave privada asociada está almacenada en la UICC 16, entonces se esperaría que una solicitud de este tipo tuviera un alto grado de confianza debido a que se puede esperar que el UE solo permita un acceso seguro a, o un uso seguro de, la clave privada. En este caso, se usaría el valor de Key_origin 1 que se ha indicado en lo que antecede.

En la figura 4, el UE 6 incluye un elemento o módulo 17, tal como un módulo inalámbrico de identidad (WIM, *wireless identity module*), el cual no es específicamente conocido por el emisor de certificados, pero aun así el UE 6 asevera que es un elemento o módulo seguro. En este caso, se usaría el valor de Key_origin 2 que se ha indicado en lo que antecede.

En la figura 5, el UE 6 incluye un elemento o módulo de almacenamiento 18, tal como un módulo de memoria flash en el que se almacena la clave privada. Esta no es una ubicación segura y las claves pueden ser vulnerables a hurto o modificación por parte de un programa de tipo virus, o alguien que robe el dispositivo. En este caso, se usaría el valor de Key_origin 3 que se ha indicado en lo que antecede, de tal modo que el emisor de certificados puede limitar el riesgo al restringir las capacidades que se conceden a la clave pública en el certificado.

En la figura 6, el ordenador portátil 3 y el UE 6 podrían pertenecer al mismo usuario, el cual puede desear usar el UE 6 para solicitar un certificado para transacciones usando la clave pública del ordenador portátil 3. El ordenador portátil 3 y el UE 6 se comunican usando un enlace de comunicación local 19, tal como un enlace de comunicación de infrarrojos o de Bluetooth. Por ejemplo, el enlace 19 se puede usar para transferir la clave pública desde el ordenador portátil 3 al UE 6 o el certificado de vuelta del UE 6 al ordenador portátil 3. En ese caso, se usaría el valor de Key_origin 4 que se ha indicado en lo que antecede. A pesar de que en este caso el mismo usuario tiene el control del ordenador portátil 3 y el UE 6, esto no se puede asegurar; además, debido a que la clave privada se encuentra en una ubicación externa cuya seguridad no se puede conocer, esta puede ser vulnerable a hurto, por lo que el uso del valor de Key_origin 4 puede ayudar a reducir el riesgo (por ejemplo, el riesgo de que un dispositivo pueda solicitar certificados para transacciones que no están asociadas a ese dispositivo o su usuario) al limitar las capacidades que se conceden a la clave pública en el certificado.

La presente invención se podría poner en práctica, de forma ventajosa, en un sistema de telecomunicaciones móviles de 3G (tercera generación) o un derivado del mismo.

A continuación, los inventores de la presente invención describen un ejemplo en el que se usan el Key_origin y el certificado digital. El emisor de certificados puede establecer límites sobre el valor que está asociado a un certificado, dependiendo del parámetro Key_origin que se especifica en la solicitud para el certificado. Por ejemplo, el emisor puede autorizar certificados para unos valores de hasta 42 EUR si el valor de Key_origin es de 1 en lo que antecede, unos valores de hasta 1 EUR si el valor de Key_origin es de 3 en lo que antecede, y con un certificado que autoriza el acceso a un determinado servicio pero sin transacciones monetarias si Key_origin es el valor 5 en lo que antecede. Los límites se pueden aplicar de forma global a todas las emisiones de certificado, o se pueden permitir diferentes límites para diferentes usuarios o clases de usuarios.

Además, el emisor de certificados se puede conectar a un servidor financiero 14, por ejemplo, en un banco, mediante un enlace de datos seguro 13. Cuando se va a emitir un certificado a un usuario para un cierto valor, el emisor de certificados puede reservar ese valor en fondos de la cuenta del usuario en el banco al comunicarse a través del enlace 13. Cuando el usuario usa el certificado en una transacción, por ejemplo, para comprar bienes, los fondos se pueden transferir a la cuenta del beneficiario de la transacción. El beneficiario puede iniciar esta transferencia a través de otro enlace seguro 15 al servidor financiero. Si el certificado expira o se cancela sin haber sido usado para una transacción, entonces el emisor de certificados puede devolver los fondos reservados a la cuenta.

La figura 2 ilustra el procedimiento de un procedimiento para solicitar, emitir y usar un certificado en el ejemplo tal como se ha descrito en lo que antecede.

En el procedimiento de la figura 2, un usuario da lugar a que una solicitud se transmita del ordenador portátil 3 al emisor de certificados 8 para un certificado con respecto a un valor de n EUR. La solicitud incluye una clave pública que está asociada a una clave privada que se almacena en la unidad de disco duro 10 del ordenador portátil, o indica la identidad del ordenador portátil/usuario de tal modo que el emisor de certificados puede recuperar, del directorio 12, la clave pública relevante. Tal como se ha indicado en lo que antecede, el valor de Key_origin se establece a 3. (Etapas 30 y 31).

Si la solicitud se ha firmado, entonces la firma se verifica en el emisor de certificados y, si tal verificación no tiene éxito, se rechaza la solicitud. La firma se realiza preferiblemente por medio de la clave privada que se corresponde con la clave pública para la cual se ha emitido el certificado. Dependiendo del algoritmo de firma que se ha usado, la verificación se puede realizar por medio de la clave pública asociada, o por medio de la propia clave privada si esta es conocida por el emisor de certificados. Si la solicitud no se ha firmado, entonces el emisor de certificados puede limitar el valor de las potenciales transacciones que se realizan usando un certificado resultante a un nivel previamente determinado, por ejemplo, al suponer que el campo de Key_origin tiene el valor que está asociado a el grado más bajo de confianza. Otra forma de asegurar la solicitud es el uso de un secreto compartido entre el terminal y la red y un canal de comunicación que es asegurado por el secreto compartido, mediante el uso, por ejemplo, de códigos de autenticación de mensaje.

El emisor de certificados comprueba, en la etapa 32, si el valor solicitado (n EUR) se encuentra dentro del límite establecido para los certificados en respuesta al valor de Key_origin tal como se especifica en la solicitud. (En el presente caso, Key_origin = 3). Si este se encuentra por encima de ese límite, entonces se rechaza la solicitud para un certificado. (Etapa 33).

Si la cantidad solicitada se encuentra dentro del límite, entonces el emisor de certificados reserva n EUR de fondos de la cuenta del usuario. La identidad de esta cuenta se puede indicar en la solicitud, o se puede almacenar en una base de datos tal como el directorio 12. (Etapa 34). Si la reserva de fondos no tiene éxito, entonces se rechaza la solicitud. La reserva de fondos puede ser realizada, como alternativa, por alguna entidad que no sea el propio emisor de certificados.

Si la reserva tiene éxito, entonces se emite el certificado. (Etapa 35). Posteriormente, el usuario puede transmitir el certificado a otra parte con la que él mismo desee llevar a cabo una transacción (por ejemplo, el usuario del servidor 9), y ese servidor puede entonces verificar el certificado con el emisor de certificados 8. (Etapas 36 y 37). Si la verificación tiene éxito, entonces puede tener lugar la transacción. (Etapa 38). De lo contrario, por ejemplo si el certificado ha expirado o se ha revocado, se rechaza la transacción. (Etapa 39).

Se prefiere que el dispositivo que genera la solicitud esté preprogramado para aplicar el valor de Key_origin correcto a una solicitud. El emisor puede también ser capaz de conocer qué tipo de dispositivo está creando la solicitud en, para ejemplo, un caso en el que las capacidades de terminal se comunican al lado de red. En la situación en la que el emisor de certificados no confía en que el dispositivo solicitante aplique el valor correcto de Key_origin, el emisor de certificados puede aplicar otro límite previamente determinado al valor que se puede certificar, por ejemplo, al suponer que el campo de Key_origin tiene el valor que está asociado al grado más bajo de confianza.

El solicitante de la presente invención divulga por la presente, de forma aislada, cada característica individual que se describe en el presente documento y cualquier combinación de dos o más de tales características, en la medida en la que tales características o combinaciones se puedan llevar a cabo sobre la base de la presente memoria descriptiva como un todo a la luz del conocimiento general y común de un experto en la materia, con independencia de si tales características o combinaciones de características solucionan cualquier problema que se divulgue en el presente documento, y sin limitación al alcance de las reivindicaciones. El solicitante indica que algunos aspectos de la presente invención pueden consistir en cualquier característica individual o combinación de características de este tipo. A la vista de la descripción anterior, será evidente a un experto en la materia que se pueden realizar diversas modificaciones.

REIVINDICACIONES

1. Un método para solicitar a un emisor de certificados (8) un certificado para una clave pública que está asociada a una clave privada correspondiente almacenada por una entidad de almacenamiento (B), comprendiendo el método:

generar, por medio de una entidad de generación (A), un mensaje de solicitud de certificado indicativo de una solicitud para un certificado; y
transmitir el mensaje de solicitud de certificado al emisor de certificados; y **caracterizado por que**:

el mensaje de solicitud de certificado incluye una indicación de la relación entre la entidad de almacenamiento y la entidad de generación.

2. Un método de acuerdo con la reivindicación 1, en el que la indicación es de una relación física entre la entidad de almacenamiento y la entidad de generación.

3. Un método de acuerdo con las reivindicaciones 1 o 2, en el que la indicación es de una relación de seguridad entre la entidad de almacenamiento y la entidad de generación.

4. Un método de acuerdo con la reivindicación 3, en el que la indicación es de conocimiento de la entidad de generación en lo que respecta al nivel de seguridad de la clave privada almacenada por la entidad de almacenamiento.

5. Un método de acuerdo con cualquier reivindicación anterior, en el que la indicación puede adoptar una de un conjunto previamente determinado de formas y una de las formas indica que la entidad de almacenamiento está físicamente comprendida en la entidad de generación y que la entidad de almacenamiento es físicamente segura.

6. Un método de acuerdo con cualquier reivindicación anterior, en el que la indicación puede adoptar una de un conjunto previamente determinado de formas y una de las formas indica que la entidad de almacenamiento está físicamente comprendida en la entidad de generación y que la entidad de almacenamiento no es físicamente segura.

7. Un método de acuerdo con cualquier reivindicación anterior, en el que la indicación puede adoptar una de un conjunto previamente determinado de formas y una de las formas indica que la entidad de almacenamiento no está físicamente comprendida en la entidad de generación.

8. Un método de acuerdo con cualquier reivindicación anterior, en el que la indicación puede adoptar una de un conjunto previamente determinado de formas y una de las formas indica que se ha proporcionado la clave pública a la entidad de generación mediante una entrada de usuario.

9. Un método de acuerdo con cualquier reivindicación anterior, que comprende las etapas del emisor de certificados de
analizar el mensaje de solicitud para determinar si este es una solicitud aceptable; y,
si se determina que la solicitud es aceptable, emitir un certificado en respuesta a la solicitud.

10. Un método de acuerdo con la reivindicación 9, en el que el certificado incluye una indicación de la relación entre la entidad de almacenamiento y la entidad de generación.

11. Un método de acuerdo con las reivindicaciones 9 o 10, en el que el mensaje de solicitud de certificado comprende unos datos que son una función de una clave de firma, con lo que el mensaje de solicitud de certificado puede ser autenticado por el emisor de certificados.

12. Un método de acuerdo con la reivindicación 11, que comprende la etapa del emisor de certificados de autenticar el mensaje de solicitud por medio de una clave de verificación.

13. Un método de acuerdo con la reivindicación 11, en el que hay una clave simétrica que es conocida tanto por la entidad de generación como por el emisor de certificados y el método comprende la etapa del emisor de certificados de autenticar el mensaje de solicitud por medio de la clave simétrica compartida.

14. Un método de acuerdo con cualquiera de las reivindicaciones 9 a 13, en el que se dispone el emisor de certificados para limitar el certificado a un nivel previamente determinado si no se autentica el mensaje de solicitud.

15. Un método de acuerdo con cualquiera de las reivindicaciones 9 a 14, en el que se dispone el emisor de certificados para limitar el certificado dependiendo de la indicación de la relación incluida en el mensaje de solicitud de certificado.

16. Un método de acuerdo con cualquier reivindicación anterior, en el que la entidad de generación es un elemento de equipo de usuario de una red celular de comunicaciones.

17. Un método de acuerdo con la reivindicación 16, en el que la entidad de almacenamiento es una tarjeta inteligente instalada en el elemento de equipo de usuario.

18. Un método de acuerdo con las reivindicaciones 16 o 17, en el que la entidad de almacenamiento es una tarjeta universal de circuito integrado (UICC) instalada en el elemento de equipo de usuario.

19. Un método de acuerdo con las reivindicaciones 16 o 17, en el que el emisor de certificados es parte de la red celular de comunicaciones.

20. Una entidad de generación (A) para generar un mensaje de solicitud de certificado para solicitar a un emisor de certificados (8) un certificado con respecto a una clave pública que está asociada a una clave privada correspondiente almacenada por una entidad de almacenamiento (B), estando la entidad de generación **caracterizada por** estar dispuesta para generar el mensaje de solicitud de certificado que incluye una indicación de la relación entre la entidad de almacenamiento y la entidad de generación.

21. Un emisor de certificados (8) para procesar mensajes de solicitud de certificado generados por una entidad de generación (A), estando dispuesto el emisor de certificados para analizar el mensaje de solicitud para determinar si este es una solicitud aceptable; y, si se determina que la solicitud es aceptable, emitir un certificado en respuesta a la solicitud, siendo dicho certificado para una clave pública que está asociada a una clave privada correspondiente almacenada por una entidad de almacenamiento (B), y **caracterizado por** estar dispuesto para limitar el certificado dependiendo de una indicación de una relación entre la entidad de generación (A) y la entidad de almacenamiento (B) incluida en el mensaje de solicitud de certificado.

22. Un sistema de comunicación que comprende una entidad de generación de acuerdo con la reivindicación 20 y un emisor de certificados de acuerdo con la reivindicación 21.

23. Un sistema de comunicación de acuerdo con la reivindicación 22, en el que la entidad de almacenamiento y la entidad de generación se encuentran en el mismo equipo.

24. Un sistema de comunicación de acuerdo con la reivindicación 22, en el que la entidad de almacenamiento y la entidad de generación se encuentran en equipos diferentes.

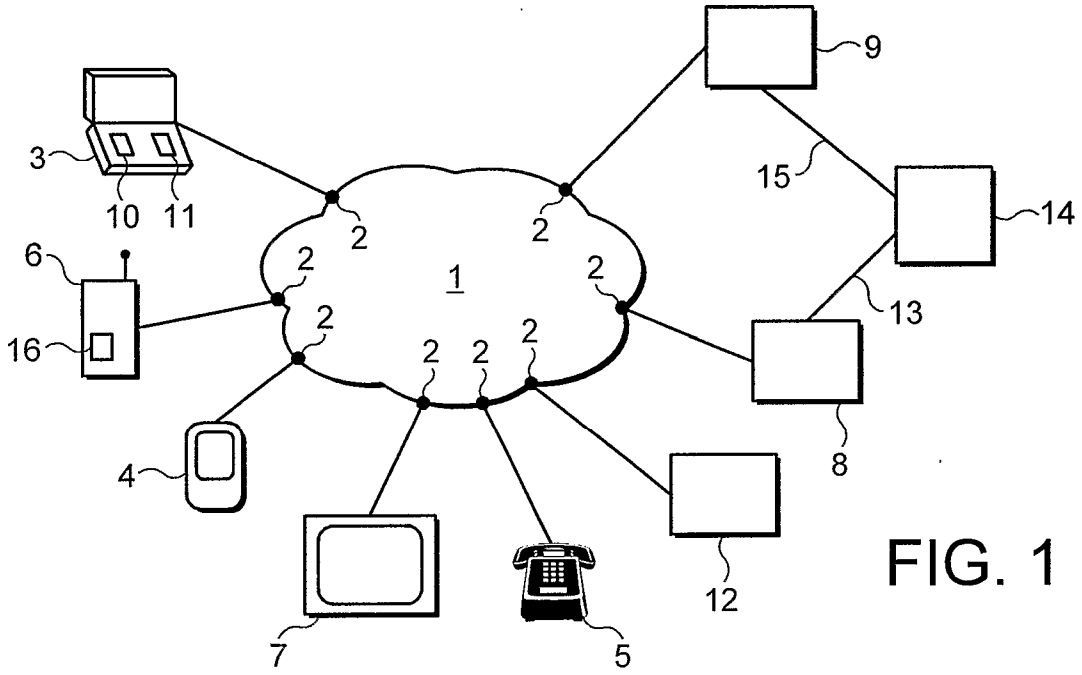

FIG. 1

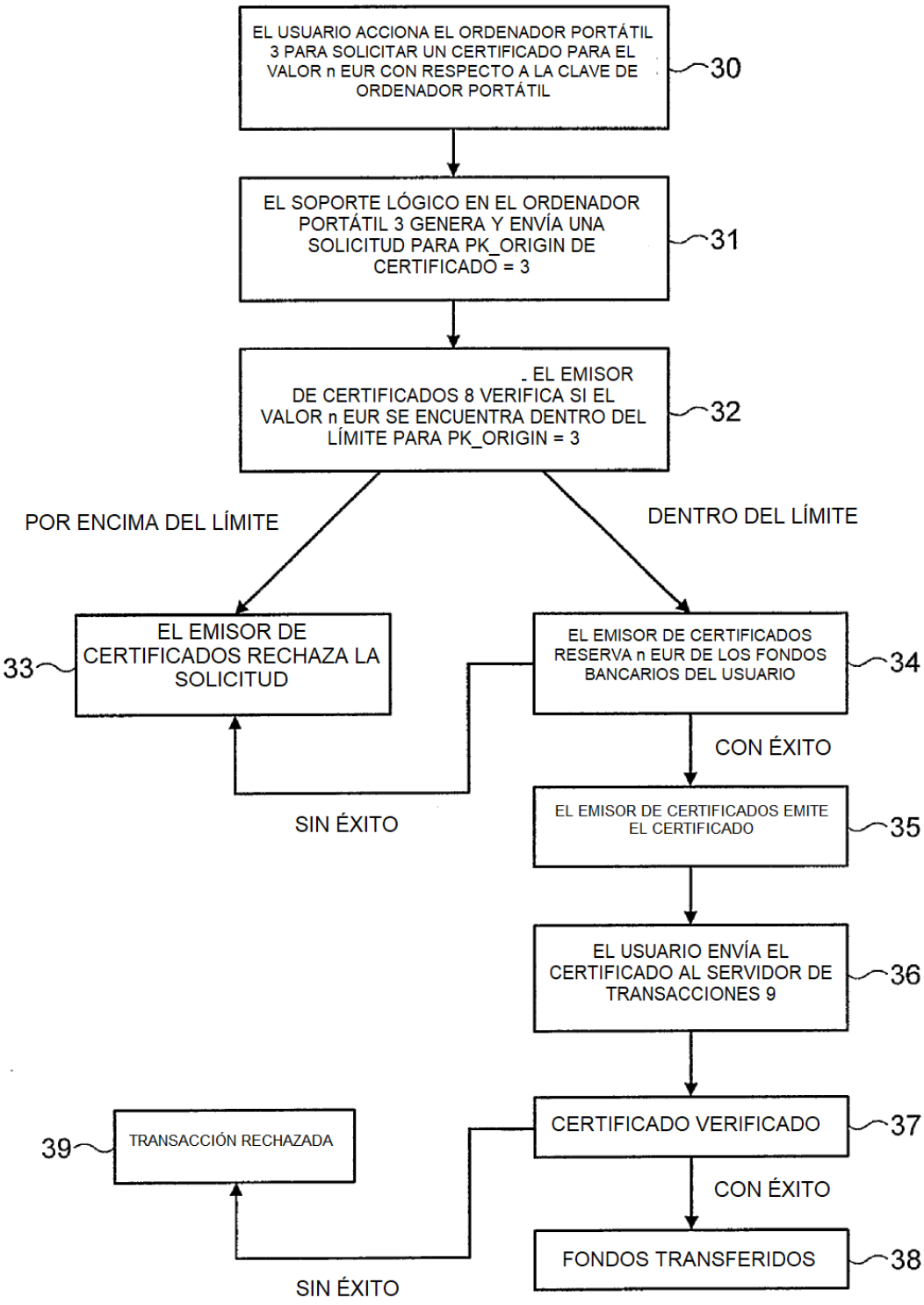
EL USUARIO ACCIONA EL ORDENADOR PORTÁTIL 3 PARA SOLICITAR UN CERTIFICADO PARA EL VALOR n EUR CON RESPECTO A LA CLAVE DE ORDENADOR PORTÁTIL
30
EL SOPORTE LÓGICO EN EL ORDENADOR PORTÁTIL 3 GENERA Y ENVÍA UNA SOLICITUD PARA PK_ORIGIN DE CERTIFICADO = 3
31
. EL EMISOR DE CERTIFICADOS 8 VERIFICA SI EL VALOR n EUR SE ENCUENTRA DENTRO DEL LÍMITE PARA PK_ORIGIN = 3
32
POR ENCIMA DEL LÍMITE
DENTRO DEL LÍMITE
EL EMISOR DE CERTIFICADOS RECHAZA LA SOLICITUD
33
EL EMISOR DE CERTIFICADOS RESERVA n EUR DE LOS FONDOS BANCARIOS DEL USUARIO
34
CON ÉXITO
SIN ÉXITO
EL EMISOR DE CERTIFICADOS EMITE EL CERTIFICADO
35
EL USUARIO ENVÍA EL CERTIFICADO AL SERVIDOR DE TRANSACCIONES 9
36
CERTIFICADO VERIFICADO
37
39
TRANSACCIÓN RECHAZADA
CON ÉXITO
FONDOS TRANSFERIDOS
38
SIN ÉXITO

FIG. 2

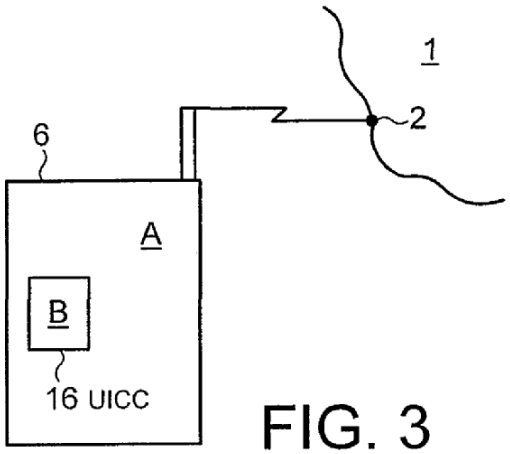

FIG. 3

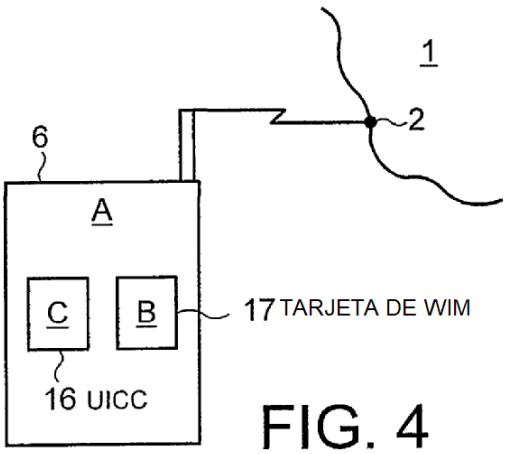

FIG. 4

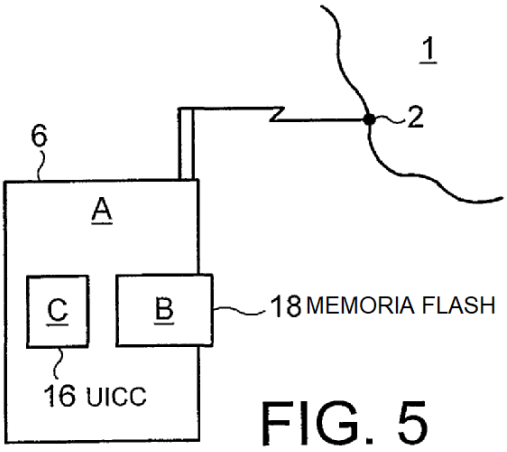

FIG. 5

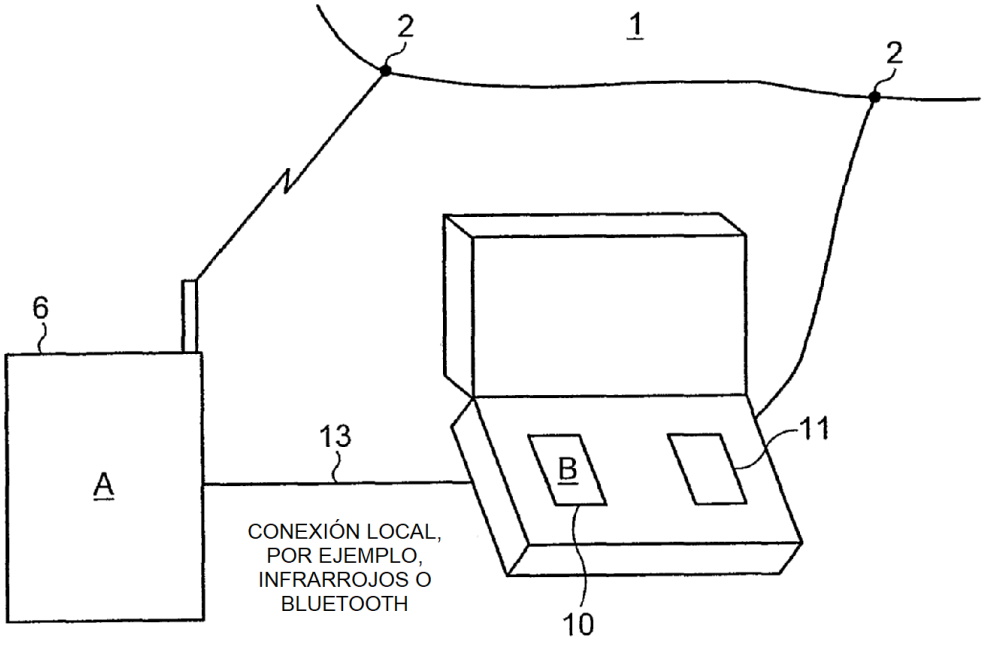
2
1
2
6
A
13
B
11
CONEXIÓN LOCAL,
POR EJEMPLO,
INFRARROJOS O
BLUETOOTH
10

FIG. 6