(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 666 326**

(51) Int. CI.:

H04W 12/10 (2009.01)
H04L 9/32 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **02.07.2009 PCT/IB2009/052886**

(87) Fecha y número de publicación internacional: **07.10.2010 WO10112981**

(96) Fecha de presentación y número de la solicitud europea: **02.07.2009 E 09786503 (4)**

(97) Fecha y número de publicación de la concesión europea: **24.01.2018 EP 2415200**

(54) Título: **Método y sistema para efectuar una firma electrónica cualificada en modo remoto**

(30) Prioridad:

01.04.2009 IT VR20090044

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
04.05.2018

(73) Titular/es:

ALIASLAB S.P.A. (100.0%)
Via Durini 25
20122 Milano, IT

(72) Inventor/es:

MAGAGNOTTI, ROMEO y
DIANATI, DAVIDE

(74) Agente/Representante:

RUO , Alessandro

DESCRIPCIÓN

Método y sistema para efectuar una firma electrónica cualificada en modo remoto

[0001] La presente invención se refiere, en general, a un método y a un sistema relativo para efectuar una firma electrónica cualificada en el modo remoto de un documento electrónico. Más particularmente, la invención se refiere a un método y a un sistema relativo para efectuar una firma digital de un documento electrónico por medio de un teléfono inalámbrico u otro dispositivo electrónico de comunicación móvil.

[0002] Como es sabido, para el envío de documentos electrónicos para los que el receptor solicita la autenticidad del firmante del propio documento, se utiliza la llamada "firma electrónica", es decir una matriz de datos en forma electrónica, encerrada o conectada a través de una asociación lógica con otros datos electrónicos, utilizada como método de identificación electrónica.

[0003] Para una mejor garantía en el envío de documentos electrónicos firmados, ha sido introducida la llamada "firma electrónica cualificada", es decir, una firma electrónica basada en un procedimiento que permita una identificación inequívoca del titular a través de medios en los que el firmante debe tener un control exclusivo, estando certificada la propiedad de dichos medios con un certificado calificado por una agencia certificadora.

[0004] Dicho procedimiento prevé que la agencia de certificación cree, a través de un algoritmo adecuado y para cada firmante, un par de claves, en particular, una clave pública y una clave privada, a saber, un par de algoritmos relacionados que procesan los códigos electrónicos.

[0005] En la fase de envío de un documento para el que se solicita la firma electrónica cualificada, el remitente procesa el documento que se enviará por medio de un algoritmo de procesamiento público y obtiene un código electrónico llamado "hash". Dicho "hash", a su vez, se procesa, es decir es encriptado a través del algoritmo en la clave privada para que se obtenga un código electrónico adicional, llamado "firma".

[0006] El receptor del documento puede verificar si el documento ha sido efectivamente firmado por el remitente, utilizando el algoritmo de procesamiento y la clave pública. En particular, el receptor puede descifrar la "firma" por medio de la clave pública y obtener un primer "hash"; si esta operación se lleva a cabo correctamente, se verifica la autenticidad del emisor. Entonces, el receptor puede obtener un segundo "hash" procesando el documento enviado por el emisor con el algoritmo de procesamiento. Si los dos "hashes" son idénticos, significa que el documento no ha sido alterado.

[0007] El procedimiento puede tener lugar en orden inverso en el caso de que el receptor envíe un mensaje de modo que el único firmante (antes era el remitente) puede tener acceso a ella. En este caso, la clave pública que se refiere a ese firmante encripta el mensaje que el único titular de la firma puede descifrar por medio de su clave privada.

[0008] Mientras que la clave pública está disponible en la agencia certificadora, la clave privada debe mantenerse secreta con el fin de hacer un uso sustancialmente imposible por parte de terceros, aparte de la persona que firma, es decir, el titular. Por esta razón, la clave privada se memoriza en un dispositivo electrónico que mantiene el firmante, como los discos de ordenador o tarjetas de memoria que comprenden dispositivos específicos de procesamiento y memorización electrónicos, comúnmente conocidos como "tarjetas inteligentes" o llaves USB u otros dispositivos.

[0009] En esencia, la clave privada, denominada más simplemente certificado digital o certificado de firma digital, se memoriza en un dispositivo electrónico que se mantiene por el titular usuario y se utiliza a nivel local por medio de aparatos adecuados: en caso de una "tarjeta inteligente" , se proporcionan lectores adecuados para conectarse con un ordenador personal u otro tipo de ordenador; en el caso de otros dispositivos como las llaves USB o los discos de memoria, se proporcionan puertas USB u otros sistemas de conexión para la conexión con el ordenador personal.

[0010] En consecuencia, el usuario siempre debe mantener uno o más dispositivos electrónicos y comprobar que el equipo del usuario que tiene la intención de utilizar puede estar conectado con tales dispositivos y, por lo tanto, la utilización del sistema de firma de acuerdo con la técnica conocida es limitativa y onerosa.

[0011] El documento WO03015370 muestra un esquema para proporcionar la firma digital de un documento digital a través de un servidor remoto y una conexión doble con el servidor. Se describe específicamente en el preámbulo de la reivindicación 1.

[0012] El propósito y el objetivo de esta invención es llevar a cabo un método y un sistema relativo para efectuar una firma electrónica cualificada en modalidad remota y mantener un alto nivel de seguridad en las operaciones de firma.

[0013] Dicho propósito y otros se consiguen mediante un método para efectuar una firma electrónica cualificada de uno o más documentos electrónicos por más usuarios firmantes mediante la utilización de un software que funciona en un ordenador, por ejemplo un ordenador personal, un ordenador portátil, un ordenador de bolsillo, u otro dispositivo similar, conectado con un servidor remoto, cada usuario firmante estando en posesión de un certificado de firma digital y un dispositivo electrónico de comunicación móvil con el que un número de identificación se asocia inequívocamente. El método se caracteriza porque el servidor obtiene un hash del documento que se debe firmar al recibir dicho hash del ordenador directamente después de que el ordenador ha calculado el hash sobre la base del documento electrónico o, como alternativa, el servidor calcula el hash sobre la base del documento electrónico que se debe firmar, enviado al servidor por el ordenador. El servidor es adecuado para comunicarse telefónicamente, los certificados de firma digital se recopilan en dicho servidor, cada certificado de firma digital se refiere a un único usuario firmante, y en el servidor también hay una base de datos en la que un código respectivo de identificación diferente de cada usuario firmante está asociado con un número de identificación de cada dispositivo electrónico para la comunicación móvil de cada usuario. Además, el método de acuerdo con la invención se caracteriza porque el ordenador envía un código de identificación del usuario firmante al servidor remoto, y porque tiene lugar una comunicación telefónica entre el usuario emisor, a través del dispositivo electrónico de comunicación móvil, y el servidor remoto y durante dicha comunicación telefónica, el servidor remoto verifica la correspondencia entre el usuario firmante en la comunicación telefónica y el emisor del código de identificación del usuario. De esta forma, en el caso de una coincidencia real, el servidor remoto efectúa el cifrado del hash a través del certificado de firma digital correspondiente con el usuario en la comunicación telefónica y obtiene una firma digital.

[0014] En otras palabras, el método de acuerdo con la invención permite llevar a cabo la firma electrónica cualificada de un documento electrónico, sin necesidad de que el usuario lleve consigo dispositivos electrónicos tales como "tarjetas inteligentes", llaves USB, discos de memoria, u otros dispositivos en los que se proporciona la clave privada o el certificado digital, pero solo a través de la utilización de un dispositivo de comunicación móvil, como un teléfono inalámbrico convencional que todo el mundo posee en la actualidad.

[0015] Además, el método según la presente invención establece que las operaciones de firma electrónica cualificada se efectúan con cualquier tipo de ordenador simplemente utilizando un software para ser puesto en comunicación con un servidor remoto, por ejemplo, a través de conexión a Internet. El software se puede instalar en un servidor remoto y se puede acceder a él a través de un navegador de Internet en caso de que el ordenador se pueda conectar a Internet.

[0016] En relación con el dispositivo electrónico para la comunicación móvil, que debe ser destinado el propio dispositivo junto con los abonados telefónicos unidos a SIM (en el caso de un dispositivo GSM) o unidos a USIM (en el caso de un dispositivo UMTS). En consecuencia, en relación con el número de identificación asociado al dispositivo de comunicación móvil, debe entenderse el número de teléfono relacionado con los abonados telefónicos (CLI/MSISDN) u otros códigos utilizados por la red telefónica, como el código IMSI correspondiente a la serie número de SIM o USIM, el código IMEI correspondiente al número de serie del dispositivo de comunicación, o dos o más de dichos códigos.

[0017] El método proporciona que al principio el hash se calcula por el software del ordenador desde el que el usuario firmante controla el inicio de las operaciones de firma y, a continuación, el hash se envía al servidor remoto. De lo contrario, el hash puede ser calculado por el servidor remoto sobre la base del documento electrónico enviado al servidor remoto por el ordenador.

[0018] Ventajosamente, el método según la invención prevé que una vez que la firma digital se ha calculado, el servidor remoto puede enviar dicha firma al ordenador del usuario firmante. Sin embargo, es posible enviar la firma así obtenida a un usuario diferente, elegido por el usuario firmante, incluso en asociación con el documento electrónico firmado, para apresurar las operaciones de envío del documento firmado por el usuario firmante.

[0019] De acuerdo con una última posibilidad, el documento electrónico firmado se puede enviar a un servidor remoto adicional para una presentación electrónica sustituta, centralizada o remota, en cumplimiento de los requisitos de la ley.

[0020] Ventajosamente, la comunicación telefónica entre el servidor remoto y el usuario firmante puede establecerse como sigue: después del envío del código de identificación del usuario firmante con el servidor remoto y la obtención del hash por el mismo servidor remoto (después de haber recibido el mismo desde el ordenador que calcula el hash sobre la base del documento electrónico, o después de haberlo calculado sobre la base del documento electrónico recibido), el servidor remoto puede enviar un número de teléfono al usuario, o como alternativa al ordenador para que el usuario pueda visualizar dicho número de teléfono a través del software o enviar el número de teléfono al dispositivo para la comunicación móvil; de esta forma, el usuario puede marcar el número de teléfono en el dispositivo para la comunicación móvil en su poder y establecer la comunicación con el servidor remoto. Durante la comunicación, el servidor remoto verifica, sobre la base de la información de su base de datos, la correspondencia entre el código de identificación del usuario firmante enviado previamente y el número de identificación del dispositivo que llama con el que ha establecido la comunicación. Luego, en caso de coincidencia entre el código de identificación y el número de identificación, el servidor remoto encripta el hash obtenido

previamente mediante el certificado de firma digital que hace referencia al usuario firmante, es decir, el usuario que ha enviado el hash y ha establecido la comunicación telefónica, y, por lo tanto, se crea un código electrónico o firma digital para el documento en cuestión.

[0021] De esta manera, es el usuario firmante quien llama, con su teléfono inalámbrico u otro dispositivo, al servidor remoto cuyo número se ha notificado al ordenador personal o teléfono inalámbrico del usuario firmante. Es muy ventajoso para el controlador del sistema que más números de teléfono correspondan al servidor remoto, estos números se indican de forma selectiva a un usuario que necesita la firma electrónica. De esta manera, un único sistema puede manejar más usuarios al mismo tiempo.

[0022] Ventajosamente, el método según la invención prevé que en caso de una coincidencia no satisfactoria entre el código de identificación enviado al servidor remoto y el número de identificación que llama, el servidor remoto envía un mensaje al ordenador personal para notificar la no coincidencia y la imposibilidad de efectuar la firma electrónica cualificada.

[0023] Además, el método aumenta el grado de seguridad en que, además del número de teléfono a ser llamado, el servidor remoto envía un código numérico al ordenador, el código numérico que se visualiza por el usuario firmante y asociado al número de identificación, que es uno o más de los siguientes números: número de teléfono, código IMSI, código IMEI, u otro, del dispositivo de comunicación móvil del mismo usuario. En consecuencia, para efectuar la operación de firma durante la comunicación con el servidor remoto, el usuario debe teclear el código numérico visualizado previamente para que el servidor remoto verifique tanto la coincidencia entre el código de identificación del usuario firmante y el número de identificación de la llamada con el cual el servidor remoto ha establecido la comunicación, y la coincidencia de éste con el código numérico enviado por el usuario durante la comunicación.

[0024] Con el fin de aumentar aún más el grado de seguridad del método en cuestión, un código secreto personal puede estar asociado a cada usuario firmante quien enviará dicho código durante la comunicación telefónica con el servidor remoto de modo que el propio servidor puede verificar la coincidencia entre el número de identificación de llamada y el código secreto personal tecleado.

[0025] Con el fin de evitar que el usuario firmante incurra en los costes para llamar al servidor remoto o para evitar que el mismo se encuentre impedido de efectuar llamadas salientes, el método de firma electrónica de acuerdo con esta invención puede proporcionar que el propio servidor remoto llame al número de teléfono asociado al código de identificación enviado por el ordenador personal al servidor en la fase inicial de la operación de firma. De esta forma, será suficiente que el usuario firmante responda a la llamada por medio del dispositivo de comunicación móvil correspondiente a dicho número de teléfono y envíe por si acaso al servidor remoto, a través de la misma comunicación telefónica, un código de reconocimiento unívoco acordado antes de establecer la comunicación en sí. Una vez que el servidor ha verificado la coincidencia entre el número llamado y el código de reconocimiento, el servidor efectúa el cifrado del hash mediante el certificado de firma digital correspondiente al usuario en la comunicación telefónica y obtiene la firma digital.

[0026] Dicho código de reconocimiento unívoco se le puede asignar solo una vez en la fase de atribución del certificado de firma digital. De lo contrario, dicho código de reconocimiento unívoco puede ser enviado por el servidor al ordenador después de enviar el hash al servidor mismo.

[0027] Ventajosamente, el método según la invención puede prever que el servidor remoto envíe un código numérico que es recibido por el usuario firmante, no en el ordenador personal con el que él/ella está operando, sino en su dispositivo de comunicación móvil. Para proceder con la firma, el usuario firmante envía el código numérico recibido a través del ordenador personal al servidor remoto para que el servidor verifique la identidad entre el código enviado y el código recibido y, en el caso afirmativo, el servidor valida la operación de cifrado del hash y obtiene la firma digital. Con este procedimiento, no es necesario que el usuario realice una llamada.

[0028] Por razones de seguridad, el método de acuerdo con esta invención puede proporcionar que después de que el servidor ha efectuado el cifrado del hash y la consiguiente obtención de la firma digital, el usuario firmante puede ser notificado por el servidor del resultado exitoso de la operación y envía un mensaje de texto al dispositivo de comunicación móvil del usuario firmante.

[0029] Además, los objetivos y ventajas de esta invención se consiguen mediante un sistema para efectuar la firma electrónica cualificada de un documento electrónico por un usuario firmante, que comprende un ordenador (por ejemplo, un ordenador personal, un ordenador de bolsillo), un servidor remoto conectado con el ordenador, un dispositivo electrónico de comunicación móvil (por ejemplo, un teléfono inalámbrico que comprende su usuario de teléfono) para cada usuario que tiene la intención de efectuar la firma electrónica. El sistema establece que un número de identificación se asocia de manera unívoca al dispositivo electrónico para la comunicación móvil y que el servidor remoto puede recibir el hash del documento para ser firmado directamente desde el ordenador una vez que ha sido calculado por él: De lo contrario, el servidor remoto puede calcular el hash sobre la base del documento electrónico recibido por el ordenador. El servidor remoto puede comunicarse telefónicamente y comprende tanto un

certificado de firma digital para cada usuario firmante que utiliza el sistema como una base de datos en la que un código de identificación de un usuario está asociado a un número de identificación del dispositivo de comunicación móvil del mismo usuario. Además, dicho sistema proporciona que el software pueda enviar un código de identificación del usuario para iniciar las operaciones de firma, y que se establezca una comunicación telefónica entre el usuario, a través del dispositivo electrónico de comunicación móvil, y el servidor remoto y durante dicha comunicación telefónica el servidor remoto verifica la correspondencia entre el usuario firmante en la comunicación telefónica y el remitente del código de identificación del usuario. En caso de una coincidencia real, el servidor remoto efectúa el cifrado del hash mediante el certificado de firma digital correspondiente al usuario en la comunicación telefónica y obtiene una firma digital.

[0030] Ahora se describirá una operación de firma electrónica cualificada de acuerdo con un modo de realización del método de acuerdo con la invención.

[0031] En primer lugar, un usuario que desea firmar documentos electrónicos en un modo remoto debe solicitar un certificado de firma digital o clave privada a la agencia de certificación competente. Si bien la clave pública del usuario en cuestión se coloca a disposición de cualquiera que quiera adquirirla, el certificado de firma digital o clave privada del usuario se almacena en un servidor remoto de forma segura.

[0032] Además, la oficina de certificación solicita al usuario un número de identificación de su servicio de telefonía móvil, por ejemplo, el número de teléfono y/o el código IMSI (código de serie SIM o USIM), o un número de identificación de su dispositivo de comunicación móvil, por ejemplo, el código IMEI del teléfono inalámbrico (código de serie del dispositivo). Este número de identificación, a saber, el número del servicio telefónico o el número del dispositivo se llama en lo sucesivo número de teléfono de identificación.

[0033] Naturalmente, en el caso de que se utilicen más códigos juntos, la oficina de certificación debe ser notificada por el usuario de cualquier cambio, en particular cuando el teléfono inalámbrico se sustituye o cuando se cambia el número o cuando se reemplaza la tarjeta SIM/USIM.

[0034] La oficina de certificación asocia el número de identificación del teléfono, es decir, uno o más de los códigos mencionados anteriormente, al certificado de firma digital del mismo usuario, así como a un código de identificación de usuario, a fin de crear una base de datos que contiene la información de todos los usuarios con firma digital certificada. Esta base de datos se guarda en el servidor remoto que está equipado con un módulo adecuado para la comunicación telefónica.

[0035] Cuando el usuario tiene que firmar un documento electrónico, él/ella calcula en un primer momento el hash del documento a firmar mediante la utilización del software instalado en su ordenador, por ejemplo, un ordenador personal, y luego, el usuario envía el hash, en caso de estar junto con el documento, al servidor remoto con el que está conectado al ordenador, por ejemplo, a través de una conexión a Internet.

[0036] En caso de que el servidor remoto pueda calcular el hash de un documento electrónico, el usuario puede enviar sólo el documento para ser firmado con el mismo servidor de manera que se obtiene el hash directamente desde el servidor.

[0037] Cuando el ordenador envía el hash y/o el documento que debe ser firmado por el software al servidor, también es enviado un código de identificación del usuario firmante. Como resultado de estas operaciones, el servidor envía un número de teléfono al usuario: esta comunicación puede tener lugar aprovechando la conexión entre el servidor y el ordenador, en este caso el software muestra el número de teléfono, o el servidor, que puede contener el número de teléfono de los usuarios, envía un mensaje de texto que contiene el número de teléfono al que se llamará al teléfono inalámbrico del usuario en cuestión.

[0038] A continuación, el usuario firmante llama al número de teléfono indicado y se pone en comunicación con el servidor remoto. Con esta comunicación, el servidor remoto verifica el número de teléfono de identificación del usuario que llama, a saber, el número de teléfono que llama y/u otros códigos tales como el código IMSI y/o el código IMEI. Por lo tanto, el servidor verifica si el código de identificación del usuario enviado en las fases iniciales corresponde al número de teléfono de identificación según los datos insertados en su base de datos.

[0039] En el caso positivo, el servidor remoto continúa con la encriptación del hash a fin de obtener la firma digital del documento electrónico en proceso. Para esta operación, el servidor debe utilizar el certificado de firma digital correspondiente al código de identificación de usuario y el número de teléfono de identificación del usuario firmante, obtenido de las comunicaciones entre el ordenador y el servidor y entre el dispositivo de comunicación y el servidor.

[0040] A continuación, el servidor remoto envía la firma al ordenador del usuario firmante. Como alternativa, el servidor puede enviar el documento firmado, a saber, el documento electrónico junto con la firma digital, a otra entidad de acuerdo con las instrucciones del usuario firmante; en este caso, las operaciones de envío para enviar un documento firmado se aceleran.

[0041] El método y el sistema relativo según la invención pueden proporcionar que el servidor remoto envíe un mensaje de texto al dispositivo de comunicación móvil para notificar el resultado positivo o negativo de la operación de firma.

[0042] El hecho de que el servidor envíe el número de teléfono a llamar al usuario permite que el sistema maneje simultáneamente más números de teléfono y, en consecuencia, más usuarios.

[0043] Según una variante del método así descrito, a fin de aumentar el nivel de seguridad, durante la comunicación con el servidor, el usuario firmante debe enviar un código secreto para el servidor.

[0044] Dicho código secreto puede ser un código personal estático, recibido de la oficina de certificación en la obtención del certificado de firma digital. Obviamente, este código personal se almacena sobre la base de datos justo al lado de los otros números de identificación/códigos del usuario.

[0045] Además, el código secreto puede ser enviado por el servidor al ordenador o al dispositivo móvil en el comienzo de cada operación de firma, y el usuario debe devolver dicho código secreto al servidor mediante la utilización de un canal de comunicación diferente del canal de recepción

[0046] Según otra realización del método de acuerdo con la invención, una vez que el servidor remoto que sostiene los números de teléfono de los usuarios ha obtenido el hash y recibido el código de identificación del usuario, el servidor remoto realiza una llamada al dispositivo de comunicación móvil asociado al mismo código de identificación. El usuario del firmante que responde a la llamada envía un código de reconocimiento unívoco, asignado previamente al servidor remoto durante la misma comunicación telefónica. Si el código insertado corresponde a uno conservado en la base de datos del servidor, el cifrado del hash se efectúa mediante el certificado de firma digital correspondiente al usuario en comunicación telefónica y obtiene la firma digital.

[0047] Incluso en este caso, el código de reconocimiento unívoco puede ser estático, asignado una única vez para todas las operaciones, o puede variar y es enviado al comienzo de cada transacción.

[0048] Otras variantes y cambios en el método y el sistema según la invención pueden ser concebidos, pero deben ser considerados como incluidos en el alcance de protección como se define por las siguientes reivindicaciones.

REIVINDICACIONES

1. Método para efectuar una firma electrónica cualificada de un documento electrónico por uno o más usuarios firmantes, en el que se proporciona
un servidor remoto, adecuado para comunicarse telefónicamente a través de una red telefónica,
un ordenador conectado al servidor remoto,
un software adaptado para operar en el ordenador y en el servidor,
un certificado de firma digital respectivo en posesión de cada uno de los usuarios firmantes almacenados en dicho servidor remoto,
un dispositivo electrónico respectivo de comunicación móvil asociado a cada uno de los usuarios a los que está asociado un número de identificación,
una base de datos almacenada en el servidor remoto que contiene un código de identificación del usuario firmante asociado a dicho número de identificación,
comprendiendo dicho método las siguientes etapas:

- el usuario firmante controla el comienzo de la operación de firma para la firma del documento electrónico a través del software mediante el envío de un código de identificación al servidor remoto,
- el servidor remoto recibe o calcula un hash del documento electrónico creado mediante un algoritmo de cálculo hash,
- el servidor autentica al usuario y, en un caso positivo
- el servidor remoto encripta el hash a través del certificado de firma digital correspondiente al usuario y obtiene la firma digital,
- la firma digital está insertada en el documento electrónico por el software;

caracterizado por que el método comprende las siguientes etapas:

- el servidor remoto envía selectivamente un número de teléfono al ordenador o a dicho dispositivo electrónico de comunicación móvil, más números de teléfono correspondientes al servidor remoto y recibe una llamada de uno o más usuarios firmantes a través del dispositivo electrónico de comunicación móvil mediante el cual se establece una comunicación telefónica,
- el servidor remoto verifica la coincidencia del número de identificación recibido de la red telefónica y el número de identificación asociado al usuario firmante almacenado sobre la base de datos.

2. Método según la reivindicación 1, en el que el hash recibido por el servidor corresponde al hash calculado al principio a partir del documento electrónico a ser firmado mediante un algoritmo de cálculo hash por el software utilizado por el usuario, y enviado por el ordenador al servidor remoto.

3. Método según cualquiera de las reivindicaciones anteriores, en el que el servidor remoto envía la firma digital así obtenida a un ordenador personal del usuario firmante.

4. Método según cualquiera de las reivindicaciones anteriores, en el que el código de identificación no corresponde con el número de identificación del dispositivo electrónico de comunicación móvil que llama al servidor remoto, el servidor remoto envía un mensaje no coincidente al ordenador para comunicar la falta de correspondencia y la imposibilidad de efectuar una firma electrónica cualificada.

5. Método según cualquiera de las reivindicaciones anteriores, en el que se incluyen las siguientes fases:

- el servidor remoto obtiene el hash calculando dicho hash desde el documento electrónico enviado por el usuario al servidor remoto a través del software, a través del software, el equipo envía un código de identificación del usuario firmante al servidor remoto;
- el servidor remoto comunica un número de teléfono al usuario;
- el usuario marca el número de teléfono en el dispositivo electrónico para la comunicación móvil en su poder y establece una comunicación con el servidor remoto;
- durante la comunicación, sobre la base de la información de la base de datos, el servidor remoto verifica la correspondencia entre el código de identificación del usuario firmante y el número de identificación de llamada del dispositivo de comunicación móvil con el que ha establecido la comunicación;
- en caso de coincidencia entre el código de identificación y el número de identificación, el servidor remoto encripta el hash obtenido previamente utilizando el certificado de firma digital y crea la firma digital del documento electrónico.

6. Método según la reivindicación 5, en el que el número de teléfono comunicado por el servidor remoto al usuario es un número que ha sido enviado por el servidor remoto al ordenador y visualizado por el usuario a través del software.

7. Método según cualquiera de las reivindicaciones 5 o 6, en el que además del número de teléfono a llamar, el servidor remoto envía al ordenador un código numérico visualizado por el usuario y asociado con el número de

identificación del dispositivo para la comunicación móvil del usuario y donde durante la comunicación con el servidor remoto, el usuario teclea el código numérico visualizado previamente de modo que además de verificar la coincidencia entre el código de identificación del usuario firmante y el número de identificación del dispositivo de comunicación móvil llamante con el que ha establecido la comunicación, el servidor remoto verifica la coincidencia del código de identificación y el número de identificación de llamada con el código numérico tecleado por el usuario durante la comunicación.

8. Método según cualquiera de las reivindicaciones 5 a 7, en el que se asocia un código secreto personal con cada usuario firmante, estando dicho código secreto almacenado sobre la base de datos del servidor remoto asociado con el número de identificación del dispositivo de comunicación móvil del usuario firmante correspondiente y en el que durante la comunicación con el servidor remoto, el usuario envía su código secreto personal para que el servidor remoto verifique la coincidencia del número de identificación de llamada del dispositivo para la comunicación móvil con el código secreto personal tecleado por el usuario durante la comunicación.

9. Método según cualquiera de las reivindicaciones 1 a 4, en el que el servidor remoto llama al dispositivo de comunicación móvil y el usuario firmante que responde a la llamada a través del dispositivo de comunicación móvil envía un código de referencia unívoca a través de la misma comunicación telefónica al servidor remoto, dicho código de referencia unívoca siendo asignado al usuario firmante antes del comienzo de la comunicación telefónica para que sea posible efectuar el cifrado del hash por medio del certificado de firma digital que corresponde al usuario en la comunicación telefónica y para obtener una firma digital.

10. Método según la reivindicación 9, en el que el código de reconocimiento unívoco asociado con el usuario firmante es enviado por el servidor remoto al ordenador después del comienzo de las operaciones de firma.

11. Método según la reivindicación 9, en el que el código de reconocimiento unívoco asociado con el usuario firmante se asigna al mismo usuario en la fase de asignación de su certificado de firma digital.

12. Método según cualquiera de las reivindicaciones anteriores, en el que el servidor remoto envía un código numérico al dispositivo de comunicación móvil del usuario firmante, cuyo código numérico es luego enviado por el ordenador al servidor remoto por el mismo usuario para que el servidor remoto mismo verifique la identidad entre el código enviado y el código recibido y, en caso de identidad, el servidor remoto confirma la operación de cifrado del hash y obtiene la firma digital.

13. Método según cualquiera de las reivindicaciones anteriores, en el que después de que el servidor remoto ha llevado a cabo el cifrado y obtenido la firma digital, el servidor remoto notifica al usuario firmante enviando un mensaje de texto al dispositivo de comunicación móvil del mismo usuario firmante.

14. Sistema para efectuar una firma electrónica cualificada de un documento electrónico por uno o más usuarios firmantes, que comprende:

un servidor remoto, adecuado para comunicarse telefónicamente,
un ordenador conectado al servidor remoto,
un certificado de firma digital respectivo referido a cada uno de los usuarios firmantes almacenados en dicho servidor remoto,
una base de datos almacenada en el servidor remoto que contiene un código de identificación asociado a dicho número de identificación para cada usuario firmante,

- un software para operar en el servidor remoto y en el ordenador,
- un dispositivo electrónico de comunicación móvil para cada uno o más de los usuarios firmantes, al que se asocia un número de identificación de manera unívoca;
- el software es adecuado para enviar el documento electrónico a firmar y/o el hash calculado por dicho documento electrónico junto con el código de identificación del usuario, para recibir un número de teléfono de servidor selectivo, entre más números de teléfono correspondientes al servidor remoto, para establecer una comunicación telefónica entre el usuario y el servidor remoto a través del dispositivo electrónico de comunicación móvil, verificar durante la comunicación telefónica la correspondencia entre el usuario firmante en la comunicación telefónica y el código de identificación del usuario, en caso de una coincidencia real, encriptar en el servidor remoto el hash a través del certificado de firma digital para obtener una firma digital, para insertar la firma digital en el documento electrónico.