(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 563 212**

(51) Int. CI.:

H04L 29/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **10.10.2012 E 12188046 (2)**

(97) Fecha y número de publicación de la concesión europea: **09.12.2015 EP 2582115**

(54) Título: **Sistema de firma electrónica reconocida, método asociado y dispositivo de teléfono móvil para una firma electrónica reconocida**

(30) Prioridad:

10.10.2011 IT TO20110902

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
11.03.2016

(73) Titular/es:

BONSIGNORE, ANTONIO SALVATORE PIERO VITTORIO (100.0%)
Via Paisiello 21
20011 Corbetta (MI), IT

(72) Inventor/es:

BONSIGNORE, ANTONIO SALVATORE

DESCRIPCIÓN

Sistema de firma electrónica reconocida, método asociado y dispositivo de teléfono móvil para una firma electrónica reconocida.

La presente invención se refiere a un sistema de firma electrónica reconocida (QES, *Qualified Electronic Signature*) configurado para intercambiar datos con primeros medios de procesamiento del peticionario configurados para permitir a un peticionario generar peticiones solicitando una firma electrónica reconocida a través de dicho sistema a un destinatario, comprendiendo dicho sistema segundos medios de procesamiento del destinatario configurados para permitir al destinatario de la petición firmar con su firma electrónica reconocida, comprendiendo dichos segundos medios de procesamiento un dispositivo de teléfono móvil para firma electrónica reconocida de tipo móvil, adaptado para intercambiar comunicaciones basadas en texto sobre redes de telecomunicaciones móviles en base a un identificador del destinatario que está suscrito al servicio de telefonía móvil comprendido en un módulo de identidad de suscriptor con el que está asociado.

La identidad se certifica comúnmente firmando documentos en papel con firmas manuscritas. Por motivos de eficiencia y practicidad hoy en día resulta a menudo preferible operar en la red, en particular Internet, de manera digital; sin embargo el usuario debe identificarse con seguridad para permitir el acceso a datos sensibles y a servicios en la red, órdenes de pago, autorizaciones y suscripciones en formato electrónico.

Normalmente, el acceso a servicios de red tiene lugar por medio del uso de un par de parámetros de identificación digitales, tales como nombre de usuario y contraseña, conocidos para el usuario al que se le asignaron estos parámetros de identificación. Estos parámetros de identificación también están presentes en una base de datos del servicio relacionado al que está accediendo el usuario. Esta solución es vulnerable en términos de seguridad debido a la relativa facilidad con la que pueden interceptarse estos parámetros en la red para suplantar al usuario físico autorizado. Además, la presencia de estos parámetros dentro de una base de datos expone a los mismos a una copia efectuada a través de un ataque de piratas informáticos, con el posterior robo y uso de la identidad digital. El aumento del uso de servicios de red también multiplica para cada usuario los parámetros identificadores que han de recordarse, lo que representa un problema de comodidad de uso que no ha de infravalorarse.

Un tipo más avanzado de identificación digital está representado por el uso de dispositivos de OTP (contraseña de un solo uso). En este caso, además de nombre de usuario y contraseña, normalmente el usuario posee un dispositivo que, tras la interrogación, suministra un código que ha de añadirse como contraseña adicional y temporal válida solo para esa operación y que expira rápidamente. El dispositivo calcula este código a través de un algoritmo basándose en la hora actual y en un código alfanumérico (semilla) guardado en el dispositivo, pero también en una base de datos central, con el consecuente riesgo de un ataque de piratas informáticos.

El uso de dispositivos de OTP sólo satisface en parte un requisito expresado normalmente por el sector bancario según el cual, para una mayor seguridad, el usuario debería autenticarse tanto a través de información conocida por el mismo (tal como nombre de usuario y contraseña) como a través de un dispositivo que el usuario posee. De hecho, el dispositivo de OTP no corresponde realmente a algo único que el usuario posee, ya que la información (contraseña temporal) vinculada a este dispositivo es realmente información que puede replicarse. Los sistemas de banca desde casa usados más ampliamente hoy en día hacen uso de esta tecnología.

Otra forma de autenticación digital de identidad en la esfera de los pagos electrónicos está representada por códigos de tarjeta de crédito. Estos códigos son relativamente fáciles de copiar por piratas informáticos expertos o más fácilmente en puntos de venta. Para compensar esta vulnerabilidad, algunos circuitos de comercio electrónico usan una contraseña adicional y solicitan la respuesta a cuestiones adicionales relativas a información adicional del usuario, para poder producir una autorización de pago. Por tanto, es necesario recordar una nueva contraseña, aunque sin excluir los riesgos de que piratas informáticos copien información.

Otra forma de autenticación digital de identidad está representada por el uso de la tecnología PKI (infraestructura de clave pública) y firmas electrónicas basadas en claves privadas no protegidas. En estas soluciones la clave privada está archivada en una zona, tal como el sistema de archivos del cliente, que habitualmente no tiene un alto nivel de protección, en particular sin certificación frente a la extracción de la clave privada, y por tanto pueden realizarse copias de la misma clave privada. En la bibliografía, las firmas estampadas a través de esta tecnología se denominan firmas electrónicas y a veces firmas digitales. Además en este caso la posibilidad de realizar copias de la clave privada menoscaba la seguridad de la solución. De hecho, se usa la clave privada para implementar el algoritmo de firma y, si se copia, compromete la seguridad de la solución.

Otras formas de autenticación digital de identidad usan la firma electrónica reconocida, tal como se define, por ejemplo, en el Código de Administración Digital (Decreto Ley del 30 de diciembre de 2010, n.º 235) y en la Directiva europea 1999/99/CE, habitualmente a través del uso de ordenadores cliente en los que normalmente es necesario instalar dispositivos de testigo USB o tarjeta inteligente con lector relacionado. Estos dispositivos están certificados según los niveles de seguridad nacionales e internacionales requeridos para garantizar que la clave privada es imposible de copiar. Estos dispositivos garantizan la autenticación digital de identidad con un alto nivel de seguridad

a través de la implementación de una firma electrónica reconocida. El algoritmo usado es de tipo asimétrico, para garantizar un alto nivel de seguridad. Sin embargo, deben instalarse testigos USB y tarjetas inteligentes con un lector relacionado en un ordenador cliente y se requiere un mantenimiento. Además, en este caso la autenticación de identidad requiere habitualmente el uso de un procesador de tipo ordenador personal que, incluso si es portátil, limita su uso en cuanto a movilidad.

También se conocen formas de autenticación que usan teléfonos móviles o teléfonos inteligentes como medio para garantizar la identidad digital en movilidad.

Algunas de estas soluciones se basan en claves privadas o certificados digitales archivados en repositorios, es decir módulos de almacenamiento, que no están certificados frente a la extracción de la clave privada.

Algunas soluciones móviles usan claves simétricas para la identificación, firma y cifrado y por tanto tienen un nivel de seguridad limitado.

Otras soluciones móviles se basan en el uso de un Elemento de Seguridad o Seguro incorporado en el teléfono móvil o teléfono inteligente que limita el uso a modelos específicos, sin garantizar el uso de repositorios certificados frente al copiado de la clave privada.

En algunas soluciones, la información presente en el Elemento Seguro no corresponde a la clave privada, sino al número de tarjeta de crédito o equivalente en efectivo disponible para pagos desde un dispositivo móvil.

En algunos casos el proceso de firma electrónica tiene lugar de manera remota y normalmente a través de dispositivos de firma de servidor certificado de módulo de seguridad de hardware (HSM); en este caso, para activar el proceso de firma debe enviarse un PIN (número de identificación personal) de activación a través del teléfono móvil y/o un dispositivo de OTP; independientemente de lo seguro que sea el canal usado para enviar el PIN, se transmite sobre la red, reduciendo la seguridad de la solución.

Algunas soluciones se basan en el uso del SIM como dispositivo certificado para firma electrónica reconocida, pero en este caso la compañía de teléfono y los bancos deben llegar a un acuerdo sobre los métodos, protocolos e ingresos. Esto es necesario debido a que la parte que gestiona el SIM, habitualmente la compañía de teléfono es, de hecho, la propietaria. Este tipo de solución se describe en el artículo por Martin Whitehead, “GSMA Europe response to European Commission consultation on eSignatures and eIdentification”, GSMA Europe (15/04/2011), XP002683918.

Esta solución es difícil de llevar a la práctica ya que para una experiencia de usuario satisfactoria, el banco que ofrece los servicios de pago al usuario genérico debe tener un acuerdo con la compañía del usuario, ya que es poco probable que el usuario cambie de compañía o, viceversa, que cambie de banco. Este proceso no es sencillo de lanzar al mercado debido al número de sujetos implicados, tanto por parte del banco como de la compañía.

Algunas soluciones móviles, no basadas en firma electrónica reconocida, excluyen a los bancos, limitando los pagos en casos en los que las compañías de teléfono pueden funcionar de manera autónoma, tal como en el caso de adquisición de contenidos digitales, normalmente deduciendo éstos del crédito del teléfono.

Un objeto de la presente invención es proporcionar un sistema que permita a un firmante firmar digitalmente las peticiones enviadas por un peticionario a través del sistema. En particular, el sistema permite al firmante, como destinatario de una petición de pago o petición de suscripción mediante firma o un acceso seguro a servicios de red, por ejemplo, operar con seguridad a través de una firma electrónica reconocida usando su propio teléfono móvil.

Con el término “firmante” quiere decirse, en la presente descripción, una persona, una empresa u otro destinatario físico o no físico dotado de una identidad electrónica y que puede firmar documentos, y peticiones en general, por medio de firma electrónica reconocida o firma electrónica no reconocida. En la presente invención los términos “firmante” y “destinatario” corresponden a la misma entidad.

Según la presente invención, este objeto se consigue a través de un sistema de firma electrónica reconocida que tiene las características especificadas en las reivindicaciones adjuntas.

La invención también se refiere a un correspondiente procedimiento de firma electrónica reconocida, y a un dispositivo terminal que opera en este sistema según la invención para la firma electrónica reconocida de tipo móvil.

En breves palabras, esta invención se refiere a un sistema de firma electrónica reconocida con certificación de identidad digital, implementado en un dispositivo de teléfono móvil para producir la firma electrónica reconocida por un destinatario de una petición que va a firmarse digitalmente.

Este dispositivo telefónico para producir la firma electrónica reconocida es un teléfono móvil dotado de un sistema operativo, en particular un teléfono inteligente, que proporciona el uso de una memoria de seguridad y una

aplicación, instalada en este teléfono móvil o en esta memoria de seguridad instalada, con una configuración para operar con esta memoria de seguridad. La memoria de seguridad habitualmente está instalada en un medio extraíble, que permite alojarla de manera extraíble en el teléfono móvil para poder efectuar, en particular a través de dicha aplicación, las operaciones de firma electrónica reconocida usando la clave privada del firmante. Por tanto, la memoria de seguridad puede estar instalada en un soporte de memoria que puede extraerse e insertarse en el teléfono inteligente en una ranura que es diferente de una ranura de la UICC (tarjeta universal de circuito integrado)/uSIM (módulo universal de identidad de suscriptor)/SIM (módulo de identidad de suscriptor). De hecho, la memoria de seguridad no es un UICC/uSIM/SIM o parte de los mismos, tiene diferente forma y dimensión, y es independiente del operador de red móvil (MNO) elegido por el usuario de teléfono inteligente y de la red móvil como la red GSM/UMTS.

Habitualmente, la memoria de seguridad puede usarse en un soporte (o ranura) adecuado para una microSD común pero no es una memoria SD sencilla. La memoria de seguridad tiene al menos una partición de seguridad para implementar una doble función: una primera partición que es la parte de seguridad de la memoria, puede realizar una firma electrónica reconocida, mantener y proteger claves privadas de firma frente a su extracción; las otras particiones son particiones de almacenamiento comunes que pueden almacenar una mayor cantidad de datos genéricos (2 GB o más). De este modo, la memoria de seguridad tiene una dimensión de almacenamiento mayor que un UICC/uSIM/SIM. Una memoria de seguridad como ésta, denominada tarjeta de seguridad móvil, la ha producido recientemente Giesecke & Devrient.

La memoria de seguridad comprende al menos una partición segura en la que está almacenada al menos la clave privada del firmante.

La memoria de seguridad es diferente del módulo de identidad de suscriptor (SIM) pero es accesible por el dispositivo de teléfono móvil en combinación con el identificador de módulo de identidad de suscriptor del firmante con el que está asociada la memoria de seguridad cuando se intercambian datos a través de redes de telecomunicaciones móviles. La memoria de seguridad puede ser accesible también en combinación con datos electrónicos intercambiados por medio de redes de proximidad, mediante dispositivos de proximidad en el teléfono móvil.

La firma electrónica se realiza en la partición de seguridad de la memoria de seguridad certificada para firma electrónica reconocida y para almacenar la clave privada de un modo independiente respecto al servicio de telefonía móvil, a las redes de telecomunicaciones móviles y al módulo de identidad de suscriptor. En particular, la memoria segura se activa con el fin de realizar una firma electrónica reconocida en base a un código de activación introducido por el firmante a través del dispositivo de teléfono móvil.

La memoria certificada se usa para mantener la identidad digital del usuario independiente de operadores de red móvil (MNO) y servicios de red móvil, y para alcanzar los niveles de seguridad requeridos por reglamentos nacionales e internacionales para proteger la clave privada del usuario final frente a la extracción, en un contexto de firmas electrónicas reconocidas, básicamente cumpliendo con la certificación CC EAL 4+ (o superior) y los denominados perfiles de protección requeridos.

La memoria de seguridad también puede ser un testigo, con características análogas de una memoria de seguridad de tipo SD descrita, para introducir en la clavija de audio/micrófono del teléfono inteligente.

El teléfono móvil está configurado para conectarse, preferiblemente por medio de SMS (servicio de mensaje corto) a una red de comunicación para la firma electrónica reconocida, o red dedicada, que comprende una arquitectura específica de componentes de servidor.

En la red de firma electrónica reconocida se habilitan tanto los usuarios que solicitan que se firmen peticiones usando una firma electrónica reconocida, pudiendo implementarse cada una mediante una o más peticiones de operación en sucesión, como los usuarios que reciben peticiones de operación que van a firmarse usando una firma electrónica reconocida. Frente a una o más peticiones de operación generadas por la misma petición de firma original por el peticionario, solo una petición de operación llegará, tras modificarse, al destinatario para la confirmación por medio de firma electrónica reconocida.

El usuario destinatario, habilitado para usar esta red de firma electrónica reconocida a través del teléfono móvil, puede usar este teléfono móvil, si es necesario, en asociación con un procesador de soporte opcional que puede estar dotado de una pantalla mayor. En cualquier caso, la operación para identificar el destinatario tiene lugar a través del teléfono móvil, en particular el teléfono inteligente, que, gracias a sus dimensiones normalmente portátiles, es adecuado para operar como instrumento de identificación en movilidad, para procesos de autorización que se inician en otros dispositivos o en el mismo teléfono inteligente.

Se llega al usuario destinatario a través de mensajes sobre la red de telecomunicaciones móviles, preferiblemente por medio de mensajes de texto SMS, mediante peticiones procedentes de esta red dedicada en base a su número de teléfono móvil, asociado con un SIM ubicado en el teléfono inteligente.

El destinatario puede interactuar también directamente por medio de redes de proximidad mediante un dispositivo de proximidad en su dispositivo de teléfono móvil.

Según un aspecto importante de la invención, un usuario destinatario también puede proceder de manera activa a efectuar peticiones que requieren su firma electrónica reconocida, dirigiéndose estas peticiones a sí mismo; el usuario destinatario puede efectuar estas peticiones a través del teléfono móvil habilitado para el uso de la red de firma electrónica reconocida o a través de procesadores de soporte, si se proporcionan. La confirmación de las peticiones por el usuario siempre tiene lugar a través de dicho teléfono móvil.

El usuario peticionario también puede habilitarse como destinatario para el uso de la red dedicada, o no habilitarse para este uso, operando en este último caso a través de los servicios proporcionados por dicha red tal como peticiones de pago y suscripción dirigidas a terceros destinatarios. Solo los mismos destinatarios efectúan peticiones de acceso.

Pueden efectuarse peticiones que requieren firma electrónica reconocida, por ejemplo, a través de una aplicación de software en el teléfono móvil, en particular la misma aplicación que gestiona la firma certificada, o, por ejemplo, a través del navegador de un ordenador personal.

La aplicación de software en el teléfono móvil está configurada en general para gestionar la confirmación por medio de firma electrónica reconocida de mensajes de petición de operación que llegan al destinatario, tras modificarse, recibidos tras enviar una petición efectuada por terceros o por el mismo usuario destinatario.

Las peticiones originales del usuario peticionario se descomponen en una o más peticiones de operación enviadas en sucesión, gestionadas y reenviadas a un servidor frontal de la red dedicada, es decir la fase inicial con respecto a la llegada de dichas peticiones, que:

- asigna a cada petición de operación individual un identificador de petición único y un sello de tiempo que indica al menos fecha, hora, minutos, segundos, e

- interroga a su propia base de datos de usuarios en la que están registrados los usuarios destinatarios para el uso de la red dedicada en base a su número de teléfono o a un respectivo código de identificación, o registro, en el sistema de firma electrónica reconocida para verificar sus derechos con respecto al uso de la red dedicada;

- en base al usuario identificado, extrae de la base de datos de usuarios información del usuario, tal como una dirección de correo electrónico y referencias de dirección de uno o más servidores aplicativos a los que el servidor frontal dirige las peticiones de operación en base al tipo de estas peticiones.

El servidor frontal también está configurado para efectuar una verificación del formato correcto de la petición de operación y de la presencia del número de teléfono o identificador presente en la misma petición de operación. Una capa de software para la conexión a la red dedicada se instala en el servidor frontal y en los servidores aplicativos.

El servidor aplicativo implicado en base al usuario destinatario y el tipo de petición de operación se instala en una entidad, por ejemplo un banco, en la que se registra el destinatario signatario de la red dedicada. El servidor aplicativo valida además las peticiones en base al formato específico y busca en su propia base de datos de usuarios la presencia del usuario registrado con la información recibida tal como el identificador dentro de la red dedicada o número de teléfono. En el caso en el que la comprobación es satisfactoria y si la petición de operación requiere que la firme el destinatario, el servidor aplicativo envía un mensaje de petición basado en texto obtenido de la correspondiente petición de operación al teléfono móvil del usuario destinatario, enviando en particular un mensaje de texto SMS al número de teléfono registrado.

Tras la recepción del mensaje de petición basado en texto que solicita la firma, la aplicación en el teléfono móvil automáticamente visualiza en la pantalla del mismo teléfono móvil una interfaz gráfica de modo que el usuario puede confirmar o rechazar esta petición, estampando una firma electrónica reconocida del usuario destinatario; esta firma se estampa en datos específicamente recibidos por medio del mensaje basado en texto, normalmente mensaje de texto SMS, correspondiente al mensaje de petición de operación mencionado anteriormente.

El usuario destinatario introduce un código PIN de firma para confirmar el estampado de la firma electrónica reconocida que activa la memoria de seguridad. Este código PIN de firma no se transmite sobre la red dedicada, sino que se usa solo para activar la firma de manera local.

El sistema de firma electrónica reconocida permite la suscripción digital, por medio del teléfono móvil dotado de memoria de seguridad, de las siguientes peticiones de firma basadas en texto, cada una a través de la gestión del correspondiente mensaje de petición de operación recibido que requiere firma:

- pago

- suscripción de documentos

- acceso a sitios web y servicios de red.

El usuario destinatario puede aplicar, a través del teléfono móvil, una firma electrónica reconocida con la clave privada.

El teléfono móvil también puede visualizar notificaciones y enviar confirmación de recepción de la notificación y preferiblemente también está configurado para permitir efectuar activamente peticiones para los tipos de operación mencionados anteriormente.

La firma electrónica reconocida se aplica a la información que va a suscribirse, en particular aplicando un cifrado a través de la clave privada en una cadena *hash* calculada en el mensaje basado en texto de la petición recibida en el dispositivo móvil o en el *hash* contenido en el mensaje. En el caso de pagos y accesos, la información que va a suscribirse se diferencia cada vez de las anteriores, ya que está asociada con al menos una parte variable única añadida por el servidor frontal de la red dedicada a la que los peticionarios envían las peticiones; la parte variable incluye, al menos, un identificador único e indicación del sello de tiempo de implementación de la petición. El hecho de que la firma solicitada siempre deba ser diferente evita problemas en el caso de que la copien piratas informáticos; no puede confirmar otra petición. En cambio, en el caso de suscripción de documentos, se aprovecha el hecho de que los documentos son generalmente diferentes cada vez, al menos para un usuario destinatario dado, y por tanto la información que va a suscribirse también varía. En el caso de sustitución de la firma electrónica reconocida por la de otro sujeto, el sistema de verificación de firma, del que está dotado el servidor aplicativo, detectaría que dicha firma la estampó un tercero diferente al destinatario correcto.

Debido al uso de la memoria de seguridad, la clave privada está protegida frente a copia y extracción.

El algoritmo de cifrado usado para la firma electrónica reconocida es el algoritmo RSA, que es de tipo asimétrico; la firma electrónica reconocida es la firma electrónica que se considera que tiene un alto grado de seguridad, tal como para ser legalmente equivalente a la firma manuscrita en muchos sistemas legales nacionales.

La identificación del usuario habilitado en la red dedicada, en respuesta a un mensaje de petición de operación que requiere una firma, tiene lugar enviando desde el teléfono móvil una firma electrónica reconocida en forma separada, con respecto a los certificados y, en la mayoría de realizaciones, con respecto al mensaje de texto sin formato al que hace referencia.

El usuario destinatario de la red dedicada puede acceder de manera exclusiva, con su propia identidad, a las operaciones que pueden efectuarse a través de la aplicación de firma electrónica reconocida en el teléfono móvil, ya que la firma electrónica reconocida que las activa solo puede efectuarse a través de la memoria de seguridad asociada con el teléfono móvil, en el que reside la clave privada protegida de este usuario, única en esta red, ya que se refiere a una clave pública única dentro de esta red y registrada en la misma junto con el certificado reconocido que contiene dicha clave pública. Además, el código PIN para la activación de la firma solo lo conoce el usuario en posesión de la clave privada y no es información replicada dentro del sistema. El código PIN para la activación de la firma solo puede interpretarlo la memoria de seguridad, pero no puede deducirlo. Por tanto, la contraseña o pluralidad de contraseñas enviadas por la red, usadas habitualmente para acceder a servicios/entidades específicos, se sustituye(n) por el uso de un único código PIN en el teléfono inteligente, no transmitido por la red.

Según un aspecto adicional, el servidor aplicativo, tras enviar el mensaje de texto SMS con el mensaje de petición basado en texto al teléfono móvil, espera un tiempo configurable para recibir la firma electrónica reconocida desde el teléfono móvil; si este tiempo no ha expirado, con la llegada del mensaje que contiene dicha firma electrónica reconocida, el servidor aplicativo verifica la firma. En base al tipo de petición firmada, el servidor aplicativo efectúa transacciones que se integran con otros servicios de la entidad que hospeda el servidor aplicativo; por ejemplo, en el caso de pagos normalmente está hospedado en el banco del usuario. De este modo, la información sensible del usuario para realizar el pago (por ejemplo, número de tarjeta de crédito) normalmente solo está presente dentro del banco, dando ventaja a la seguridad. Más en general, la adopción del sistema por una entidad/servicio, a través del uso normalmente interno de la capa de servidor aplicativo, permite a la entidad y sus clientes certificar la identidad del usuario sin transferirse los datos sensibles del usuario por la red.

El servidor aplicativo según un aspecto adicional de la invención recibe retroalimentación sobre la transacción desde los servicios de la entidad y la envía al teléfono móvil del usuario destinatario, y actualiza el estatus de la operación en el servidor frontal en base al identificador único de cada petición de operación, originándose cualquier petición de operación diferente a partir de una misma petición original vinculada, a través de la presencia del identificador de la petición de operación anterior en la petición de operación posterior; el estatus llega al peticionario a través de los medios de procesador usados por el mismo para la petición. La red para la firma digital a través de este servidor frontal envía una notificación al peticionario por medio de correo electrónico, si la correspondiente dirección está presente en los datos de petición. Si el peticionario está registrado en la red dedicada y proporcionó su identificador

único dentro de la red dedicada en la petición, recibe un mensaje de notificación sobre el estatus de la operación en su teléfono móvil habilitado.

Según un aspecto adicional de la invención, para cada petición original, el usuario que recibió un mensaje de petición basado en texto también recibe un correo electrónico de notificación, además de un mensaje de texto SMS.

Según un aspecto adicional de la invención, en el lado del servidor frontal, las firmas electrónicas reconocidas validadas acompañan a la información de texto sin formato, al certificado de firma y al certificado de la autoridad de certificación que emitió el certificado de firma. Si el documento es una factura de ventas, se produce por tanto una factura electrónica a través de la firma. Los documentos y los mensajes de petición suscritos se almacenan digitalmente en los servidores de almacenamiento de la red dedicada según el proceso de almacenamiento digital legal del país de uso, por ejemplo en Italia se denomina “Conservazione Sostitutiva” (Almacenamiento electrónico). Preferiblemente, se asocia un sello de tiempo legalmente válido con estas firmas. El usuario puede consultar, verificar y visualizar estos documentos a través de un servicio específico de la red dedicada.

Según la invención, se describe un procedimiento de firma electrónica reconocida. El procedimiento comprende las operaciones implementadas por el sistema de firma electrónica reconocida descrito anteriormente.

Según un aspecto adicional de la invención, el procedimiento comprende también: usar una contraseña temporal (ATP), mostrar en pantalla una cadena de base sin *hash* o un *hash* de la cadena de base y la contraseña temporal en los segundos medios de procesamiento del firmante, mostrar en pantalla la cadena de base sin *hash* o el *hash* de la cadena de base y la contraseña temporal en los primeros medios de procesamiento del peticionario. Además, el método comprende calcular mediante el servidor aplicativo la cadena de base sin *hash* o el *hash* de la cadena de base en base a la información de la petición y de la contraseña temporal (ATP), y a información adicional que comprende un identificador de sesión en el servidor de interfaz correspondiente al identificador de la petición.

Según la invención, se describe un dispositivo de teléfono móvil para firma electrónica reconocida. El dispositivo de teléfono móvil está adaptado para intercambiar comunicaciones basadas en texto sobre redes de telecomunicaciones móviles, o para intercambiar datos electrónicos con módulos de proximidad sobre redes de proximidad, en base a un identificador del suscriptor de un servicio de telefonía móvil comprendido en un módulo de identidad de suscriptor con el que está asociado el suscriptor, que comprende un sistema operativo y medios para operar con una memoria de seguridad que comprende al menos una partición segura en la que está almacenada al menos la clave privada del suscriptor, teniendo la memoria de seguridad las características técnicas descritas anteriormente.

El dispositivo de teléfono móvil está configurado, a través de una aplicación de software dedicada ejecutada en el sistema operativo, para usar la clave privada en la memoria de seguridad y estampar una firma electrónica reconocida mediante cifrado de un mensaje de petición o datos o partes de los mismos por medio de la clave privada.

El dispositivo de teléfono móvil puede operar la firma electrónica en la partición de seguridad de la memoria de seguridad manteniendo la clave privada de un modo independiente con respecto al servicio de telefonía móvil, a las redes de telecomunicaciones móviles y al módulo identificador de suscriptor en base a un código de activación introducido por el firmante a través del dispositivo de teléfono móvil.

Características y ventajas adicionales de la invención resultarán evidentes a partir de la siguiente descripción con referencia a los dibujos adjuntos, proporcionados meramente a modo de ejemplo no limitativo, en los que:

- la figura 1 representa un dispositivo de teléfono móvil convencional;

- la figura 2 representa un dispositivo de teléfono móvil según la invención;

- la figura 3a representa esquemáticamente una primera arquitectura del sistema de firma electrónica reconocida según la invención;

- la figura 3b representa esquemáticamente una segunda arquitectura del sistema de firma electrónica reconocida según la invención;

- la figura 4 representa esquemáticamente una tercera arquitectura del sistema de firma electrónica reconocida según la invención;

- la figura 5 representa esquemáticamente una cuarta arquitectura del sistema de firma electrónica reconocida según la invención;

- la figura 6 representa esquemáticamente una quinta arquitectura del sistema de firma electrónica reconocida según la invención;

- la figura 7 representa esquemáticamente una sexta arquitectura del sistema de firma electrónica reconocida según la invención.

A continuación se describirá en detalle el sistema de firma electrónica reconocida según la invención.

La figura 1 describe un dispositivo de teléfono móvil, en particular un teléfono inteligente, 100, es decir un teléfono móvil dotado de la capacidad para operar como usuario terminal en una red de telecomunicaciones móviles y con un sistema operativo para la ejecución de aplicaciones de software, dotado de una pantalla 110, un teclado 115 numérico, una tarjeta 105 de memoria de tipo microSD (micro Secure Digital) alojada en un correspondiente lector del teléfono 100 inteligente, un módulo de conexión inalámbrica a la red 125 de telecomunicación para enviar/recibir mensajes de texto SMS, un SIM (módulo de identidad de suscriptor) 120, y un módulo opcional, usado solo en algunos ejemplos de realización, para conexión 121 inalámbrica de corta distancia (por ejemplo NFC, Bluetooth, Wi-Fi) y/o tráfico de datos de Internet, incluyendo la capacidad para enviar y recibir correos electrónicos o mensajes *push* (de inserción) que pueden usarse en lugar de mensajes de texto SMS. Puede incluirse, entre las redes de proximidad, o sistemas de intercambio de datos inalámbricos, el sistema de código QR, en el que los datos se intercambian leyendo una imagen de código QR a través de una cámara digital en un teléfono inteligente. La disposición de los elementos de los que está compuesto el teléfono 100 inteligente depende del modelo.

La figura 2 representa un teléfono 210 inteligente, análogo al teléfono 100 inteligente, configurado para producir la firma en el sistema de firma electrónica reconocida según la invención. En este teléfono 210 inteligente para firma electrónica reconocida, se proporciona una memoria 200 de seguridad en lugar de la tarjeta 105 de memoria. Además, el teléfono 210 inteligente para firma electrónica reconocida está configurado para interactuar, en cuanto a lectura y si es necesario en cuanto a escritura, con esta memoria 200 de seguridad a través de una aplicación 220 de firma electrónica reconocida específica, por ejemplo implementada como programa informático adecuado para ejecutarse en asociación con el sistema operativo del teléfono móvil, que configura el teléfono 210 inteligente para producir la firma electrónica reconocida según el sistema y procedimiento según la invención. Esta aplicación 220 de firma electrónica reconocida es preferiblemente multifuncional, por tanto tiene la capacidad de procesar todo o parte de los diferentes tipos de mensajes de texto para peticiones de pago, suscripción de documentos, accesos web o servicios de red. Esta aplicación 220 de firma electrónica reconocida puede cargarse, al igual que en la figura 2, en el teléfono 210 inteligente para firma electrónica reconocida, pero también puede instalarse en la misma memoria 200 de seguridad o estar ya instalada en la misma, lista para su uso por parte del usuario. El teléfono 210 inteligente para firma electrónica reconocida se usa por tanto para la firma electrónica reconocida y posterior identificación del usuario dentro del sistema de firma electrónica reconocida según la invención.

Los teléfonos 210 inteligentes para firma electrónica reconocida corresponden en general a teléfonos inteligentes convencionales, tales como el teléfono 100 inteligente, aunque están dotados de una memoria 200 de seguridad, preferiblemente extraíble, en un correspondiente lector de memoria microSD (Micro Secure Digital), que además de permitir el almacenamiento de datos comunes en general, tales como fotografías o música, también comprende una partición certificada según el nivel de seguridad requerido por las disposiciones nacionales e internacionales para firma electrónica reconocida y para la protección de una clave 201 privada almacenada en esta partición. Por ejemplo, para países de la Unión Europea, este nivel de certificación requerido es fundamentalmente el Criterio Común EAL4+ (o superior), dependiendo de los “perfiles de protección” requeridos.

Estas memorias certificadas difieren de las tarjetas SIM, por ejemplo, debido al hecho de que son independientes de la compañía de teléfono y tienen diferente forma y dimensiones. Una tarjeta inteligente o una tarjeta SIM almacena una cantidad limitada de datos, tiene diferente forma y dimensiones con respecto a la memoria de seguridad y no puede alojarse en un lector microSD. Además de poder alojarse en este lector y tener las dimensiones de una microSD, aparte de tener una notable capacidad, por ejemplo 2 GB, una memoria de seguridad es adecuada para contener una partición segura para la ejecución de la firma electrónica reconocida y para el almacenamiento de la clave 201 privada. Por tanto, la memoria de seguridad puede satisfacer tanto las funciones normales de una tarjeta microSD común para almacenar grandes cantidades de datos (mapas de navegador, fotografías u otros datos), como las funciones vinculadas a la firma electrónica reconocida.

Recientemente el fabricante Giesecke & Devrient produjo una memoria de seguridad similar, denominada tarjeta de seguridad móvil.

Es importante observar que la memoria 220 de seguridad se usa en combinación con un número de teléfono (o un identificador de suscriptor) codificado en el SIM 120.

Dado que el SIM 120 y la memoria 220 de seguridad son extraíbles, el usuario puede usar estos elementos juntos en otros teléfonos 210 inteligentes. El hecho de que los mensajes de texto SMS se envíen a un SIM dado correspondiente al número de teléfono registrado para ese usuario en el sistema de firma electrónica reconocida aumenta el nivel de seguridad, en cualquier caso ya garantizado por la firma electrónica reconocida ya que la firma electrónica reconocida estampada por el usuario que adopta la memoria de seguridad puede verificarse en cualquier caso, permitiendo la posterior comprobación de si el mensaje de texto SMS estaba firmado por la clave 201 privada

asociada, incluso si se desconoce, con el certificado correspondiente al usuario destinatario y, además, con ese número de teléfono. Si el usuario cambia de número de teléfono, puede actualizar su registro en la red dedicada.

Otro requisito para la firma electrónica reconocida reside en el uso de un certificado de firma que contiene la clave pública que emite una autoridad de certificación (CA), o entidad de certificación, ya sea una entidad gubernamental o se reconozca por esta entidad. Los certificados digitales de este tipo se usan para la firma electrónica reconocida dentro del sistema de firma electrónica reconocida. Para obtener un certificado de este tipo, normalmente es necesario que un administrador (operador de registro) autorizado por la autoridad de certificación (a través de una autoridad de registro) lleve a cabo una etapa de reconocimiento visual del usuario para el que va a emitirse el certificado, para garantizar también legalmente su identidad.

También pueden usarse certificados digitales técnicamente equivalentes, emitidos por entidades pertenecientes a la misma red dedicada pero que no emiten certificados de firma electrónica reconocida. En este último caso, se garantizan en cualquier caso el mismo proceso y los mismos requisitos tecnológicos, tanto en relación con las certificaciones sobre los niveles de seguridad requeridos en el proceso, como con la firma y los dispositivos de protección de la clave 201 privada. En este último caso, la firma efectuada no es realmente una firma electrónica reconocida, sino una firma definida en este caso como firma electrónica reconocida equivalente. Según la dificultad o adecuación de emisión del certificado de firma reconocida en sentido estricto, el usuario puede decidir si optar o no por una firma electrónica reconocida equivalente, que en cualquier caso desde el punto de vista de la seguridad es equivalente en la práctica, y por tanto satisface los mismos requisitos técnicos de seguridad establecidos por las disposiciones internacionales para la firma electrónica reconocida. Si el usuario requiere una validez de obligado cumplimiento con pleno valor legal, debe optar por la firma electrónica reconocida en sentido estricto. A continuación en el presente documento el término firma electrónica reconocida también se ampliará para indicar la firma electrónica reconocida equivalente, si el usuario opta por la misma. Los certificados emitidos por diferentes autoridades de certificación, también de diferentes países, se utilizan dentro del sistema de firma electrónica reconocida según la invención. En la etapa de registro del usuario en la red dedicada, se efectúa una comprobación para garantizar que la clave pública del certificado es única dentro del sistema de firma electrónica reconocida según la invención. Si no lo es, es necesario emitir un nuevo certificado para el usuario, volviendo a generar una nueva clave 201 privada.

La firma en la memoria de seguridad puede activarse por medio de un respectivo código PIN que habilita la firma a través de la clave 201 privada, mientras que la clave pública y el correspondiente certificado reconocido también pueden residir en una zona no protegida de la memoria de seguridad. El código PIN lo usa de manera exclusiva en el terminal el usuario para implementar firmas electrónicas reconocidas o, si es necesario, cifrados asimétricos, sin transmitirse este código PIN sobre la red dedicada u otra red. La operación para cambiar el código PIN está disponible para el usuario en todo momento e implica solo al mismo usuario, a través del uso de la aplicación 220 de firma electrónica reconocida o la controladora de base de la memoria de seguridad.

El usuario registrado en el sistema de firma electrónica reconocida propuesto está dotado de un teléfono 210 inteligente para firma electrónica reconocida con clave 201 privada protegida presente en la memoria 200 de seguridad, combinándose la clave 201 privada con un certificado de firma reconocida relacionado con el mismo usuario y con el certificado de firma relacionado de la autoridad de certificación que emitió este certificado. El usuario se registra en el sistema de firma electrónica reconocida, por ejemplo indicando durante la etapa de registro su número de teléfono o código de identificación opcional dentro de este sistema de firma electrónica reconocida, una dirección/referencia de un servidor aplicativo para cada tipo de petición que el usuario pretende gestionar (pago, suscripción, acceso) y, si es necesario, la dirección de correo electrónico; esta información se registra en el servidor 310 frontal o en una base de datos conectada al mismo. Otra información requerida para el registro del usuario en un servidor 315 aplicativo es el certificado de firma reconocida y el certificado de la autoridad de certificación que lo emitió; en cada servidor aplicativo cuyos servicios usa el usuario, estos certificados están registrados en relación con el número de teléfono del usuario, si es necesario su correo electrónico y cualquier código de identificación dentro de la red dedicada. El servidor 310 frontal y el servidor 315 aplicativo se describen con referencia a los diagramas en las figuras 3a, 3b, 4, 5, 6 y 7, que muestran realizaciones de ejemplo de la arquitectura según la invención.

Diferentes realizaciones del sistema de firma electrónica reconocida según la invención se representan a través de ejemplos de flujos en los diagramas esquemáticos de las figuras 3a, 3b, 4, 5, 6, 7. En estos diagramas esquemáticos, se indican componentes comunes del sistema de firma electrónica reconocida propuesto con el mismo número de referencia, cuando se repiten. Los componentes comunes están representados, por ejemplo, por un servidor 302 de interfaz, el servidor 310 frontal, el servidor 315 aplicativo del destinatario y una entidad de servidor del destinatario 330. Estos servidores pueden residir cada uno en un servidor físico diferente o pueden estar asignados en un número diferente de servidores físicos o virtuales. Por ejemplo, todos los componentes podrían residir en solo un servidor, mientras que cada uno de los servidores mencionados anteriormente podría corresponder realmente a un clúster de servidores. Los mensajes intercambiados entre los servidores en la red que forma el sistema de firma electrónica reconocida según la invención están preferiblemente codificados con codificación base64 o formato hexadecimal, o con otro método que impide la pérdida o alteración de información durante la transmisión.

Las comunicaciones entre los diferentes servidores no se producen necesariamente a través de una red de comunicación inalámbrica; lo mismo puede decirse para la comunicación entre el servidor 302 de interfaz, cuando está presente en los ejemplos de realización descritos, y el cliente del peticionario si el dispositivo del peticionario no es un teléfono 100 ó 210 inteligente. En el caso de transmisión en la que otro mensaje de respuesta corresponde a un mensaje, aunque sin limitar las presentes realizaciones a este tipo de transmisión, después de un mensaje enviado a un servidor, el agente (el cliente del peticionario o uno de los servidores) que lo envía, espera un mensaje de respuesta dentro de un tiempo de espera configurado; la respuesta puede ser de tipo síncrono (por ejemplo TCP/IP), pero también de tipo asíncrono, añadiendo un identificador al mensaje de respuesta para permitir al agente llamante correlacionarlo con el mensaje enviado previamente por este último. Las realizaciones descritas en el presente documento se refieren, preferiblemente, de una manera no limitativa, al caso síncrono para estos mensajes. Además, si un mensaje es de un tipo determinado (código QR, por ejemplo) el correspondiente mensaje recibido puede ser de un tipo diferente (datos de tráfico de internet, por ejemplo).

Por tanto, los mensajes intercambiados por un teléfono 100 inteligente con el servidor 302 de interfaz y por un teléfono 210 inteligente con el servidor 310 frontal, a modo ejemplo no limitativo, son asíncronos e inalámbricos, de tipo SMS (Sistema de Mensaje Corto) o, si se usa el módulo 121 de conexión inalámbrica opcional, por ejemplo, pueden ser transmisiones con tráfico de datos de Internet genérico. De manera análoga, de nuevo de una manera no limitativa, los mensajes intercambiados por el teléfono 210 inteligente para firma electrónica reconocida con el servidor 315 aplicativo, cuando está presente, se consideran asíncronos (de tipo SMS). Por ejemplo, con referencia a las figuras 3a, 3b, 4, 5, los mensajes 340 de petición basados en texto recibidos por este teléfono 210 inteligente, y los mensajes 345 de confirmación enviados por el mismo, siendo para estos últimos la respuesta del servidor de tipo 360 estatus de destinatario, son preferiblemente mensajes de texto SMS de tipo asíncrono. También es posible considerar, por ejemplo, que los mensajes 345 de confirmación son llamadas realizadas a través del módulo 121 de conexión inalámbrica opcional que no son de corta distancia, por ejemplo correo electrónico enviado a través del campo de correo electrónico del destinatario en la base de datos de usuarios del servidor 315 aplicativo, o que son llamadas de tráfico de datos de Internet a servicios web expuestos por el servidor 315 aplicativo con respuesta por este de tipo 360 estatus de destinatario.

En general dichos mensajes 340, 345 y 360 se almacenan en la partición de la memoria de seguridad que es diferente de la partición de seguridad, con el fin de mostrar el historial de estos mensajes al usuario de manera inteligible. Esta partición, si es de tipo de gran tamaño, también pueden usarla otras aplicaciones como, por ejemplo, aplicaciones de fotografías y películas.

En el caso en el que el teléfono 210 inteligente está dotado del módulo 121 de conexión inalámbrica opcional, el mensaje de texto SMS enviado para el mensaje 340 de petición basado en texto puede sustituirse, por ejemplo, por un mensaje 340 de petición basado en texto análogo transmitido por medio de Wi-Fi o tráfico de datos de Internet; en este contexto el teléfono 210 inteligente puede estar hecho para escuchar, por ejemplo, en un puerto específico, a través de la aplicación 220, cualquier mensaje de petición mencionado anteriormente. Tras recibir un mensaje, la aplicación 220 envía un mensaje de recepción adicional al servidor aplicativo si el modelo de los mensajes lo requiere.

En lo que se refiere a los mensajes de petición 351 de cliente y confirmación 352 de cliente, respectivamente recibidos y enviados por el teléfono 210 inteligente dentro de los flujos mostrados en la figura 7, el uso de comunicación llevada a cabo con transmisión de corta distancia a través del módulo 121 de conexión inalámbrica opcional, por ejemplo Bluetooth o NFC o código QR o TCP/IP sobre Wi-Fi, se considera preferible aunque no obligatorio.

Además estos mensajes 351 y 352 se almacenan en la partición de la memoria de seguridad diferente de la partición de seguridad, con el fin de mostrar el historial de estos mensajes al usuario de un modo inteligible, tal como se describió anteriormente para los mensajes 340, 345 y 360.

Los mensajes 305 de petición de operación enviados por medio de la aplicación 220 de firma electrónica reconocida al servidor 310 frontal en el diagrama de las figuras 5 y 6, y el mensaje 370 de respuesta de estatus de peticionario pueden ser asíncronos (por ejemplo mensajes de texto SMS) o, por ejemplo, síncronos en modo inalámbrico si se usa el módulo 121 de conexión inalámbrica opcional. Las operaciones de petición se describen en general a continuación: estas operaciones de petición pueden ser operaciones de petición originales del peticionario que pueden corresponder a varios mensajes de petición de operación enviados al servidor frontal, algunos de los cuales no llegan al dispositivo de teléfono móvil para la firma electrónica del destinatario, pero que en cualquier caso contribuyen a la ejecución de la operación en su conjunto.

En general, si las respuestas esperadas de los servidores no se reciben, esto activa un periodo de tiempo de espera, tras el cual se considera que la petición no se ha ejecutado.

El primer ejemplo de realización descrito se refiere al tipo de petición de pago, por ejemplo pago por medio de transferencia bancaria o tarjeta de débito o tarjeta de crédito implementado a través de la red del sistema de firma electrónica reconocida, en el caso de un usuario que solicita el pago separado del usuario destinatario, por tanto

cuando al menos el destinatario está registrado en el sistema; el destinatario actúa a través del teléfono 210 inteligente para firma electrónica reconocida según la invención y aquí está presente al menos un servidor aplicativo para gestionar mensajes de tipo pago para el banco del destinatario, también interconectado con el sistema de firma electrónica reconocida propuesto, a través de este servidor aplicativo. Una petición original de pago da como resultado una sola petición 305 de operación.

Para el primer ejemplo de realización, se hace referencia al diagrama de las figuras 3a y 3b.

En la figura 3a un peticionario separado del destinatario se indica con 300; el peticionario es el beneficiario de la transacción, o actúa en nombre del beneficiario, para efectuar las peticiones de pago. El peticionario 300, por ejemplo, puede ser un comerciante o una empresa de servicios o administración pública que solicita un pago de un usuario de la red 365 dedicada de destinatario, quien, de hecho, es un usuario del sistema de firma electrónica reconocida propuesto.

En la figura 3a el peticionario separado del destinatario 300 está conectado por medio de un procesador 303, por ejemplo un ordenador personal. Este procesador 303 se indica en la figura, pero también podría ser un teléfono 100 inteligente convencional, por ejemplo, en el caso de venta ambulante, para efectuar peticiones de pago a través de un servidor 302 de interfaz, tal como un sitio web. Este servidor 302 de interfaz está configurado para efectuar posteriormente una petición original que se traduce en una petición 305 de operación individual, específicamente una petición de pago, en modo automático o interactivo al servidor 310 frontal.

Este servidor 302 de interfaz, por ejemplo, puede ser un sitio web desde el que efectuar peticiones a través de un navegador. La comunicación entre el servidor 302 de interfaz y el procesador 303 o el teléfono 100 inteligente convencional puede implementarse según uno de los métodos conocidos para los expertos en la técnica, siempre que permita al servidor 302 de interfaz traducir las peticiones originales del peticionario 300 en peticiones 305 de operación que puedan procesarse mediante el servidor 310 frontal, tal como se especifica mejor a continuación en el presente documento, e interpretar los mensajes 370 de estatus de peticionario recibidos por el mismo servidor 302 de interfaz procedentes del servidor 310 frontal en información inteligible para el usuario 300 peticionario.

La figura 3b en cambio indica un caso en el que también el peticionario separado del destinatario 300 está conectado por medio de un respectivo teléfono 210 inteligente para firma electrónica reconocida, que está configurado para efectuar peticiones 305 de operación directas al servidor 310 frontal a través del uso por parte del peticionario 300 de un software de aplicación que coincide con la aplicación 220 de firma electrónica reconocida, e interpretar a través de esto los mensajes 370 de estatus de peticionario recibidos en información inteligible para el usuario 300 peticionario. La conexión del teléfono 210 inteligente para firma electrónica reconocida con el servidor 310 frontal puede llevarse a cabo enviando mensajes de texto SMS sobre la red de telecomunicaciones móviles o enviando datos sobre la red en otro modo inalámbrico. En vista de la diferencia mencionada anteriormente entre los diagramas 3a y 3b, a menos que se especifique, se hará referencia al diagrama 3a por motivos de simplicidad, sin perder la generalidad.

La petición 305 de operación enviada al servidor 310 frontal comprende datos de petición que comprenden

- indicación del tipo de petición de pago,

- datos de identificación del destinatario de la red 365 dedicada, que pueden comprender el número de teléfono móvil del destinatario de la red 365 dedicada o un identificador del mismo dentro del sistema de firma electrónica reconocida asociado con este número de teléfono móvil, o la identificación del destinatario reconocido por medio de redes inalámbricas, en particular por el módulo 121 de proximidad de conexión inalámbrica (como código QR o Bluetooth),

- datos de transacción financiera; estos datos de transacción financiera comprenden uno o más datos tales como la cantidad total en efectivo de la suma solicitada para el pago, la moneda relacionada, el método de pago seleccionado (por ejemplo transferencia bancaria o tarjeta de crédito o débito), la referencia relacionada para el pago, por ejemplo respectivamente el código IBAN del peticionario o su número de tarjeta de crédito o débito, el nombre del beneficiario/titular, el motivo para el pago, lugar, cualquier dirección de correo electrónico del peticionario y/o del beneficiario, cualquier identificador único en la red dedicada o número de teléfono del peticionario o beneficiario si pertenece a la red dedicada; también puede estar presente en general otra información adicional en base al método de pago.

El servidor 310 frontal asigna un identificador de petición único y un sello de tiempo a la petición 305 de operación individual, verifica el formato correcto de la petición y la presencia en su propia base de datos de usuarios registrados del usuario destinatario de la petición 365, en base a los datos de identificación, es decir su número de teléfono o identificador en el sistema de firma electrónica reconocida, presentes en la misma petición 305 de operación. Si estos datos de identificación no se encuentran en la base de datos de usuarios registrados del servidor 310 o los datos recibidos en el mensaje 305 de petición de operación están incompletos o contienen errores, el servidor 310 frontal envía al servidor 302 de interfaz un mensaje 370 de estatus de peticionario completo con el

identificador único de la petición y con el sello de tiempo asignado previamente; el mensaje 370 de estatus de peticionario en este caso indica un error. En cambio, si la verificación es satisfactoria, el servidor 310 frontal interroga a esta base de datos de usuarios registrados, en busca del usuario de la red 365 dedicada de destinatario, una referencia de dirección del servidor 315 aplicativo (por ejemplo, su URL, localizador de recursos uniforme, para una conexión de Internet) al que el servidor 310 frontal debe dirigir la petición 305 de operación en base al tipo de petición indicada aquí, en este caso una petición de pago.

Otros servidores aplicativos conectados al servidor 310 frontal, para otros tipos de petición, representados en la figura 3a solo por motivos de simplicidad por el enésimo servidor 325 aplicativo, no están implicados en el proceso.

Si falta la referencia de dirección, el servidor 310 frontal envía el mensaje 370 de estatus de peticionario completo con identificador único y sello de tiempo asignados previamente, indicando el error que se ha producido.

En cambio, si la referencia de dirección está presente, el servidor 310 frontal envía un mensaje 308 de petición reenviado al servidor 315 aplicativo de recepción, es decir un mensaje completo con la información de la petición 305 de operación, al que añade el identificador único y sello de tiempo asignados previamente por el servidor 310 frontal a la correspondiente petición 305 de operación. El servidor 315 aplicativo valida además la petición 308 en base al formato específico y busca en su propia base de datos de usuarios registrados la presencia de un usuario asociado con la información recibida como datos de identificación, es decir el identificador en el sistema de firma electrónica reconocida o el número de teléfono. El certificado de firma electrónica reconocida asociado con cada usuario y el certificado relacionado de la autoridad de certificación que lo emitió también están disponibles para los servidores aplicativos. El servidor 315 aplicativo comprueba el estado de validez del usuario (tal como se describe a continuación en el presente documento) y del certificado en base a la última lista disponible de revocaciones y suspensiones de dicha autoridad de certificación descargada periódicamente del servidor 315 aplicativo y por tanto ya disponible. Entonces se repite esta comprobación tras recibir la firma electrónica reconocida, en base a una lista de revocaciones y suspensiones actualizada posteriormente a la hora a la que se efectuó la firma, ya que hasta la hora de la firma estas listas podrían haberse actualizado en la autoridad de certificación con respecto a las usadas en la primera comprobación. La comprobación preliminar hace posible evitar el envío de mensajes a usuarios no válidos en base a las listas disponibles.

Si una de estas comprobaciones es negativa, el servidor 315 aplicativo envía un mensaje 366 de reenvío de estatus con respuesta negativa al servidor 310 frontal en respuesta al mensaje 308 de petición reenviado anterior; el servidor 310 frontal envía entonces un correspondiente mensaje 370 de estatus de peticionario negativo, en respuesta al mensaje 305 de petición de operación anterior. El mensaje 370 de estatus de peticionario llega al peticionario 300 a través de un programa de cliente en el procesador 303 ó 100 que procesa el estatus recibido del servidor 302 de interfaz. El mensaje 370 de estatus de peticionario está completo con el identificador de la petición y el sello de tiempo asignados por el servidor 310 frontal a la petición 305 de operación y posteriormente presente en el mensaje 308 de petición reenviado anteriormente.

En cambio, en el caso de estatus positivo de las comprobaciones mencionadas anteriormente, el servidor 315 aplicativo envía un mensaje 340 de petición basado en texto de lado de destinatario al teléfono 210 inteligente, que envía un mensaje de texto SMS al número de teléfono almacenado en la base de datos de usuarios del servidor 315 para el mismo usuario 365 destinatario dado. El servidor 315 aplicativo usa, como identificador de remitente, el número de teléfono del destinatario 365 para enviarlo.

El mensaje 340 de petición basado en texto enviado al destinatario concatena en un mensaje de texto SMS la información de la petición 308 reenviada, incluyendo el identificador del tipo de petición relacionada con el pago. Con concatenación se quiere decir la disposición en secuencia de información en formato de texto, si es necesario dividida por separadores o según un esquema compartido, de modo que el destinatario, si se requiere, puede reconocer e interpretar la diferente información en el mismo mensaje. El mensaje 340 de petición basado en texto se formula para representar una clara autorización de pago en lenguaje natural, por ejemplo “Yo, autorizo el pago de 321,00 euros al IBAN IT96R0123454321000000012345 a nombre de Giochi y Giocattoli S.r.l, Milán, via Salici 32, hora 16:43:54, identificador de petición 23456789”

El mensaje 340 de petición basado en texto se almacena en zonas persistentes específicas, por ejemplo una memoria masiva, conectada al servidor 315 aplicativo; la referencia de dirección para el archivo correspondiente al mensaje 340 de petición basado en texto almacenado, junto con el identificador de la petición que asignó el servidor 310 frontal a la petición 305 de operación y por tanto presente en la petición 308 reenviada y en el mensaje 340 de petición basado en texto se mantiene dentro de una base de datos de dicho servidor 315; estos datos se mantienen correlacionados con el identificador de la petición 305 de operación junto con el sello de tiempo de la misma petición y junto con el usuario 365 destinatario, y con los otros datos del mensaje 340 de petición basado en texto. El sello de tiempo permite la evaluación de si ha expirado el tiempo de espera, configurado en el sistema para considerar las peticiones expiradas.

El servidor 315 aplicativo envía el mensaje de texto SMS del mensaje 340 de petición basado en texto al número de teléfono obtenido de la base de datos conectada al mismo servidor. En general, el teléfono 210 inteligente para firma

electrónica reconocida del destinatario 365, a través de la aplicación 220 de firma electrónica reconocida de la que está dotado, analiza sintácticamente los mensajes de texto SMS recibidos. La aplicación 220 de firma electrónica reconocida distingue en base al formato y el número de teléfono del remitente si el mensaje de texto SMS genérico se ha enviado o no a través del protocolo de la red del sistema de firma electrónica reconocida.

En caso de que el teléfono 210 inteligente esté apagado o la aplicación 220 de firma electrónica reconocida esté desactivada, el mensaje 340 de petición basado en texto se recibe y procesa cuando el teléfono inteligente se enciende de nuevo o cuando la aplicación 220 de firma electrónica reconocida se reinicia; si el tiempo de espera de la petición ha expirado, el mensaje 340 de petición basado en texto se considera rechazado por el servidor 315 aplicativo. Si se reciben otros mensajes 340 de petición basados en texto, se suspende el procesamiento de los mismos por parte de la aplicación 220 de firma electrónica reconocida hasta que se ha ejecutado el primer mensaje 340 de petición basado en texto. Posteriormente, se procesan los siguientes mensajes 340 de petición basados en texto en orden de llegada.

Cuando la aplicación 220 de firma electrónica reconocida reconoce que el mensaje de texto SMS recibido es un mensaje 340 de petición basado en texto, la aplicación 220 de firma electrónica reconocida está configurada para mostrar automáticamente en la pantalla 110 del teléfono 210 inteligente una interfaz gráfica configurada según el tipo de petición indicada en el mensaje 340, es decir petición de pago, suscripción de documentos o acceso a servicio de red.

En el caso de una petición de pago, la aplicación 220 de firma electrónica reconocida calcula el *hash* del mensaje 340 de petición basado en texto y lo muestra en la interfaz 110 junto con el mensaje 340 de petición basado en texto. Como el *hash* puede contener caracteres ocultos, está codificado con notación hexadecimal o en base64 u otro formato en la pantalla 110. El sistema también puede configurarse de modo que el mensaje 340 de petición basado en texto ya incluya este *hash*, calculado previamente por el servidor 315 aplicativo. En este caso la aplicación 220 multifuncional aun calcula el *hash* del mensaje 340 y lo compara con el recibido, visualizando el estatus en la pantalla 110. La longitud de los mensajes 340 de petición basados en texto es corta y por tanto el cálculo del *hash* en el teléfono 210 inteligente no provoca problemas de rendimiento.

El *hash* del mensaje 340, como se visualiza en texto sin formato en el teléfono 210 inteligente y el algoritmo de cálculo de *hash* es de tipo estándar, también puede recalcularlo el usuario de manera autónoma para una comprobación adicional, por ejemplo a través de software de cálculo disponible en Internet.

La elección del algoritmo de *hash* viene dictada por la legislación de referencia en el país de uso en el caso de un cumplimiento estricto con la firma electrónica reconocida. Por ejemplo, en Italia se usa el algoritmo SHA-256. En base a la legislación del país de uso, antes de la firma, el *hash* debe rellenarse si es necesario con cualquier información adicional requerida por la legislación, tal como el relleno pkcs#1 versión 2.1. La cadena *hash* puede visualizarse en la pantalla 110; si el *hash* también se calcula mediante el servidor 315 aplicativo, debe estar presente en el mensaje 340 de petición basado en texto para permitir que la aplicación 220 implemente la comprobación.

El usuario destinatario puede decidir no confirmar la petición. En este caso, es posible operar, en particular seleccionando una opción desde la aplicación 220 de firma electrónica reconocida, para poder procesar cualquier otro mensaje 340 de petición basado en texto; seleccionando esta opción, el mensaje 345 de confirmación no se envía dentro del tiempo de espera configurado, y por tanto la red de firma electrónica reconocida considera la petición 305 de operación rechazada. También es posible configurar el sistema de modo que este rechazo sea explícito, enviando desde el teléfono 210 inteligente a través de la aplicación 220 de firma electrónica reconocida un mensaje 345 de confirmación negativo sin firmar que contiene el identificador solicitado de la petición 305 de operación anterior asignada por el servidor 310 frontal y por tanto presente en el mensaje 308 de petición reenviado. El mensaje 345 de confirmación negativo se interpreta mediante el servidor aplicativo que responde con un mensaje 360 de estatus de destinatario que confirma la recepción; el servidor 315 aplicativo envía el contenido del mensaje 345 de confirmación al servidor 310 frontal a través de un mensaje 366 de reenvío de estatus en respuesta a la petición 308 reenviada anterior, que contiene de nuevo el identificador de la correspondiente petición 305 de operación. El servidor 310 frontal interpreta el mensaje y lo envía al peticionario como mensaje 370 de estatus de peticionario negativo en respuesta a la petición 305 de operación inicial relacionada.

En cambio, si el usuario de la red 365 dedicada de destinatario desea confirmar, es decir firmar la petición digitalmente, usa el teclado 115 numérico para introducir el código PIN solicitado por la aplicación 220 de firma electrónica reconocida y efectúa la firma electrónica reconocida en la cadena *hash* mencionada anteriormente. En particular, se aplica cifrado RSA a través de la clave 201 privada en el *hash* (decodificada por ejemplo a partir de base64 o formato hexadecimal, útil en este contexto solo para visualización o transmisión) activada a través de la introducción de un código PIN de firma solicitado por la aplicación 220 de firma electrónica reconocida.

Si el código PIN de firma es incorrecto, la aplicación 220 de firma electrónica reconocida debido al error recibido de la memoria 200 de seguridad visualiza el error en la pantalla 110. Según un esquema conocido, si se supera un número permitido de intentos incorrectos, configurado en la memoria 200 de seguridad y si es necesario también en la aplicación 220 de firma electrónica reconocida, debe tomarse una medida para desbloquear la memoria 200 de

seguridad a través del PUK (código de desbloqueo personal) usando la aplicación 220 de firma electrónica reconocida o las controladoras de base de la misma memoria 200 de seguridad, si es necesario para restablecer el mismo código PIN. Una vez se ha desbloqueado la memoria 200 de seguridad, puede continuarse con la operación introduciendo el código PIN correcto. Si, mientras tanto, se supera el tiempo de espera configurado, la petición 305 de operación se considera rechazada. Alternativamente, también en una situación con el código PIN bloqueado, es posible aclarar y gestionar el rechazo explícito tal como se describió anteriormente, ya que no requiere una firma.

Si el código PIN se introduce correctamente, la firma electrónica reconocida se implementa en el *hash* en la memoria 200 de seguridad del teléfono 210 inteligente empezando por el mensaje 340 de petición basado en texto, a través de la aplicación 220 de firma electrónica reconocida que opera sobre la memoria 200 de seguridad. Este código PIN de firma no se transmite ni sobre ni fuera de la red dedicada, sino que se usa solo para activar la firma de manera local en el teléfono 210 inteligente.

Para permitir la verificación e identificación, se envía una firma electrónica reconocida separada desde el teléfono 210 inteligente al servidor 315 aplicativo a través de un mensaje 345 de confirmación, que contiene el identificador único de la petición 305 de operación asociada. Esta firma electrónica reconocida separada, también denominada firma electrónica separada, no tiene ningún mensaje de texto sin formato al que haga referencia el *hash*, ningún certificado de firma asociado, y ningún certificado de la autoridad de certificación que emitió el certificado de firma. Por el contrario, se denomina firma electrónica reconocida adjunta. El mensaje 345 de confirmación llega al servidor 315 aplicativo. Efectúa una primera comprobación de formato del mensaje 345 de confirmación y, si es positiva, verifica la firma contenida en el mensaje 345 de confirmación en base al mensaje 340 de petición basado en texto, sin el *hash* de control si está presente en el mismo como texto, que por tanto se considera el documento de texto sin formato con respecto a la firma, almacenado previamente en base al identificador único asociado por el servidor 310 frontal con la petición 305 de operación; la verificación de firma también se lleva a cabo en base al certificado de firma asociado con el número de teléfono en la base de datos, y con el certificado de la autoridad de certificación que emitió el certificado de firma.

En general, el servidor 315 aplicativo efectúa una descarga periódica de los servidores que contienen las listas de revocación y suspensión o CRL-CSL (lista de revocación de certificado – lista de suspensión de certificado) de las autoridades de certificación que emiten los certificados de firma presentes en su respectiva base de datos, registrando para cada descarga de estas listas el sello de tiempo correspondiente a la implementación de la petición de descarga. Si se ha revocado o suspendido un certificado del sistema de firma electrónica reconocida, o ha expirado, el estatus del correspondiente usuario se considera inhabilitado por el servidor 315 aplicativo para cualquier petición dirigida al mismo con sello de tiempo posterior a, o igual a la hora a la que expiró la validez del certificado; esta hora se indica en la correspondiente CRL-CSL. Este es también el caso si un usuario de la red dedicada cancela el acuerdo para el sistema de firma electrónica reconocida. La información relacionada con la inhabilitación del usuario, validez del certificado, el sello de tiempo a partir del cual el certificado no es válido, el sello de tiempo de descarga de la lista CRL-CSL con el que se llevó a cabo la verificación de validez, está disponible en la base de datos del servidor 315 aplicativo.

Específicamente, el servidor 315 aplicativo compara el sello de tiempo de descarga de la lista CRL-CSL de la autoridad de certificación relacionada con el usuario identificado por ese número de teléfono, con el sello de tiempo con el que se recibió la firma. Si el sello de tiempo de petición de descarga es posterior en el tiempo al sello de tiempo de recepción de firma, el servidor 315 aplicativo considera la última lista CRL-CSL para validar el certificado, de otro modo el servidor 315 aplicativo descarga dicha lista CRL-CSL actualizada por adelantado con respecto a la hora establecida para la descarga y registra un nuevo sello de tiempo correspondiente a la hora a la que se efectuó la petición de descarga, que es válida para considerar el estatus del certificado, ya que es posterior a la recepción de la firma. Si se ha revocado o suspendido el certificado vinculado en la base de datos al número de teléfono o ha expirado a la hora que coincide con el sello de tiempo correspondiente a la recepción de la firma, o si la operación para verificar la firma contenida en el mensaje 345 de confirmación falla, entonces el mensaje 345 no se valida. Esto puede deberse, por ejemplo, a que la firma se efectúe tras la revocación del certificado, o si la firma la efectúa un usuario diferente con respecto al designado, usando una clave 201 privada diferente de la combinada con la clave pública relacionada con el certificado con el que el usuario está registrado en el servidor 315 aplicativo. Si el mensaje 340 de petición basado en texto SMS llega al SIM 120 correcto vinculado al número de teléfono en base a la información registrada en la base de datos, y por encima de todo si la firma se implementó con la clave 201 privada correcta relacionada con el certificado correcto registrado en la base de datos, la firma efectuada puede validarse.

El servidor 315 aplicativo también compara la hora actual con el sello de tiempo de la petición 305 de operación asignada por el servidor 310 frontal y presente entre los metadatos relacionados con el mensaje 340 de petición basado en texto disponible para el servidor 315 aplicativo; si la diferencia es mayor que el tiempo de espera configurado en el sistema para el tipo de petición particular, la verificación falla.

Si la verificación del mensaje 345 de confirmación a nivel del servidor 315 aplicativo falla, se envía un mensaje 360 de estatus de error de destinatario al teléfono 210 inteligente en respuesta al mensaje 345 de confirmación anterior, y posteriormente se envía un mensaje 366 de reenvío de estatus de error al servidor frontal en respuesta al mensaje

308 de reenvío de estatus anterior; el servidor 310 frontal envía un mensaje 370 de estatus de error de peticionario en respuesta a la petición 305 de operación inicial; el mensaje 370 de estatus de peticionario se completa con el sello de tiempo y con el identificador único asignado a la petición 305 de operación (y por tanto a los mensajes originados para gestionar esta petición) por el servidor 310 frontal. El mensaje 370 de estatus de peticionario se interpreta y se pone a disposición del peticionario separado del destinatario 300 a través de la interpretación del servidor 302 de interfaz y la posterior visualización o actualización en el procesador 303 o en el teléfono 100 inteligente.

El servidor 315 aplicativo en el caso de peticiones de pago normalmente está instalado en el banco del usuario 365 destinatario; si la verificación de firma y otras operaciones de verificación son satisfactorias, el servidor 315 aplicativo envía una petición 350 de orden de pago al servidor del banco 330 conectado a la red del sistema de firma electrónica reconocida propuesto; la petición 350 de orden contiene los datos presentes en el mensaje 340 de petición basado en texto y otros datos que puede solicitar el banco y disponibles en el servidor 315 aplicativo o su base de datos.

El servidor del banco 330 comprende, a través de su base de datos dentro de la red del banco, una asociación entre sus clientes y los usuarios del sistema de firma electrónica reconocida, basándose en los identificadores y números de teléfono con los que están registrados en el sistema de firma electrónica reconocida. En base a esta asociación, el servidor del banco 330 puede asignar la cuenta corriente correcta o, por ejemplo, la tarjeta de crédito/débito correcta correspondiente al usuario 365 desde la que efectuar el pago.

Si no hay disponible efectivo suficiente en la correspondiente cuenta, o en el caso de datos incongruentes o formateados de manera incorrecta, se emite un mensaje 355 de retroalimentación de orden negativa en respuesta a la petición 350 de orden, que se transmite al servidor 315 aplicativo, que envía un respectivo mensaje 360 de estatus de error de destinatario al teléfono 210 inteligente en respuesta al mensaje 345 de confirmación anterior. El servidor 315 aplicativo también envía un mensaje 366 de reenvío de estatus de error específico al servidor 310 frontal, en respuesta al mensaje 308 de reenvío de estatus anterior. El servidor 310 frontal envía entonces un mensaje 370 de reenvío de estatus de error de peticionario al peticionario, en respuesta al mensaje 305 de petición de operación inicial anterior. El mensaje 370 de estatus de peticionario se gestiona del mismo modo que los otros casos mencionados anteriormente.

En el caso de validación por parte del servidor de la entidad del destinatario 330, envía un mensaje 355 de retroalimentación de orden positiva al servidor 315 aplicativo, en respuesta al mensaje 350 de petición de orden anterior. El servidor 315 aplicativo envía a su vez un mensaje 360 de estatus de destinatario positivo al teléfono 210 inteligente en respuesta al mensaje 345 de confirmación recibido previamente, y un mensaje 366 de reenvío de estatus positivo al servidor 310 frontal, en respuesta al mensaje 308 de petición reenviado anterior. El servidor 310 frontal envía un mensaje 370 de estatus de peticionario positivo al peticionario 300, en respuesta a la petición 305 de operación inicial. El mensaje 370 de estatus de peticionario se gestiona del mismo modo que en los casos anteriores, enviando el mensaje de estatus positivo al peticionario separado del destinatario 300.

Si el mensaje 305 de petición de operación se completa con la dirección de correo electrónico del peticionario 300 y/o del beneficiario, el servidor 310 frontal envía a la/s correspondiente/s dirección/direcciones de correo electrónico el correo electrónico que traduce el mensaje 370 de estatus de peticionario en lenguaje natural, tanto en el caso de estatus positivo como en el caso de estatus negativo de la transacción.

En el caso de estatus positivo, si el identificador en la red dedicada o el número de teléfono del peticionario o beneficiario que pertenece a la red dedicada estaba presente en la petición 305 de operación, el servidor 310 frontal gestiona una notificación para este usuario, que se recibe en el teléfono 210 inteligente del peticionario/beneficiario.

Para cada mensaje 340 de petición basado en texto SMS, el servidor 315 aplicativo también envía al usuario 365 un correo electrónico con el mismo contenido, si esta información se proporcionó en la etapa de registro del usuario en la red dedicada.

El servidor 310 frontal actualiza el estatus de la operación iniciada con la petición 305 de operación inicial, en base al mensaje 366 de reenvío de estatus que se recibe, para poder comprobar, también posteriormente, el estatus de la transacción, identificado con el identificador único asignado por el mismo servidor 310 frontal, que conlleva tal como se indicó anteriormente también un sello de tiempo. A través del método de pago configurado por medio del sistema de firma de la petición de pago descrita, ni el número de tarjeta de crédito del usuario que pertenece a la red 365 dedicada, ni otra información sensible de la misma, tal como la contraseña, se envía sobre la red. La información sensible del usuario de la red 365 dedicada se gestiona dentro del banco, dando ventaja a la seguridad.

Si el banco del beneficiario establecido por el peticionario 300 separado del destinatario es el mismo que el destinatario 365, es posible evitar, en la petición 305 de operación, que se asigne como parámetro la referencia de cuenta de beneficiario (por ejemplo, número de tarjeta de crédito del beneficiario) vinculada al método de pago establecido por el peticionario, aumentando la confidencialidad para el beneficiario, y en cambio se asigna el identificador o número de teléfono dentro del sistema de firma dedicado según la invención también en relación con

el beneficiario en la petición 305 de operación. De hecho, en este caso el banco tiene los datos tanto del destinatario como del beneficiario.

Si la entidad que usa el servidor 315 aplicativo es una entidad de intermediación que tiene datos sensibles tanto del beneficiario establecido por el peticionario 300 como del destinatario 365 con la respectiva información relacionada, por ejemplo, con las respectivas tarjetas de crédito u otros métodos de pago, y pone a disposición estos datos como base de datos accesible para el servidor 315, es posible evitar que se introduzcan datos sensibles (por ejemplo el número de tarjeta de crédito) en la petición 305 de operación también en relación con el beneficiario. Los sitios y comerciantes de comercio electrónico pueden interactuar con la red a través de una pasarela de pago dedicada mediante el servidor 315 aplicativo. En estos casos es posible mantener los datos de tarjeta de crédito durante la fase de registro en la pasarela, de modo que un requisito generado a partir de dicha pasarela genera una petición para uno de dichos operadores. Otra posibilidad es que los servidores 315 aplicativos estén en los bancos, y los bancos de los destinatarios 365 dotados de servidores 315 aplicativos, a través de una red segura y dedicada soliciten los datos sensibles para el pago procedentes de los bancos de los beneficiarios a través de los servidores 315 aplicativos de estos últimos y se obtiene una mayor confidencialidad para los beneficiarios, y además en este caso las peticiones 305 de operación no contienen ningún dato sensible de estos beneficiarios.

El servidor 315 aplicativo puede enviar a un servidor de almacenamiento electrónico los mensajes 340 de petición de pago basados en texto, con la firma, el certificado de firma y el certificado de la autoridad de certificación que emitió el certificado de firma. Normalmente, al menos un sello de tiempo legalmente válido está asociado con estas firmas. Estos elementos puede consultarlos el usuario 365 firmante y el peticionario, si pertenecen al sistema de firma propuesto. La función de verificación de firma también está disponible.

Por tanto, finalmente en los sistemas de las figuras 3a y 3b descritos anteriormente, la petición 305 de operación se valida y procesa mediante el servidor 310 frontal del sistema de firma electrónica reconocida, convirtiéndose en una petición 308 reenviada al servidor 315 aplicativo, que a su vez reenvía esta petición como comunicación 340 basada en texto al terminal de usuario, es decir el teléfono 210 inteligente, donde se estampa la firma electrónica reconocida en base a esta comunicación basada en texto enviada sobre la red de telecomunicaciones móviles o partes de la misma.

La figura 4 muestra un diagrama de una variante en relación con un procedimiento de pago adicional en el que 400 indica un usuario destinatario de la petición 305 de pago que también corresponde al peticionario que realiza dicha petición 305 de operación.

El diagrama de la figura 4 en comparación con lo que se muestra en la figura 3a presenta la diferencia indicada anteriormente.

De hecho, el usuario 400 usa el teléfono 210 inteligente para gestionar una confirmación a través de la firma electrónica reconocida, concretamente el procesamiento del mensaje 340 de petición basado en texto, del mensaje 345 de confirmación y del mensaje 360 de estatus de destinatario. Sin embargo, en este caso es el mismo destinatario 400 el que también efectúa la petición 305 de operación, preferiblemente a través de otro procesador, es decir el procesador 303 de soporte, tal como se muestra en la figura 4, aunque este procesador en una variante también puede ser el teléfono 100 inteligente convencional, que está separado del teléfono 210 inteligente usado en el sistema de firma electrónica reconocida propuesto. Naturalmente, el mismo teléfono 210 inteligente que gestiona la confirmación también puede usarse como teléfono 100 inteligente convencional también para efectuar la petición usando funciones que no usan la memoria 200 de seguridad y la aplicación 220 de firma electrónica reconocida, solo para efectuar la petición. Por ejemplo, el usuario 400 podría usar el navegador de dicho teléfono 210 inteligente para efectuar peticiones 305 de operación.

El usuario 400 del sistema de firma electrónica reconocida, por ejemplo, puede corresponder a un usuario que opera en un sitio web de comercio electrónico asociado con este sistema de firma electrónica reconocida; el sitio web corresponde al servidor 302 de interfaz, y el usuario, por ejemplo, puede pretender efectuar activamente una compra o enviar dinero a través de la red del sistema de firma electrónica reconocida a través del servidor 302 de interfaz a favor de un beneficiario. El usuario 400 introduce, por ejemplo, en lugar de sus datos de tarjeta de crédito, su número de teléfono o identificador dentro de la red dedicada.

De la misma manera que se describió con referencia a la arquitectura de la figura 3a, la información introducida, por ejemplo, a través de un procesador 303, por ejemplo un procesador de ordenador portátil conectado al sitio web de comercio electrónico u otro servidor 302 de interfaz, por ejemplo para el pago de multas o tasas de aparcamiento, implica en cualquier caso la confirmación por medio del teléfono inteligente de la red 210 dedicada y a través del teléfono 210 inteligente el usuario puede autorizar el pago por medio de firma electrónica reconocida al igual que en el caso de la realización descrita con referencia a la figura 3a.

La figura 5 representa una realización adicional, en la que, con respecto a la figura 4, la interfaz de usuario del usuario 400 que es al mismo tiempo peticionario y destinatario viene representada solo por el teléfono 210 inteligente tanto para efectuar la petición como para gestionar la confirmación. En este caso, a diferencia de la

realización relacionada con la figura 4, la aplicación 220 de firma electrónica reconocida envía la petición 305 de operación directamente al servidor 310 frontal, sin interconectarse con el servidor 302 de interfaz. Opcionalmente, parte de los datos necesarios para componer la petición 305 (por ejemplo, la referencia del destinatario y el precio) pueden leerse previamente por medio del módulo 121 de conexión inalámbrica en la red de proximidad, por ejemplo por medio de código QR en los productos que van a adquirirse, en un anuncio o en un sitio de comercio electrónico.

En esta arquitectura, el mensaje 360 de estatus de destinatario solo devuelve notificación de recepción de confirmación 345 a la aplicación 220 de firma electrónica reconocida, ya que el teléfono 210 inteligente para firma electrónica reconocida en cualquier caso recibe el estatus final de la petición 370 de estatus de peticionario.

La figura 6 representa una arquitectura adicional que implementa el sistema según la invención, en la que el usuario 400, peticionario del pago y destinatario de la petición de pago, usa solo el teléfono 210 inteligente para firma electrónica reconocida para conectarse directamente al servidor 310 frontal, incluso leyendo los datos necesarios a través del módulo 121 de conexión inalámbrica; en esta realización, además, la petición 305 de operación asociada con una transacción dada está ya completa con la firma electrónica reconocida, lo que se implementa antes de la misma etapa de petición. A través de la aplicación 220, el teléfono 210 inteligente propone un identificador único de la transacción (es decir de la petición 305 de operación y posteriores mensajes) y un sello de tiempo, que entonces se someten a validación por parte del servidor 310 frontal en lugar de generarse mediante el mismo, como ocurre en las realizaciones anteriores. Preferiblemente, este identificador único de la transacción es una cadena *hash* calculada sobre la concatenación de la información que va a firmarse, de información pseudoaleatoria proporcionada por la aplicación 220 de firma electrónica reconocida; si el servidor 310 frontal rechaza la petición 305 de operación con un mensaje 370 de estatus de peticionario indicando como motivo, por ejemplo, un identificador incorrecto, porque ya está presente en el sistema o indicando como motivo, por ejemplo, un sello de tiempo de la petición incorrecto, porque difiere del que se ha detectado, en el momento de recepción de la petición 305 de operación, por parte del servidor frontal más allá de una tolerancia configurada, la aplicación 220 de firma electrónica reconocida recalcula automáticamente la petición 305 de operación, el identificador y el sello de tiempo, que cambian y se usan en una petición 305 de operación adicional. Como el mensaje que va a suscribirse es diferente, dada la modificación de la información mencionada anteriormente, la firma también debe volver a implementarse, solicitando el código PIN de firma del usuario.

En el caso de la petición 305 de operación validada por el servidor 310 frontal, el servidor 315 aplicativo recibe la firma electrónica reconocida dentro de la petición 308 reenviada, ya que la firma se recibe mediante el servidor 310 frontal dentro de la petición 305 de operación y el servidor 310 frontal la reenvía al servidor 315 aplicativo.

En contraposición, por ejemplo, al primer ejemplo de realización descrito con referencia a la figura 3a, en este caso el servidor 315 aplicativo no intercambia mensajes con el teléfono 210 inteligente, ya que la firma ya es conocida para el mismo servidor aplicativo. El servidor 315 aplicativo verifica no obstante la firma tal como se describe con referencia a la figura 3a.

Entonces, al igual que en los casos anteriores, al final de las operaciones la retroalimentación 355 de orden se reenvía mediante el servidor que efectúa el pago al servidor 315 aplicativo, que envía el mensaje 366 de reenvío de estatus al servidor 310 frontal, que envía el mensaje 370 de estatus de peticionario recibido en el teléfono 210 inteligente y por tanto se muestra el estatus de la operación. En esta realización la firma se envía también con la información en texto sin formato en el mensaje 305 de petición de operación.

Una realización adicional se refiere al tipo de petición de suscripción de documentos, que no necesariamente son autorizaciones de pago sino que pueden ser documentos de cualquier tipo, a través de firma electrónica reconocida, donde el peticionario de la firma difiere del suscriptor o destinatario, como en los diagramas de las figuras 3a y 3b. Además en este caso, la diferencia del proceso relacionado con la figura 3b con respecto a la 3a consiste en el hecho de que en el caso de la 3b la comunicación entre teléfono 210 inteligente y servidor 310 frontal tiene lugar sin la intermediación del servidor 302 de interfaz. Dada esta diferencia, a continuación en el presente documento se hará referencia por motivos de simplicidad al diagrama 3a, sin perder la generalidad. El peticionario separado del destinatario 300, a través de estas arquitecturas, puede efectuar peticiones de suscripción de documentos para el destinatario 365. Una petición original de este tipo está compuesta normalmente por dos peticiones 305 de operación en sucesión: la primera para la subida del documento, la segunda para la suscripción real, incluso, por ejemplo, si la realización basada en la figura 6, comentada más adelante en el presente documento, solo tiene una petición 305 de operación que contempla tanto información de suscripción como de subida. Volviendo al diagrama de la figura 3a, el usuario de la red 365 dedicada de destinatario está registrado en el sistema de firma electrónica reconocida según la invención, con un servidor 315 aplicativo que gestiona mensajes de petición original de tipo de suscripción de documentos.

En el caso de suscripción de documentos, por ejemplo en el caso de una empresa aseguradora que solicita la suscripción de un contrato por parte del usuario del sistema 365 de firma electrónica reconocida de destinatario, la primera petición 305 de operación para la subida de documentos se envía al servidor 310, que no llega al usuario 365 destinatario; esta petición de subida se completa con metadatos para la posterior búsqueda de documentos. El servidor 310 frontal envía una petición 308 reenviada al servidor 315 aplicativo que almacena la información recibida

asignando al documento un respectivo identificador único del documento a través del cual se almacena en memoria persistente junto con la información del identificador de la petición 305 de operación de subida; en respuesta el servidor 315 aplicativo proporciona en el mensaje 366 de reenvío de estatus el identificador de documento, que envía el servidor 310 frontal a través del estatus 370 de peticionario, en respuesta a la petición 305 de operación de subida, al procesador 303 con el que operaba el peticionario, tal como se indica con referencia al diagrama de la figura 3a; alternativamente al procesador 303 éste puede operar a través del teléfono 100 inteligente.

Posteriormente, de nuevo a través de un procesador 303 o teléfono 100 inteligente se envía una petición 305 de operación mediante el mismo peticionario 300, o mediante otro peticionario, para la suscripción del documento previamente almacenado, que, al igual que para las peticiones de pago descritas previamente, requiere la indicación del tipo de petición de operación, específicamente de tipo de suscripción de documentos, el número de teléfono móvil del destinatario registrado en la red 365 dedicada o el identificador del sistema de firma electrónica reconocida asociado con este número, el identificador único del documento y/o de la petición 305 de operación de subida anterior, y la dirección de correo electrónico del peticionario o un identificador del peticionario en el sistema de firma electrónica reconocida.

Dentro de la base de datos del servidor 315 aplicativo se mantiene una referencia de dirección al correspondiente identificador de documento, junto con el identificador de la petición de operación de suscripción relacionada, del sello de tiempo relacionado y del usuario destinatario.

Entonces se envía un mensaje 340 de petición basado en texto al teléfono 210 inteligente; el mensaje contiene el identificador de la petición 305 de operación de suscripción, la cadena *hash* del documento y la referencia de dirección (por ejemplo URL) del documento mientras tanto publicada por el servidor 315 aplicativo en una zona accesible por el usuario 365. El mensaje 340 de petición basado en texto incluye el identificador del tipo de petición en relación con suscripción y si es necesario el identificador del documento, el sello de tiempo asignado por el servidor 310 frontal a la petición 305 de operación de suscripción, tal como se indica en relación con la operación de este servidor con referencia a la figura 3a.

El mensaje 340 de petición basado en texto lo interpreta la aplicación 220 de firma electrónica reconocida y se visualiza en la pantalla 110 para representar una clara petición de suscripción de documento en lenguaje natural. Dentro de la pantalla es posible leer claramente la referencia de dirección, por ejemplo el URL, donde se publica el documento para su visualización y la cadena *hash* del documento, calculada por el servidor 315 aplicativo y enviada al teléfono 210 inteligente, ya que el documento podría ser de dimensiones considerables y el cálculo de la cadena *hash* en el teléfono 210 inteligente podría resultar problemático. Como la cadena *hash* puede contener caracteres ocultos está codificada con notación hexadecimal o en base64, u otro formato en la pantalla 110. Además en este caso es posible seleccionar la opción de la aplicación 220 que permite volver a calcular el *hash* en el teléfono 210 inteligente y la verificación del recibido, o este *hash* podría volver a calcularse usando otro software en un procesador de soporte, descargando en primer lugar el documento en la referencia de dirección indicada en el mensaje.

Si el usuario 365 proporcionó una dirección de correo electrónico durante la etapa de registro, también puede hacérsele llegar simultáneamente un mensaje de correo electrónico que contiene el mismo mensaje visualizado en el teléfono 210 inteligente y enviado por el servidor 315 aplicativo; de este modo, por ejemplo, el destinatario 365 puede recibir el correo electrónico consultando el buzón de correo en un procesador de soporte y haciendo clic sobre la referencia de dirección del documento, presente en el correo electrónico, visualizarlo en una pantalla mayor. El nombre de archivo presente en esta referencia puede estar representado por el mismo *hash* para permitir una comprobación adicional disponible para el usuario.

Con esta operación el usuario de la red 365 dedicada de destinatario puede descargar el archivo de documento y volver a calcular el *hash* usando otras herramientas, por ejemplo presentes en Internet.

En cualquier caso, el documento puede visualizarse en la pantalla 110 del teléfono 210 inteligente a través de la elección de una correspondiente opción en la aplicación 220 de firma electrónica reconocida.

La cadena *hash* se calcula mediante el servidor 315 aplicativo, como ya se describió con respecto a la realización de la figura 3a, donde el mensaje 345 de confirmación está constituido de hecho por el identificador de la petición 305 de operación de suscripción, por la firma electrónica reconocida separada efectuada en el *hash* del documento, y si es necesario por el identificador único del documento. La firma corresponde al cifrado RSA a través de la clave privada del *hash*, una vez se ha decodificado del formato de presentación tal como base64 o hexadecimal. Además en este caso, en base a la legislación adoptada en el país de uso, puede ser obligatorio o no añadir otra información al *hash* antes de la firma.

El servidor 315 aplicativo verifica la firma contenida en el mensaje 345 de confirmación recuperando el archivo de documento, el certificado de firma asociado con el número de teléfono en la base de datos relacionada con el usuario al que se envió la petición 305 de operación de suscripción de documentos, siendo innecesario efectuar una petición 350 de orden al servidor 330.

En este caso también, al igual que en las realizaciones descritas con referencia a la figura 3a, si el mensaje 305 de petición de operación de suscripción se completa con la dirección de correo electrónico del peticionario, el servidor 310 frontal envía a la(s) correspondiente(s) dirección/direcciones de correo electrónico el correo electrónico que traduce el mensaje 370 de estatus de peticionario en lenguaje natural, tanto en el caso de estatus positivo como en el caso de estatus negativo de la transacción. El correo electrónico enviado contiene como adjunto la firma del documento, si es necesario en modo adjunto, es decir a la firma acompaña, es decir se adjunta a la misma, también el documento, el certificado de firma y el certificado de la autoridad de certificación correlacionada; el correo electrónico también contiene detalles de la petición 305 de operación de suscripción y el identificador del documento. Puede enviarse un correo electrónico análogo a la dirección de correo electrónico del usuario 365.

Si la petición 305 de operación de suscripción contenía el identificador del peticionario en la red dedicada o el número de teléfono del peticionario, el servidor 310 frontal le envía una notificación al teléfono 210 inteligente relacionado del peticionario a través de su número de teléfono registrado en la red dedicada.

En general, se aplican entonces los aspectos adicionales de los flujos descritos con referencia a la figura 3a, donde se considera el documento en lugar del mensaje 340 de petición basado en texto.

A través de este método de firma, el usuario 365 puede suscribir documentos con movilidad a través de su teléfono 210 inteligente para firma electrónica reconocida, después de una petición por parte de terceros, almacenar estos documentos suscritos a tiempo y enviarlos al peticionario.

Si el documento es una factura o un recibo, este proceso permite la suscripción digital de los mismos y por tanto la producción de una factura o recibo electrónico. Esta gestión puede combinarse con su pago electrónico por parte del cliente registrado en el sistema de firma electrónica reconocida: si los metadatos de la factura o recibo subido contienen el identificador único del cliente o su número de teléfono dentro de la red dedicada y la información para una petición de pago, tras la gestión del mensaje 305 para la suscripción de la factura por parte del vendedor, ésta puede generarse automáticamente mediante el servidor 302 de interfaz en la realización de la figura 3a, o en la realización de la figura 3b puede generarse una petición 305 de operación de pago mediante la aplicación 220 en el teléfono 210 inteligente, dirigida al cliente, quien puede efectuar el pago por medio del teléfono 210 inteligente. Una realización adicional del sistema de suscripción de documentos puede operar con la arquitectura de la figura 4, tal como se describió previamente, en la que el usuario 400 que es peticionario y destinatario opera, por ejemplo, sobre un documento o sistema de contabilidad asociado con la red de firma electrónica reconocida dedicada; el documento o sistema de contabilidad u otro servicio está representado por un sitio web o servidor de interfaz con la red de certificación dedicada, a través de los que el usuario 400 puede firmar facturas electrónicas o documentos también de dimensiones considerables a través del teléfono 210 inteligente y puede usar el campo de correo electrónico del peticionario con una dirección de correo electrónico a la que el usuario 400 pretende enviar el documento firmado.

Una realización adicional del sistema de suscripción de documentos puede operar con la arquitectura de la figura 5, tal como se describió previamente, en la que la interfaz de usuario está representada únicamente por el teléfono 210 inteligente que está interconectado directamente con el servidor 310 frontal sin intermediación del servidor 302 aplicativo, tanto para efectuar la petición como para gestionar la suscripción de documentos. En este flujo el mensaje 360 de estatus de destinatario solo devuelve la notificación del recibo de la confirmación 345 a la aplicación 220 de firma electrónica reconocida, puesto que el teléfono 210 inteligente en cualquier caso recibe el estatus final de la petición 370 de estatus de peticionario.

Una realización adicional del sistema de suscripción de documentos puede operar con la arquitectura de la figura 6, tal como se describió previamente, pero en ésta el *hash* siempre se calcula mediante la aplicación 220 de firma electrónica reconocida, y por tanto permite una operación en el caso de documentos de dimensiones limitadas, tales como mensajes de texto SMS introducidos en el teléfono 210 inteligente, que después se firman. En este caso el documento se envía por medio de un mensaje 305 de petición de operación de suscripción, simultáneamente con cualquier metadato para una posterior búsqueda en los sistemas de almacenamiento de la red dedicada, y simultáneamente con la firma electrónica reconocida del documento; el documento puede introducirse con el teclado 115 numérico del teléfono 210 inteligente o puede recuperarse como archivo.

El usuario 400 puede usar el campo de correo electrónico del peticionario con una dirección de correo electrónico a la que pretende enviar el documento firmado. Alternativamente, puede usar el campo adicional en la petición que corresponde al identificador único o número de teléfono de un usuario de la red dedicada al que va a enviarse el documento firmado. En este caso, tras la recepción del estatus 370 de peticionario positivo, la aplicación 220 de firma electrónica reconocida presente en el teléfono inteligente de la red 210 dedicada notifica al usuario 400 que la operación ha tenido lugar; además, la red dedicada envía una notificación al teléfono 210 inteligente del usuario de la red dedicada que designa el firmante; el destinatario de la notificación puede leer, a través de la aplicación 220, el documento desde su teléfono 210 inteligente, proporcionándose la certificación de la identidad del servidor mediante la red dedicada.

Una realización adicional se refiere al acceso seguro y certificado a servicios de red integrados con la red dedicada,

tales como sitios web, incluyendo banca desde casa y sitios web de administración pública. Esta realización adicional de acceso seguro y certificado puede operar con la arquitectura de la figura 4, en la que el usuario de la red 400 dedicada está registrado en la red dedicada con un servidor 315 aplicativo que habilita los accesos al servidor 302 de interfaz y está conectado a la red dedicada para efectuar una petición de acceso a un servidor 302 de interfaz a través del procesador 303 de soporte con pantalla o si es necesario el teléfono 100 inteligente convencional, incluyendo en este caso el mismo teléfono 210 inteligente usado posteriormente en la etapa de confirmación, que sin embargo no usa la aplicación 220 de firma electrónica reconocida y la memoria 200 de seguridad para la etapa de petición. La petición de acceso está compuesta normalmente por dos peticiones 305 de operación en sucesión. El servidor 302 de interfaz está representado por el servicio o sitio web en el que el usuario 400 desea autenticarse. El peticionario de acceso y el usuario que lo confirma son en este caso el mismo usuario 400, que opera, como peticionario, de la misma manera que el peticionario 300 descrito con referencia a la arquitectura de la figura 3a. Por tanto, el servidor 302 de interfaz, por ejemplo, puede implementar un sitio web al que el usuario 400 efectúa peticiones a través de un navegador del procesador 303 o del teléfono 100 inteligente según protocolos conocidos, que permiten al servidor 302 de interfaz traducir las peticiones del usuario 400 en peticiones 305 de operación e interpretar los mensajes 370 de estatus de peticionario recibidos por el mismo servidor 302 de interfaz en información inteligible para el usuario 400 en el papel de peticionario.

Según un aspecto adicional de la invención, el servicio/sitio 302 web genérico que pertenece al sistema de comunicación con firma certificada solicita que se introduzca información en campos específicos según el esquema usuario/contraseña, en el que en este caso sin embargo la contraseña es una contraseña temporal aleatoria, o ATP.

El código de usuario se refiere al usuario 400 y puede ser su número de teléfono o su identificador único dentro del sistema según la invención o su identificador único dentro del servicio/sitio 302 web específico. En este último caso, la asociación con uno de los dos identificadores mencionados anteriormente está presente dentro del servicio/sitio 302 web.

La ATP representa un código alfanumérico aleatorio decidido por el usuario en el momento en el que la introduce, es decir en el momento en el que se le pide introducir una contraseña para una transacción dada, tal como inicio de sesión o autorización de una orden. La primera petición 305 de operación comprende la indicación del tipo de petición de acceso, el número de teléfono móvil del destinatario de la red 400 dedicada o el identificador de la red dedicada asociada con este número, el identificador de la sesión de usuario en el servicio/sitio 302 web, la ATP y si es necesario la referencia (por ejemplo URL) del servicio al que va a accederse. La petición 305 de operación se envía al servidor 310 frontal.

El usuario 400 en el papel de destinatario opera sustancialmente del mismo modo que se describió para el destinatario 365 con referencia a la figura 3a; sin embargo, antes de enviar el mensaje 340 de petición basado en texto al usuario 400 como destinatario en el teléfono 210 inteligente, el servidor 315 aplicativo lleva a cabo comprobaciones específicas adicionales; de hecho, el servidor 315 aplicativo almacena el historial de las últimas n ATP usadas por el usuario, siendo n un número entero configurable. En el caso de una petición con la misma ATP que la presente en el historial, la petición falla. A la inversa, el servidor 315 aplicativo prepara una cadena definida en el presente documento como cadena de base; la cadena de base es una cadena de caracteres que forma parte del mensaje 340 de petición basado en texto.

La cadena de base puede representar información de texto sin formato o ser el *hash* de esta información de texto sin formato, en base a la configuración del sistema. La información de texto sin formato mencionada anteriormente es una cadena de caracteres obtenida de la concatenación de información presente en la petición 308 reenviada, incluyendo la ATP, el identificador único de la petición 305 de operación, si es necesario junto con el sello de tiempo del servidor 310 frontal, si es necesario el identificador de sesión, y si es necesario la referencia del servicio, además de otros datos opcionales. Por tanto, la cadena de base coincide con toda esta cadena o con su *hash*, según la configuración. La información en la sesión se conoce por el servidor 302 de interfaz y está presente en el servidor 315 vinculado al identificador de la correspondiente petición 305 de operación. Además, este vínculo también es conocido posteriormente para el servidor 302 de interfaz, a través del mensaje 370 de estatus de peticionario correspondiente a la primera petición 305 de operación. El mensaje 370 de estatus de peticionario indica entre los datos la cadena de base en el caso de estatus positivo, y en cualquier caso el identificador de sesión y el identificador de primera petición 305 de operación, de modo que el servidor 302 de interfaz puede relacionarlos así como recibir la información sobre el estatus de la petición de operación y de la cadena de base para la sesión indicada. Al nivel del mensaje 340 podría omitirse la información sobre la sesión, ya que la confirmación implementada por el teléfono 210 inteligente que comprende como información el identificador de la primera petición 305 de operación, estaría asociada por el servidor 315 aplicativo con una confirmación para la sesión vinculada a esta petición 305 de operación.

Si la cadena de base está en texto sin formato contiene en texto sin formato al menos la ATP y el identificador de la primera petición 305 de operación, y el mensaje 340 de petición basado en texto está compuesto por la cadena de base y el identificador del tipo de petición (petición de tipo acceso); por el contrario, si la cadena de base es el *hash* mencionado anteriormente, está formada por la concatenación de cadena de base de tipo de petición, ATP e identificador de la primera petición 305 de operación, si es necesario el identificador de sesión y otra información

opcional que puede estar presente en la información de texto sin formato sobre la que se calcula el *hash* mencionado anteriormente.

Después de que el servidor 315 aplicativo haya recibido la ATP en la petición 308 reenviada, si no es válida en base a las comprobaciones mencionadas anteriormente, envía al servidor 310 frontal a través del mensaje 366 de reenvío de estatus una indicación de que la ATP introducida no es válida o, si es válida, envía un mensaje 366 de reenvío de estatus positivo. Este mensaje 366 de reenvío contiene el identificador de la petición 305 de operación, la cadena de base y la sesión. El servidor 310 frontal reenvía entonces un correspondiente mensaje 370 de estatus de peticionario con la misma información, si es necesario incluyendo toda la información presente en el mensaje 308 de petición reenviado, al servidor 302 de interfaz que para la sesión coincidente con la recibida actualiza la indicación de ATP, sesión e identificador no válido de la primera petición 305 de operación o, si es positiva, el valor de la cadena de base y del identificador de la petición 305 de operación recibido, asociado con la sesión junto con cualquier información opcional recibida. La interfaz gráfica presente en el procesador 303 o teléfono 100 inteligente se actualiza automáticamente o bajo petición del usuario 400 y el mensaje de error o, en caso positivo, la cadena de base, se visualiza en el mismo.

Si la cadena de base está en texto sin formato la ATP contenida en la misma puede estar oculta. Si la cadena de base es un *hash*, si es necesario, la información se presenta de modo que el usuario puede calcular este *hash* de manera autónoma con las otras herramientas, sobre la concatenación de la información visualizada en el dispositivo de petición, para poder comparar este *hash* con el visualizado, conociendo las normas con las que la información presente en la interfaz gráfica está concatenada para calcular el *hash*. Estas normas también pueden explicarse en la interfaz gráfica del sitio 302 web de interfaz como nota de información. Además en este caso, si el *hash* está presente, está codificado preferiblemente con notación hexadecimal o en base64.

Sin embargo, enviando el mensaje 370 de estatus de peticionario correlacionado con el mensaje 305 de petición de operación anterior las operaciones no se han terminado; el servidor 315 almacena los datos de la primera petición 305 de operación, del mensaje 308 y 340. Además, se crea un mensaje 305 de petición de operación adicional automáticamente mediante el servidor 302 de interfaz, tras la petición automática por el procesador 303 o por el teléfono 100 inteligente del peticionario, para terminar las actividades. Este mensaje 305 de petición de operación indica entre los datos de tipo de petición, el identificador del mensaje 305 de petición de operación anterior obtenido del mensaje 370 de estatus de peticionario anterior, y el tiempo de ejecución de identificador de sesión recuperado que debe coincidir con el anterior para que la nueva petición sea válida.

Al nuevo mensaje 305 de petición de operación se le asigna un sello de tiempo y un nuevo identificador a través del servidor 310 frontal. El servidor 310 frontal envía el contenido del nuevo mensaje 305 de petición de operación, completo con identificador de petición y sello de tiempo, a través del mensaje 308 de petición reenviado al servidor 315 aplicativo en el que se registró el primer mensaje 305 de petición, marcado por su identificador, junto con sus datos con un estatus de operación global de tipo “esperar”. El nuevo mensaje 308 de petición reenviado y su identificador son, al nivel del servidor 315 aplicativo, en este punto parámetros análogos correlacionados de la petición anterior, debido al identificador de la primera petición 305 de operación presente en el nuevo mensaje; además, el servidor aplicativo efectúa una comprobación de igualdad entre el identificador de sesión contenido en los mensajes de petición primero y segundo. En paralelo al envío del primer mensaje 366 de reenvío de estatus, si el servidor 315 aplicativo valida positivamente la ATP, mientras tanto ha preparado el mensaje 340 de petición basado en texto que se envía al teléfono 210 inteligente, con el contenido descrito anteriormente. El mensaje 340 de petición basado en texto indica el identificador del correspondiente mensaje 305 de petición de operación, es decir el primero, y se almacena en zonas persistentes específicas, por ejemplo memorias masivas conectadas al servidor 315 aplicativo; una referencia al correspondiente archivo, junto con el identificador de la petición, del sello de tiempo y del usuario destinatario representado por su número de teléfono o identificador único, se mantienen dentro de la base de datos de dicho servidor 315, junto con otros datos del mensaje 340 de petición basado en texto, incluyendo información de texto sin formato correspondiente al *hash* si la cadena de base está en forma de *hash*.

El servidor 315 aplicativo envía el mensaje 340 de petición basado en texto en base al número de teléfono del destinatario recibido en el primer mensaje 308 de petición reenviado o deducido de su propia base de datos en base al identificador único del usuario 400 recibido en el primer mensaje 308 de petición reenviado. En general, los métodos de enviar el mensaje 340 reflejan lo que ya se ha descrito con respecto al caso general de la figura 3a.

El mensaje 340 de petición normalmente corresponde a una clara petición de acceso en lenguaje natural que indica los datos presentes en el mismo mensaje, visualizados en la pantalla 110 del teléfono 210 inteligente; si la cadena de base está en forma de *hash*, se muestra el valor de *hash*, siempre codificado preferiblemente en notación hexadecimal o en base64. La aplicación 220 de firma electrónica reconocida pide estampar la firma electrónica reconocida en la cadena de base si es un *hash*, de lo contrario en el *hash* de todo el mensaje 340, ya que este *hash* se calcula mediante la aplicación 220; es decir según el caso, o bien en el *hash* que coincide con la cadena de base visualizada en la pantalla 110 tras la decodificación a partir del formato de visualización, normalmente hexadecimal/base64, o bien en el caso de cadena de base de texto sin formato, el *hash* se calcula mediante la aplicación 220 en el mensaje 340 de texto sin formato visualizado en la pantalla 110. La firma consiste en el cifrado RSA del *hash* a través de una clave 201 privada. Antes de la firma, el usuario 400 puede comparar en el caso de

una cadena de base que coincide con el *hash*, la ATP y el *hash* que muestra la aplicación 220 multifuncional respectivamente con la ATP introducida por el mismo por medio del procesador 303 de soporte o teléfono 100 inteligente, así como cualquier otro parámetro opcional.

En el caso de cadena de base de texto sin formato, el usuario 400 puede comparar la ATP y el identificador de la petición 305 de operación que muestra la aplicación 220 multifuncional respectivamente con la ATP introducida por el mismo en el dispositivo 303 ó 100 de petición y el identificador de la petición 305 de operación, que muestra de nuevo el procesador 303 de soporte o teléfono 100 inteligente, así como cualquier otro parámetro opcional. En el caso de que esté presente información adicional en el mensaje 340 de petición basado en texto y por tanto en la pantalla 110 del teléfono 210 inteligente, ésta está también presente en cualquier caso en la interfaz gráfica del procesador 303 de petición o teléfono 100 inteligente, permitiendo por tanto al operador comprobar que la información presente en la petición y el medio de confirmación es congruente. Si los datos son congruentes, el usuario puede proceder con la firma electrónica reconocida separada.

En lo que se refiere a los métodos para calcular el *hash*, se aplica lo que se describió anteriormente con referencia a la figura 3a, en particular con referencia a la necesidad de añadir cualquier información adicional al *hash* antes de la firma, después de cualquier requisito adicional para la firma electrónica reconocida en el país de uso. El mensaje 345 de confirmación está representado en este caso por la firma electrónica reconocida separada efectuada sobre el *hash* mencionado anteriormente coincidente con la cadena de base si ésta está en forma de *hash* o, por el contrario, sobre el *hash* calculado por la aplicación 220 en el mensaje 340. La firma viene acompañada por el identificador único de la primera petición 305 de suscripción asignada previamente por el servidor 310 frontal.

El servidor 315 aplicativo verifica la firma contenida en el mensaje 345 de confirmación que recupera la correspondiente información de texto sin formato registrada previamente: la información de texto sin formato a partir de la cual se calculó el *hash* si era la cadena de base; a la inversa, se recupera todo el mensaje 340. Además, se recuperan el certificado de firma asociado con el número de teléfono en la base de datos relacionada con el usuario al que se envió la primera petición 305 de operación, y el certificado relacionado de la autoridad de certificación.

Si falla la verificación de la firma o de otras comprobaciones, el servidor 315 aplicativo envía un mensaje 360 de estatus de error de destinatario específico al teléfono 210 inteligente y el mensaje 366 de reenvío de estatus de error específico al servidor 310 frontal, en respuesta al segundo mensaje 308 de petición reenviado. Este envía el estatus 370 de error de peticionario al peticionario, en respuesta al segundo mensaje 305 de petición de operación.

En el presente ejemplo de aplicación no es necesario efectuar una petición 350 de orden al servidor 330. En lo que se refiere al segundo estatus 370 de peticionario se aplica generalmente lo que se describió anteriormente con referencia a la figura 3a, ya que el usuario 400 en el papel de destinatario corresponde al peticionario y considerando sin embargo que en la segunda petición 305 de operación la dirección de correo electrónico del peticionario/destinatario no está normalmente presente. En el caso de verificaciones positivas, el mensaje 370 de estatus de peticionario contiene la indicación para que el servidor 302 de interfaz considere como auténtico al usuario en la sesión inicialmente indicada en la primera y segunda petición 305 de operación; por tanto, el usuario 400 puede visualizar o acceder a los datos sensibles ya que su sesión en el servidor 302 de interfaz está autorizada para ello. En el fondo, el usuario 400 efectúa el inicio de sesión de manera satisfactoria.

La información adicional que puede gestionar el servidor 302 de interfaz consiste en la especificación en peticiones 305 de operación de autorización o información específica dentro de la sesión actual; de este modo, puede efectuarse una doble petición 305 de operación específica, como en el caso mencionado anteriormente; estas peticiones 305 de operación de tipo acceso se usan también para permitir el acceso a esta información específica o para confirmar una orden. Por ejemplo, el valor de la sesión establecida por el servidor 302 de interfaz, en la petición 305 de operación, puede contener el identificador de la acción particular que va a autorizarse o información a la que va a accederse; en este caso se gestiona una doble petición 305 de operación similar a la mencionada anteriormente, en la que el código de usuario para la etapa de petición opcionalmente ya no se solicita al usuario ya que es conocida para el servidor 302 de interfaz; normalmente, solo se solicita una ATP desde la interfaz gráfica de usuario.

Para los otros aspectos no descritos en este caso, el sistema opera de la misma manera que se describe para el sistema que opera con la arquitectura de la figura 3a.

También es posible usar el mismo procedimiento descrito en este caso sin usar la ATP. Puede usarse el método para obtener seguridad a través de una contraseña temporal aleatoria para acceder a banca en casa o móvil, así como para el acceso a cualquier servicio/sitio web. En el caso de banca en casa-móvil, el servidor 315 aplicativo está instalado normalmente dentro de la red del banco. La comparación entre contraseñas temporales y la otra información presente tanto en el lado del peticionario como en el lado del destinatario, la implementa preferiblemente el usuario 400. Naturalmente es posible, en particular, que el usuario 400 use como terminal para la petición y para la firma un teléfono 210 inteligente para firma electrónica reconocida, usando para la etapa de petición sus funciones de un teléfono 100 inteligente; en este caso la comparación mencionada anteriormente puede efectuarse a través de un software de aplicación específica o la misma aplicación.

También es posible integrar la petición dentro de la misma aplicación 220, y en este sentido es posible extender la realización de la petición a través del servidor 302 de interfaz al teléfono 210 inteligente. El software de aplicación, si la visualización tiene lugar en dos procesadores diferentes, puede hacer uso por ejemplo de un canal de comunicación de corta distancia, por ejemplo Bluetooth, a través del uso en el teléfono 210 inteligente del módulo 121 de conexión inalámbrica opcional o similar en el caso de procesadores 303 o teléfonos 100 inteligentes, tales como los usados por los mensajes 351 y 352 de cliente descritos a continuación en el presente documento, en este caso para comparación automática.

De nuevo, para efectuar el inicio de sesión en un servicio de red o autorizar una orden, también es posible visualizar ya inicialmente el identificador de sesión en el dispositivo 303 ó 100 a través de la comunicación con el servidor de interfaz y promover en el mismo una petición 305 de operación sin referencia al usuario implicado; en este caso el teléfono 210 inteligente se usa inmediatamente de una manera activa sin el uso del mensaje 340 basado en texto, porque el usuario 400 introduce el identificador de sesión en la aplicación 220 y realiza la firma adjunta en la misma, enviándola con un mensaje 345 de confirmación al servidor 315 aplicativo; si es necesario, el mensaje se completa con el identificador del usuario en la red dedicada o número de serie del certificado con identificador relacionado del certificado de la autoridad de certificación que lo emitió, o tras la recepción del mensaje 345 de confirmación el usuario se deduce del número de teléfono, si es un mensaje de texto SMS. El servidor 315 aplicativo, tras verificar la firma usando los certificados presentes en su propia base de datos asociados con el usuario, envía el identificador del firmante o número de teléfono con la sesión a través de un mensaje 366 de reenvío de estatus al servidor 302 de interfaz; el servidor 302 de interfaz con el mensaje 370 de estatus de peticionario recibe el identificador o número de teléfono del usuario y completa el inicio de sesión o la orden solicitada en el dispositivo 303 ó 100. También es posible añadir el nombre de usuario o número de teléfono o identificador de la red dedicada en la etapa inicial en el dispositivo 303 ó 100; en este caso la información sobre el usuario para la sesión indicada está presente en el mensaje 305 hasta que llega al servidor 315 aplicativo: con la restricción de que no es posible para un usuario dado activar más de un inicio de sesión simultáneamente, el mensaje 345 puede no contener la información de texto sin formato sobre la sesión ya que ya está presente en asociación con el usuario en el servidor 315, y portar con el mismo la firma adjunta y si es necesario el identificador de usuario en la red dedicada o la información mencionada anteriormente sobre los certificados, o de nuevo el número de teléfono de usuario se deduce del servidor 315 aplicativo si es un mensaje de texto SMS. En este uso de la red dedicada para acceso o para órdenes también es posible añadir la ATP en el dispositivo 303 ó 100 al comienzo del procedimiento, activando el nuevo cálculo del identificador de sesión que aparece en la pantalla relacionada; si es necesario, la información de ATP llega al servidor 315 aplicativo al que el usuario envía un primer mensaje 345 con indicación de la sesión visualizada en el dispositivo 303 ó 100 y recibe la ATP en respuesta con un mensaje 360 de estatus de destinatario; si las dos ATP son iguales, promueve un mensaje 345 de firma adicional tal como se indicó anteriormente.

Ha de observarse que el procedimiento con contraseña temporal aleatoria descrito anteriormente, si es necesario, también puede usarse en sistemas de firma electrónica reconocida que hacen uso de una clave 201 privada, que sin embargo no está almacenada en una memoria 200 de seguridad.

Además, el procedimiento de firma a través del uso de una ATP que se describe con referencia a los sistemas según la presente invención, también puede usarse con diferentes sistemas, configurando una firma electrónica o procedimiento de firma electrónica reconocida según el cual tras la visualización de un identificador de sesión en los primeros medios de procesamiento, el usuario 400 peticionario y destinatario introduce este identificador en la aplicación 220 de los segundos medios 210 de procesamiento y estampa una firma en el mismo a través de la aplicación 220, enviándola por medio de un mensaje 345 de confirmación de modo que el servidor 315 aplicativo puede identificar al usuario firmante a través de la verificación de la firma, suministrar esta información por medio del mensaje 366 de reenvío de estatus al servidor 302 de interfaz que se comunica con los primeros medios 303 (ó 100 ó 210) de procesamiento para permitir al usuario, si está registrado en el servidor 315 de interfaz, efectuar una orden o acceder a una página adicional en los primeros medios de procesamiento, pudiendo también recibir en los segundos medios 210 de procesamiento antes de dicha firma, esta ATP si se introdujo previamente en los primeros medios 303 (ó 100 ó 210) de procesamiento.

Una realización adicional se refiere a pagos y suscripciones implementados según una de las arquitecturas en las figuras 3a, 3b, 4 y accesos según la arquitectura en la figura 4, tal como se ilustra con referencia a la arquitectura de la figura 7. El mensaje 360 de estatus de destinatario se representa con una línea de trazos ya que podría estar ausente y sustituirse por otro mensaje, como se indica a continuación en el presente documento. En esta realización, el mensaje 340 de petición basado en texto puede sustituirse por un mensaje enviado por el procesador 303 de cliente, tal como se representa en la figura 7, que puede sustituirse alternativamente por un teléfono 100 ó 210 inteligente, y se dirige al teléfono 210 inteligente del suscriptor. El peticionario 300 en la figura 7 puede sustituirse por el peticionario que coincide con el destinatario 400, y el destinatario 365 en la figura 7 también puede sustituirse por el peticionario que coincide con el destinatario 400.

El servidor 302 de interfaz se representa con una línea de trazos ya que puede no estar presente si la petición se efectúa desde el teléfono 210 inteligente. En este contexto, cada uno de los mensajes 305 de petición de operación de pago y los mensajes 305 de petición de operación de suscripción posteriores a la subida de datos, y el primero de

los dos mensajes 305 de petición de operación de tipo acceso, se sustituye ahora por dos nuevos mensajes 305 de petición de operación en sucesión. Los dos nuevos mensajes 305 de petición de operación, cada uno con su propio identificador, están vinculados en general de modo que el identificador del primero se indica entre los datos en el segundo. En el caso de accesos, sigue una petición 305 de operación adicional, al igual que en la realización descrita previamente. El primer nuevo tipo de mensaje 305 de petición de operación a través de los mensajes y los servidores descritos en las realizaciones anteriores, aparte de procesarse como en los casos anteriores, si es necesario, puede contener una indicación del dispositivo 303 ó 100 ó 210 de petición a través de un identificador, si es posible única. La petición 305 de operación, tras llegar al servidor 315 aplicativo, también consigue el efecto de hacer que el servidor 315 aplicativo envíe la misma información que habría estado contenida en el mensaje 340 de petición basado en texto, con indicación del número de teléfono del destinatario y, si es necesario, del identificador del dispositivo de peticionario, a través del mensaje 366 de reenvío de estatus, que a través del mensaje 370 de estatus de peticionario llega al procesador 303 o teléfono 100 inteligente. En este caso el servidor 315 aplicativo en cualquier caso espera el mensaje que contiene la firma, asociado con la primera petición. El mensaje 370 de estatus de peticionario actualiza el estatus de espera de la firma del suscriptor en el dispositivo 303 ó 100 ó 210 que efectuó la petición; si la petición efectuada es de tipo acceso, los datos para actualizar la interfaz gráfica del procesador 303 ó 100 se deducen del mensaje 370 de estatus de peticionario, tal como se describió previamente. En general, el mensaje 370 contiene la información dirigida al teléfono 210 inteligente del destinatario y por tanto la misma, o parte de la misma, al transferirse a través del dispositivo 303 ó 100 ó 210 de petición, puede visualizarse en la interfaz gráfica relacionada del dispositivo de petición cuando se recibe el mensaje 370. Por ejemplo, el *hash* que va a suscribirse puede presentarse en esta interfaz gráfica también para pagos o suscripciones, para permitir una comprobación adicional por parte del usuario.

El procesador 303 de petición o el teléfono 100 ó 210 inteligente también envía la información recibida al teléfono 210 inteligente del destinatario de modo que puede estampar su firma. La transmisión entre el procesador 303 o teléfono 100 inteligente y el teléfono 210 inteligente normalmente tiene lugar a través de tecnologías alternativas al mensaje de texto SMS y normalmente mediante el módulo 121 inalámbrico a través de la red inalámbrica (por ejemplo Bluetooth o NFC o Wi-Fi o código QR) o tráfico de datos de Internet. En presencia del identificador del dispositivo de petición en la petición 305 de operación, esta indicación también está presente entre los datos del mensaje 351 y por tanto también puede comprobarse mediante la aplicación 220 del teléfono 210 inteligente del destinatario, en base al remitente detectado para el mensaje 351. Para identificarse mediante el dispositivo 303, 100 ó 210 de petición, el teléfono 210 inteligente del destinatario, por ejemplo, puede identificarse a través del identificador del destinatario dentro de la red dedicada, o su número de teléfono, u otro identificador adicional presente en la base de datos del servidor 315 aplicativo, contenido en el mensaje 366 de reenvío de estatus y por tanto en el mensaje 370 de estatus de peticionario, cuyo contenido pasa por tanto a estar disponible para el dispositivo de peticionario. Por tanto, se envía un mensaje 351 de petición de cliente al teléfono 210 inteligente mediante el dispositivo 303, 100 ó 210 de petición. Del mismo modo, el procesador 303 o teléfono 100 ó 210 inteligente debe estar habilitado para esta recepción/transmisión.

La firma a través del teléfono 210 inteligente tiene lugar como ya se describió en los casos anteriores y el mensaje 345 de confirmación puede sustituirse por un mensaje 352 de confirmación de cliente análogo, enviado al procesador 303 o teléfono 100 ó 210 inteligente que efectuó la petición, normalmente a través del módulo 121 de conexión inalámbrica opcional. En este contexto, el procesador 303 o el teléfono 100 ó 210 inteligente envía el mensaje recibido a través de una segunda petición 305 de operación, adaptada para enviar la firma al servidor 315 aplicativo en sustitución del mensaje 345 de confirmación; la segunda petición 305 de operación presenta entre los datos el identificador de la primera petición 305 de operación descrita anteriormente. La segunda petición 305 de operación implica un mensaje 308 de reenvío de estatus análogo, recibido por el servidor 315 aplicativo. Debido a la presencia, entre los datos de dicho mensaje, también del identificador de la primera petición, el servidor 315 aplicativo asocia el segundo mensaje con el primero que está esperando para su confirmación y cuyos datos se registraron, y el proceso continúa al igual que en las otras realizaciones. El mensaje 360 de estatus de destinatario puede enviarse desde el servidor 315 aplicativo o sustituirse por un mensaje análogo enviado a través del módulo 121 de conexión inalámbrica opcional desde el procesador 303 o teléfono 100 ó 210 inteligente, tras la recepción del mensaje 370 de estatus de peticionario relacionado con la segunda petición 305 de operación. En el caso de transmisión síncrona, el teléfono 210 inteligente envía el mensaje que confirma la recepción al dispositivo 303 ó 100 ó 210 de petición. Es posible añadir la ATP también para pagos y suscripciones y ésta puede introducirse en el procesador 303 o teléfono 100 ó 210 inteligente junto con otros datos de la petición y compararse por parte del usuario con lo indicado a través del mensaje 351 de petición de cliente en el teléfono 210 inteligente.

Además, el teléfono 100 inteligente desde el que puede efectuarse la petición puede coincidir físicamente con el mismo teléfono 210 inteligente del destinatario, pero no usa directamente, para la etapa de petición, las funciones puestas a disposición por la memoria 200 de seguridad y por la aplicación 220 de firma electrónica reconocida, e interroga a la aplicación 220 de firma electrónica reconocida por medio de otra aplicación; en este contexto los mensajes 351 y 352 pueden representarse, por ejemplo, mediante transmisión TCP/IP, en la que la aplicación de petición envía mensajes 351 a la aplicación 220 de firma electrónica reconocida, que responde con los mensajes 352.

En una variante adicional de la realización descrita anteriormente, con respecto a esta última, es posible calcular los

datos obtenidos de la primera petición 305 de operación a través de la respuesta 370 de estatus de peticionario de otra manera; la alternativa consiste en no realizar la primera petición 305 de operación, y en calcularla por medio del teléfono 210 inteligente o procesador 303 o teléfono 100 inteligente del peticionario, a través de la aplicación 220 en el primer caso y a través de una aplicación diferente en el caso del procesador 303 o teléfono 100 inteligente. En el caso de la petición de acceso, la información relacionada con el identificador de sesión, si es necesario combinada con el identificador de una acción que ha de autorizarse, está presente en la interfaz gráfica del dispositivo de petición, y esta información está disponible para el mismo dispositivo y se incluye en la información de texto sin formato que coincide con la cadena de base o desde donde se calcula el *hash* para establecerlo igual a la cadena de base. Normalmente, se usa el módulo 121 de conexión inalámbrica opcional. En este contexto para todos los tipos de peticiones el identificador de la petición 305 de operación y el sello de tiempo están definidos por la aplicación que envía la petición, y entonces deben validarse por el servidor 310 frontal, tal como se describió previamente en las otras realizaciones. En el caso de petición de acceso, el identificador de la petición 305 de operación calculado se visualiza en la interfaz gráfica del peticionario. El dispositivo 303 ó 100 ó 210 de petición solicita la firma en el teléfono 210 inteligente del destinatario a través del mensaje 351, indicando en el caso de accesos normalmente también el identificador de sesión. En general, no solo para accesos, en respuesta el teléfono 210 inteligente del destinatario envía un mensaje 352 que contiene la firma electrónica reconocida, tal como se describió previamente. El dispositivo 303 ó 100 ó 210 de petición envía entonces una petición 305 de operación, completa con la firma electrónica reconocida obtenida. El proceso continúa tal como se describió previamente, considerando que la firma ya está disponible para el servidor 315 aplicativo cuando el mensaje 308 de reenvío de estatus llega al mismo, sin la necesidad de obtenerse a través de otros mensajes.

En una realización adicional, es posible crear la clave 201 privada en la memoria 200 de seguridad y el certificado, antes de la etapa de suscripción de un contrato por parte de un cliente con un distribuidor, para suscribir el contrato ya con firma electrónica reconocida y ahorrarle al distribuidor y a la organización para la que trabaja el distribuidor tener que gestionar la copia en papel del contrato y de los documentos posteriores intercambiados con el cliente. Estos pueden ser distribuidores que operan como operadores de registro para una autoridad de certificación, en nombre de un operador de telefonía para emitir tarjetas SIM o que operan para abrir una cuenta bancaria en nombre de un banco; en cualquier caso, el cliente puede ser el suscriptor digital con firma electrónica reconocida del contrato y cualquier otro documento. En particular, el cliente puede adelantar un formulario por medio de Internet para solicitar el certificado, proporcionando también su número de teléfono, dirección de correo electrónico, e identificación general del documento de identidad, referencias a cualquier banco conectado con la red dedicada en relación con la firma 220 de aplicación en el que el cliente tiene una cuenta bancaria, y obtener así reserva en un distribuidor para el reconocimiento físico. Mientras tanto, una memoria de seguridad o un testigo u otro dispositivo seguro se envía desde dicho distribuidor o la dirección del solicitante, después el distribuidor reconocerá físicamente al cliente y validará los datos proporcionados por el sistema, presentando el cliente documentos dotados de identidad. El distribuidor puede comprobar el número de teléfono del cliente enviando a través de la aplicación de registro un mensaje SMS al cliente y verificando la recepción real mediante el teléfono inteligente relevante. En el caso de la firma electrónica reconocida del distribuidor éste imprime copias en papel del contrato de petición de certificado generado automáticamente por el sistema para registrar y mostrar los datos introducidos por el cliente en primer lugar, y también el distribuidor y el cliente firmarán el documento en papel, en el caso de controles con resultado positivo. El distribuidor recibirá una petición de suscripción similar a un documento electrónico a través del teléfono 210 inteligente. El procedimiento proporciona un código único al cliente, por ejemplo por medio de SMS o se muestra en la pantalla del distribuidor y lo lee el cliente. El cliente puede crear la petición de certificado según el estándar PKCS10 (o similar) insertando la nacionalidad, a través del número de seguridad social o la identificación del código de acceso e identidad obtenido por el distribuidor, y la aplicación 220 multifuncional, situando el testigo o dispositivo de memoria certificado o recibido por medio del distribuidor o su dirección. En este dispositivo, el cliente creará la clave privada de manera segura a través de la aplicación 220. El cliente puede pagar al distribuidor por el hardware recibido y/o el reconocimiento realizado. Los datos proporcionados por el cliente también se usarán para registrar desde la red dedicada conectada con la aplicación 220 de la firma. Si el cliente desea operar a través de uno o más bancos definidos en el registro, acordará con los mismos el modo de pago por defecto (banco, tarjeta de crédito, etc...), conociendo ya el banco todos los datos necesarios. Alternativamente, puede proporcionar el número y detalles de la tarjeta de crédito durante el registro en el distribuidor y el distribuidor puede controlarlos si lo requiere el procedimiento. Alternativamente, el cliente puede enviar estos detalles a través de la aplicación 220, una vez se obtiene el certificado firmado.

En las realizaciones descritas anteriormente, se ha considerado un único servidor 315 aplicativo para un tipo dado de petición y usuario que pertenece al sistema según la invención. Sin embargo, sería posible tener una pluralidad de servidores aplicativos para el tipo de petición y usuario que pertenece al sistema según la invención. El sistema según la invención proporciona normalmente solo un servicio de servidor 310 frontal, aunque podría haber más de uno.

Por ejemplo, sería posible tener un servicio del servidor 310 frontal y que el usuario destinatario de las peticiones esté registrado en el mismo. El servidor 302 de interfaz al que está conectado el peticionario 300 o el peticionario que coincide con el destinatario 400, está conectado a este servidor 310 frontal. El usuario 365 destinatario o el destinatario que coincide con el peticionario 400 del sistema según la invención que recibe las peticiones está registrado en el servidor 310 frontal con su número de teléfono o identificador único y las direcciones de los

servidores aplicativos con los que el usuario destinatario está registrado para cada tipo de petición.

Después de una petición procedente del peticionario (separado o el mismo que el destinatario), el servidor 302 de interfaz puede conectarse con el servidor 310 frontal especificando el servidor 315 aplicativo del usuario destinatario que ha de considerarse para la transacción, si esta información es conocida para el mismo servidor 302 de interfaz o para el peticionario que añadió esta información a la petición. Por ejemplo, si el servidor de interfaz es un sitio web de banca desde casa, conoce la dirección/referencia del servidor aplicativo en la que se basa el banco para gestionar, por ejemplo, peticiones de acceso al mismo servicio de banca desde casa. Si esta información no es conocida para el peticionario 300 o para el servidor 302 de interfaz, hay dos posibilidades:

- es posible que el peticionario 300 o el servidor 302 de interfaz envíe una petición para una petición 305 de operación particular de tipo lista de información a través del servidor 302 de interfaz para aprender la lista de servidores aplicativos habilitados, obteniendo esta información por medio del mensaje 370 de estatus de peticionario. La gestión de estos mensajes solo implica al servidor 310 frontal y no se propaga a los otros nodos de red. Con la petición posterior, el peticionario y el servidor de interfaz pueden establecer el servidor aplicativo en la misma petición que va a enviarse al destinatario.

- De otro modo el usuario peticionario y el servidor 302 de interfaz envían la petición al servidor 310 frontal sin especificar esta información.

Si el usuario destinatario está registrado en el servidor frontal para una pluralidad de servidores aplicativos para el tipo de petición, el servidor 315 aplicativo indicado, en el servidor frontal, como servidor aplicativo por defecto relacionado con el tipo de petición considerado y con el usuario considerado, se considera por el servidor frontal. El usuario, con el procedimiento de registro a la red dedicada puede indicar, para cada tipo de petición, cuál es el servidor aplicativo por defecto. Si solo hay un servidor aplicativo para el tipo particular, se considera por defecto.

En el caso de peticiones efectuadas por la aplicación 220 de firma electrónica reconocida con un peticionario que coincide con el destinatario, tal como se ilustra, por ejemplo, en las figuras 5 y 6, también es posible guardar la lista de los servidores aplicativos de manera local en la aplicación 220 multifuncional según el tipo, para poder especificar el servidor aplicativo en la petición.

En el caso de pagos implementados por el peticionario separado del destinatario, normalmente el peticionario 300 no conoce la institución financiera del destinatario 365, ni la referencia relacionada del/de los servidor(es) 315 aplicativo(s), sino que solo conoce el número de teléfono o identificador dentro del sistema según la invención. Por tanto, en este caso la petición 305 de operación de pago normalmente no contiene indicación del servidor aplicativo del destinatario. Por tanto, se llega al destinatario 365 mediante un mensaje 340 de petición basado en texto relacionado con el servicio 315 de aplicación por defecto, es decir normalmente desde el servicio de aplicación de uno de los bancos del que es cliente.

En el caso de pagos implementados por un usuario 400 que es peticionario y destinatario, tal como se describe, por ejemplo, con referencia a las figuras 4, 5, 6 y 7, puede especificar fácilmente el servidor 315 aplicativo que va a considerarse en la petición. De este modo, puede implementar el pago solicitando que la operación tenga lugar a través de un banco específico, de entre cualquier banco diferente en el que está registrado en la red dedicada, pudiendo especificar el servidor 315 aplicativo en la petición 305 de operación. De otro modo, la operación tendrá lugar a través del servidor 315 aplicativo por defecto.

En las realizaciones relativas a la suscripción de documentos, si la petición 305 de operación que va a firmarse digitalmente para la suscripción de documentos se efectúa por parte de un peticionario 300 a través de un servidor 302 de interfaz que también ofrece el servicio del servidor 315 aplicativo, la referencia del servidor 315 aplicativo puede especificarse fácilmente en la petición de suscripción por parte del servidor 302 de interfaz. Por ejemplo, este puede ser el caso de una petición efectuada por una empresa a un director de la misma, como destinatario 365, invitado a suscribir una autorización formal y quien al mismo tiempo tiene el servidor 315 aplicativo. Si es el usuario destinatario el que también efectúa la petición, es probable que conozca la referencia del servidor 315 aplicativo o esta referencia puede añadirla el servidor 302 de interfaz. Naturalmente, también en este caso en ausencia de información en el servidor aplicativo se usa el que es por defecto.

En los ejemplos de realización en relación con el acceso a servicios de red, el usuario 400 que es peticionario y destinatario al mismo tiempo, conoce probablemente del mismo modo la referencia del servidor 315 aplicativo que va a introducirse en la petición 305 de operación. De manera más sencilla, el servidor 302 de interfaz que es específico para un determinado servicio, tras recibir la petición genérica por parte del usuario 400, añade los datos en relación con el servidor 315 aplicativo en la petición 305 de operación al servidor frontal. En el caso de accesos a los servicios de red, es posible eliminar el concepto por defecto, en el caso en el que los servidores aplicativos registrados para el usuario sean más de uno en el servidor frontal.

Los mensajes de texto SMS usados pueden enviarse a través de Internet de una manera independiente con respecto a las compañías de teléfono, por ejemplo usando el sistema SKEBBY, o pueden enviarse a través de sus

redes. En cualquier caso, se requiere una tarjeta SIM, correspondiente al número de teléfono del usuario, para recibir los mensajes de petición en el teléfono inteligente.

El uso de mensajes de texto SMS permite recibir una petición de confirmación en el teléfono inteligente sin que el usuario tenga que permanecer en espera, incurriendo en posibles cargos por tráfico de datos. En lugar de mensajes de texto SMS, pueden usarse mensajes de correo electrónico a través del módulo 121 de conexión inalámbrica opcional, si el usuario ha acordado con el sistema esta opción, particularmente útil en el caso de uso de teléfonos inteligentes dotados de un mecanismo de correo electrónico *push*, tal como dispositivos BlackBerry.

Todos los mensajes pueden cifrarse, en particular los mensajes dirigidos al teléfono 210 inteligente del sistema pueden cifrarse con la clave pública del certificado del usuario vinculado a un número de teléfono particular. De hecho, el certificado es conocido para el servidor aplicativo y tras la recepción del mensaje en el teléfono inteligente es posible descifrar el mismo mensaje, para usar el código PIN para activar la clave 201 privada e implementar el descifrado. La clave 201 privada para el descifrado, la clave pública relacionada y el certificado pueden ser posiblemente diferentes de los de la firma; en este caso el certificado adicional se registra en la base de datos del servidor aplicativo.

Para aumentar la seguridad, todos los mensajes, especialmente los recibidos por el teléfono 210 inteligente y enviados al mismo por el servidor 315 aplicativo, también pueden estamparse con la firma electrónica reconocida implementada por el servidor 315 aplicativo a través de un dispositivo de firma remota y masivo de tipo HSM (módulo de seguridad de hardware), certificado según los requisitos de las disposiciones nacionales e internacionales para firma electrónica reconocida; en este caso el código PIN de firma en el HSM se introduce por un administrador del servidor 315 aplicativo conectado con dicho HSM que promueve un proceso de firma masivo de los mensajes 340 de petición basados en texto salientes; en este caso la aplicación 220 multifuncional está dotada del certificado digital correspondiente a la clave privada de firma presente en el HSM, y al certificado de la autoridad de certificación que lo emitió.

A través de este certificado, la aplicación 220 multifuncional puede verificar la firma recibida y validarla como enviada por el servidor aplicativo considerado asociado en la aplicación multifuncional con el servicio usado.

Además, los mensajes 351 de petición de cliente y mensajes 352 de confirmación de cliente pueden firmarse y/o cifrarse, como todos los mensajes entre los otros nodos de servidor y cliente de la red dedicada. En general, el contenido de los mensajes puede firmarse o cifrarse, o firmarse en primer lugar y después cifrarse.

Normalmente, el certificado de firma y la clave 201 privada de firma para un usuario dado son únicos en la red dedicada; el mismo certificado de firma se copia en los servidores aplicativos usados por el usuario, pero en este contexto de firma electrónica reconocida, como el certificado es público por definición y no contiene la clave privada, esto no implica un problema de seguridad. También es posible definir pares de certificados y claves privadas de firma separadas, en base al servidor aplicativo. En este caso una pluralidad de claves privadas está presente en el teléfono inteligente, para seleccionarse en el momento de introducir el código PIN de firma.

Tras haberse implementado la operación de firma, el mensaje enviado por el teléfono inteligente también puede contener el número de serie del certificado de firma y la indicación de la autoridad de certificación relacionada, extraídos de la aplicación 220 de firma electrónica reconocida por la memoria de seguridad para permitir un control adicional del certificado por parte del servidor.

La memoria de seguridad, si es necesario, puede alojarse en otro lector conectado al teléfono inteligente, con respecto a la incorporada a menudo en el mismo teléfono inteligente. El lector, por ejemplo, puede estar situado dentro de una carcasa que también contiene el teléfono inteligente o conectarse a través de una interfaz de entrada/salida disponible, tal como el puerto de auriculares y micrófono. También es posible considerar el uso, dentro de la red dedicada, de diferentes repositorios de claves privadas con respecto a la memoria de seguridad, que están, por ejemplo, integrados en el teléfono móvil, o conectados al mismo o que coinciden con el SIM. Dependiendo de la aplicación 220 multifuncional de configuración, puede buscar el repositorio más seguro, integrado o conectado con el teléfono inteligente, en términos de imposibilidad de extracción de los datos de la clave privada y ejecución del algoritmo RSA, en ausencia de la memoria certificada. En los contextos en los que no se requiere el uso de la firma electrónica reconocida o de la firma electrónica reconocida equivalente, es posible usar repositorios de claves privadas no certificados para la firma electrónica reconocida, algoritmos de *hash* diferentes de los requeridos para la firma electrónica reconocida, y puede evitarse el reconocimiento preliminar visual del usuario.

La solución descrita anteriormente tiene diversas ventajas con respecto a la técnica anterior.

El sistema de firma y el procedimiento de firma según la invención permiten ventajosamente, a través del uso de la memoria de seguridad, en conexión con un dispositivo de teléfono móvil y una red de firma electrónica reconocida, la protección de la clave 201 privada frente a copiado y extracción, y el uso de esta clave privada para la firma electrónica reconocida para permitir al usuario suscribir documentos, ordenar pagos y acceder a servicios de información, con seguridad y movilidad, protegiéndose también la información sensible al nivel de los servidores

aplicativos de la red dedicada, ya que estos servidores aplicativos están protegidos, y en su lugar no siendo sensible la información usada dentro de la red dedicada al nivel del servidor frontal y del servidor 302 de interfaz. Al adoptar el algoritmo RSA de firma de tipo asimétrico y con los requisitos para la firma electrónica reconocida, se consigue un alto grado de seguridad, para hacer que esta firma electrónica sea legalmente equivalente a la firma manuscrita en muchos sistemas legales nacionales.

La memoria de seguridad se instala ventajosamente en un medio extraíble y no requiere acuerdos con operadoras telefónicas para su uso, ni está necesariamente vinculada al circuito de tarjeta de crédito. El medio extraíble puede estar alojado en el teléfono móvil, que está configurado para conectarse normalmente por medio de SMS (servicio de mensaje corto) a una red de telecomunicaciones dedicada para las operaciones de firma basándose en una arquitectura dada de componentes de servidor dentro de la cual están registrados los usuarios del sistema. La arquitectura de la red dedicada, si es necesario, permite el uso de otros dispositivos de almacenamiento para contener la clave privada.

Ventajosamente, el sistema hace uso en la mayoría de las realizaciones de una firma electrónica reconocida en forma separada que no está incluida en el mismo mensaje con la información de texto sin formato y por tanto ni la correspondiente información de texto sin formato ni los datos sensibles puede extraerlos un pirata informático. Una excepción a esto son las realizaciones, por ejemplo, según la arquitectura de la figura 6 en las que la petición de operación se firma en el origen antes de enviarse. En general, ninguna contraseña reutilizable, código PIN o número de tarjeta de crédito, en el caso de comercio electrónico, se transfiere sobre la red del sistema de firma propuesto.

La propia firma no puede copiarse y usarse de nuevo para diferentes peticiones: en este caso, las firmas electrónicas reconocidas usadas varían cada vez como también la información de texto sin formato asociada cambia cada vez; está presente en los servidores aplicativos de la red dedicada y les permite verificar la firma recibida y por tanto autenticar al usuario firmante y verificar si la firma se refiere a información de texto sin formato específica.

Naturalmente, sin prejuicio del principio de la invención, los detalles de construcción y las realizaciones pueden variar ampliamente con respecto a los descritos e ilustrados meramente a modo de ejemplo, sin apartarse sin embargo del alcance de la presente invención.

Es posible, además de la memoria de seguridad, considerar el uso, dentro de la red dedicada, u otros medios de almacenamiento, o repositorios de claves privadas con respecto a la memoria de seguridad, que están, por ejemplo, integrados en el teléfono móvil, o que están conectados al mismo, o que coinciden con el SIM. En contextos en los que no se requiere el uso de la firma electrónica reconocida o de la firma electrónica reconocida equivalente, es posible usar, por ejemplo, estos repositorios de claves privadas no certificados para la firma electrónica reconocida, diferentes cifrados y algoritmos de *hash* con respecto a los necesarios para la firma electrónica reconocida, si es necesario evitar preliminarmente el reconocimiento visual del usuario.

REIVINDICACIONES

1. Sistema de firma electrónica reconocida configurado para intercambiar datos con primeros medios (100; 303; 210) de procesamiento de un peticionario (300; 400) configurados para permitir que dicho peticionario (300, 400) genere en dicho sistema peticiones (305) relacionadas con un firmante (365; 400) a través de dicho sistema, comprendiendo dicho sistema segundos medios (210) de procesamiento del firmante (365; 400) configurados para permitir que dicho firmante (365; 400) firme con su firma electrónica reconocida, comprendiendo dichos segundos medios (210) de procesamiento un dispositivo de teléfono móvil para permitir que dicho firmante firme con su firma electrónica reconocida de tipo móvil, adaptado para recibir (340) y enviar (345) comunicaciones basadas en texto sobre redes de telecomunicaciones móviles que comprenden uno o más servidores, o para recibir (351) y enviar (352) datos electrónicos con módulos de proximidad sobre redes de proximidad, en base a un identificador de dicho firmante como suscriptor de un servicio de telefonía móvil, estando comprendido dicho identificador en un módulo (120) de identidad de suscriptor con el que dicho firmante está asociado, en el que:

dichos segundos medios (210) de procesamiento comprenden medios (220) para realizar dicha firma electrónica reconocida a través de una memoria (200) de seguridad que comprende al menos una partición segura en la que está almacenada al menos una clave (201) privada de dicho firmante, realizándose dicha firma electrónica en dicha partición de seguridad de dicha memoria de seguridad certificada para la firma electrónica reconocida y almacenar dicha clave privada de un modo independiente con respecto a dicho servicio de telefonía móvil, a dichas redes de telecomunicaciones móviles y a dicho módulo (120) de identidad de suscriptor, activándose dicha memoria (200) de seguridad con el fin de realizar una firma electrónica reconocida en base a un código de activación introducido por dicho firmante a través de dicho dispositivo de teléfono móvil;

siendo dicha memoria de seguridad diferente de dicho módulo de identidad de suscriptor y siendo accesible por dicho dispositivo de teléfono móvil en combinación con dicho identificador de módulo de identidad de suscriptor de dicho firmante con el que dicha memoria de seguridad está asociada, cuando se intercambian datos a través de dichas redes de telecomunicaciones móviles, o en combinación de dichos datos (351, 352) electrónicos cuando se intercambian datos a través de dichas redes de proximidad,

comprendiendo también dicho sistema de firma electrónica reconocida una red (302, 310, 315) de servidores dedicada, diferente de dichos servidores de dichas redes de telecomunicaciones móviles, para realizar una comunicación entre dichos primeros medios (100; 303; 210) de procesamiento del peticionario y dichos segundos medios (210) de procesamiento del firmante;

comprendiendo dicha red de servidores dedicada al menos:

• un servidor (310) frontal configurado para recibir, validar y distribuir dichas peticiones (305) de sistema, que requieren dicha firma electrónica reconocida o que contienen dicha firma electrónica reconocida, para generar peticiones (308) distribuidas, enviándose dichas peticiones (305) de sistema mediante dichos primeros medios (100; 303; 210) de procesamiento

• uno o más servidores (315) aplicativos configurados para recibir y validar dichas peticiones (308) distribuidas y, cuando se intercambian datos a través de dichas redes de telecomunicaciones móviles, enviar también dichas comunicaciones (340) basadas en texto sobre dichas redes de telecomunicaciones móviles;

estando dicho servidor (310) frontal configurado para enviar dicha petición (308) distribuida a un respectivo servidor (315) aplicativo en base al identificador del firmante (365; 400) o su número de teléfono, asociado a dicho módulo de identidad de suscriptor, y en base al tipo de petición (305);

estando dicho servidor (315) aplicativo configurado para reenviar dicha petición (305) como comunicación (340) basada en texto sobre la red de telecomunicaciones móviles mediante dicho identificador del suscriptor del servicio de telefonía móvil en dicho módulo (120) de identidad de suscriptor a dichos segundos medios (210) de procesamiento, cuando se intercambian datos a través de dichas redes de telecomunicaciones móviles;

estando dichos segundos medios (210) de procesamiento también configurados (220) para:

• usar dicha clave (201) privada en dicha memoria (200) de seguridad y firmar con dicha firma electrónica reconocida mediante cifrado de un *hash* de dicha comunicación basada en texto sobre la red (340) de teléfono móvil, o mediante cifrado de un *hash* de dichos datos (351) electrónicos recibidos a través de dichas redes de proximidad, o de partes de los mismos por medio de dicha clave (201) privada;

• enviar dicha firma al servidor (315) de aplicación a través de un mensaje (345) de confirmación, cuando se

intercambian datos a través de dichas redes de telecomunicaciones móviles, o enviar un mensaje (352) a dichos primeros medios del peticionario, cuando se intercambian datos a través de dichas redes de proximidad.

2. Sistema según la reivindicación 1, caracterizado porque dicho mensaje (345) de confirmación se da en forma de mensaje de texto SMS (sistema de mensaje corto), o se da en forma de datos (352) electrónicos adecuados para intercambiarse en una red de proximidad, y dicha petición (308) distribuida se reenvía como comunicación (340) basada en texto sobre la red de telecomunicaciones móviles en forma de mensaje de texto de tipo SMS.

3. Sistema según la reivindicación 1 ó 2, caracterizado porque dicha petición (305) es una petición de pago o una petición de suscripción de documentos o una petición de acceso u orden sobre servicios de red, conteniendo dicha petición (305) dicho identificador de dicho firmante.

4. Sistema según una o más de las reivindicaciones anteriores, caracterizado porque dicho servidor (310) frontal está configurado, en dicha operación de validación, para añadir una parte variable que comprende al menos un identificador único y un sello de tiempo de la petición (305) o para validar dicha parte variable y dicho sello de tiempo si se reciben en dicha petición (305).

5. Sistema según una o más de las reivindicaciones anteriores, caracterizado porque el dispositivo (210) de teléfono móvil está configurado para mostrar automáticamente en la pantalla (110) la petición (340) basada en texto recibida y enviar, tras firmar con dicha firma electrónica, una firma electrónica reconocida separada, al servidor (315) de aplicación para permitir la identificación certificada del firmante por medio de un certificado en el servidor (315) aplicativo en base al certificado de la autoridad de certificación que lo emitió, estando asociados ambos certificados con dicho firmante,

o estando también dicho dispositivo (210) de teléfono móvil configurado para mostrar automáticamente en la pantalla (110) la petición (351) recibida, y para enviar, tras firmar con dicha firma electrónica, una firma (352) electrónica reconocida separada a dichos primeros medios del peticionario para permitir la identificación certificada del firmante por medio de un certificado en el servidor (315) aplicativo en base al certificado de la autoridad de certificación que lo emitió, estando asociados ambos certificados con dicho usuario (365; 400) firmante.

6. Sistema según una o más de las reivindicaciones anteriores, caracterizado porque dicho al menos un servidor (310) frontal comprende una base de datos de usuarios registrados de la red (302, 310, 315) de servidores dedicada y está configurado para verificar en dicha base de datos de usuarios registrados, la presencia del firmante (365; 400) e información asociada con dicho firmante (365; 400), para dirigir la petición (305) a dicho respectivo servidor (315) aplicativo del firmante (365; 400).

7. Sistema según la reivindicación 5 ó 6, caracterizado porque dicho servidor (315) aplicativo está configurado para verificar dicha firma electrónica reconocida enviada por el dispositivo (210) de teléfono móvil y activar instrucciones de transacción determinadas en base al tipo de petición (305).

8. Sistema según una o más de las reivindicaciones 5 a 7, caracterizado porque dicho servidor (315) aplicativo está configurado para actualizar un correspondiente estatus de la operación en el servidor (310) frontal en base al identificador único de la petición (305) operativa.

9. Sistema según una o más de las reivindicaciones anteriores, caracterizado porque dichos primeros medios de procesamiento del peticionario también están configurados como dichos segundos medios (210) de procesamiento, comprendiendo un dispositivo de teléfono móvil, adecuado para intercambiar comunicaciones basadas en texto sobre redes de telecomunicaciones móviles, o para intercambiar datos electrónicos con módulos de proximidad sobre redes de proximidad, en base a un identificador del suscriptor del servicio de telefonía móvil incluido en un módulo (120) de identidad de suscriptor con el que está asociado y medios (220) para operar con una memoria de seguridad que comprende una partición segura en la que está almacenada una clave (201) privada.

10. Sistema según una o más de las reivindicaciones anteriores, caracterizado porque dichos primeros medios (100; 303; 210) de procesamiento del peticionario corresponden a dichos segundos medios (210) de procesamiento del firmante.

11. Sistema según una o más de las reivindicaciones anteriores, caracterizado porque comprende un ordenador dotado de medios de pantalla mayores que los medios de pantalla de dicho dispositivo de teléfono móvil y porque dicha petición (308) distribuida también se envía como mensaje de correo electrónico a una dirección a la que puede acceder dicho firmante, conteniendo dicho mensaje de correo electrónico información, en particular una referencia de dirección, para visualizar uno o más documentos asociados con dicha petición (308) distribuida, en particular documentos que van a suscribirse, en dichos

medios de pantalla mayores.

12. Sistema según una o más de las reivindicaciones anteriores, caracterizado porque dicho mensaje (345) de confirmación o el mensaje (340) basado en texto o ambos de dichos mensajes se transmiten y reciben respectivamente en forma de comunicación inalámbrica a través de un módulo (121) de conexión inalámbrica, en particular como mensaje de correo electrónico o mensaje *push* u otra comunicación transmitida por Internet.

13. Sistema según una o más de las reivindicaciones anteriores, caracterizado porque usa certificados emitidos por autoridades de certificación asociadas con dicha red (302, 310, 315) de servidores dedicada para un procedimiento de firma electrónica equivalente a la firma electrónica reconocida o un procedimiento de firma electrónica en general.

14. Sistema según una o más de las reivindicaciones anteriores, caracterizado porque dichos segundos medios (210) de procesamiento comprenden uno o más medios de almacenamiento para dicha clave privada, siendo dichos medios de almacenamiento diferentes de dicha memoria (200) de seguridad y, en particular, estando incorporados a, o conectados a dichos segundos medios (210) de procesamiento del firmante o integrados en el módulo (120) de identidad de suscriptor, certificados o no certificados para la firma electrónica reconocida, pudiendo dichos medios (220) para realizar dicho proceso de firma electrónica encontrar y usar los medios de almacenamiento más seguros de entre dichos medios de almacenamiento en base a criterios de garantía predefinidos para impedir la extracción de clave privada y/o ejecutar el algoritmo RSA de un modo seguro.

15. Procedimiento de firma electrónica reconocida, caracterizado porque comprende las operaciones implementadas por el sistema de firma electrónica reconocida según una o más de las reivindicaciones 1 a 14.

16. Procedimiento de firma electrónica reconocida según la reivindicación 15, caracterizado porque comprende:

en la petición (305) introducida en los primeros medios (303; 100; 210) de procesamiento también una contraseña temporal (ATP);

mostrar en pantalla una cadena de base sin *hash* o un *hash* de dicha cadena de base y dicha contraseña temporal en los segundos medios de procesamiento del firmante (400);

mostrar en pantalla dicha cadena de base sin *hash* o dicho *hash* de dicha cadena de base y dicha contraseña temporal en los primeros medios (303; 100; 210) de procesamiento del peticionario, comprendiendo dicho método en particular calcular mediante dicho servidor (315) aplicativo dicha cadena de base sin *hash* o dicho *hash* de dicha cadena de base en base a la información de la petición (305) y de dicha contraseña temporal (ATP), y a información adicional que comprende un identificador de sesión en el servidor (302) de interfaz correspondiente al identificador de la petición (305).

17. Dispositivo de teléfono móvil para firma electrónica reconocida, adaptado para intercambiar comunicaciones basadas en texto sobre redes de telecomunicaciones móviles, o para intercambiar datos electrónicos con módulos de proximidad sobre redes de proximidad, en base a un identificador del suscriptor de un servicio de telefonía móvil comprendido en un módulo (120) de identidad de suscriptor con el que está asociado dicho suscriptor, que comprende un sistema operativo y medios (220) para operar con una memoria de seguridad que comprende al menos una partición segura en la que está almacenada al menos una clave (201) privada de dicho suscriptor, siendo dicha memoria de seguridad diferente de dicho módulo de identidad de suscriptor y siendo accesible por dicho dispositivo de teléfono móvil solo en asociación con dicho identificador de módulo de identidad de suscriptor de dicho firmante con el que dicha memoria de seguridad está asociada, estando configurado dicho dispositivo de teléfono móvil, a través de una aplicación de software dedicada ejecutada en dicho sistema operativo, para usar dicha clave (201) privada en dicha memoria (200) de seguridad y firmar con una firma electrónica reconocida mediante cifrado de un mensaje (340) de petición o datos (351) o partes de los mismos por medio de dicha clave (201) privada, pudiendo procesar dicho dispositivo de teléfono móvil dicha firma electrónica en dicha partición de seguridad de dicha memoria de seguridad manteniendo dicha clave privada de un modo independiente con respecto a dicho servicio de telefonía móvil, a dichas redes de telecomunicaciones móviles y a dicho módulo (120) identificador de suscriptor en base a un código de activación introducido por dicho firmante a través de dicho dispositivo de teléfono móvil.

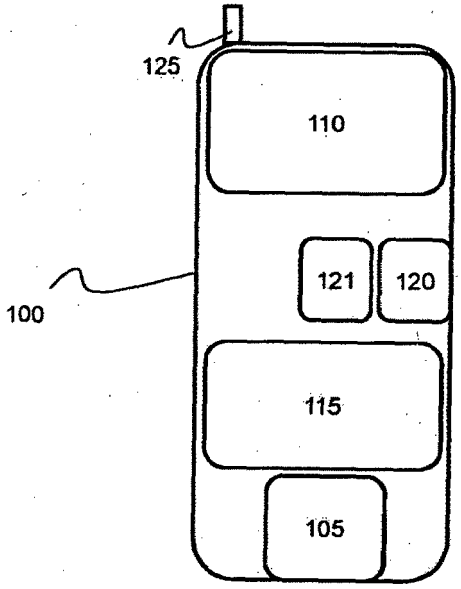

FIG. 1

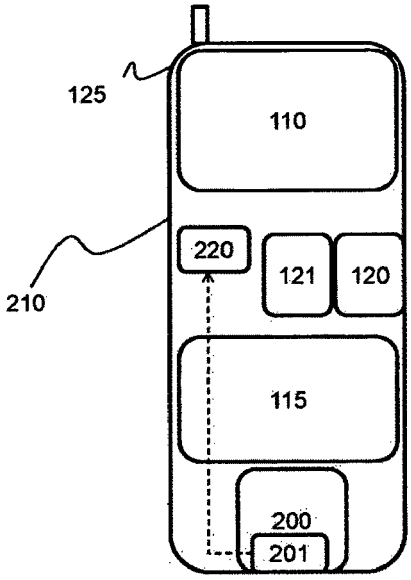

FIG. 2

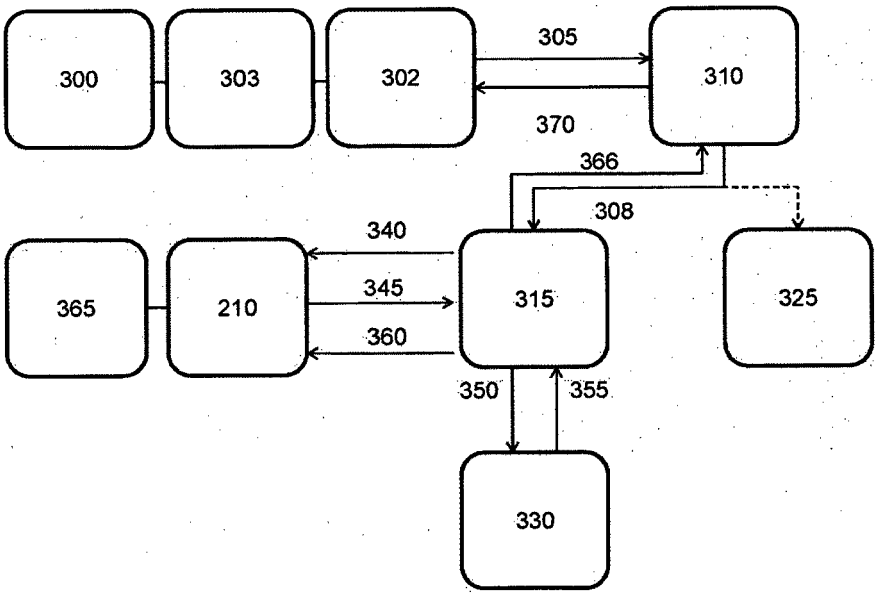
300
303
302
305
310
370
366
308
340
345
360
365
210
315
325
350
355
330

FIG. 3a

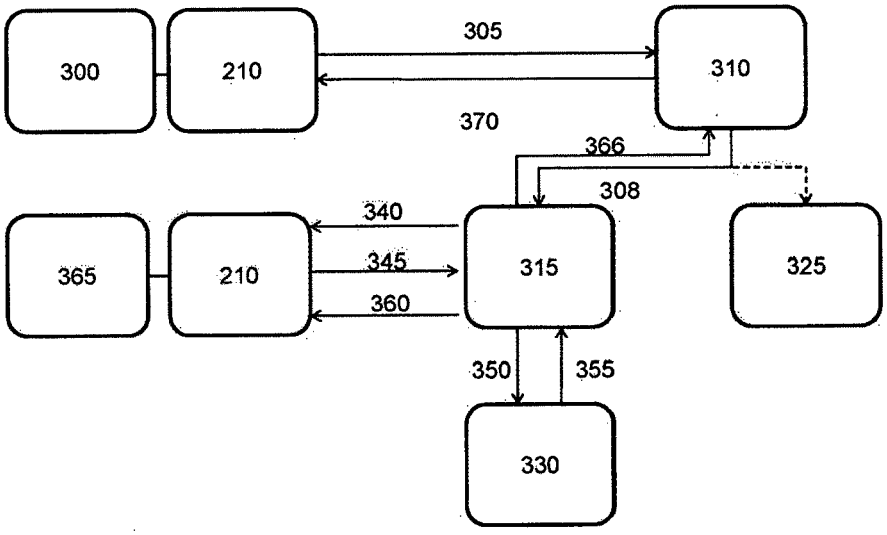
300
210
305
310
370
366
308
340
345
360
365
210
315
325
350
355
330

FIG. 3b

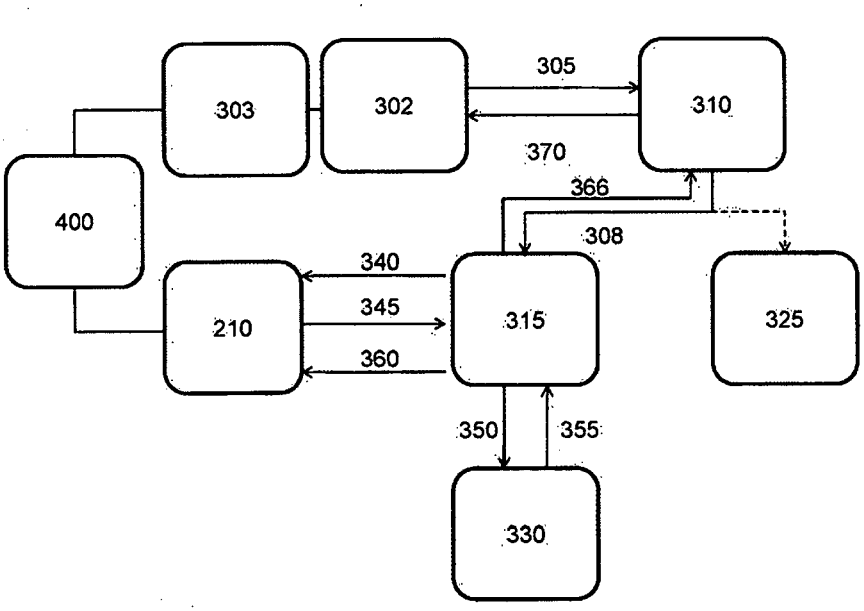
303
302
305
310
370
366
400
308
340
210
345
315
325
360
350
355
330

FIG. 4

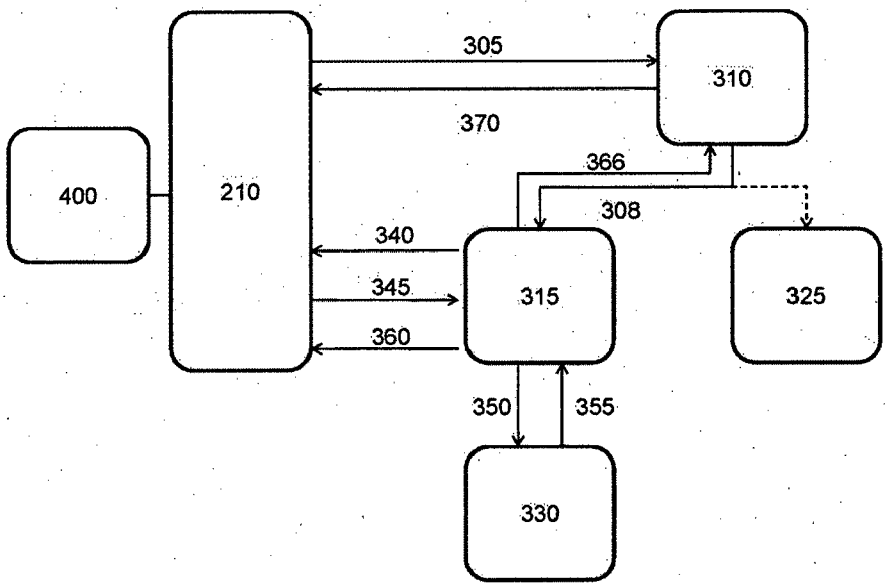

FIG. 5

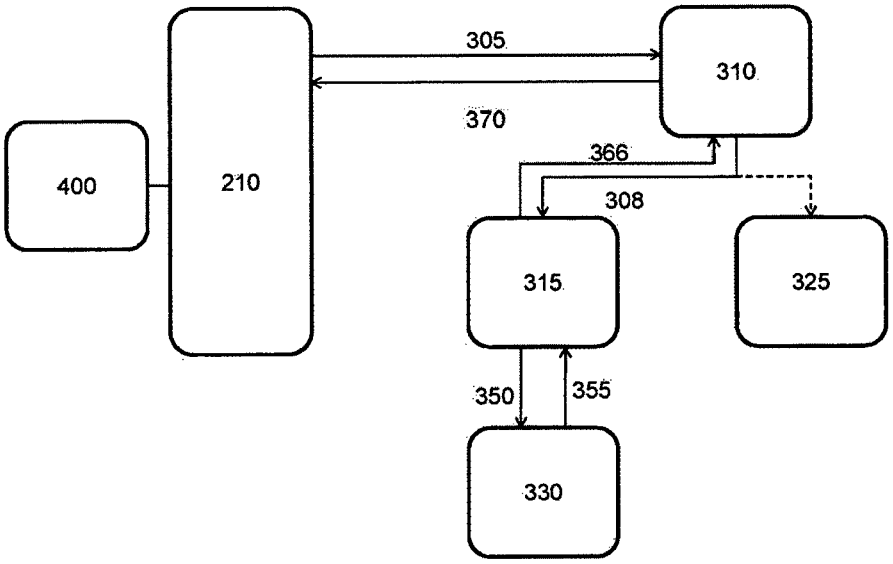

FIG. 6

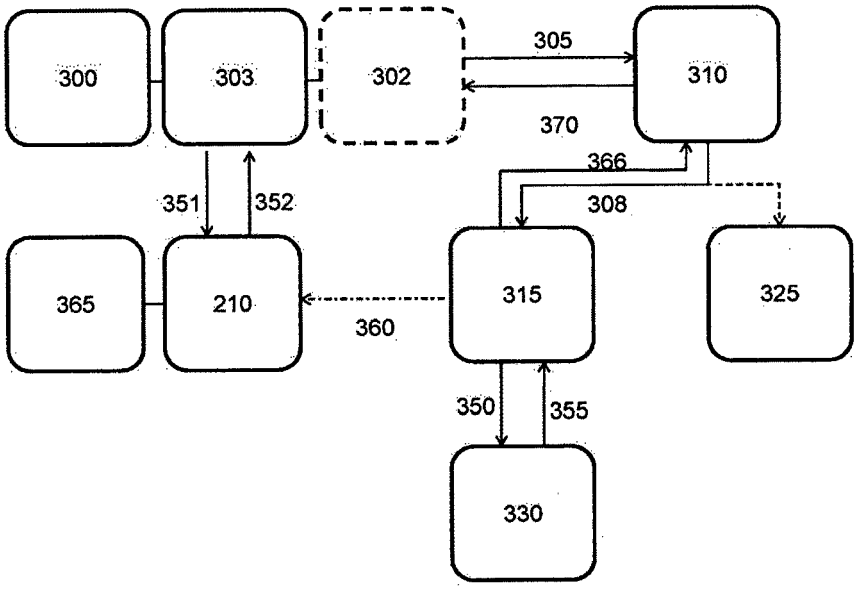
300
303
302
305
310
370
366
308
351
352
365
210
315
325
360
350
355
330

FIG. 7