(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 779 750**

(51) Int. CI.:

G06F 21/31 (2013.01)
G06F 21/42 (2013.01)
G06F 21/64 (2013.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **24.06.2014 E 14173645 (4)**

(97) Fecha y número de publicación de la concesión europea: **25.12.2019 EP 2819050**

(54) Título: **Sistema de firma electrónica para un documento electrónico que utiliza un circuito de autenticación de terceros**

(30) Prioridad:

25.06.2013 IT RM20130363
25.06.2013 IT RM20130364

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
19.08.2020

(73) Titular/es:

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

(72) Inventor/es:

BUELLONI, GIANLUCA y
MAGAGNOTTI, ROMEO

(74) Agente/Representante:

RUO , Alessandro

DESCRIPCIÓN

Sistema de firma electrónica para un documento electrónico que utiliza un circuito de autenticación de terceros

Campo de la invención

[0001] La presente invención se refiere a un sistema de firma electrónica, en particular en el campo de la firma electrónica avanzada.

Antecedentes de la técnica

[0002] Los procesos de firma electrónica se conocen desde hace mucho tiempo. Esencialmente, se han creado para garantizar la autenticidad de la firma adherida a un documento electrónico y la integridad del documento electrónico firmado.

[0003] La firma electrónica está definida por la Directiva Europea 1999/93/CE: "firma electrónica" que significa "datos en forma electrónica que se adjuntan o están asociados lógicamente con otros datos electrónicos y que sirven como método de autenticación".

[0004] La firma electrónica avanzada con certificado calificado es un tipo de firma electrónica avanzada, en la que se proporciona el uso de un par de claves digitales asimétricas, de las cuales una clave privada se atribuye exclusivamente a un sujeto, denominado titular y una clave pública correspondiente para verificar la autenticidad de la firma.

[0005] En dicho contexto se define el concepto de "certificado calificado", cf. art. 2, par. 10 Directiva europea 1999/93/CE, como "un certificado electrónico que vincula los datos de verificación de firma a una persona y confirma la identidad de esa persona".

[0006] El documento W003015370 muestra una solución llamada "fuera de banda", en la que para mejorar la seguridad de la comunicación entre la fuente del documento a firmar (ordenador del usuario) y el servidor de certificación, se usa un canal adicional, como por ejemplo una línea telefónica, a la que se envía un "token" que contiene una contraseña de un solo uso generada en el extremo del servidor. Por lo tanto, el uso de la contraseña recibida por medio de una línea telefónica contribuye a identificar de manera única al firmante. El contexto de dicho documento, sin embargo, se relaciona con la asociación de una clave privada a cada firmante.

[0007] Además de la firma digital con certificado calificado como se definió anteriormente, se proporciona un segundo tipo de firma electrónica, la llamada "firma electrónica avanzada" en la que no se requiere un certificado de firma para cada firmante. Tal es la firma electrónica que cumple con los siguientes requisitos: a) estar vinculada de manera única al firmante; b) ser capaz de identificar al firmante; c) ser creada utilizando medios que el firmante puede mantener bajo su exclusivo control; d) estar vinculada a los datos con los que se relaciona de tal manera que cualquier cambio posterior de los datos sea detectable.

[0008] Por lo tanto, la firma digital con certificado calificado representa un caso más restrictivo de firma electrónica avanzada.

[0009] En el contexto de la firma electrónica avanzada, de hecho, no es obligatorio que el firmante único tenga un certificado de firma y una clave privada del mismo para firmar un documento.

[0010] Tanto la clave pública como la clave privada utilizada para completar el proceso de firma del documento pertenecen a la entidad o autoridad que supervisa/gestiona el proceso avanzado de firma electrónica.

[0011] La autoridad puede utilizar el par de claves públicas y privadas antes mencionado, para todos los usuarios firmantes y para todas las firmas.

[0012] Tal escenario es particularmente adecuado para aquellos entornos corporativos en los que es necesario que los documentos se firmen electrónicamente, por múltiples empleados, sin embargo, sin la necesidad de que cada uno de ellos cuente con un dispositivo de firma digital con un certificado calificado.

[0013] Sin embargo, es complicado garantizar la identificación del firmante dentro de una empresa en la que los firmantes pueden ser potencialmente cientos.

[0014] Tal problema también se siente en el campo de la firma digital en sí, en eso es conocido y reconocido, la práctica de los gerentes, que tienen dispositivos de firma digital con certificado calificado, de dejar el dispositivo de firma en manos de sus colaboradores, quienes pueden hacer un uso fraudulento del mismo.

[0015] Un método divulgado en el documento US7039805 proporciona la creación de una firma que contiene un

número de autorización de tarjeta de crédito.

Sumario de la invención

[0016] Un objeto de la presente invención es proporcionar un sistema avanzado de firma electrónica adaptado para resolver el problema mencionado anteriormente, garantizando de manera segura la identidad de la persona que autoriza la firma.

[0017] Un objeto de la presente invención es un método para la firma electrónica avanzada de un documento electrónico por un usuario, de acuerdo con la reivindicación 1.

[0018] Una implementación preferida del presente método utiliza dos conexiones de datos diferentes.

[0019] Otra implementación preferida del presente método utiliza dos conexiones de datos diferentes y un servicio de telefonía móvil. En tal circunstancia, dicha implementación puede definirse fuera de banda.

[0020] De acuerdo con un primer aspecto de la invención, un ID de la tarjeta bancaria o asociada a ella, asociada de forma exclusiva al usuario involucrado en el procedimiento de firma y/o una identificación de teléfono asociada de forma exclusiva a la línea de teléfono móvil del usuario involucrado en el procedimiento de firma está directamente impreso en el documento firmado.

[0021] De acuerdo con una variante preferida de la invención, un conjunto de datos, referido como blob, se ingresa de manera segura dentro del documento en la etapa de firma, para hacer imposible la extracción y el uso de cualquier parte de los mismos en otros documentos. Dicho blob comprende una identificación relacionada con una tarjeta bancaria o con un procedimiento de autorización de una transacción ejecutada por una tarjeta bancaria, en donde la tarjeta bancaria está asociada al usuario.

[0022] De acuerdo con la presente invención, dicho ID puede ser uno o más de

- ID o PAN de la tarjeta bancaria,
- IBAN o código único similar de la cuenta bancaria asociada a la tarjeta bancaria,
- cualquier identificador de transacción único generado durante el uso de la misma tarjeta bancaria, al menos en una etapa de autorización para una transacción bancaria.

[0023] Dicha autorización bancaria debe realizarse durante la autenticación relacionada con la misma firma electrónica avanzada.

[0024] El hecho de que, por medio de dicha tarjeta bancaria, se determina una autorización para una transacción, no implica que se realice una transacción. Lo que importa, si se desea ingresar un ID de transacción en el blob de firma, es que se inicia un procedimiento de autorización, mediante el cual se obtiene un identificador de transacción único asociado a dicha tarjeta bancaria.

[0025] Por lo tanto, el procedimiento de autorización para una transacción puede ser conocido per se.

[0026] Además, opcionalmente, se puede ingresar uno de los siguientes datos: hora de la transacción, un ID de transacción, ID del terminal del banco, ID del minorista, ID del adquiriente, esa es la ID de la compañía que administra las autorizaciones de las tarjetas bancarias, cualquier cantidad, incluso simbólica, de la transacción.

[0027] En el contexto de la presente descripción, transacción bancaria significa cualquier transacción realizada con una tarjeta bancaria, tal como, por ejemplo, débito, recarga y/o autorización y/o preautorización y/o revocación.

[0028] De acuerdo con una variante de la presente invención, la transacción bancaria no se usa para permitir la transferencia de dinero, sino que la misma transacción es una parte integral del proceso de autenticación, y especialmente del proceso de firma electrónica avanzada, las técnicas de autorización para las transacciones bancarias son per se seguras.

[0029] De acuerdo con una variante adicional de la invención, alternativamente o en combinación con lo anterior, se ingresa un ID de teléfono asociado de forma exclusiva a la línea de teléfono móvil del usuario en el blob para aumentar aún más el nivel de seguridad en lo que respecta a la identificación del usuario firmante y opcionalmente se puede proporcionar al usuario firmante para establecer una llamada telefónica por medio de una red de telefonía móvil que proporciona la recuperación de un código adicional entre los siguientes:

- el número de teléfono móvil asociado al usuario,
- el IMSI asociado a dicha línea de teléfono móvil,
- el MSISDN.

[0030] Se pueden usar otros códigos asociados al establecimiento de una conexión de teléfono móvil en este contexto y para los fines descritos.

[0031] Además, también el IMEI del dispositivo móvil del usuario puede estar impreso en el documento electrónico que se firmará.

[0032] Todos los acrónimos anteriores son bien conocidos.

[0033] Además, opcionalmente se puede ingresar uno de los siguientes datos: hora de la llamada, un identificador de sesión, una contraseña de un solo uso.

[0034] En el contexto de la presente descripción, llamada significa cualquier llamada de voz o, por ejemplo, USSD (datos de servicio suplementario no estructurado).

[0035] De acuerdo con la presente invención, el canal adicional, externo, no solo se usa para permitir ingresar una contraseña, sino que se convierte en una parte integral del proceso de autenticación, y especialmente del proceso de firma electrónica avanzada, la tecnología GSM/UMTS/LTE es per se extremadamente segura.

[0036] De acuerdo con una variante preferida de la invención, tal blob, que contiene dicho ID de usuario, se encripta mediante un algoritmo de cifrado usando una clave aleatoria. La misma clave aleatoria se cifra mediante una clave pública de un par asimétrico perteneciente a la Autoridad. Tanto el blob encriptado como la clave encriptada mediante la clave pública se ingresan en el archivo electrónico a firmar. Por lo tanto, se logra un primer objeto. Posteriormente, un signo (hash) del archivo obtenido en la etapa anterior se calcula mediante un algoritmo predefinido y con el mismo algoritmo predefinido se calcula un signo (hash) del blob. Los dos signos obtenidos están vinculados o no y se cifran mediante el algoritmo de cifrado mencionado anteriormente utilizando la clave aleatoria mencionada anteriormente. Se logra un segundo objeto. El primer y el segundo objeto están conectados entre sí, por ejemplo, unidos entre sí o incrustados en otro objeto. El hecho de tener un signo del documento que debe firmarse, incluido el blob cifrado y el signo cifrado del blob por separado, permite garantizar que un blob específico se empareje con un documento específico, evitando que un blob cifrado se pueda extraer de un documento original ingrese de manera fraudulenta en otro documento.

[0037] De acuerdo con la presente invención, la firma se autoriza al menos cuando se autoriza una transacción bancaria con la tarjeta asociada al usuario para verificar la identidad del usuario. Por lo tanto, se incluye al menos uno de los ID del blob de firma mencionados anteriormente.

[0038] El proceso de autorización bancaria por sí mismo puede requerir que el usuario ingrese un PIN relacionado, conocido per se, por lo tanto, en el curso de la firma de un documento, puede ser necesario ingresar uno o más PIN.

[0039] También se puede solicitar ingresar una contraseña de un solo uso, por ejemplo, recibida por medio de una conexión de datos o por medio de una conexión telefónica en una red móvil y utilizada por el usuario, correspondientemente a través de la red móvil o la conexión de datos.

[0040] De acuerdo con una variante preferida de la invención, la firma está autorizada cuando se realiza/recibe una llamada telefónica por medio del número de teléfono móvil asociado al usuario para verificar la identidad del usuario no solo por medio de su propio número de teléfono, sino que también ingresando un PIN personal y/o una contraseña de un solo uso enviada a través de Internet.

[0041] De acuerdo con una variante preferida de la invención, la contraseña de un solo uso y/o el PIN personal pueden enviarse a través de la red de telefonía móvil en el dispositivo móvil del usuario.

[0042] Es evidente que el sistema puede implementarse en cualquier red informática, incluso aparte de Internet.

[0043] De acuerdo con una variante preferida de la invención, la llamada telefónica se inicia desde el teléfono del usuario. De acuerdo con otra variante preferida de la invención, la llamada telefónica se inicia desde el teléfono del usuario y luego se termina, para que el sistema recuerde dicho número, opcionalmente detectando la presencia de desvíos de llamadas, para aumentar el nivel de seguridad de la operación.

[0044] Por lo tanto, está claro que la conexión fuera de banda mediante una línea de teléfono móvil no solo permite la identificación única del usuario, sino también una identificación de teléfono respectiva contribuye a definir el blob ingresado en el documento a firmar.

[0045] La siguiente descripción detallada ilustra un ejemplo de sistema/infraestructura tecnológica además del dispositivo móvil del usuario, para implementar la presente invención.

[0046] Ventajosamente, no se necesita una aplicación específica instalada en el teléfono móvil del usuario, por lo tanto, incluso un teléfono GSM obsoleto puede usarse para realizar una parte del método descrito anteriormente.

[0047] La presente invención encuentra una aplicación particular en el campo de la firma electrónica avanzada y de la firma digital con certificado calificado, con el fin de aumentar aún más su nivel de seguridad.

[0048] Es otro objeto de la presente invención una infraestructura de red, de acuerdo con la reivindicación 13, que permiten lograr el método descrito anteriormente.

[0049] Las reivindicaciones dependientes describen realizaciones preferidas de la invención, formando parte integral de la presente descripción.

Breve descripción de los dibujos

[0050] Otras características y ventajas de la invención aparecerán más claramente a partir de la descripción detallada de realizaciones preferidas pero no exclusivas de un sistema avanzado de firma electrónica, ilustrado a modo de ejemplo no limitativo con la ayuda de las tablas de dibujo adjuntas, en las que:

La figura 1 muestra un diagrama de flujo representativo de una variante preferida del método de firma electrónica de acuerdo con la presente invención,
La figura 2 muestra un diagrama de tiempo de intercambio de datos entre entidades físicas involucradas en el proceso de firma electrónica de acuerdo con el método de la figura 1;
La figura 3 muestra un diagrama de tiempo que comprende otras etapas opcionales del proceso descrito en la figura 2.

[0051] Los mismos números y letras de referencia en las figuras identifican los mismos elementos o componentes.

Descripción detallada de una realización preferida de la invención

[0052] De acuerdo con la presente invención, dentro del documento a firmar se ingresa un llamado blob que contiene, además de los datos personales del sujeto que firma el documento, también una identificación única asociada a una tarjeta bancaria o a una transacción bancaria asociada a una tarjeta bancaria asociada al usuario firmante mediante la cual se realiza el procedimiento de autenticación del mismo sujeto, y/o también un número de teléfono móvil, por medio del cual se realiza otro procedimiento de autenticación del mismo usuario.

[0053] Vale la pena informar que los mismos recibos en papel impresos por un dispositivo de pago de punto de venta (POS) incluyen una gran cantidad de información, entre los que se incluye al menos un ID de transacción. El sistema bancario de autenticación y autorización almacena dicha identificación de transacción además del identificador de la tarjeta bancaria y los datos del titular durante muchos años. Por lo tanto, la entrada del ID de la tarjeta, pero aún mejor, del ID de una autorización/transacción realizada con una tarjeta bancaria en los datos de firma, permite identificar al usuario firmante de una manera prácticamente única.

[0054] Con referencia a la figura 1, una variante preferida de la firma electrónica de un documento, de acuerdo con la presente invención, comprende las siguientes etapas:

A. entrada, en un archivo a firmar, generalmente en formato PDF, de un elemento/campo de autenticación que, de acuerdo con algunas regulaciones, se ingresa en el llamado "diccionario de firmas": (opcionalmente) dicha etapa puede realizarse en una copia, previamente realizada, del documento que se firmará;
B. primer cifrado de un blob que comprende datos de autenticación del sujeto firmante, preferentemente por medio de un algoritmo AES y usando una clave generada aleatoriamente;
C. segundo cifrado de la clave utilizada para el primer cifrado mediante un algoritmo preferentemente RSA que utiliza una clave pública asignada a la autoridad que gestiona el proceso de firma;
D. primer enlace del blob cifrado y de la clave cifrada obtenida en las etapas B y C y entrada en dicho elemento/campo de autenticación;
E. cálculo de un primer signo (hash), preferentemente por medio de un algoritmo SHA-256 de todo el documento, incluyendo el elemento de autenticación ingresado anteriormente;
F. cálculo de un segundo signo (hash), preferentemente por medio de un algoritmo SHA-256, del blob no cifrado;
G. segundo enlace de dichos primer y segundo signos (obtenidos en las etapas E y F) y tercer cifrado del enlace por medio de dicha clave generada aleatoriamente, y preferentemente por medio del mismo algoritmo (AES) de la etapa B.
H. el resultado de dicho tercer cifrado está incrustado en un objeto, preferentemente del tipo CAdES (ETSI TS 101 733) que encripta el signo con la clave privada asignada a la autoridad que supervisa/gestiona el proceso de firma.

[0055] Dicho blob comprende una identificación de la tarjeta bancaria o asociada a una transacción, ya sea en términos de autorización, realizado con una tarjeta bancaria asociada únicamente al usuario involucrado en el procedimiento de firma y/o una identificación telefónica asociada a la misma línea telefónica necesaria para la autenticación del usuario.

[0056] Las etapas antes mencionadas pueden ser realizadas por un solo ordenador o sinérgicamente por un ordenador local y un servidor remoto.

[0057] Por ejemplo, de acuerdo con una variante preferida de la invención, las etapas A-H las realiza un servidor remoto. De acuerdo con otra variante, el servidor remoto realiza solo las etapas G y H, mientras que el ordenador local realiza las restantes.

[0058] A modo de ejemplo, el método puede resumirse como sigue:

1) se le solicita al usuario firmante que ejecute una transacción a través de una tarjeta de crédito/débito/prepago;
2) preferentemente, un dispositivo conocido per se adquiere información biométrica del usuario: dicho dispositivo puede ser un denominado POS bancario y dicha información biométrica puede ser una firma biométrica, una señal digital, una grabación de voz o un escaneo del iris del usuario, etc.;
3) el usuario, concurrentemente, ingresa su tarjeta bancaria en el dispositivo, por ejemplo, el mismo TPV para realizar una transacción de débito o autorización previa/autorización, que podría requerir la entrada de un PIN de autorización específico;
4) adquisición de al menos una identificación, ya sea de la tarjeta bancaria o asociada a la tarjeta o asociada a la transacción autorizada/ordenada con la misma tarjeta bancaria;
5) adquisición opcional de un ID de teléfono único adicional del usuario obtenido durante una sesión de autorización a través de la red de telefonía móvil;
6) entrada de los ID en el BLOB de firma, para firmar electrónicamente un documento (por ejemplo, PDF).

[0059] Es evidente que el usuario firmante utiliza una primera conexión de datos a un primer servidor remoto de firmas (autoridad), y una segunda conexión de datos a un segundo servidor bancario (adquirente) para la autenticación/autorización de una transacción bancaria.

[0060] Una conexión de datos adicional permite transferir dicho ID desde dicho segundo servidor a dicha autoridad (o primer servidor) por medio del PC/entidad local utilizada por el usuario para solicitar la firma de un documento electrónico, para que la autoridad lo ingrese en el blob de firmas mencionado anteriormente.

[0061] Alternativamente o en combinación con el ID asociado a una transacción bancaria, el sistema proporciona el uso de la identificación única del teléfono móvil del usuario.

[0062] De acuerdo con la presente invención, dicho ID puede ser uno o más de

- el número de teléfono móvil asociado al usuario,
- el IMSI asociado a dicha línea de teléfono móvil,
- el MSISDN,
- el IMEI del dispositivo móvil.

[0063] El blob, preferentemente, comprende al menos uno de los siguientes datos adicionales: hora de la llamada, un identificador de sesión, una contraseña de un solo uso.

[0064] El término "blob" también es bien conocido en el alcance de la presente invención y deriva del acrónimo de la frase "objeto grande binario".

[0065] El método de firma descrito aquí asegura, en un amplio alcance, es decir, en el que un único par de claves asimétricas en posesión de la autoridad es compartido por múltiples usuarios, la identidad del sujeto firmante, que es el usuario.

[0066] El método también permite un aumento adicional en el nivel de seguridad en los paradigmas de la firma electrónica, en el cual, a cada usuario se asocia un certificado calificado.

[0067] Además, si una copia del documento firmado electrónicamente en modo avanzado se almacena adecuadamente en un servidor de almacenamiento, por ejemplo, de un tercero, es posible en cualquier momento encontrar de manera única y segura la identidad del sujeto que ha firmado el documento mediante un certificado compartido, por ejemplo, con un nivel corporativo.

[0068] Para que se autorice la firma del documento, mostrado por medio de las etapas A-H mencionadas anteriormente, el sujeto firmante debe iniciar una transacción bancaria mediante una tarjeta bancaria asociada a él/ella.

[0069] Para aumentar el nivel de seguridad, se le puede solicitar al usuario que ingrese un PIN de firma (opcionalmente diferente del PIN utilizado en la autorización para la transacción bancaria) para enviarlo a dicho primer servidor por medio de la primera conexión de datos mencionada anteriormente.

[0070] Para aumentar aún más el nivel de seguridad, puede proporcionarse el uso de un canal fuera de banda, eso es diferente de las conexiones de datos anteriores.

[0071] Se le puede solicitar al usuario que interactúe con su propio teléfono móvil para ingresar dicho PIN de firma. Es posible que el usuario reciba una contraseña de un solo uso a través de la primera conexión de datos y la ingrese a través de su propio teléfono móvil o viceversa.

[0072] Además, la infraestructura tecnológica, que puede esquematizarse con el primer servidor remoto (autoridad) mencionado anteriormente, también puede proporcionar la verificación de que el número de teléfono utilizado por el usuario se haya asociado previamente a él/ella.

[0073] Alternativamente, el sujeto de la firma puede ser requerido para marcar un número específico de USSD. Para aumentar la seguridad, el sistema puede proporcionar la finalización de la sesión telefónica iniciada por el sujeto firmante y luego devolver la llamada al mismo, para aumentar la seguridad del intercambio de datos.

[0074] Como una opción adicional, la aplicación local a través de la cual se solicita la firma electrónica de un documento puede permitir especificar que el usuario está en el extranjero o que prefiere que se le devuelva la llamada. En tal caso, el sistema, es decir, el servidor remoto (autoridad), inicializará una llamada telefónica al dispositivo móvil del usuario, opcionalmente, someter la finalización exitosa del procedimiento de firma a una verificación de la ausencia de un desvío de llamadas activado en el número de teléfono móvil asociado al sujeto firmante.

[0075] Cuando el usuario está en el extranjero, de hecho, el número de teléfono de la persona que llama y/o su IMSI y/o MSISDN, etc. puede no estar disponible para el servidor remoto, por lo tanto, es ventajoso que el servidor inicialice la llamada.

[0076] Según una variante preferida adicional de la invención, en lugar de una llamada telefónica entre un dispositivo móvil y un servidor remoto, puede implementarse una conexión telefónica marcando códigos USSD, por ejemplo, una secuencia telefónica del tipo *123* 13#.

[0077] De acuerdo con la presente invención, por lo tanto, se necesitan al menos tres entidades de hardware y cuatro de software para implementar el proceso de firma, como se explica a continuación:

- una primera solicitud local de firma electrónica, generalmente un software que se ejecuta en un PC o tableta o dispositivo adecuado del sujeto firmante, por el cual es posible solicitar la firma electrónica de un documento a través de una red informática,
- una segunda aplicación local provista de un lector de tarjetas bancarias y opcionalmente de información biométrica; dicha aplicación puede ejecutarse en el mismo PC o tableta que el punto anterior o en otro dispositivo conocido per se. Además, la primera aplicación local es capaz de adquirir automáticamente, desde la segunda aplicación local, dicha identificación asociada a la tarjeta bancaria;
- una primera aplicación remota de firma electrónica, asociada a la autoridad o entidad de firma electrónica, a la que está asociada una interfaz con la red informática mencionada anteriormente para dicha primera aplicación y opcionalmente una interfaz de teléfono fijo o móvil,
- una segunda aplicación remota asociada a la segunda aplicación local, conocida per se, para autorizar una transacción bancaria por medio de dicha tarjeta bancaria y adaptada para generar una transacción o ID de autorización asociada a esa tarjeta bancaria específica;
- opcionalmente un GSM/UTMS/LTE, etc. teléfono móvil asociado al sujeto firmante (usuario).

[0078] Con la ayuda de la figura 2, se ilustra en detalle un proceso de firma realizado sinérgicamente a través de una red informática y una red informática bancaria

a. (usuario final) generando un archivo para firmar electrónicamente,
b. (usuario final)) enviando el archivo a firmar, a través de una primera conexión de ordenador, a la autoridad de firma, es decir, al servidor de firmas de la autoridad (también denominado primer servidor remoto),
c. (autoridad final, servidor 1) inicializando una sesión de autenticación, opcionalmente creando una contraseña de un solo uso,
d. (autoridad final, servidor 1) enviando una solicitud para que el usuario se autentique en el circuito bancario de la tarjeta bancaria asociada a él/ella, o para hacer una llamada telefónica a un número de teléfono predeterminado mediante un teléfono móvil previamente asociado al usuario,
e. (usuario final) mostrando dicha solicitud, y
f1. (usuario final) solicitando una autorización para realizar una transacción bancaria con la tarjeta bancaria, a través de una segunda conexión de ordenador, por ejemplo, mediante un TPV conectado al PC en la que se ejecutan la primera y la segunda aplicación local, o un dispositivo de pago independiente que comprende una interfaz significa con dicho PC para que el PC adquiera dicho ID asociado a la tarjeta bancaria y/o
f2; (usuario final) haciendo una llamada telefónica por medio de una red móvil a un número de teléfono

predeterminado en relación con dicho servidor de dicha autoridad,
g1. (adquiriente final, servidor 2) enviando la aprobación para ejecutar dicha transacción bancaria al usuario, en particular al TPV a disposición del usuario, junto con un identificador de la tarjeta bancaria y/o del procedimiento de autenticación y/o de la transacción bancaria,
h1. (usuario final) enviando dicho ID asociado a la tarjeta bancaria a dicho servidor de firma, en la autoridad, a través de dicha primera conexión de datos;
h2. (autoridad final, servidor 1) adquirir dicho ID asociado a dicha línea de teléfono móvil del usuario;
i. (autoridad final, servidor 1) firma electrónica de dicho documento que se firmará de acuerdo con las etapas anteriores A-H de acuerdo con la reivindicación 6, y
j. (autoridad final, servidor 1) enviar, a través de la red informática, el documento electrónico firmado.

[0079] Opcionalmente, durante o después de dicha etapa i, puede proporcionarse un almacenamiento del documento firmado electrónicamente. Por ejemplo en un servidor de almacenamiento diferente.

[0080] Las referencias 1 y 2 de h1 o h2, por ejemplo, indican claramente las dos posibilidades de obtener una identificación única por medio de un circuito de autenticación de terceros. Por lo tanto, solo se pueden realizar las etapas marcadas con 1 o 2 o ambas.

[0081] Si también se proporciona la verificación fuera de banda, etapa f2, el método de la invención comprende las etapas que se muestran en la figura 3, para ser realizadas antes, durante o después de las etapas d-h.

[0082] Por conveniencia, se indican como f1-f8, pero esto solo significa que se realizan antes del etapa i de la figura 2.

F1. (autoridad final, servidor l) enviando un número de teléfono o una secuencia de teléfono de referencia - a través de una red informática 1 - y opcionalmente dicha contraseña de un solo uso,
F2. (usuario final) que muestra dicho número de teléfono o servicio telefónico de referencia USSD y, opcionalmente, dicha contraseña única,
F3. (usuario final) enviando una llamada a dicho número de teléfono de autenticación o una solicitud de servicio a dicha secuencia de autenticación, a través de una red de telefonía móvil
F4. (autoridad final, servidor 1) opcionalmente solicitando la escritura de dicha contraseña de un solo uso con el teléfono móvil - a través de la red de telefonía móvil
F5. (usuario final) opcionalmente escribiendo dicha contraseña de un solo uso a través de la red de telefonía móvil -,
F6. (autoridad final, servidor 1) opcionalmente solicitando la escritura de un código PIN asociado al cliente, a través de la red de telefonía móvil,
F7. (usuario final) opcionalmente escribiendo dicho código PIN - a través de la red de telefonía móvil -,
F8. (autoridad final, servidor 1) verificar la asociación de dicho ID de teléfono móvil a dicho usuario y opcionalmente de dicho PIN y/o dicha contraseña de un solo uso.

[0083] Según una variante preferida de la infraestructura tecnológica previamente indicada como " autoridad final, servidor 1" se puede entender un conjunto de unidades de procesamiento diferentes.

[0084] Por ejemplo, las operaciones de interfaz con la red de telefonía móvil pueden ser gestionadas por un servidor de autenticación dedicado conectado, por medio de una conexión de datos segura, al servidor, en la autoridad, destinado a firmar electrónicamente el documento electrónico, en adelante "aparato de firma".

[0085] Por ejemplo, la etapa c puede ser realizado completamente por el servidor de autenticación a pedido explícito del servidor del dispositivo de firma. Por lo tanto, en la etapa c, los intercambios de solicitudes e información entre el servidor del dispositivo de firma y el servidor de autenticación pueden considerarse implícitos.

[0086] Ventajosamente, el sistema descrito aquí es particularmente seguro porque permite que la autenticación sea realizada por un ordenador bancario y/o una red de telefonía móvil, eso es inherentemente seguro, en el que al menos un código de identificación asociado a la tarjeta bancaria y/o número de teléfono del usuario se genera/adquiere y se ingresa al blob. Si se implementan ambos ID, entonces la autenticación también se realiza por medio de una conexión "fuera de banda", eso es por medio de una red de telefonía móvil asociada, a través de la cual se ingresa un código de identificación asociado a la línea de teléfono móvil del usuario en el blob de firma del documento que se firmará electrónicamente.

[0087] Opcionalmente, la misma información biométrica se puede cifrar e ingresar al blob de firma.

[0088] Se puede lograr un mayor aumento de la seguridad al proporcionar el número de teléfono al que se llamará, asociado al servidor remoto, para que sea diferente en relación con la sección de firma.

[0089] Además, el sistema puede solicitar la entrada tanto del PIN en posesión del usuario como de la contraseña que se envió una vez por Internet. Por lo tanto, la cantidad de datos de verificación es alta, aumentando así el nivel

de seguridad.

[0090] De acuerdo con una variante preferida de la invención, en la etapa h3, después de enviar una llamada al usuario a través de su dispositivo móvil, el servidor de autenticación puede finalizar automáticamente la llamada que inmediatamente después devuelve el número de teléfono móvil del usuario para obtener de allí la contraseña de un solo uso y el PIN como se describe en las siguientes etapas h4-h8.

[0091] Esto garantiza la inmunidad contra ataques fraudulentos.

[0092] La presente invención puede lograrse ventajosamente por medio de un programa informático que comprende medios de cifrado para realizar una o más etapas del método, cuando el programa se ejecuta en un ordenador. Por lo tanto, se entenderá que el alcance de la protección se extiende a dicho programa informático y más allá a los medios legibles por ordenador que comprenden un mensaje grabado, dichos medios legibles por ordenador que comprenden medios de cifrado de programa para realizar una o más etapas del método, cuando dicho programa se ejecuta en un ordenador.

[0093] Son posibles variantes de realización del ejemplo no limitativo descrito, sin apartarse sin embargo del alcance de protección de la presente invención, que comprende todas las versiones equivalentes para un experto en la materia.

[0094] De la descripción anterior, el experto en la materia es capaz de lograr el objeto de la invención sin añadir más detalles de construcción. Los elementos y las características mostradas en las diferentes realizaciones preferidas pueden combinarse sin apartarse del alcance de protección de la presente solicitud.

REIVINDICACIONES

1. Un método para la firma electrónica avanzada de un documento electrónico por un usuario, en el que un certificado de firma está en manos de una autoridad o autoridades de terceros, proporcionado para firmar dicho documento electrónico, comprendiendo el documento electrónico un campo de autenticación adaptado para contener un conjunto de datos (blob) relacionados con la transacción/autenticación, comprendiendo el método

- una etapa de autenticación del usuario en dicha autoridad(es), por medio de un circuito de autenticación de terceros que comprende

  • un circuito bancario y
  • un canal de teléfono móvil,

- una etapa de adquisición de un primer y un segundo ID de identificadores únicos asociados al usuario por dicho circuito de autenticación de terceros en el que dicho primer ID de identificador único comprende un ID de una tarjeta bancaria o asociada a la misma y dicho segundo ID de identificador único que comprende un ID de teléfono asociado de forma exclusiva a una línea móvil del usuario, y
- una etapa de entrada de cada uno de dichos identificadores únicos (ID) en dicho conjunto de datos (blob) por dicha(s) autoridad(es) de terceros.

2. El método de acuerdo con la reivindicación 1, en el que dicho conjunto de datos (blob), que contiene dichos ID únicos de usuario, se cifra mediante un algoritmo de cifrado que utiliza una clave aleatoria y la misma clave aleatoria se cifra mediante una clave pública de un par asimétrico perteneciente a dicha(s) autoridad(es) de terceros y tanto el conjunto cifrado de datos (blob) como la clave encriptada por medio de la clave pública se ingresa en el archivo electrónico a firmar.

3. El método de acuerdo con la reivindicación 1, en el que dicho circuito bancario es un circuito de autenticación bancaria para autorizar una transacción con una tarjeta de crédito o débito y en el que dicho primer identificador único de identificación comprende un identificador único o PAN de la tarjeta bancaria y/o un código IBAN asociado a la tarjeta bancaria y/o un identificador de transacción único generado mientras se usa la misma tarjeta bancaria, al menos en una etapa de autorizar la ejecución de una transacción bancaria, requerido por el procedimiento de autenticación del usuario durante el procedimiento de firma en sí.

4. El método de acuerdo con cualquiera de las reivindicaciones anteriores, en el que dicha segunda identificación de identificador único comprende un identificador único asociado a dicho usuario por una red de telefonía móvil por medio de una línea de teléfono móvil asociada al usuario que comprende uno o más de

- el IMSI asociado a dicha línea de teléfono móvil,
- el MSISDN asociado a dicha línea de teléfono móvil.

5. El método de acuerdo con la reivindicación 4, que comprende además una etapa de ingresar en dicho conjunto de datos de firma también uno entre

- el IMEI del dispositivo móvil del usuario,
- una contraseña de un solo uso.

6. El método de acuerdo con una de las reivindicaciones anteriores, que comprende además una etapa de ingresar en dicho conjunto de datos de firma también uno entre

- tiempo de autenticación,
- un identificador de sesión de autenticación,

7. El método de acuerdo con una cualquiera de las reivindicaciones anteriores, que comprende las siguientes etapas en una secuencia:

A. entrada de un elemento/campo de autenticación en un archivo a firmar;
B. primer cifrado del conjunto de datos (blob) que comprende los datos de autenticación del usuario firmante, mediante un algoritmo AES y utilizando una clave generada aleatoriamente;
C. segundo cifrado de la clave utilizada para el primer cifrado mediante un algoritmo preferentemente RSA que utiliza una clave pública asignada a la autoridad de firma;
D. primer enlace del blob cifrado y de la clave cifrada obtenida en las etapas B y C y entrada en dicho elemento/campo de autenticación;
E. cálculo de un primer hash, incluyendo el elemento de autenticación ingresado previamente;
F. cálculo de un segundo hash, preferentemente por medio de un algoritmo SHA-256, del blob no encriptado;
G. segundo enlace de dichos primer y segundo hashes y tercer cifrado del enlace por medio de dicha clave generada aleatoriamente, por medio del mismo algoritmo AES de la etapa B;

H. incrustando el resultado de dicho tercer cifrado en un objeto, preferentemente del tipo CAdES cifrando el hash con la clave privada asignada a la autoridad de firma.

8. El método de acuerdo con la reivindicación 7, en el que al menos uno de dichos hashes se obtiene por medio de un algoritmo SHA-256 de todo el documento.

9. El método de acuerdo con una cualquiera de las reivindicaciones anteriores, en el que dicha etapa de autenticación incluye:

- la solicitud de un usuario de firmar un documento electrónico para dicha autoridad de firma electrónica, enviada a través de una primera red informática,
- se solicita al usuario firmante que realice una transacción mediante una tarjeta de crédito/débito/prepago mediante un dispositivo dedicado (POS) y/o una llamada telefónica a un número de teléfono predeterminado;
- adquisición opcional de información biométrica de un usuario a través de un dispositivo dedicado POS,
- adquirir dicho ID único asociado a la tarjeta bancaria o asociado a la transacción autorizada/ordenada a través de la propia tarjeta bancaria, y/o asociado a dicha línea de teléfono móvil
- ingresar dicho ID único en dicho conjunto de datos de firma.

10. El método de acuerdo con la reivindicación 9, en el que cuando el sujeto firmante adquiere información biométrica durante el procedimiento de autorización/autenticación de una transacción bancaria, dicha información biométrica está integrada en dicho conjunto de datos de firma.

11. El método de acuerdo con una de las reivindicaciones anteriores, que comprende las siguientes etapas en sucesión:

a. en el usuario final, generar un archivo para ser firmado electrónicamente,
b. en el usuario final enviar el archivo a firmar
- a través de una primera conexión informática a la autoridad de firma,
c. en la autoridad final de firma iniciar una sesión de autenticación, opcionalmente creando una contraseña de un solo uso,
d. en la autoridad final de firma enviar una solicitud para que el usuario se autentique en el circuito bancario de la tarjeta bancaria asociada a él/ella y en una red de telefonía móvil llamando a un número de teléfono predeterminado,
e. en el usuario final, mostrar dicha solicitud, y
f1. en el usuario final, solicitar una autorización para realizar una transacción bancaria con la tarjeta bancaria, a través de una segunda conexión de ordenador, por ejemplo, mediante un POS conectado al PC en la que se ejecutan la primera y la segunda aplicación local, o un dispositivo de pago independiente que comprende medios de interfaz con dicha PC para que el PC adquiera dicho primer ID único asociado a la tarjeta bancaria y
f2. en el usuario final, realizar una llamada telefónica mediante un teléfono móvil asociado a dicho usuario a un número de teléfono predeterminado en relación con dicho servidor de dicha autoridad,
g1. en el adquirente final, enviar aprobación para ejecutar dicha transacción bancaria al usuario, en particular al TPV a disposición del usuario, junto con un identificador de la tarjeta bancaria y/o del procedimiento de autenticación y/o de la transacción bancaria,
h1. en el usuario final, enviar dicha primera identificación única asociada a la tarjeta bancaria a dicho servidor de firmas, en la autoridad, a través de dicha primera conexión de datos;
h2. en la autoridad final de firma adquirir dicha segunda identificación única asociada a dicha línea de teléfono móvil del usuario;
i. en la autoridad final de firma, proporcionar una firma electrónica de dicho documento de acuerdo con las etapas A-H de acuerdo con la reivindicación 7, y
j. en la autoridad final de firma enviar, a través de la red informática, el documento electrónico firmado.

12. El método de acuerdo con la reivindicación 11, en el que dicha etapa f2 de hacer una llamada telefónica por medio de un teléfono móvil asociado a dicho usuario comprende las siguientes etapas:

F1. en la autoridad final de firma, enviar un número de teléfono o servicio telefónico de referencia, a través de una red informática 1 y, opcionalmente, una contraseña única,
F2. en el usuario final, mostrar dicho número de teléfono o servicio telefónico de referencia USSD y opcionalmente dicha contraseña de un solo uso,
F3. en el usuario final, enviar una llamada a dicho número de teléfono de autenticación o una solicitud de servicio a dicha secuencia de autenticación, a través de una red de telefonía móvil,
F4. en la autoridad final de la firma, opcionalmente solicitar que se teclee dicha contraseña de un solo uso a través del teléfono móvil, a través de la red del teléfono móvil,
F5. en el usuario final, opcionalmente escribir dicha contraseña de un solo uso a través de la red de telefonía móvil,
F6. en la autoridad final de firma, opcionalmente solicitar que se teclee un código PIN asociado al cliente, a través de la red de telefonía móvil,

F7. en el usuario final, opcionalmente escribir dicho código PIN, a través de la red de telefonía móvil,
F8. en la autoridad final de firma verificar la asociación de dicha identificación de teléfono móvil con dicho usuario y, opcionalmente, dicho PIN y/o dicha contraseña de un solo uso,

13. Infraestructura tecnológica que comprende un primer servidor remoto de una autoridad de firma electrónica de un documento digital que comprende medios de procesamiento configurados para ejecutar todas las etapas de A a H de la reivindicación 7.

14. La infraestructura tecnológica de acuerdo con la reivindicación 13, que comprende

- un ordenador local en uso para un usuario que comprende primeros medios de comunicación con un primer servidor remoto,
- dicho primer servidor remoto asociado a dichas autoridades de autenticación de firma de terceros y/o
- una autoridad de autenticación de terceros que comprende:

    un segundo servidor remoto; y
    medios dedicados (POS) para leer dicha tarjeta bancaria y segundos medios distintos para la conexión de datos a dicho segundo servidor remoto,

en el que dicho ordenador local comprende medios de procesamiento configurados para extraer dicha primera identificación única y enviarla a dicho primer servidor remoto y/o
- un teléfono móvil asociado a dicho usuario

en el que dicho primer servidor comprende medios de interfaz telefónica con dicho teléfono móvil para extraer dicha segunda ID única asociada a dicho teléfono móvil de dicho usuario,
en el que dicho ordenador local está configurado para ejecutar las etapas a, b, e, f1, h1 de la reivindicación 11, y en el que dicho primer servidor remoto está configurado para ejecutar las etapas c, d, h2, i, j de la reivindicación 11
y en el que dicho segundo servidor remoto está configurado para ejecutar la etapa g1 de la reivindicación 11 y en el que dicho teléfono móvil está configurado para ejecutar la etapa f2 de la reivindicación 11.

15. Un programa de ordenador que comprende medios de codificación de programa adaptados para ejecutar todas las etapas de una cualquiera de las reivindicaciones 1 a 12, cuando dicho programa se ejecuta en un ordenador.

16. Medios legibles por ordenador que comprenden un programa grabado, comprendiendo dichos medios legibles por ordenador medios de codificación de programa adaptados para ejecutar todas las etapas de una cualquiera de las reivindicaciones 1 a 12, cuando dicho programa se ejecuta en un ordenador.

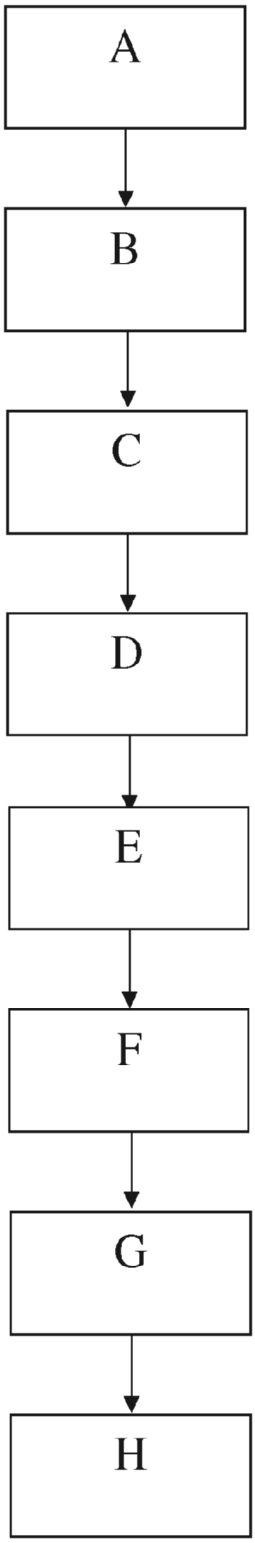

Fig. 1

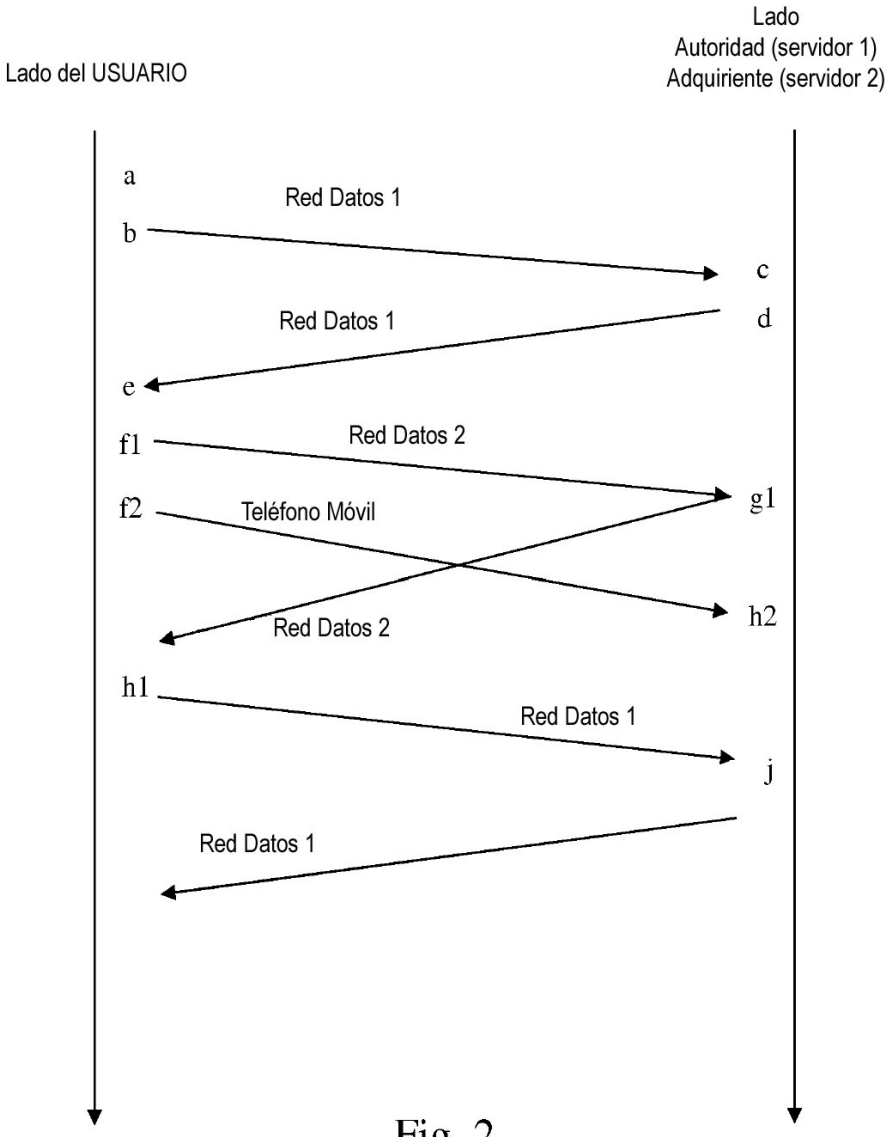
Lado del USUARIO
Lado
Autoridad (servidor 1)
Adquiriente (servidor 2)
a
Red Datos 1
b
c
Red Datos 1
d
e
f1
Red Datos 2
g1
f2
Teléfono Móvil
h2
Red Datos 2
h1
Red Datos 1
j
Red Datos 1

Fig. 2

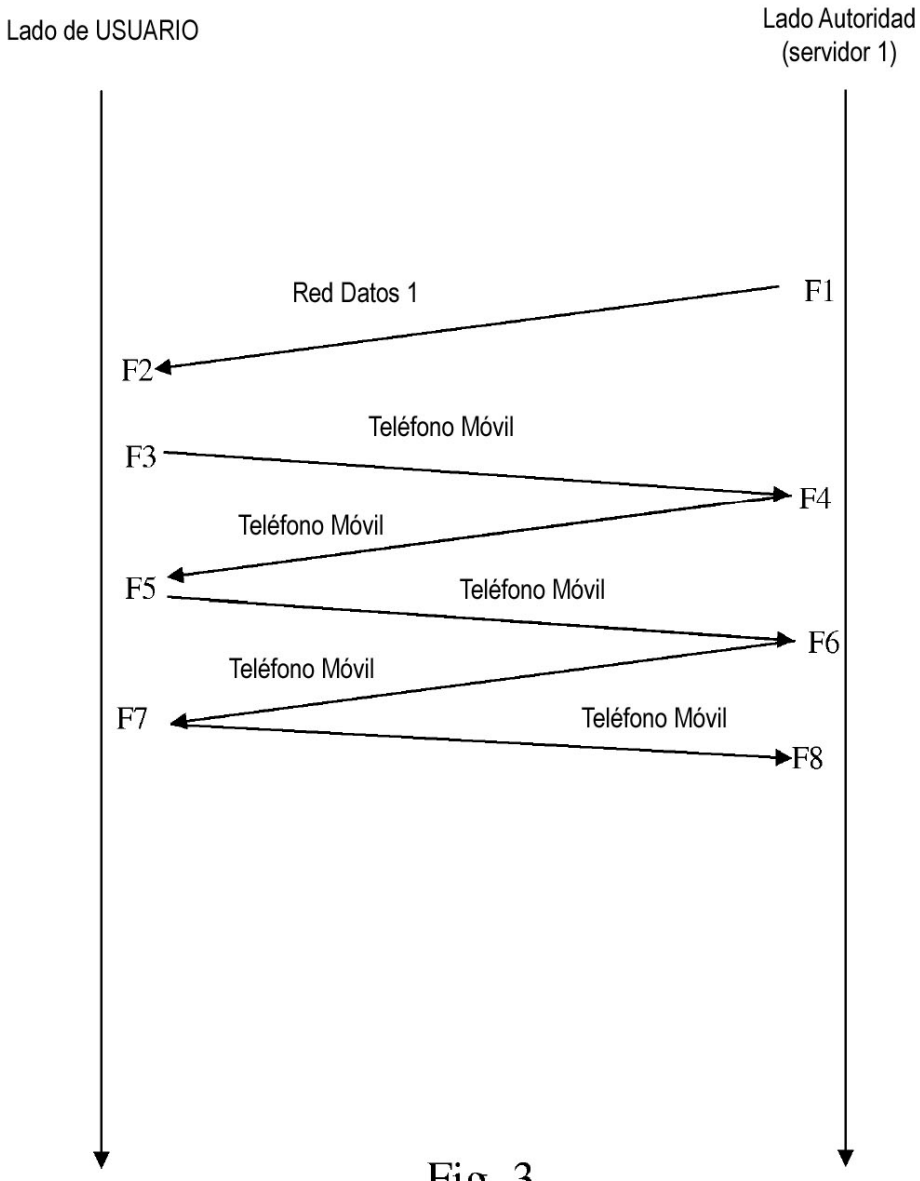
Lado de USUARIO
Lado Autoridad
(servidor 1)
Red Datos 1
F1
F2
Teléfono Móvil
F3
F4
Teléfono Móvil
F5
Teléfono Móvil
F6
Teléfono Móvil
F7
Teléfono Móvil
F8

Fig. 3